DAS PRIVACY HANDBUCH

Ein Ratgeber für digitale Privatsphäre und Sicherheit

TIMO VOLKOV

Die Benutzung dieses Buches und die Umsetzung der darin enthaltenen Informationen erfolgt ausdrücklich auf eigenes Risiko.

Das Werk inklusive aller Inhalte und Anleitungen wurde unter größter Sorgfalt erarbeitet. Der Autor übernimmt jedoch keine Gewähr für die Aktualität, Korrektheit, Vollständigkeit und Qualität der bereitgestellten Informationen. Druckfehler und Falschinformationen können nicht vollständig ausgeschlossen werden. Es kann keine juristische Verantwortung sowie Haftung in irgendeiner Form für fehlerhafte Angaben und daraus entstandene Folgen von dem Autor übernommen werden.

Externe Links und Informationen bezüglich Anleitungen, Software und Webseiten wurden bis zum Zeitpunkt der Veröffentlichung des Buches geprüft. Auf etwaige Änderungen zu einem späteren Zeitpunkt hat der Autor keinen Einfluss. Eine Haftung des Autors ist daher ausgeschlossen.

Erste Auflage, Mai 2025

ISBN 000-0-00000-000-0

Für Anfragen oder Rückmeldungen wenden Sie sich bitte an die oben genannte E-Mail-Adresse

Haftungsausschluss: Die Inhalte dieses Buches dienen ausschließlich der allgemeinen Information und stellen keine individuelle Finanz-, Steuer-, IT- oder Rechtsberatung dar. Die dargestellten Informationen basieren auf gründlicher Recherche und persönlichen Erfahrungen des Autors. Sie sind jedoch nicht auf die individuelle Situation des Lesers zugeschnitten und sind keine Beratung.

Der Autor übernimmt keine Haftung für die Vollständigkeit, Richtigkeit oder Aktualität der Inhalte. Jegliche Haftung für direkte oder indirekte Schäden, die durch die Anwendung der in diesem Buch dargestellten Informationen entstehen, wird ausgeschlossen. Die Anwendung der beschriebenen Methoden und Ratschläge erfolgt auf eigenes Risiko des Lesers. Leser sollten stets die aktuellen rechtlichen und technischen Standards prüfen.

Alle im Buch genannten Marken und Warenzeichen sind Eigentum ihrer jeweiligen Inhaber und werden nur zum Vorteil des Markeninhabers genutzt, ohne die Absicht, das Markenzeichen zu verletzen. Die Nennung dient lediglich der Information.

Über den Autor
Timo Volkov

Timo Volkov ist Berater mit Schwerpunkt auf digitale Privatsphäre, IT-Sicherheit und Bitcoin. Als erfahrener Workshop-Leiter, Berater und Speaker unterstützt er Privatpersonen unterschiedlichster Hintergründe dabei, ihre individuelle Freiheit zurückzugewinnen und ihre Selbstständigkeit zu stärken.

Als Gründer von Privatopia sowie Partner bei Bitcoinlighthouse verfügt er über fundiertes Fachwissen und langjährige praktische Erfahrung. Er entwickelt maßgeschneiderte Lösungen, die exakt auf die individuellen Bedürfnisse und Herausforderungen seiner Klienten abgestimmt sind.

Durch seine Unterstützung konnten bereits zahlreiche Klienten ihre Online-Präsenz absichern, persönliche Daten effektiv schützen und ihre finanzielle Unabhängigkeit nachhaltig verbessern. Sein Ziel ist es, Menschen zu befähigen, eigenverantwortlich Entscheidungen zu treffen und ihre Zukunft selbstbestimmt zu gestalten.

Inhalt

Einleitung **9**
„Ich habe doch nichts zu verbergen!“ 11
Digitaler Minimalismus 13
Threat-Modell 14
Freies Internet 18

Kapitel 1 Computer **23**
Neuer Linux Computer Konfiguration 26
Computer für Linux 27
Ubuntu (Linux) installieren 30
Updates 33
Apps herunterladen 34
Dateien 35
Terminal 35
Daten entfernen 39
Antivirus 40
Virtuelle Maschinen 41
Hardware-Sicherheit 41
Tails 42

Kapitel 2 Handys **47**
GrapheneOS 49
Die benötigte Hardware 50
Welches Handy sollte man kaufen? 51
Installation von GrapheneOS 52
Installation von GrapheneOS über die Webseite 53
Erste Schritte nach der Installation 54
WLAN 55
Auto-Reboot 56

Fingerabdruck ... 56
PIN-Scrambling ... 57
Duress-Passwort ... 57
Schnelleinstellungen ... 58
Nutzerprofile ... 59
Nutzerprofil erstellen ... 61
Installieren von Apps ... 62
Apps ... 64
Backups ... 66
Updates ... 67
Berechtigungen ... 67
Storage Scopes ... 68
Contact Scopes ... 68
WiFi Calling ... 69
VoIP ... 70
Faraday-Taschen ... 70
Mikrofon und Kamera ... 71
Privacy Screen ... 72
Handy-Nutzung ... 73
Kapitel 3 Anonym surfen ... 77
Was macht ein gutes Programm aus? ... 78
Webbrowser LibreWolf ... 80
uBlock Origin ... 82
Container Tabs ... 83
Yandex ... 84
Cookies ... 85
Tor-Browser ... 85
VPN ... 88
Mullvad VPN ... 90
ProtonVPN ... 91

DNS ... 92
NextDNS ... 93
Öffentliche WLANs ... 95

Kapitel 4 Passwörter und Verschlüsselung ... 99
Sichere Passwörter ... 99
Passwortmanager ... 101
Bitwarden ... 102
2FA (Zwei-Faktor-Authentifizierung) ... 105
Verschiedene Arten von 2FA ... 106
EnteAuth ... 107
Probleme ohne 2FA ... 108
Benachrichtigungen für Account-Zugriff ... 109
Verschlüsselte Backups und USB-Sticks ... 109
Welche Daten sollten verschlüsselt werden? ... 111

Kapitel 5 Private Kommunikation ... 117
E-Mail ... 117
ProtonMail ... 118
Weitere E-Mail-Adressen ... 122
Alternativen zu ProtonMail ... 124
E-Mail-Import und Weiterleitung ... 125
E-Mail-Backups ... 127
E-Mail-Aliase ... 128
Weitere Ideen ... 131
Telefonnummern und SMS ... 132
Anonyme Nummern ... 134
Überlegungen zu anonymen SIM-Karten ... 135
SMS und der Schutz vor Spam ... 136
Messenger ... 137
Was ist Ende-zu-Ende-Verschlüsselung (E2EE)? ... 137
Was sind Metadaten? ... 138

Signal 138
Molly 139
SimpleX 139
Wire 139
Matrix 140
Threema 140
Jitsi 140
WhatsApp 141
Telegram 141
Selbstlöschende Nachrichten 142

Kapitel 6 Digitale Werkzeuge und Alternativen 145

Kalender 145
Kontakte 146
Notizen 149
Microsoft-Office-Alternative 151
Musik, Podcasts und YouTube 151
Social Media 153
Nostr 154
Künstliche Intelligenz 155
PGP 159
Finanzmanagement 164
Karten und Navigation 165
OpenStreetMap 166
Organic Maps 167
Magic Earth 167
Google Maps 167

Kapitel 7 Unsichtbar werden 171

Informationen löschen 172
Methoden 172
Wer hat alles deine Daten? 174

Google ... 176
Social Media ... 178
Weitere Accounts ... 179
Alte Geräte ... 179
Google-Suchergebnisse aktualisieren ... 180
Google-Suchergebnisse entfernen ... 181
Regelmäßige Überprüfung persönlicher Daten ... 182
Datenbroker ... 182
Unbenutzte Apps entfernen ... 186
Freunde und Familie ... 186
Newsletter abbestellen ... 186
Aliase (Pseudonyme) ... 188
Anonymität vs. Pseudonymität ... 190
Das Pseudonym erstellen ... 190
Pseudonym anwenden ... 192
Falschinformationen gezielt einsetzen ... 195
Profil erstellen ... 197
Falschinformationen als falsche Fährte ... 198

Kapitel 8 Zahlungen, Finanzen und Bitcoin ... 203

Zahlungen ... 204
Bargeld ... 204
Gutscheine ... 205
Kreditkarten und Banküberweisungen ... 208
Bitcoin ... 209
Privat Investieren ... 209
Edelmetalle ... 210
Sammlerstücke ... 211
Bitcoin ... 211
Bitcoin sicher und privat nutzen ... 211
Warum Bitcoin? ... 212

Bitcoin und Privatsphäre 214
Bitcoin sicher und privat aufbewahren 215
Wallets 216
Privater Schlüssel 217
Passphrase 218
Software-Wallets 219
Hardware-Wallets 220
Sparrow 220
Test-Transaktion 221
Coin Control und Labeling 221
Bitcoin anonym erhalten 222
Bitcoin Node 224
Spuren verwischen 226
Coinjoin 226
Bitcoin Sidechains 227
Bitcoin ausgeben 229
Steuern 229
Mit Bitcoin bezahlen 230
Das Lightning-Netzwerk 231
Custodial Lighting Wallets 232
Non-custodial Lightning Wallets 233
Altcoins 233

Kapitel 9 Sicher und privat bleiben 237

To-dos 237
Wöchentliche To-dos 238
Monatliche To-dos: 239
Metadaten 240
„Plant your flag“ 243
Private Informationen schützen 245
Daten nach dem Tod? 246

Adresse schützen 247
Postfach 247
Postadresse bei Unternehmen 248
Postadresse für Reisen 249
Postadresse bei privaten Kontakten 250
Autos 250
Welche Daten sammelt unser Auto? 251
Automodell 252
Autosoftware 255
Physische Sicherheit und Privatsphäre 257
Müll entsorgen 258
Alte Geräte 258
Verstecke vermeiden 258
Aufmerksamkeit vermeiden 259
Reisen 259
Inlandsflüge 259
Flüge innerhalb der Schengen-Zone 260
Internationale Reisen 260
Fazit 265
Wichtige Begriffe zur Privatsphäre – einfach erklärt 269
Tool Sektion, Links und weiterführende Artikel 275
Quellen 282
Abbildungsverzeichnis 283

Einleitung

„Zu argumentieren, dass Sie keine Privatsphäre brauchen, weil Sie nichts zu verbergen haben, ist so, als würden Sie sagen, dass Sie keine Meinungsfreiheit brauchen, weil Sie nichts zu sagen haben."
~ Edward Snowden

Das Internet, unsere Smartphones und Computer erscheinen wie eine riesige, leuchtende Fassade. Was wir sehen, sind Apps, Websites, Klicks und benutzerfreundliche Oberflächen. Doch was geschieht hinter dieser Fassade? Welche Mechanismen greifen, wenn wir auf einen Knopf oder Button drücken? Wie funktionieren all diese Dienste im Hintergrund? Die meisten von uns haben kaum eine Vorstellung davon. Obwohl wir diese Technologien täglich nutzen, bleiben sie für uns größtenteils unsichtbar.

Hinter dieser unsichtbaren Wand sitzen Unternehmen, Geschäftsleute und Institutionen. Sie bieten uns scheinbar kostenlose Dienste an, jedoch nicht aus Großzügigkeit. Wenn wir eine App verwenden oder eine Webseite besuchen, bezahlen wir grundsätzlich immer – nur nicht mit Geld. Stattdessen zahlen wir mit unseren Daten.

Jeder Klick, jeder Like, jede Suche, sie alle sind Teile eines gigantischen Puzzles, das unser Verhalten, unsere Vorlieben und Interessen offenbart. Jedes Mal, wenn wir online sind, hinterlassen wir Spuren. Diese Spuren werden gesammelt, analysiert und oft auch verkauft. Cookies, Standortdaten, Browserverläufe und Klicks werden aufgezeichnet. Selbst unser Smartphone, das wir täglich bei uns tragen, verfolgt über GPS und andere Funktionen mit hoher Genauigkeit unsere Bewegungen.

Doch wozu all das? Wofür werden all diese Daten genutzt? Einerseits helfen sie dabei, uns bessere und angepasste Dienste anzubieten. Empfehlungen werden personalisiert, Werbung auf unsere Interessen zugeschnitten, und die Qualität der Dienste verbessert sich insgesamt. Aber es gibt nicht nur Vorteile.

Denn wer garantiert uns, dass es dabei bleibt? Vielleicht verkaufen Unternehmen unsere Daten für Millionen an Dritte? Was passiert, wenn diese Daten in die falschen Hände geraten? Können Hacker darauf zugreifen? Haben Mitarbeiter dieser Unternehmen freien Zugriff auf unsere Informationen? Und was ist mit Regierungen – überwachen sie wirklich nur Kriminelle oder wird die gesamte Bevölkerung unter die Lupe genommen? Wer versichert uns, dass es nur unsere eigenen Regierungen sind? Es könnten auch ausländische Mächte aktiv sein.

Diese Fragen bleiben oft unbeantwortet. Wir wissen jedoch, dass unsere Daten wertvoll sind – und dass wir die Kontrolle darüber zurückgewinnen müssen. Denn es sollte unser aller Recht sein, unser Leben zu leben, ohne heimlich überwacht zu werden. Doch diese Kontrolle zurückzuerlangen, ist nicht einfach. Unternehmen, deren Geschäftsmodell auf der Datenerhebung basiert, machen es uns bewusst schwer, unsere Privatsphäre zu schützen. Das bedeutet jedoch nicht, dass wir machtlos sind.

Die kommenden Kapitel zeigen dir, wie du Schritt für Schritt deine Privatsphäre schützen und deine digitale Freiheit zurückgewinnen kannst. Wir werden gemeinsam lernen, wie du deine Computer und Handys sicherer machst, welche Programme dich schützen, wie du deine Spuren im Internet verwischst und wie du sicher und privat bleibst. Außerdem werden wir in die Welt der finanziellen Privatsphäre eintauchen, um auch hier ein Stück unabhängiger zu werden.

Jedes Kapitel ist als in sich geschlossene Anleitung zum Vollzug eines Schrittes auf dem Weg zur umfassenden digitalen Autonomie geschrieben. Es geht nicht darum, alle Schritte auf einmal zu gehen – das wäre zu überwältigend. Nimm dir Zeit, nutze dieses Buch als Handbuch und mache die Schritte, die dir zunächst am einfachsten und/oder wichtigsten erscheinen. Kehre zurück, wenn du bereit bist für den nächsten Schritt. Jeder noch so kleine Schritt zählt, denn er bringt dir mehr Sicherheit und Freiheit. Das Allerwichtigste ist, dass du den ersten Schritt wagst – denn der Schutz deiner Privatsphäre liegt in deinen Händen.

„Ich habe doch nichts zu verbergen!“

Ein häufiges Argument gegen den Schutz der eigenen Privatsphäre lautet: „Ich brauche keine Privatsphäre, ich habe ja nichts zu verbergen.“ Doch oft glauben die Menschen selbst nicht an diese Aussage. Man behauptet verbal, nichts verbergen zu müssen, aber die eigenen Handlungen sprechen eine andere Sprache.

Jeder von uns hat etwas, das er privat halten möchte. Sei es der Moment, in dem wir die Zimmertür abschließen, um uns kurz zurückzuziehen, oder das Bedürfnis, an einen ruhigen Ort zu gehen, um ein vertrauliches Gespräch zu führen – Privatsphäre ist ein grundlegendes menschliches Bedürfnis. Wir alle haben Geheimnisse, die wir nicht mit der Welt teilen möchten.

Jeder bewegt sich irgendwo in dem Spektrum zwischen dem Wunsch nach einem abgeschlossenen Zimmer und dem Streben nach völliger Abgeschiedenheit.

Ein interessantes Beispiel für diesen Widerspruch zeigt sich bei Mark Zuckerberg, dem Gründer von Facebook. In einem Interview im Jahr 2010 sagte er: „Privatsphäre ist keine soziale Norm mehr.“[1] Doch nur wenige Jahre später kaufte er nicht nur eine Villa in Palo Alto, sondern auch die vier angrenzenden Häuser für insgesamt 30 Millionen Dollar – allein, um sicherzustellen, dass niemand in sein privates Leben hineinsehen kann. [2] Selbst er, der über die Daten von Milliarden Menschen verfügt, erkennt den Wert von Privatsphäre nur zu gut.

„If we cannot protect ourselfes, we cannot be ourselves”
~ Michael Crichton

Das Streben nach Privatsphäre ist zutiefst menschlich. Obwohl wir soziale Wesen sind und gerne unser Leben mit anderen teilen – sei es durch soziale Medien oder in persönlichen Gesprächen – benötigen wir ebenso dringend Rückzugsorte. Orte, an denen wir allein mit unseren Gedanken und Gefühlen sein können, sei es beim Arzt, bei einem Anwalt oder im vertraulichen Gespräch mit Freunden.

Denn sobald wir uns überwacht fühlen, verändern wir uns. Zahlreiche Studien belegen, dass Menschen, die das Gefühl haben, beobachtet zu werden, gehorsamer, konformer und unterwürfiger handeln. [3] Es entsteht ein Gefühl der Beklommenheit, und wir treffen Entscheidungen nicht mehr so, wie wir es aus freiem Willen tun würden, sondern so, wie wir glauben, dass andere es von uns erwarten.

Der Philosoph Jeremy Bentham entwickelte im 18. Jahrhundert das Konzept des Panopticons[4] – eine kraftvolle Metapher für Überwachung und Kontrolle. Ursprünglich als Modell für Gefängnisse konzipiert, beschreibt es ein kreisförmiges Gebäude mit einem zentralen Wachturm. Von diesem aus kann ein Wächter jeden Gefangenen jederzeit beobachten, jedoch niemals alle gleichzeitig. Da die Insassen nicht wissen, wann sie tatsächlich beobachtet werden, zwingt diese ständige Unsicherheit sie dazu, sich so zu verhalten, als wären sie permanent unter Beobachtung – ein perfider Mechanismus, der letztlich ein Gefängnis im Kopf schafft.

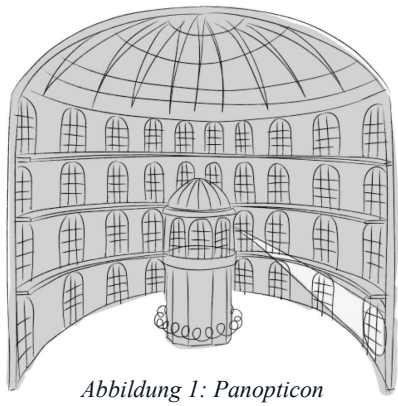

Abbildung 1: Panopticon

In unserer heutigen digital vernetzten Welt spiegelt das Konzept des Panopticons die unsichtbare Überwachung wider, die uns durch Unternehmen, Regierungen und andere Akteure umgibt. Die ständige Möglichkeit, beobachtet zu werden, beeinflusst unser Verhalten oft unbewusst. Wie viel Freiheit geben wir auf, wenn wir ständig das Gefühl haben, unter einem unsichtbaren Blick zu stehen?

Diese Technologien verändern nicht nur unser Verhalten, sondern mindern auch unsere Motivation, Dinge zu hinterfragen oder Neues zu entdecken. Viele Menschen bevorzugen die Bequemlichkeit und nehmen den Verlust ihrer Privatsphäre in Kauf. Oft möchten sie gar nicht wissen, was mit ihren Daten geschieht oder wie viel Unternehmen und Regierungen bereits über sie wissen.

„He who does not move does not notice his chains."
~ *Rosa Luxemburg*

„Wer sich nicht bewegt, bemerkt nicht seine Fesseln", heißt es in einem bekannten Zitat. Diese Fesseln, geschmiedet durch bequeme Technologien, halten uns in einer Spirale der Bequemlichkeit gefangen. Anstatt zu entdecken, zu innovieren und aktiv zu gestalten, verharren wir in einem Zustand der Passivität – nicht nur im Bewusstsein der Überwachung, sondern ihr gegenüber in gewisser Weise auch gleichgültig. Doch wer die Kontrolle über seine Privatsphäre verliert, verliert auch ein Stück weit die Kontrolle über sein Leben.

Digitaler Minimalismus

Auch in Bezug auf die Privatsphäre gilt: „Weniger ist mehr." Digitaler Minimalismus bedeutet, bewusst weniger digitale Dienste im Alltag zu nutzen und somit die Angriffsfläche zu verringern, durch die Daten gesammelt werden können. Dies ist eine der effektivsten Methoden, um den eigenen Datenschutz zu stärken – indem wir erst gar nicht die Gelegenheit bieten, Daten zu erfassen.

Durch diesen Ansatz können wir uns zunehmend von Datenkraken, Social-Media-Unternehmen und anderen Big-Tech-Unternehmen lösen. Die Menge an Informationen, die sie über uns sammeln können, wird auf ein Minimum reduziert. Dies führt nicht nur zu mehr Privatsphäre und Sicherheit, sondern auch zu einem entspannteren, weniger technologiedominierten Leben.

Anstatt uns auf Dienste zu verlassen, die uns mit maßgeschneiderter Werbung bombardieren, wählen wir Alternativen, die mit anderen Einnahmequellen arbeiten. So kaufen wir bewusster nur, was wir wirklich benötigen, und vermeiden endlose Konsumspiralen.

Anstatt von „Für-dich-Seiten" (wie bei YouTube) gelenkt zu werden, die perfekt auf unsere Vorlieben abgestimmt sind, entscheiden wir wieder selbst, was und wie viel wir konsumieren möchten.

Anstatt darauf zu vertrauen, dass Unternehmen unsere Daten sicher speichern, übernehmen wir diese Verantwortung selbst und müssen uns weniger um Datenlecks sorgen.

Anstatt uns von Smartphones ständig mit Benachrichtigungen überfluten zu lassen, reduzieren wir diese auf ein Minimum und schaffen so mehr Ruhe in unserem Alltag.

Die folgenden Kapitel werden dir nicht nur dabei helfen, deine Privatsphäre und Sicherheit deutlich zu verbessern, sondern auch dein digitales Leben einfacher und minimalistischer zu gestalten. Der Weg dorthin mag etwas Zeit und Mühe erfordern, aber das Ergebnis wird ein digitales Leben sein, in dem du die Kontrolle hast – du entscheidest, welche Dienste du nutzen möchtest, statt dass Unternehmen dein Leben bestimmen.

Threat-Modell

Um herauszufinden, welche Tipps und Tools in diesem Buch für dich am besten geeignet sind, musst du zunächst dein persönliches „Threat Model“ (Gefahrenmodell) bestimmen.

Denn jeder hat verschiedene Anforderungen, Wünsche und auch Möglichkeiten seine eigene Privatsphäre zu schützen.

Das Threat Model
Einfach gesagt beantwortet das Threat Model die Fragen, was du schützen möchtest, vor wem du dich schützen willst und wie weit du dafür zu gehen bereit bist.

Hier folgen einige Beispiele:

Journalist: Er möchte die eigenen Quellen schützen. Sein Threat-Modell konzentriert sich darauf, seinen Standort, seine Kommunikation, seine Daten und seine Treffen vor denen zu verbergen, die seinen Informanten schaden könnten.

Polizisten: Sie wollen die eigene Familie vor Kriminellen schützen, die es auf ihn oder sie abgesehen haben. Der Fokus liegt darauf, persönliche Informationen wie Adressen oder Daten seiner Angehörigen aus dem Internet zu entfernen, um sich vor möglichen Racheakten zu schützen.

Aktivist in einem repressiven Staat: Aktivistinnen und Aktivisten müssen ihre Aktivitäten vor der Regierung geheim halten, um sich und die Angehörigen zu schützen. Ihr Threat Model umfasst die Verschlüsselung von Kommunikation und Anonymität bei der Internetnutzung.

Prominenter: Möchte sein Privatleben von der Öffentlichkeit abschirmen. Sein Ziel ist es, private Informationen wie Adresse, Telefonnummer, Standort und Familienverhältnisse zu verbergen, um sich von aufdringlichen Fans abzugrenzen.

Stalking-Opfer: Dieses versucht, vor seinem Angreifer zu fliehen und sich zu verstecken. In diesem Fall liegt der Schwerpunkt des Tat-Modells auf physischem Schutz und Anonymität im Internet.

Alltagsnutzer: Die meisten von uns möchten ihre digitale Privatsphäre und Sicherheit verbessern. Unser Threat-Modell zielt darauf ab, uns vor überwachenden Unternehmen und Institutionen zu schützen, die persönliche Daten sammeln. Es geht darum, uns selbst, unsere Finanzen und persönlichen Informationen vor Missbrauch zu bewahren und ein freies Leben zu führen.

Es ist wichtig zu verstehen, dass Privatsphäre immer mit Aufwand verbunden ist. Auch wenn Tools und Dienstleistungen in diesem Bereich zunehmend einfacher und benutzerfreundlicher werden, erfordert es dennoch Zeit und Engagement, die eigene Privatsphäre und Freiheit zurückzugewinnen und aufrechtzuerhalten. Man kann es sich wie einen Balanceakt zwischen Bequemlichkeit und Privatsphäre vorstellen: Je mehr wir uns in Richtung Sicherheit und Freiheit bewegen, desto größer wird der Aufwand. Jeder muss für sich entscheiden, wo er in diesem Spektrum steht und was genau er schützen möchte.

Abbildung 2 Privatsphäre oder Bequemlichkeit

Einige fragen sich vielleicht: „Muss ich mich überhaupt schützen, wenn ich keine spezifische Bedrohung sehe? Ich vertraue meiner Regierung und habe kein Problem mit den Unternehmen, die meine Daten sammeln." Doch die Antwort ist eindeutig: „Ja, Schutz ist wichtig." Jährlich gibt es Hunderte von Datenlecks, bei denen nicht nur Benutzerkonten, sondern auch Passwörter und persönliche Informationen von Hackern und anderen Parteien gestohlen werden.

Ashley Madison (2015): Der Hack auf die Dating-Website „Ashley Madison" veröffentlichte die Daten von über 32 Millionen Nutzern. Da die Plattform auf außereheliche Affären spezialisiert war, hatte dieser Leak verheerende persönliche Folgen für viele Betroffene.

Equifax-Datenleck (2017): Ein riesiges Datenleck bei der Kreditagentur „Equifax" betraf die persönlichen Daten von 147 Millionen Menschen. Darunter befanden sich Sozialversicherungsnummern, Geburtsdaten und Adressen – Informationen, die ein erhebliches Risiko für Identitätsdiebstahl bergen.

Gigantisches plattformübergreifendes Datenleck (2024): Am 24. Januar 2024 wurde ein enormer Datensatz mit 26 Milliarden Einträgen von Nutzerdaten veröffentlicht. Diese stammten offenbar aus verschiedenen Datenlecks von Online-Plattformen wie Facebook, Twitter und LinkedIn. Die Veröffentlichung dieses Datensatzes hat eine intensive Debatte über die Sicherheit persönlicher Daten im Internet ausgelöst.

Volkswagen (2024): Durch eine Fehlkonfiguration waren über Monate hinweg Bewegungsdaten von rund 800.000 Elektrofahrzeugen der Marken Volkswagen, Audi, Seat und Skoda ungeschützt im Internet zugänglich. Diese Daten umfassten präzise GPS-Positionen, die es ermöglichten, detaillierte Bewegungsprofile der Autofahrer

zu erstellen. Dazu waren persönliche Informationen wie E-Mail-Adressen und Telefonnummern mit den Fahrzeugdaten verknüpft.

Dies sind nur einige Beispiele, die zeigen, dass Unternehmen oft nicht in der Lage oder willens sind, unsere Daten ausreichend zu schützen. In solche Fallen sollten wir nicht tappen.

Schauen wir uns ein anderes Problem an. Selbst wenn wir gesetzestreue Bürger sind, die sich nichts zuschulden kommen lassen, bleibt die Frage: Können wir sicher sein, dass das Sammeln von Daten in der Zukunft keine negativen Konsequenzen hat? Was passiert, wenn die Regierung in eine Krise gerät und plötzlich auf Vermögensregister zugreift, um Geld einzutreiben? Oder wenn ein Gesetz eingeführt wird, das rückwirkend Handlungen unter Strafe stellt, die heute noch vollkommen legal sind? So abwegig es klingen mag, solche Szenarien sind in der Geschichte bereits mehrfach vorgekommen.

Ein beunruhigendes Beispiel ist die Volkszählung in den Niederlanden während des Zweiten Weltkriegs. Die zuvor gesammelten Daten ermöglichten es den Nazis, gezielt die jüdische Bevölkerung zu verfolgen. Diese Informationen wurden genutzt, um jüdische Familien zu identifizieren, was zur Deportation und Ermordung von über 75 % der jüdischen Bevölkerung führte. Diese Volkszählungen galten ursprünglich als harmlos und modern, doch in den falschen Händen wurden sie zu Werkzeugen der Verfolgung.

Wenn jemand glaubt, dieses Buch könne helfen, sich vor Geheimdiensten oder Strafverfolgung zu verstecken, muss ich leider enttäuschen. Regierungen und Geheimdienste verfügen über enorme Macht und sind in der Lage, nahezu jeden aufzuspüren – selbst Menschen, die sich in der tiefsten Wildnis ohne digitale Geräte verstecken. Wenn man gezielt gesucht wird, hat man kaum eine Chance.

Doch dieses Buch kann dir helfen, deine privaten Informationen aus dem Internet zu entfernen, detaillierte Nutzerprofile zu vermeiden und dich vor den neugierigen Blicken von Unternehmen und Institutionen zu schützen. Es geht darum, deine Freiheit zurückzugewinnen – die Kontrolle über dein eigenes Leben.

Freies Internet

Fünfzig Jahre nach der ersten Vernetzung von Computern und dreißig Jahre nach der Entstehung des World Wide Web ist die Vision einer freien und offenen Online-Welt, wie sie von den Pionieren erträumt wurde, stark gefährdet. Unternehmen festigen ihre Monopolstellungen mit proprietärer Software und drängen die Konkurrenz zunehmend aus dem Markt.

In den frühen Jahrzehnten der Softwareentwicklung basierte vieles auf offenem, für alle zugänglichem Code. Dieser Code war frei nutzbar, veränderbar und teilbar – ein Konzept, das wir heute als Open Source (offener Quellcode) kennen. Zu dieser Zeit spielte das Urheberrecht eine untergeordnete Rolle, und die Open-Source-Bewegung lebte von der Überzeugung, dass Software zum Wohl der Allgemeinheit frei zugänglich sein sollte.

Heute, 40 Jahre später, generieren Tech-Unternehmen Milliarden mit proprietärer Software – von Microsoft über ChatGPT bis hin zu „intelligenten" Haushaltsgeräten. Das Problem dabei ist, dass wir bei vielen dieser Programme kaum noch eine echte Wahl haben. Die Monopolstellungen dieser Unternehmen haben die Konkurrenz verdrängt. Der ursprüngliche Wunsch, Software frei und offen zugänglich zu machen, wird von großen Institutionen aktiv unterdrückt.

Dennoch hat die Open-Source-Bewegung in den vergangenen Jahren wieder an Dynamik gewonnen und spielt heute eine zentrale Rolle in der Technologiebranche. Tatsächlich enthalten 96 % aller heute entwickelten Software irgendeine Form von Open-Source-Code. Open-Source-Software bringt das Internet nicht nur ein Stück weit in die Freiheit zurück, wie es die Pioniere einst erträumt haben, sondern bietet auch zwei wesentliche Vorteile.

Sicherheit: Da der Quellcode öffentlich zugänglich ist, können Entwickler weltweit die Programmzeilen überprüfen und nach Schwachstellen suchen. Auch wenn du selbst kein Programmierer bist, ist es besser, der geballten Intelligenz der globalen Entwicklergemeinschaft zu vertrauen als nur einem Unternehmen. Fehler,

Hintertüren und Sicherheitslücken werden schneller entdeckt und behoben, was die Sicherheit der Software erheblich erhöht.

Transparenz und Schutz: Weil der Code offenliegt, kann man sicherstellen, dass ein Programm nur das tut, was es soll. Bei proprietärer Software wie derjenigen von Microsoft weiß niemand genau, welche Daten gesammelt werden oder was im Hintergrund abläuft. Wir können es vermuten, aber sicher wissen wir es nicht. Mit Open-Source-Software hingegen kann man genau sehen, ob Daten erfasst oder weitergeleitet werden. Hier hilft die breite Gemeinschaft der Entwickler, sicherzustellen, dass die Software transparent und vertrauenswürdig bleibt.

Ein weiterer Vorteil von Open-Source besteht darin, dass es kostenfrei ist. Das bedeutet jedoch auch, dass die Entwickler, die an diesen Projekten arbeiten, kaum Geld verdienen, da der Code frei kopierbar ist. Viele Programmierer engagieren sich in ihrer Freizeit für diese Projekte und stellen ihre Ergebnisse der Allgemeinheit zur Verfügung – kostenlos. Viele der Tools, die in diesem Buch vorgestellt werden, sind Open Source, das heißt, du musst nichts dafür zahlen.

Dennoch sollten wir nicht nur nehmen, sondern auch etwas zurückgeben. Wenn du programmieren kannst, hilf mit, den Code zu verbessern. Wenn du mehrere Sprachen sprichst, unterstütze bei Übersetzungen. Und wenn du weder programmieren noch übersetzen kannst, kannst du zumindest eine kleine Spende geben. Eine solche Geste zeigt deine Wertschätzung für die Arbeit der Entwickler und unterstützt die Open-Source-Bewegung, damit sie weiter wachsen kann. Genauso wie du für kostenpflichtige Programme oder Abos wie Microsoft Office oder Spotify zahlst, solltest du auch für die freien Programme, die du nutzt, etwas zurückgeben.

Auch ich möchte einen Teil der Einnahmen aus diesem Buch an die hier vorgestellten Open-Source-Projekte spenden. Überlege dir, das Gleiche zu tun, um die Entwickler zu unterstützen und die Zukunft des freien Internets zu sichern. Hier findest du einige Links zu Open-Source-Projekten und Organisationen, die auch im Buch später vorgestellt werden: privatopia.de/spenden.

Die Welt, in der wir heute leben, ist digital und vernetzt, doch wir dürfen nicht in einer orwellschen Zukunft enden, in der wir ständig überwacht werden und uns bei jeder Handlung Gedanken darüber machen müssen, wer uns gerade zusieht. Ich möchte nicht in einer Welt leben, in der Freiheit und Privatsphäre einer dauerhaften Überwachung und Kontrolle geopfert werden.

Zum Glück gibt es sichere Wege, um im digitalen Raum anonym und geschützt unterwegs zu sein – Wege, die jedem von uns zur Verfügung stehen, wenn wir sie bewusst nutzen. In diesem Buch zeige ich dir so viele dieser Tools und Methoden wie möglich. Nutze diese Werkzeuge, schütze deine Daten und erzähle deinen Freunden davon. Denn je mehr Menschen diese Möglichkeiten nutzen, desto freier und sicherer wird unsere digitale Welt.

Es geht nicht nur darum, sich vor Überwachung zu schützen, sondern auch darum, bessere Innovationen zu fördern, gesündere Geschäftsmodelle zu unterstützen und mehr Wettbewerb und Menschlichkeit in die digitale Wirtschaft zu bringen. Wenn wir uns gegen die übermäßige Datensammlung der großen Unternehmen wehren, schaffen wir Raum für fairere, menschlichere und nachhaltigere Alternativen.

• • •

Dieses Buch soll dein Begleiter sein, um dir zu zeigen, wie du die Kontrolle über deine digitale Welt zurückgewinnen kannst – Schritt für Schritt. Wir beginnen in den Kapiteln 1 und 2 mit sicheren privaten Handys und Computern.

Danach erfährst du in den Kapiteln 3 und 4 alles, was wichtig ist, um sicher und anonym im Internet zu surfen und mit anderen zu kommunizieren. Anschließend stelle ich dir in den Kapiteln 5 und 6 Tools vor, die du verwenden kannst, um deine Privatsphäre zu schützen, sowie Alternativen zu bestehenden Diensten.

Außerdem erstellen wir in Kapitel 7 einen Alias (Pseudonym), um damit nichts mehr im Internet preiszugeben. Kapitel 8 enthält dann alle wichtigen Punkte zur finanziellen Privatsphäre und zur Freiheit.

Abschließend behandelt Kapitel 9 verschiedene kleine Tipps und Anleitungen zu Themen, die täglich unsere Privatsphäre und Sicherheit beeinflussen.

Du musst nicht alles und alle Kapitel sofort umsetzen, aber jeder kleine Schritt zählt. Zusammen können wir eine Zukunft schaffen, in der Privatsphäre, Freiheit und Innovation Hand in Hand gehen und niemand das Gefühl haben muss, ständig beobachtet zu werden.

Bleibe auf dem Laufenden
In der schnelllebigen Welt der Technologie ist es schwierig, immer auf dem neuesten Stand zu bleiben. Mit unserem Newsletter erhältst du regelmäßig Updates und Neuigkeiten zu Privatsphäre und Sicherheit. So bleibst du stets auf dem Laufenden und kannst deine Privatsphäre effektiv schützen. Jetzt hier anmelden: privatopia.de/newsletter

Kapitel 1
Computer

„Wir sollten nicht die Wahl zwischen Privatsphäre und Technologie haben müssen. Wir können beides haben."
~ Al Gore

Computer sind das Herzstück unserer digitalen Welt. Ein sicherer und privater Computer sollte daher eine Grundvoraussetzung sein, wenn du deine Privatsphäre schützen möchtest. Obwohl das Thema für viele überwältigend erscheint, steht es in diesem Ratgeber an erster Stelle. Wir nutzen unsere Computer für nahezu alles, und wenn sie kompromittiert sind, sind ab dann alle Bemühungen um unsere Privatsphäre vergeblich. Viele von uns verwenden ihren Laptop seit Jahren, was nicht nur Datenschutzprobleme, sondern auch erhebliche Sicherheitsrisiken mit sich bringt. Da wir Computer nicht nur zur Unterhaltung, sondern auch für Kommunikation und Bankgeschäfte nutzen, hat es höchste Priorität, einen sauberen und sicheren Computer zu nutzen — frei von Tracking- oder Schadsoftware, Viren und Überwachungsprogrammen.

Vor zwanzig Jahren konnte man einen neuen Computer kaufen und sofort loslegen, ohne sich Gedanken über die eigene Privatsphäre zu machen. Heute verlangen Unternehmen wie Microsoft bei der Einrichtung eines neuen Computers erstmal die Registrierung mit einem Online-Konto. Anschließend sammeln sie umfangreiche Daten über unsere persönliche Nutzung und speichern diese unbegrenzt. Diese Datensammlung, oft als „Telemetrie" bezeichnet, wird als Mittel zur Verbesserung der Benutzerfreundlichkeit beworben. Doch es ist besorgniserregend, wie viele persönliche Informationen dabei erfasst werden. Ich möchte nicht, dass große Unternehmen detaillierte Einblicke in meine Computernutzungsgewohnheiten nehmen.

Bei Apple ist die Situation ähnlich. Trotz Marketingkampagnen, die Privatsphäre in den Vordergrund stellen, speichern sie möglicherweise noch mehr persönliche Details als Microsoft.

Auch Apple verlangt einen Online-Account, um Apps herunterzuladen, und nutzt diesen zur genauen Identifikation der Nutzer. Haben wir einen Film heruntergeladen und nur die ersten fünf Minuten angesehen? Apple weiß das und speichert diese Informationen. Haben wir eine Produktbewertung geschrieben? Auch das wird erfasst und genutzt, um gezieltere Werbung anzuzeigen. Zusätzlich sammeln sie Standortinformationen durch das Netzwerk ihrer Geräte, etwa dazu, wer sich wo befindet, mit wem man sich verbindet und wer in der Nähe ist.

Das Ausmaß der Informationen, die Apple und Microsoft über uns und unsere Geräte speichern, ist oft unvorstellbar.

- Ungefährer Standort
- IP-Adressen
- Suchverlauf
- Geschriebene Texte
- Heruntergeladene Programme
- Zeitpunkt und Dauer der Nutzung der Programme
- Nutzungszeit des Geräts
- Geräte in der Nähe
- und vieles mehr...

Dies sind lediglich die grundlegenden Überlegungen. Ist ein Mikrofon vorhanden und der Sprachassistent aktiviert? Dann ist es wahrscheinlich, dass auch Audioaufnahmen gemacht werden. Ist die Kamera abgeklebt? Sind die Berechtigungen deaktiviert? Es ist wichtig, diese Aspekte im Auge zu behalten und Maßnahmen zu ergreifen, um unsere Privatsphäre zu schützen.

Während ich anfangs empfohlen habe, Mac und Windows sicherer zu machen, liegt der Schwerpunkt heute verstärkt auf Linux. Obwohl Mac und Windows größere Nutzerzahlen haben, bietet Linux erhebliche Vorteile in Bezug auf Sicherheit und Kontrolle. Während man bei Windows und Mac in der Vergangenheit noch das Sammeln von Daten deaktivieren konnte, hat man jetzt oft nur die Wahl zwischen „Ich möchte einige meiner Daten mit Microsoft teilen“ oder „Ich möchte alle meine Daten mit Microsoft teilen“. [5]

Mit dem Aufstieg der Künstlichen Intelligenz (KI) hat sich vieles verändert. Moderne Betriebssysteme wie Windows und MacOS integrieren zunehmend KI-Funktionen, die dein Verhalten analysieren und personalisierte Empfehlungen geben. Microsoft implementiert beispielsweise den (nicht abschaltbaren) „Copilot“, einen KI-Assistenten, der in verschiedene Anwendungen eingebunden ist. Auch Apple nutzt eine plattform- und geräteübergreifende KI, um das Nutzererlebnis zu verbessern. [6] Mit anderen Worten, jeder deiner Klicks und jede der eigenen Aktionen wird vom System erfasst und genutzt. Obwohl beide Unternehmen betonen, dass diese Analysen lokal auf deinem Computer stattfinden und nicht geteilt werden, kannst du nie ganz sicher sein, ob deine Daten nicht doch zur Verbesserung der KI verwendet und ob sie sicher vor Hackern aufbewahrt werden.

Diese KI-Funktionen sind zwar äußerst praktisch und wissen genau, was du möchtest, wodurch sich das Nutzererlebnis erheblich verbessert. Doch dies geschieht auf Kosten deiner Privatsphäre und persönlichen Daten. Wenn du deine Privatsphäre wirklich schützen möchtest, ist es nicht ausreichend, nur einige Einstellungen bei Windows oder MacOS zu ändern. In diesem Fall solltest du auf ein offenes Betriebssystem wie Linux zurückgreifen.

Linux wird oft als komplex und schwer zugänglich wahrgenommen. Doch das stimmt schon lange nicht mehr. Die Benutzerfreundlichkeit von Linux ist mittlerweile mit der von Windows oder MacOS vergleichbar. Ein Umstieg ist also nicht mehr so schwierig wie vor einigen Jahren, und auch weniger technikaffine Nutzer kommen gut mit Linux zurecht.

Viele meiner Kunden sind mit der Benutzerfreundlichkeit von Linux sogar zufriedener als mit der von Windows. Es gibt keine störende Werbung, keine unerwünschten Benachrichtigungen von vorinstallierten Programmen und keine ständigen Ablenkungen.

In Bezug auf Sicherheit und Privatsphäre übertrifft Linux selbst die besten Einstellungen bei Mac und Windows. Daher konzentrieren wir uns in diesem Kapitel auf Linux.

Neuer Linux Computer Konfiguration

Linux bietet dir die Möglichkeit, deine Privatsphäre und Sicherheit zurückzugewinnen. Doch gleich zu Beginn gibt es eine Herausforderung: Es gibt zahlreiche Distributionen (Varianten von Linux) und ebenso viele Meinungen darüber, welche die Beste ist. Für Anfänger und Einsteiger empfehle ich ganz klar Linux Ubuntu. Solltest du jedoch bereits eine andere Linux-Distribution bevorzugen, ist das vollkommen in Ordnung – dann kannst du die folgende Anleitung einfach überspringen. Wenn du der Meinung bist, QubesOS (eine sehr sichere und private Distribution) wäre das Nonplusultra in Sachen Privatsphäre und bereit bist, anfängliche Herausforderungen anzunehmen, nur zu!

Falls Benutzerfreundlichkeit für dich jedoch an erster Stelle steht, ohne dabei wesentliche Abstriche bei der Privatsphäre machen zu müssen, ist Ubuntu meine klare Empfehlung.

- **Einfach zu installieren und zu bedienen**: Ubuntu bietet eine benutzerfreundliche grafische Oberfläche, die die Softwareinstallation und Verwaltung erleichtert.
- **Breite Unterstützung**: Ubuntu läuft auf den meisten Computern, was die Kompatibilität sicherstellt.
- **Einfache Software-Updates**: Mit Ubuntu sind Aktualisierungen einfach und unkompliziert.
- **Große Nutzerbasis und Online-Support**: Dank einer großen Community gibt es viele Online-Ressourcen und Hilfestellungen.
- **Keine Programmierkenntnisse erfordert**: Ubuntu ist sehr benutzerfreundlich und erfordert keine Programmierkenntnisse.
- **Schnelle Lernkurve**: Die Grundlagen von Ubuntu sind sehr schnell zu erlernen, da Ubuntu Windows und MacOS sehr ähnlich ist.
- **Unauffälligkeit durch große Nutzerbasis**: In einer großen Nutzerbasis fällt der Einzelne weniger auf, was die Sicherheit erhöht.

Aus meiner Erfahrung mit Kunden in meinem Umfeld hat sich gezeigt, dass die langfristige Nutzung von Ubuntu anderen Betriebssystemen klar überlegen ist. Daher ist Ubuntu ein hervorragender Einstieg in die Welt von Linux.

Hinweis
Alle Befehle und Links in diesem Kapitel findest du auch auf der Webseite: privatopia.de/buch, um das Kopieren und Einfügen zu erleichtern

Egal welche Linux-Distribution du verwendest, bist du in puncto Privatsphäre und Sicherheit deutlich besser aufgehoben als mit einem Apple- oder Windows-System. Im Gegensatz zu Apple benötigst du keinen Linux-Account, um das System zu nutzen und Updates zu erhalten. Anders als Microsoft sammelt Linux keine personenbezogenen Nutzerdaten. Zudem ist Linux Open Source, was bedeutet, dass der Quellcode öffentlich zugänglich ist und zahlreiche Programmierer die Software auf Herz und Nieren überprüfen, bevor eine neue Version veröffentlicht wird. Wenn optimale Privatsphäre dein Ziel ist, ist Linux Ubuntu die beste Wahl.

Computer für Linux

Die erste Frage, die oft aufkommt, ist, welchen Computer man verwenden sollte. Hast du einen alten Computer und überlegst, darauf Linux zu installieren? Das ist grundsätzlich möglich und kann eine gute Option sein. Allerdings sind einige Aspekte in Bezug auf die Privatsphäre zu bedenken.

Wenn du ein Apple- oder Windows-Konto auf deinem Computer oder Smartphone verwendest, sammeln die jeweiligen Unternehmen häufig personenbezogene Informationen wie Namen, Adresse, E-Mail, Telefonnummer und vieles mehr. Diese Daten werden oft mit der eindeutigen Seriennummer deines Geräts verknüpft. So können Informationen wie deine IP-Adresse, Hardwaredetails und Internetverbindungen mit deiner Identität in Verbindung gebracht werden.

Mitarbeiter könnten diese Daten theoretisch einsehen, es wäre möglich, sie für Gerichtsverfahren anzufordern oder sie würden gegebenenfalls in Datenlecks veröffentlicht.

Selbst wenn du den Computer formatierst und ein neues Betriebssystem mit neuen Benutzerdaten installierst, können bestimmte Hardwaremerkmale weiterhin eine Identifizierung ermöglichen. Daher empfehle ich denen, die maximale Privatsphäre wünschen und über die finanziellen Mittel verfügen, den Kauf neuer Computer-Hardware.

Ich habe erfolgreich Ubuntu auf verschiedenen Windows- und Mac-Computern installiert. Wenn du also einen alten Computer hast, den du dafür verwenden möchtest, ist das eine gute Wahl. Solltest du jedoch einen neuen Laptop oder Computer speziell für Linux kaufen wollen, empfehle ich die Geräte von System76 (system76.com) oder Framework (frame.work). Diese Computer haben die Intel Management Engine deaktiviert – ein kleines Programm im Prozessor, das theoretisch unerlaubten Fernzugriff auf deinen Computer ermöglichen könnte. Obwohl diskutiert wird, wie wahrscheinlich ein solcher Zugriff ist, besteht dennoch ein gewisses Risiko.

Die folgende Anleitung zeigt dir, wie du Linux Ubuntu installieren kannst, mit kleinen Anpassungen hinsichtlich Privatsphäre und Sicherheit.

- Besuche die Webseite ubuntu.com/download/desktop und lade die neueste Long-Term-Support-Version (LTS) herunter. LTS-Versionen bieten über einen langen Zeitraum regelmäßige Updates und Sicherheitspatches. Zurzeit ist die aktuellste Ubuntu Version 24.04 (April 2024) oder in Zukunft die Version 26.04 (April 2026).
- Du kannst den Download mithilfe der Anleitung auf ubuntu.com/tutorials/how-to-verify-ubuntu#1-overview verifizieren. Dies ist zwar nicht zwingend erforderlich, kann aber hilfreich sein, um sicherzustellen, dass die heruntergeladene Datei weder beschädigt noch manipuliert wurde (Mehr dazu in Kapitel 6; „PGP“).

- Nun musst du einen bootfähigen USB-Stick erstellen, der die Ubuntu-Installationssoftware enthält. Damit kannst du später Linux auf deinem Computer starten und installieren.
- Lade dazu das Programm „Balena Etcher“ von etcher.balena.io herunter und startet es.
- Wähle die zuvor heruntergeladene ISO-Datei sowie den gewünschten USB-Stick aus und klicke auf die Schaltfläche „Flash“.

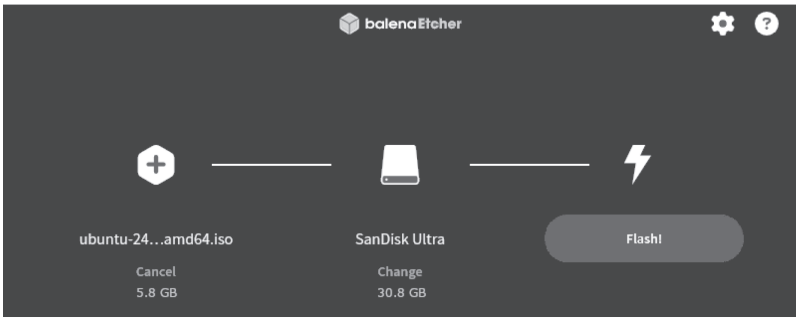

Abbildung 3 Balena Etcher

Nachdem du diese Schritte abgeschlossen hast, verfügst du über einen bootfähigen USB-Stick, mit dem du Linux Ubuntu installieren kannst. Wenn du einen älteren, ungenutzten Rechner zur Verfügung hast, kannst du Linux zunächst darauf ausprobieren.

Kannst du dir noch nicht vorstellen, nur Linux als einziges Betriebssystem zu nutzen? Mit einem sogenannten **Dual-Boot-System** kannst du sowohl Linux als auch Windows oder MacOS auf demselben Computer installieren. Wenn das interessant klingt, findest du zahlreiche Tutorials im Internet, die dir dabei helfen (mehr dazu in der Tool-Sektion). In diesem Leitfaden konzentrieren wir uns jedoch darauf, Linux als alleiniges Betriebssystem auf deinem Computer zu installieren, um maximale Privatsphäre und Sicherheit zu gewährleisten.

Hinweis
Die Schritte in diesem Kapitel können sich bei neueren Versionen ein wenig ändern, der grundlegende Ablauf bleibt jedoch gleich.

Ubuntu (Linux) installieren

- Stecke den USB-Stick in den Computer und starte ihn. Falls der Ubuntu-Installationsbildschirm nicht automatisch erscheint, öffne das BIOS-Menü. Starte dafür den Computer neu und drücke wiederholt die entsprechende Taste (je nach Computer „Delete“, „Escape“, „F1“, „F2“ oder „F10“), bis das Bootmenü erscheint. Wähle im BIOS-Menü unter „Boot-Priorität“ den USB-Stick aus.
- Wähle im Bootmenü die Option „Try or Install Ubuntu“ und bestätige mit „Enter“. Wähle im Willkommensfenster deine bevorzugte Sprache aus, in diesem Tutorial „Deutsch“. Klicke im Barrierefreiheit-Fenster auf „Weiter“.
- Wähle als Tastaturbelegung „Deutsch“ oder dein bevorzugtes Layout aus und klicke auf „Weiter“. Wähle „Ich will gerade keine Verbindung zum Internet herstellen“ und klicke auf „Weiter“.
- Wähle „Ubuntu installieren“ und klicke auf „Weiter“. Wenn du Ubuntu erst einmal ausprobieren möchtest, kannst du „Ubuntu ausprobieren“ wählen. In diesem Modus kannst du die Benutzeroberfläche und Standard-Apps testen, ohne das Betriebssystem vollständig zu installieren; alles geschieht nur auf dem USB-Stick. Für die vollständige Installation fahre wie folgt fort:
- Wähle „Interaktive Installation“ und klicke auf „Weiter“. Wähle „Standardinstallation“ und klicke auf „Weiter“. Die „Vollständige Installation“ installiert zusätzliche Programme wie LibreOffice und andere Anwendungen. Mit der Standardinstallation hast du die Möglichkeit, später selbst zu entscheiden, welche Programme du installieren möchtest, und vermeidest ungenutzte Software auf deinem Computer.
- Aktiviere „Software von Drittanbietern für Grafik und WLAN-Hardware installieren“ und klicke auf „Weiter“. Wähle „Festplatte löschen und Ubuntu installieren“ und klicke dann auf „Erweiterte Funktionen…“.
- Wähle „LVM mit Verschlüsselung verwenden“, bestätige mit „OK“ und klicke auf „Weiter“.

- Wähle das Laufwerk aus, auf dem Ubuntu installiert werden soll. In der Regel ist dies die größte verfügbare Festplatte. Klicke dann auf „Weiter“.
- Erstelle eine Passphrase für die Festplattenverschlüsselung. Dieses Passwort sollte stark genug sein, um gegen Brute-Force-Angriffe geschützt zu sein (Tipps zur Erstellung sicherer Passwörter findest du im Kapitel 4, „Passwörter“). Klicke anschließend auf „Weiter“.
- Gib hier keine persönlichen Daten ein, sondern allgemeine Angaben. Bei „Ihr Name“ und „Benutzernamen auswählen“ kannst du z. B. „Nutzer“ eingeben, und bei „Name Ihres Computers“ „Computer“. Wähle ein Passwort für deinen Benutzeraccount. Das zuvor erstellte Passwort dient der Festplattenverschlüsselung; dieses Passwort verwendest du für deinen Benutzeraccount auf dem Computer. Zur Vereinfachung kannst du dasselbe Passwort verwenden oder für zusätzliche Sicherheit ein anderes wählen. Beide Passwörter werden zukünftig beim Hochfahren des Computers benötigt. Klicke dann auf „Weiter“.
- Wähle deine Zeitzone aus und klicke auf „Weiter“. Du musst nicht deinen genauen Standort angeben; die Zeitzone genügt.
- Klicke auf „Installieren“, um die Installation von Ubuntu abzuschließen. Warte, bis die Installation abgeschlossen ist.

Achtung
Dieser Schritt formatiert die gesamte Festplatte und löscht alle vorhandenen Daten. Sichere daher vorher alle wichtigen Daten auf einem USB-Stick oder einer externen Festplatte.

- Klicke nach der Installation auf „Jetzt neu starten“, entferne den USB-Stick und drücke Enter.
- Gib nach dem Neustart beide Passwörter ein.
- Klicke zweimal „Weiter“, wähle „Nein, keine Systemdaten teilen“, nochmals auf „Weiter“ und „Fertigstellen“.

Ubuntu ist nun erfolgreich installiert, und die Festplatte ist verschlüsselt. Das bedeutet, dass selbst dann, wenn jemand physisch die

Festplatte aus deinem Computer entfernt, deine Daten weiterhin geschützt sind – ein Vorteil, den viele Windows- und Mac-Rechner nicht bieten. Dein Computer ist bereits gut gesichert und bietet ein hohes Maß an Privatsphäre. Ich empfehle jedoch, einige zusätzliche Anpassungen vorzunehmen, um die Sicherheit weiter zu erhöhen.

Öffne zunächst das Anwendungsmenü von Ubuntu (das Symbol mit den neun Punkten unten links) und starte das Terminal (alternativ kannst du auch „Strg“+„Alt“+„T“ drücken). Die dreifolgenden Befehle deaktivieren bei Ubuntu das Senden von Nutzungsstatistiken. Möglicherweise musst du nach dem ersten Befehl dein Passwort eingeben.

Das Terminal
Stelle dir das Terminal wie ein Direktgespräch mit deinem Computer vor. Anstatt Befehle über Menüs und Klicks auszuführen, gibst du sie direkt als Text ein. Es ist wie eine Kommandozentrale, mit der du schnell und effizient Einstellungen vornehmen kannst, die über die grafische Benutzeroberfläche nicht immer erreichbar sind.

```
sudo apt purge -y apport
sudo apt remove -y popularity-contest
sudo apt autoremove -y
```

Tippe diese Befehle nacheinander ein und bestätige jeweils mit „Enter“. Du findest alle Befehle aus diesem Kapitel auch auf „privatopia.de/buch“. Diese Befehle sorgen dafür, dass keine automatischen Fehlerberichte oder Nutzungsdaten mehr an Ubuntu gesendet werden.

- Öffne die Einstellungen über das Anwendungsmenü (Symbol unten links).
- Klicke auf “Benachrichtigungen” und deaktiviere beide Optionen.
- Navigiere zu “Datenschutz & Sicherheit” und wähle “Dateiverlauf & Papierkorb” aus. Deaktiviere alle Optionen.

- Unter “Fehlerdiagnose” wähle “Nie” aus.
- Schließe alle Fenster.

Jetzt kannst du Ubuntu nach deinen Wünschen anpassen. Nicht benötigte Symbole in der linken Leiste kannst du durch einen Rechtsklick und die Auswahl von „Loslösen“ entfernen.

Unter Linux gibt es zahlreiche Möglichkeiten, das Design, die Farben und das Layout des Systems nach deinen persönlichen Vorlieben anzupassen. Tatsächlich bietet Linux oft sogar noch mehr Anpassungsoptionen als die anderen Betriebssysteme. Viele dieser Anpassungen können direkt über die Systemeinstellungen vorgenommen werden.

Wenn dir diese Optionen nicht ausreichen, kannst du unter Linux die Tools **GNOME Tweaks** und den **Extension Manager** aus dem **Ubuntu Software Center** installieren, um noch umfassendere Anpassungen vorzunehmen.

Updates

Dein System stets auf dem neuesten Stand zu halten, ist entscheidend für Sicherheit und Stabilität. Es gibt zwei Möglichkeiten, Systemupdates durchzuführen.

- Öffne die App „Aktualisierungsverwaltung“ und installiere die verfügbaren Updates.
- Oder öffne das Terminal und gebe nacheinander die folgenden Befehle ein:

```
sudo apt update
sudo apt upgrade
sudo apt full-upgrade
sudo apt autoremove
sudo apt autoclean
```

Diese Befehle aktualisieren das Betriebssystem sowie Apps und löschen nicht benötigte, zwischengespeicherte Dateien.

Apps herunterladen

Die einfachste Möglichkeit, Apps zu installieren, bietet die Software-App. Hier kannst du aus einer Vielzahl von Anwendungen auswählen und diese mit nur einem Klick installieren. Wenn du also eine App herunterladen möchtest, solltest du zuerst in der Software-App nachsehen.

Tipp
Um das App-Menü zu öffnen, in dem alle Apps angezeigt werden, klicke unten links auf den Kreis mit den drei Punkten. Dort erhältst du eine übersichtliche Darstellung aller verfügbaren Apps.

Einige Programme sind jedoch nicht im Software-Center verfügbar und müssen direkt von der jeweiligen Webseite heruntergeladen werden. Suche dafür nach der gewünschten App in deinem Browser und öffne die offizielle Webseite. In der Regel bieten diese Webseiten Schritt-für-Schritt-Anleitungen von der Installation bis zum Start der App.

Neben der Installation über die Software-App stehen dir viele verschiedene Installationsmethoden zur Verfügung. Je nach Quelle und Format der App kannst du unterschiedliche Verfahren nutzen.

- **<app-name>.deb-Pakete:** Diese sind speziell für Ubuntu konzipiert. Du kannst sie direkt von der Webseite des Anbieters herunterladen und über das Terminal installieren.
- **AppImage:** Ein portables Format, das keine Installation erfordert. Du musst die AppImage-Datei lediglich herunterladen und ausführbar machen (Rechtsklick > Eigenschaften > Als Programm ausführen). Danach kannst du das Programm direkt mit einem Doppelklick starten.
- **Snap-Pakete:** Diese Pakete sind universell auf allen Linux-Distributionen einsetzbar. Um Snap zu installieren, gib in das Terminal diesen Befehl ein: „`sudo apt install snap`“. Anschließend kannst du Apps mit dem Befehl „`snap install <app-name>`“ im Terminal installieren.

- **Flatpak:** Ähnlich wie Snap ist Flatpak ein weiteres universelles Format, das plattformübergreifend funktioniert. Nach der Installation von Flatpak auf deinem System über „`sudo apt install flatpak`“ kannst du Apps mit „`flatpak install <app-name>`“ installieren.
- **PPAs (Personal Package Archives):** Diese bieten die Möglichkeit, zusätzliche Softwarequellen hinzuzufügen, um Apps zu installieren, die nicht in den Standard-Repositories enthalten sind. Dies geschieht meist über das Terminal, wie beispielsweise beim Tor-Browser (siehe Kapitel 3).

Diese verschiedenen Methoden bieten dir Flexibilität bei der Installation von Anwendungen und ermöglichen es dir, auf eine breite Palette von Software zuzugreifen.

Dateien

Bei Linux Ubuntu ist die Dateistruktur ähnlich wie bei Windows oder MacOS. Du kannst die Dateien über das Ordnersymbol in der linken Seitenleiste öffnen. Dort findest du dein Home-Verzeichnis, in dem alle deine persönlichen Daten gespeichert sind. Unter anderem gibt es hier die Verzeichnisse für den Schreibtisch (Desktop), Dokumente, Bilder, Downloads usw. Du kannst deine Dateien nach Belieben dort anordnen.

Ein großer Unterschied bei Linux ist, dass du auch Zugriff auf systemrelevante Verzeichnisse hast, wenn du das möchtest. Drücke dazu „Strg“ + „H“, um zusätzliche Ordner anzuzeigen. Diese benötigst du jedoch in der Regel nicht, also schau dort nur vorbei, wenn du genau weißt, was du tust.

Terminal

Ubuntu wurde entwickelt, um insbesondere Einsteigern die Installation und Nutzung von Linux zu erleichtern, ohne dass sie auf das Terminal angewiesen sind. Dennoch kann es in bestimmten Situationen notwendig sein, das Terminal zu verwenden, sei es zur Installation spezifischer Software oder zur Behebung größerer Probleme.

Während die meisten Nutzer von MacOS und Windows das Terminal selten verwenden, da viele grafische Programme dessen Funktionen übernehmen, bietet das Terminal unter Linux leistungsstarke Werkzeuge und eine höhere Flexibilität. Zwar gibt es auch hier grafische Alternativen, doch das Terminal kann besonders nützlich sein, wenn es um Privatsphäre und Sicherheit geht. Viele Menschen fühlen sich vom Terminal abgeschreckt, aber es ist gar nicht so kompliziert, wie es zunächst erscheint. Oft genügt es, Befehle aus dem Internet oder diesem Buch zu kopieren und sie ins Terminal einzufügen, wie bereits in diesem Kapitel mehrfach erwähnt.

- Meist kopierst du nur vorgefertigte Befehle, wie auch hier in diesem Kapitel.
- So gut wie nie musst du selbst komplexe Lösungen finden.
- Du musst das Terminal nicht unbedingt benutzen, um Linux zu verwenden.
- Es ist aber bei vielen Aufgaben hilfreich, besonders beim Lösen von Problemen oder beim Anpassen deiner Sicherheitseinstellungen.
- Die Befehle hier im Buch kannst du einfach kopieren und einfügen, meist nur einmalig.

Tipp
Es gibt viele Bezeichnungen für das Terminal, wie „Shell“, „Bash“, „Command“ oder „Prompt“

- Um das Terminal zu öffnen, klicke unten links auf das Symbol mit den drei Punkten und wähle „Terminal“.
- Alternativ kannst du auch den Shortcut „Strg“+„Alt+„T“ verwenden.
- Das Terminal ist sehr einfach aufgebaut und sieht nach dem Öffnen ungefähr aus wie folgt.

Abbildung 4 Das Terminal

`user` steht für den Benutzernamen, mit dem du angemeldet bist. `laptop` ist der Name deines Computers. Hinter dem `$`-Zeichen kannst du nun Befehle eingeben und sie mit der „Enter“-Taste (Eingabe-Taste) bestätigen. Der blinkende Cursor im Terminal zeigt dir auf der linken Seite an, wo du gerade tippst.

Tipp
Die Befehle, die du ins Terminal eintippst, werden auch „Commands“ genannt. In verschiedenen Quellen werden sie auch als „Prompt“ oder „Command Line“ bezeichnet.

Jetzt schauen wir uns ein paar grundlegende Befehle an. Es gibt einen Unterschied, ob du normale Befehle ausführst oder als „Superuser“ (mit erweiterten Rechten). Für Aufgaben wie das Installieren oder Löschen von Programmen benötigt man Superuser-Rechte, ähnlich wie bei Windows oder MacOS als Administrator.

Um Befehle als Superuser auszuführen, gebe `sudo` vor dem Befehl ein. Beispiel:

`sudo apt update` und `sudo apt upgrade`

`sudo` erteilt die notwendigen Rechte. `apt update` suchen nach neuen Updates, während `apt upgrade` diese installiert.

Nach Beendigung des Befehls erscheint eine neue Zeile mit: `user@laptop:~$`, was signalisiert, dass der Prozess abgeschlossen ist.

Um ein Programm wie „BleachBit“ zu installieren, gebe den folgenden Befehl ein.

```
sudo apt install bleachbit
```

`sudo` erteilt die notwendigen Rechte. `apt install` signalisiert, dass wir ein Programm installieren möchten. `bleachbit` ist der Name des Programms.

Kopieren und Einfügen im Terminal
Um Texte im Terminal zu kopieren oder in dieses einzufügen, kannst du nicht wie gewohnt „Strg+C“ und „Strg+V“ verwenden. Stattdessen musst du einen Rechtsklick ausführen und die entsprechenden Optionen (Einfügen oder Kopieren) auswählen.

Neben `apt install` gibt es noch andere Wege, Programme unter Linux zu installieren. Ein Beispiel ist die Installation von Veracrypt (siehe Kapitel 4, „Verschlüsselte USB-Sticks und Backups“. Dazu müsstest du die .deb-Datei von der Webseite herunterladen, die dann im Ordner „Downloads“ gespeichert wird.

Um nun die Datei über das Terminal zu installieren, musst du zuerst in den Download-Ordner wechseln. Das kannst du entweder über die grafische Oberfläche ausführen, indem du in den Ordner wechselt und mit einem Rechtsklick „Im Terminal öffnen“ wählst, oder du benutzt den Befehl `cd`. Dieser wird dafür verwendet, um zwischen verschiedenen Ordnern zu wechseln.

```
cd Downloads/
```

Mit `cd` kannt du in jedes beliebige Verzeichnis wechseln. Beispiel:

```
cd Desktop/Arbeit/Buch/.
```

Sobald du im richtigen Ordner bist, sieht das Terminal etwa wie folgt aus.

Abbildung 5Terminal-Downloads

Um Veracrypt zu installieren, gebe folgenden Befehl ein:

```
sudo apt install ./veracrypt-1.26.14-Ubuntu-
24.04-amd64.deb
```

Dieser Befehl führt als Superuser `sudo`, die Installation `apt install`, von der `veracrypt.deb` Datei aus.

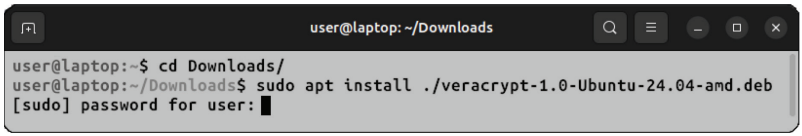

Abbildung 6 Terminal-Veracrypt-Installation

Tipp
Um lange Dateinamen nicht komplett abtippen zu müssen, kannst du die Tab-Taste verwenden, wodurch Dateinamen automatisch vervollständigt werden. Gib einfach den Anfang des Namens ein, drücke Tab, und das Terminal vervollständigt, was fehlt. Nach Abschluss des Prozesses hast du Veracrypt installiert.

Dies war nur ein Einstieg in die Nutzung des Terminals. Dieser wirkt jetzt vielleicht ein wenig überwältigend, aber mit der Zeit wirst du merken, dass es viele weitere nützliche Befehle und Möglichkeiten gibt, das Terminal zu verwenden. Und fast immer kopiert man nur etwas aus dem Internet.

Daten entfernen

Mit der Open-Source-Software „BleachBit“ kannst du deinen Computer von unnötigen Dateien befreien. Das schafft nicht nur Platz, sondern verbessert auch die Performance und Leistung. Die Benutzeroberfläche von „BleachBit“ ist übersichtlich und einfach zu bedienen. Du kannst auswählen, welche zwischengespeicherten Dateien gelöscht werden sollen und welche nicht.

Um BleachBit zu installieren, öffne das Terminal und gebe folgenden Befehl ein.

```
sudo apt install bleachbit
```

Starte danach „BleachBit“ über das Anwendungsmenü.

- Links siehst du dann eine Liste mit Optionen. Ich empfehle, alle auszuwählen, außer „Freier Speicherplatz“. Die Ausführung dieser Option kann sehr viel Zeit in Anspruch nehmen und bringt in der Regel keinen spürbaren Vorteil.
- Klicke oben links auf „Bereinigen“.
- Bestätige mit „Löschen“, und der Reinigungsvorgang beginnt.

Ich persönlich führe diese Reinigung einmal pro Woche durch. Aber auch einmal im Monat reicht aus, um deinen Computer sauber und schnell zu halten.

Antivirus

Die meisten Viren existieren für Windows- und Mac-Systeme, weshalb Linux in dieser Hinsicht von Haus aus ziemlich sicher ist. Dennoch kann ein gelegentlicher Virenscan nicht schaden. Manchmal werden dabei Windows-Viren entdeckt, die über E-Mail-Anhänge auf deinen Computer gelangt sind, aber für Linux keine Bedrohung darstellen. Diese solltest du trotzdem entfernen.

Die folgenden Befehle für das Terminal installieren und aktualisieren ein Open-Source-Programm namens „ClamAV“.

```
sudo apt update
sudo apt install -y clamav clamav-daemon
sudo systemctl stop clamav-freshclam
sudo freshclam
sudo systemctl start clamav-freshclam
```

Um einen Virenscan durchzuführen, kannst du die nächsten zwei Befehle verwenden. Der erste Befehl scannt deinen gesamten Computer und zeigt gefundene Viren an, entfernt sie aber nicht. Der zweite Befehl wiederholt den Scan und löscht alle infizierten Dateien.

```
clamscan -r -i /
clamscan -r -i --remove=yes /
```

Virtuelle Maschinen

Momentan nutzen wir unseren Computer für verschiedene Aktivitäten: fürs Surfen im Internet, für diverse Anwendungen sowie für berufliche Aufgaben und Finanzangelegenheiten. Optimal wäre es, diese Bereiche klar zu trennen, um private Aktivitäten von beruflichen Aufgaben zu isolieren und unsere Finanzangelegenheiten vollständig separat zu halten.

Hier kommen virtuelle Maschinen ins Spiel. Eine virtuelle Maschine ist eine Software, die wie ein vollständig eigenständiger und unabhängiger Computer funktioniert. Im Grunde genommen handelt es sich um einen zweiten Computer innerhalb unseres bestehenden Systems, der lediglich die Hardware teilt. Ein großer Vorteil ist, dass dieser virtuelle Computer mit einem anderen Betriebssystem ausgestattet werden kann als unser „echter" Computer. Das bedeutet, du kannst Ubuntu als Hauptbetriebssystem verwenden und gleichzeitig mehrere virtuelle Maschinen betreiben, beispielsweise eine mit Windows, eine mit MacOS und weitere mit Linux.

Das Beste daran ist, dass diese virtuellen Maschinen völlig isoliert voneinander arbeiten und nicht miteinander kommunizieren. Du kannst sie also ganz nach deinen Bedürfnissen nutzen und mit dem Betriebssystem deiner Wahl konfigurieren. Allerdings ist dieses Thema eher für Fortgeschrittene geeignet, weshalb ich in diesem Buch nicht weiter darauf eingehe. Falls du neugierig geworden bist, empfehle ich die Software **Oracle Virtual Box** (virtualbox.org), und weitere Informationen dazu, sowie Anleitungen findest du in der Tools-Sektion.

Hardware-Sicherheit

Im Gegensatz zu Windows oder MacOS musst du dich hier um weniger kümmern. Selbst im schlimmsten Fall, wenn jemand physischen Zugriff auf deinen Laptop erhält, kann dieser Angreifer nicht auf deine Daten zugreifen, da deine Festplatte verschlüsselt ist. Vorsicht ist jedoch geboten, wenn du eine zusätzliche Festplatte installiert hast oder einen USB-Stick verwendest, da diese standardmäßig

nicht verschlüsselt sind (mehr zur Verschlüsselung in Kapitel 4, „Verschlüsselte USB-Sticks“).

Aber selbst wenn deine Festplatte verschlüsselt ist, kann es doch ein Sicherheitsproblem geben. Leider sehe ich oft, dass Personen in Bibliotheken, Cafés oder anderen öffentlichen Orten ihren Laptop entsperrt liegen lassen, während sie kurz weggehen. In diesen wenigen Minuten kann das entsperrte Gerät nicht nur gestohlen werden, sondern es können auch wichtige Daten und Dokumente schnell entwendet oder Viren eingeschleust werden. Daher solltest du deinen Laptop immer sperren, bevor du ihn unbeaufsichtigt lässt. Aus dem genannten Grund sollte man ihn eigentlich aber überhaupt nicht unbeaufsichtigt lassen.

Ein bekanntes Beispiel ist die Festnahme von Ross Ulbricht, dem Gründer der Plattform „Silk Road“. Trotz seiner extremen Vorsichtsmaßnahmen und dem Einsatz modernster Verschlüsselungstechnologien wurde er festgenommen, als er in einer Bibliothek in San Francisco an seinem Laptop arbeitete. Die Ermittler warteten bewusst, bis der Laptop entsperrt war, um auf alle Daten zugreifen zu können. Um zu verhindern, dass dir Ähnliches passiert, gewöhne dir an, deinen Computer immer auszuschalten, wenn du aufstehst.

Tails

Wie bereits erwähnt, ist Ubuntu eine sehr benutzerfreundliche Lösung. Neben Ubuntu gibt es jedoch viele andere Betriebssysteme, die in Bezug auf Sicherheit und Privatsphäre noch deutlich mehr bieten können. Besonders in Situationen, in denen zusätzlicher Schutz erforderlich ist – beispielsweise, wenn man an einem fremden Rechner arbeitet oder eine zusätzliche Ebene der Anonymität wünscht – kommt **Tails** ins Spiel.

Tails ist ein Linux-Betriebssystem, das speziell dafür entwickelt wurde, keine Spuren zu hinterlassen und Viren auf dem verwendeten Rechner zu vermeiden. Es gilt als eines der sichersten portablen Betriebssysteme und wird ausschließlich von einem USB-Stick aus gestartet. Im Gegensatz zu Windows, MacOS oder Ubuntu wird nicht

der interne Speicher des Computers genutzt – alles läuft direkt über den USB-Stick. Sobald der Stick entfernt wird, bleiben keine Daten auf dem Rechner zurück. Tails eignet sich somit besonders für Situationen, in denen Anonymität entscheidend ist, sollte jedoch nicht als alltägliches Betriebssystem verwendet werden.

Privatsphäre: Tails verwendet das Tor-Netzwerk für alle Internetverbindungen. Obwohl dies nicht für den alltäglichen Gebrauch geeignet ist, bietet es maximale Anonymität, wenn sie benötigt wird. Neben Tor sind auch einige Standardprogramme wie LibreOffice, PGP und Electrum vorinstalliert, sodass Tails sofort für viele Aufgaben genutzt werden kann.

Persistenter Speicher: Standardmäßig speichert Tails keine Daten dauerhaft. Sobald der USB-Stick abgezogen wird, sind alle Daten gelöscht. Das mag zunächst unpraktisch erscheinen, doch genau dieses Feature erhöht die Privatsphäre erheblich. Es besteht jedoch die Möglichkeit, einen verschlüsselten Bereich auf dem Stick einzurichten, um wichtige Dateien für zukünftige Sitzungen zu speichern.
Aufgrund dieser Eigenschaften wird Tails häufig von Aktivisten, Journalisten und der Privacy-Community genutzt, um Zensur zu umgehen, die Identität zu schützen und die Privatsphäre zu wahren. Um selbst einen Tails-USB-Stick zu erstellen, musst du, ähnlich wie bei Ubuntu, Tails auf den USB-Stick flashen.

- Besuche dafür die Website tails.net/install/download/ und lade die neueste Version von Tails herunter.
- Nach dem Download solltest du die Datei verifizieren, um sicherzustellen, dass sie nicht manipuliert wurde. Klicke dazu auf „Select your download to verify…“ und wähle die heruntergeladene Tails-Datei aus. Alternativ kannst du die OpenPGP-Signatur und den OpenPGP-Schlüssel herunterladen und mit Kleopatra (siehe Kapitel 6, Abschnitt „PGP“) überprüfen.
- Nachdem die Datei verifiziert wurde, benötigst du wieder das Programm „BalenaEtcher“ (etcher.balena.io), um Tails auf einem USB-Stick zu installieren. Der Stick sollte mindestens 8 GB groß sein – ich empfehle jedoch einen mit 16 GB oder mehr.

- Öffne „BalenaEtcher“ und stecke den USB-Stick in den Computer.
- Wähle in BalenaEtcher die heruntergeladene Tails-Datei („tails…6.6.img“) und den USB-Stick aus.
- Klicke auf „Flash“ und warte, bis der Vorgang abgeschlossen ist. Dabei werden alle Daten auf dem USB-Stick gelöscht.

Nun ist „Tails“ auf dem USB-Stick installiert, und du kannst loslegen. Der nächste Schritt besteht darin, den Computer von diesem USB-Stick aus zu starten.

- Fahre deinen Computer herunter. Während er neu startet, drücke mehrmals eine der folgenden Tasten. „F2“, „F10“, „F11“, „F12“, „Entf“ oder „Esc“. Stelle dabei sicher, dass der Tails-USB-Stick eingesteckt ist. Es sollte sich das BIOS-Menü öffnen.
- Im BIOS-Menü wähle unter „Bootpriorität“ das Laufwerk mit dem USB-Stick aus.
- Verlasse das Bootmenü, Tails sollte daraufhin starten.
- Sobald das „Welcome-to-Tails-Fenster“ erscheint, ändere das „Keyboard-Layout“ auf „German“, um die Eingabe zu erleichtern. Die Optionen „Language“ und „Formats“ solltest du unverändert lassen, um deine Anonymität zu schützen.
- Aktiviere die Option „Create Persistent Storage“ und klicke auf „Start Tails“.
- Um den persistenten Speicher einzurichten, gehe oben rechts auf „Applications“, dann auf „System Tools“ und wähle „Persistent Storage“ aus. Klicke im neuen Fenster auf „Continue“.
- Gib daraufhin eine sichere Passphrase (Passwort) ein, um den Speicher zu verschlüsseln. Nutzte dafür am besten einen Passwortmanager, um ein sicheres Passwort zu generieren und zu speichern.
- Nach kurzer Ladezeit kannst du auswählen, welche Daten gespeichert werden sollen. Ich empfehle, „Welcome Screen“, „Tor Bridge“, „Electrum Bitcoin Wallet“ und „GnuPG“ auszuwählen.

- Schließe das Fenster, und ab sofort kannst du Dateien im „Persistent“-Ordner speichern, die bei zukünftigen Tails-Sitzungen verfügbar bleiben.

Tails ist nun erfolgreich gestartet. Die Benutzeroberfläche ähnelt Ubuntu, ist jedoch minimalistischer und enthält andere vorinstallierte Programme. Mit Tails kannst du anonym und ohne Spuren auf jedem beliebigen PC arbeiten und den Tor-Browser nutzen. Obwohl ich Tails selten verwende, empfehle ich jedem, diese Schritte einmal durchzugehen, um sich mit dem System vertraut zu machen und es für potenzielle Situationen einsatzbereit zu haben.

• • •

Gemeinsam haben wir einen sicheren und privaten Computer eingerichtet. Wir nutzen ein sicheres Betriebssystem, nämlich Ubuntu. Dadurch können wir sämtliche Funktionen und Anwendungen verwenden, ohne uns jemals bei einem Microsoft- oder Apple-Konto anmelden zu müssen. Zudem haben wir unsere gesamte Festplatte mit all unseren Daten verschlüsselt und auch einige wichtige Einstellungen vorgenommen, die uns mit Ubuntu noch mehr Privatsphäre und Sicherheit bieten. Darüber hinaus haben wir ein Antivirus-Programm sowie ein Systemreiniger-Tool installiert. Der Computer ist jetzt startklar. Du solltest jedoch nicht unüberlegt alle möglichen Apps installieren, da diese ebenfalls stark in die Privatsphäre eingreifen können.

Als Nächstes geht es darum, ein sicheres und privates Smartphone einzurichten. Falls du direkt mit dem Computer weiterarbeiten möchtest und Apps sowie Software herunterladen willst, schreite bitte zu Kapitel 3 weiter. Dort werden wir die Einrichtung des Computers abschließen, indem wir uns um sichere und private Apps, Browser und Verbindungen kümmern.

Kapitel 2
Handys

„Die größte Bedrohung der Privatsphäre lauert nicht mehr auf dem Schreibtisch, sondern in der Hosentasche.*" ~ John McAfee*

Unser ganzes Leben passt in unsere Hosentasche: Kontakte, Fotos, Banking-Apps – alles auf einem kleinen Gerät, das wir ständig bei uns tragen: unser Handy. Es sammelt Unmengen an Informationen über unser Leben, unsere Gewohnheiten und unseren Standort.

Kein Wunder, dass das Handy eines der am meisten überwachten Geräte ist. Deshalb ist es entscheidend, ein sicheres und vor allem privates Handy zu besitzen, damit wir selbst bestimmen können, welche Daten wir teilen und welche nicht.

Beim Thema „Handys und Privatsphäre" hört man oft, dass echte Privatsphäre mit einem Smartphone unmöglich sei. Egal, was man tut, Hardware und Software würden immer Daten über die Nutzung sammeln – so das Argument. Sicher steckt da etwas Wahres drin. Aber ich werde dir jetzt nicht raten, dein Handy wegzuwerfen und nie wieder zu telefonieren oder Nachrichten zu schreiben – das wäre zu viel verlangt. Stattdessen möchte ich dir eine Lösung vorstellen, die dir ein Höchstmaß an Sicherheit und Privatsphäre bietet, ohne dass du auf die Vorteile moderner Technologie verzichten musst.

Nun stellt sich wahrscheinlich die Frage: Android oder iOS – welches Betriebssystem bietet mehr Privatsphäre und Sicherheit?

Die Antwort lautet: keines von beiden. Zwar sammelt und teilt Apple in der Regel weniger Daten als Android (bzw. Google), aber auch hier werden immer noch viele Informationen erhoben und geteilt. Wer wirklich Privatsphäre und Sicherheit erreichen möchte, sollte auf ein anderes Betriebssystem umsteigen. Im vorherigen Kapitel ging es um das Betriebssystem Linux für Computer. Das gleiche machen wir auch hier mit unserem Handy.

Ein angepasstes Betriebssystem, auch Custom Operating System genannt, ist ein System, das nicht vom Handyhersteller stammt, sondern von unabhängigen Entwicklern erstellt wurde. In diesem Kapitel geht es um GrapheneOS, ein solches Betriebssystem, das von Daniel Micay ins Leben gerufen wurde und mittlerweile von einem Entwicklerteam als Non-Profit-Projekt weitergeführt wird.

Ein separates Betriebssystem klingt vielleicht kompliziert und umständlich, aber meine Erfahrung zeigt, dass es gar nicht so schwierig ist. Viele zögern anfangs, den Schritt zu einem neuen Handy und Betriebssystem zu gehen, doch hinterher sind sie froh über die Entscheidung und können sich darauf verlassen, dass ihre Daten wirklich privat und sicher sind. Auch die Benutzerfreundlichkeit leidet nicht darunter, denn diese Betriebssysteme bieten alle Funktionen, die man von einem normalen Android-Handy kennt. Optisch merkt man also keinen Unterschied.

Unsere Anforderungen an das neue Betriebssystem sind: Sicherheit, Privatsphäre und ein Android ohne Google.

Hinweis
Ein „entgoogeltes“ Android ist ein Betriebssystem, das auf der reinen Basisversion von Android aufbaut – ohne jegliche Google-Dienste. Das bedeutet: Keine Google-Apps, keine Tracker, kein Play Store und keine Play Services. Es ist die reinste Form von Android.

Zugegeben, Google bietet viele nützliche Dienste und Apps an. Doch diese gehen oft mit tiefen Eingriffen in unsere Privatsphäre einher. Dass Google Daten sammelt und teilt, ist kein Geheimnis – das eigentliche Problem ist, dass man sich kaum dagegen wehren kann, wenn man dieses Betriebssystem nutzt.

Das Android Open Source Project, der Kern der Android-Betriebssysteme, enthält noch immer einige Google-Elemente – was nicht überrascht, da Google das System entwickelt hat. Doch es gibt Entwicklergemeinschaften, die alle Google-Komponenten entfernen und diese durch alternative, sichere Lösungen ersetzen möchten. So

werden beispielsweise die Zeiterfassung oder Benachrichtigungen durch Open-Source-Alternativen ersetzt, und der bisher von Google bereitgestellte Ortungsdienst durch eine sicherere Option wie den Mozilla Location Service.

GrapheneOS

GrapheneOS ist ein „entgoogeltes" Betriebssystem, das von Grund auf mit einem klaren Fokus auf Sicherheit und Privatsphäre entwickelt wurde. Es basiert auf der Grundbasis von Android, also von der Benutzeroberfläche gibt es nicht viele Unterschiede.

Jedoch merkt man gleich beim Einrichten besteht darin, dass man keinen Account benötigt, um das Handy zu starten. Ein weiteres Merkmal ist, dass es keinen App Store oder vorinstallierte Apps gibt – lediglich eine Kamera-App, einen privaten Browser und einige wenige andere Anwendungen sind vorhanden. Denn der Nutzer selber soll entscheiden was er braucht an Apps und was nicht.

Besonders hervorzuheben ist die „App-Sandbox-Funktion" von GrapheneOS. Während bei Google-Android Apps frei miteinander und mit dem Internet kommunizieren können, bleiben die Apps bei GrapheneOS in einem „Sandkasten" isoliert. Das bedeutet, dass sie nicht einfach auf andere Apps zugreifen können und die Kommunikation vollständig blockiert ist. Zudem kannst du den Internetzugang für einzelne Apps komplett deaktivieren, sodass sämtliche Daten nur auf dem Gerät selbst bleiben – etwas, das bei Standard-Betriebssystemen nicht möglich ist.

Ein weiterer Sicherheitsaspekt von GrapheneOS ist die Art und Weise, wie Updates und die Installation des Betriebssystems gehandhabt werden. Im Vergleich zu anderen entgoogelten Betriebssystemen ist GrapheneOS das einzige, bei dem du den Bootloader nachträglich wieder sperren kannst. Das bedeutet, dass ein Angreifer mit physischem Zugriff auf dein Gerät kein anderes Betriebssystem installieren kann. Außerdem werden alle Software sowie Sicherheitsupdates durchgeführt, ohne dass der Update-Server auf dein Gerät zugreifen muss. Der Server kennt lediglich die IP-Adresse des

Geräts und die Version, die aktualisiert werden soll. Kurz gesagt, die Risiken von Cyberangriffen und der Installation von Malware werden drastisch reduziert. GrapheneOS ist also wie Android, jedoch mit einem maximalen Fokus auf Privatsphäre und Sicherheit.

Die benötigte Hardware

Wie bereits in Kapitel 1 erwähnt, rate ich dringend davon ab, ein bereits genutztes Gerät zu verwenden. Denke daran: Dein aktuelles Handy hast du über Jahre hinweg genutzt, warscheinlich ohne wirklich auf Privatsphäre oder Sicherheit zu achten. Deine Daten sind auf den Servern von Google oder Apple gespeichert und mit deiner echten Identität verknüpft. Zudem sind sie an die Seriennummer des Handys gekoppelt. Selbst wenn du das Gerät auf die Werkseinstellungen zurücksetzt, bleibt die Seriennummer bestehen. Nach einiger Zeit könnte das neue Betriebssystem möglicherweise wieder mit deiner alten Identität in Verbindung gebracht werden – und all deine Bemühungen um mehr Privatsphäre wären umsonst.

Um dieses Problem zu umgehen, empfehle ich, ein neues Gerät zu kaufen, das niemals mit deiner Identität verknüpft wurde. Auch gebrauchte oder generalüberholte Geräte sind hier keine gute Wahl. Zwar argumentieren einige Privatsphäre-Experten, dass man mit einem gebrauchten Gerät seine Spuren verwischen könnte, doch es gibt auch Risiken. Sollte das Gerät zuvor einem Kriminellen gehört haben, der von Geheimdiensten überwacht wurde, könnten diese Überwachungen bei dir fortgeführt werden. Und falls es sich um ein gestohlenes Gerät handelt, könnte die Polizei schnell vor deiner Tür stehen. Natürlich lässt sich das erklären, aber deine Identität wäre dennoch mit diesem Gerät verknüpft. Zwar ist das Risiko für diese beiden Probleme gering, aber ich möchte mir diese Kopfschmerzen ersparen und bin bereit, dafür minimal mehr zu bezahlen.

Am besten kaufst du ein neues Gerät in einem Elektronikladen und bezahlst bar. Noch besser wäre es, wenn du einen Freund oder Verwandten bittest, das Gerät für dich zu kaufen. Falls es Videoaufnahmen des Kaufs gibt, wäre dein Gesicht nicht mit dem Gerät verknüpft. Ich weiß, das klingt nach übertriebener Vorsicht, aber es minimiert das Risiko.

Welches Handy sollte man kaufen?

Leider gibt es nicht viele Optionen, da GrapheneOS ausschließlich auf Google Pixel-Geräten läuft. Das mag überraschend erscheinen – schließlich möchten wir doch von Google wegkommen, oder? Ja, das wollen wir auch. Dennoch nutzen wir lediglich die Hardware von Google, während wir die Software durch ein privates, sicheres Betriebssystem ersetzen. Pixel-Geräte sind die einzigen, die hohe Sicherheitsstandards erfüllen und offiziell die Installation eines anderen Betriebssystems erlauben.

Ich empfehle, eher die neueren Modelle zu kaufen, da diese länger Sicherheits- und Softwareupdates erhalten. Hier ist eine Liste der aktuell verfügbaren Geräte sowie der Zeitrahmen, bis wann deren Sicherheits- und Softwareupdates enden. Eine stets aktuelle Übersicht findest du unter: grapheneos.org/faq#device-lifetime.

Gerätname	**Ende von Sicherheits- und Softwareupdates**
Google Pixel 9 Pro Fold	August 2031
Google Pixel 9 Pro XL	August 2031
Google Pixel 9 Pro	August 2031
Google Pixel 9	August 2031
Google Pixel 8a	Mai 2031
Google Pixel 8 Pro	Oktober 2030
Google Pixel 8	Oktober 2030
Google Pixel Tablet	Juni 2028
Google Pixel 7a	Mai 2028
Google Pixel 7 Pro	Oktober 2027
Google Pixel 7	Oktober 2027
Google Pixel 6a	Juli 2027

Tabelle 1: Sicherheitsupdates bei GrapheneOS pro Modell

Letztlich bleibt es deine persönliche Entscheidung, welche Größe, welches Design und welche technischen Spezifikationen (wie Kamera, Speicherplatz usw.) du bevorzugst. Ich greife immer lieber zu den a-Modellen, da sie kleiner und günstiger sind und dennoch mit den technischen Spezifikationen mithalten können.

Installation von GrapheneOS

Es gibt zwei Möglichkeiten, GrapheneOS zu installieren: über die offizielle Webseite oder per Terminal. In diesem Leitfaden konzentrieren wir uns auf die einfachere webbasierte Variante, die besonders für weniger technikaffine Nutzer geeignet ist. Wenn du bereits Erfahrung mit dem Terminal hast, kannst du eine detaillierte Anleitung dafür unter grapheneos.org/install/cli einsehen.

Für alle anderen beschreibe ich nun Schritt für Schritt den webbasierten Installationsprozess. Nimm dir dafür ausreichend Zeit, denn die Installation kann unter Umständen abgebrochen werden oder länger dauern. Plane idealerweise etwa zwei Stunden ein, auch wenn der eigentliche Flash-Vorgang meist nur 20 bis 40 Minuten in Anspruch nimmt. Die folgenden Schritte sind bewusst ausführlich gehalten, um mögliche Fehler zu minimieren. Beachte, dass sich die Anleitung in Zukunft ändern kann, auch wenn der grundlegende Prozess ähnlich bleibt. Bevor wir mit der Installation von GrapheneOS beginnen können, muss das Handy vorbereitet werden. Dieser Schritt ist bei beiden Installationsmethoden erforderlich.

- Starte dein Google Pixel-Handy. Es werden einige Informationen abgefragt, und du wirst gebeten, dich mit einem Google-Konto anzumelden. Überspringe alles und gib keine persönlichen Daten ein. Auch WLAN, PIN und Zeitzone musst du nicht eingeben. Unser Ziel ist es nur, in die Einstellungen zu gelangen.
- Wisch nach oben, um das Menü mit den Apps zu öffnen, und tippe auf „Einstellungen“.
- Wähle den Punkt „Über das Telefon“ aus.
- Scrolle nach unten und tippe mehrmals (ca. 7–10 Mal) auf die „Build-Nummer“, bis die Meldung „Du bist jetzt Entwickler“ erscheint.
- Gehe zurück ins Hauptmenü der Einstellungen und öffne den Unterpunkt „System“.
- Wähle dort die „Entwickleroptionen“ aus und aktiviere sowohl „OEM-Entsperrung“ als auch „USB-Debugging“.
- Schalte danach das Handy aus.

Installation von GrapheneOS über die Webseite

- Öffne auf deinem Computer/Laptop die Webseite grapheneos.org/install/web. Hier findest du eine Übersicht über die verschiedenen Schritte – es kann hilfreich sein, diese einmal durchzulesen, bevor du weitermachst.
- Drücke gleichzeitig den Ein/Aus-Knopf und die Leiser-Taste (der oberste und unterste Knopf auf der rechten Seite des Geräts). Dies bringt dich ins Bootloader-Interface, wie auf der Webseite gezeigt.
- Verbinde das Handy mit deinem Computer, am besten mit dem originalen Kabel, das mit dem Handy geliefert wurde, um mögliche Probleme zu vermeiden.
- Klicke auf der Webseite auf „Unlock bootloader“. Eine Benachrichtigung erscheint, in der du dein Gerät (z. B. Google Pixel 7a) auswählst und mit „Connect“ bestätigst.
- Drücke auf deinem Handy die Leiser-Taste, bis „Unlock Bootloader“ ausgewählt ist, und bestätige die Auswahl mit dem Ein/Aus-Knopf. Es sollte jetzt rot „unlocked“ stehen, siehe Abbildung 7 links.
- Zurück auf der Webseite klicke auf „Download release“.
- Sobald der Download abgeschlossen ist, klicke auf „Flash release“. Dies überspielt GrapheneOS auf dein Handy – das kann ein paar Minuten dauern.
- Anschließend klicke auf der Webseite auf „Lock bootloader“.
- Wähle erneut mit der Leiser-Taste auf dem Handy „Lock Bootloader“ aus und bestätige dies mit dem Ein/Aus-Knopf.
- Zum Abschluss sollte im Handy-Interface der Eintrag „Device state: locked“ in Grün erscheinen (siehe Abbildung 7 rechts). Der Prozess ist damit abgeschlossen.
- Wähle mit der Leiser-Taste „Start“ und starte das Handy durch Drücken des Ein/Aus-Knopfes neu. GrapheneOS wird nun gestartet.

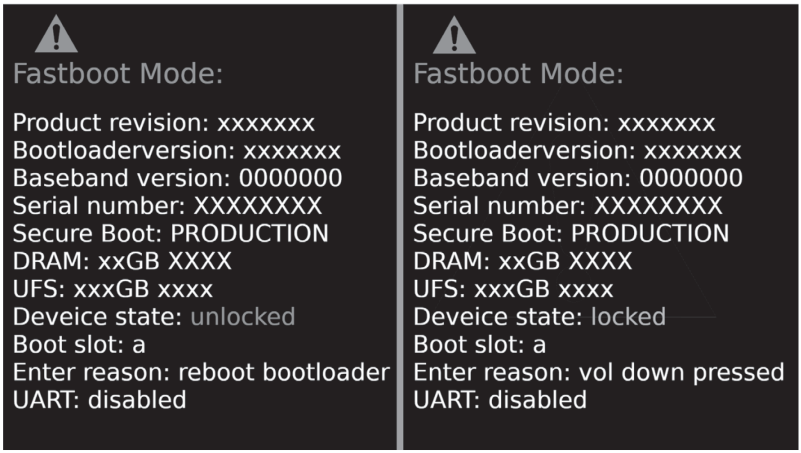

Abbildung 7 Bootemenü GrapheneOS

Es sind zwar nur wenige Schritte erforderlich, aber es kann durchaus zu Problemen kommen – das liegt jedoch meist nicht an dir. In meinen Versuchen hat der Chrome-Browser oft problemlos funktioniert, während Firefox und Brave manchmal Schwierigkeiten bereiteten, den Prozess abzuschließen.
Auch das mitgelieferte Kabel des Herstellers ist entscheidend, da die Verwendung anderer Kabel Fehler verursachen kann. Ich hoffe, dass du GrapheneOS erfolgreich installiert hast und wir nun mit der Einrichtung fortfahren können.

Während des Startvorgangs – und auch bei zukünftigen Neustarts – wird eine Meldung erscheinen: „Your device is loading a different operating system“ („Ihr Gerät lädt ein anderes Betriebssystem“). Diese Warnung kann ignoriert werden; sie ist lediglich ein Versuch von Google, dich zurückzugewinnen.

Erste Schritte nach der Installation

- Wähle deine bevorzugte Sprache und Region. Zwar kannst du hier falsche Angaben machen, aber das führt in der Praxis oft zu mehr Problemen als Nutzen. Deshalb empfehle ich, Deutschland und Deutsch auszuwählen.

- Deaktiviere den Standort. Dies kannst du später nach Belieben anpassen – dazu später mehr.
- Schütze dein Gerät mit einer sicheren PIN. Die Fingerabdruck-Option überspringen wir vorerst.
- Überspringe alle Wiederherstellungsoptionen und tippe auf „Start“.

GrapheneOS ist jetzt installiert und einsatzbereit. Es sind keine Updates unmittelbar nach der Installation erforderlich, da die neueste Version bereits heruntergeladen wurde. Dein Gerät ist nun vollständig verschlüsselt und frei von Google-Diensten. Obwohl GrapheneOS von Haus aus äußerst sicher und privat ist, nehmen wir einige zusätzliche Einstellungen vor, um das Beste aus dem System herauszuholen.

- Gehe in die Einstellungen und wähle erneut den Punkt „Über das Telefon“ aus.
- Tippe wiederholt auf die „Build-Nummer“, bis du erneut als Entwickler freigeschaltet bist. Gib deine PIN ein, falls nötig.
- Gehe dann zurück zu „System“ und öffne die „Entwickleroptionen“.
- Vergewissere dich, dass „OEM-Entsperrung“ und „USB-Debugging“ deaktiviert sind; schalte sie falls nötig aus.
- Schalte anschließend oben „Entwickleroptionen verwenden“ ab und starte das Handy neu.

WLAN

Wenn das WLAN auf deinem Handy aktiviert ist, sucht es ständig nach bekannten Netzwerken. Dabei überträgt es einzigartige Identifikationsmerkmale, die für Tracking-Zwecke genutzt werden können. Besonders in Einkaufszentren ist dies weit verbreitet. Verschiedene Geschäfte verwenden WLAN-Verbindungen, um die Bewegungen und Einkaufsgewohnheiten der Kunden zu verfolgen. Du musst dich nicht einmal mit deren WLAN verbinden; es genügt, das WLAN aktiviert zu haben. Dein Handy sucht dann nach bekannten Netzwerken und übermittelt entsprechende Informationen. Um das zu verhindern, sollte das WLAN stets deaktiviert sein, es sei denn, du verbindest dich gezielt mit einem Netzwerk. Da man jedoch

häufig vergisst, das WLAN auszuschalten, wenn man das Haus verlässt, bietet GrapheneOS eine nützliche Funktion: Es kann das WLAN automatisch deaktivieren, sobald du das Haus verlässt.

- Gehe dazu in die Einstellungen und suche nach „Turn off Wi-Fi automatically“.
- Standardmäßig ist „never“ voreingestellt. Ich empfehle, „2 min“ auszuwählen, damit das WLAN nach zwei Minuten ohne Netzwerkverbindung automatisch ausgeschaltet wird.

Auto-Reboot

Bei GrapheneOS ist standardmäßig eingestellt, dass das Gerät nach 72 Stunden automatisch neu startet. Dies ist ein Sicherheitsfeature. Wenn dein Handy gestohlen oder beschlagnahmt wird oder verloren geht und über 72 Stunden nicht entsperrt wird, erfolgt ein Neustart. Dadurch wird eine erneute PIN-Eingabe erforderlich, der Fingerabdrucksensor wird deaktiviert und zwischengespeicherte Dateien werden gelöscht. Persönlich bevorzuge ich es, den automatischen Neustart auf 24 Stunden zu setzen.

- Um dies anzupassen, gehe in die Einstellungen, suche nach „Auto-Reboot“ und wähle die gewünschte Zeitdauer aus.

Fingerabdruck

In der Privatsphäre-Community wird intensiv darüber diskutiert, ob man einen Fingerabdruck zur Entsperrung des Handys verwenden sollte. Ein Argument dafür ist, dass in öffentlichen Räumen andere Personen oder Kameras einen bei der Eingabe der PIN beobachten können. Ein Fingerabdruck ist in solchen Situationen diskreter. Andererseits besteht das Risiko, dass jemand dich unter Zwang oder im Falle einer Bewusstlosigkeit deinen Fingerabdruck nutzen könnte, um das Handy zu entsperren. In diesem Fall bietet eine PIN mehr Sicherheit. Zudem hat die Polizei das Recht, deinen Fingerabdruck zu verwenden, um Zugang zu deinem Handy zu erhalten, während dies bei einer PIN komplizierter ist. Du musst also selbst entscheiden, welchen Weg du wählen möchtest. Sollte du dich für die Einrichtung des Fingerabdrucks entscheiden, wird dieser nicht mit

anderen geteilt und auch nicht als Bild auf dem Gerät gespeichert. Es werden lediglich Daten gespeichert, die überprüfen, ob es sich um deinen Fingerabdruck handelt.

- Um den Fingerabdruck zu aktivieren, suche in den Einstellungen nach „Fingerabdruck“.
- Zum Einrichten musst du deine PIN bestätigen und den Anweisungen folgen.

PIN-Scrambling

Um zu verhindern, dass jemand deine PIN-Eingabe über die Schulter oder mit Kameras beobachtet, kannst du die Funktion des sogenannten PIN-Scramblings aktivieren. Diese Funktion verändert zufällig die Positionen der Zahlen auf dem Sperrbildschirm, sodass es unmöglich wird, deine PIN allein durch Zuschauen zu erraten. Zwar dauert die Eingabe der PIN dadurch etwas länger, aber sie erhöht die Sicherheit erheblich.

- Um diese Funktion zu aktivieren, suche in den Einstellungen nach „Scramble PIN input layout“ und aktiviere sie.

Duress-Passwort

Das Duress-Passwort ist eine Art „Selbstzerstörungscode“ in GrapheneOS, der für Situationen entwickelt wurde, in denen dein Hauptpasswort möglicherweise kompromittiert wurde. Mit einer speziellen PIN kannst du das Gerät zurücksetzen oder sensible Daten löschen. Diese Funktion sollte jedoch mit äußerster Vorsicht verwendet werden, da die Eingabe des Duress-Passworts zur sofortigen Löschung aller Daten auf dem Gerät führt. Daher sind regelmäßige Backups in diesem Zusammenhang besonders wichtig.

- Zum Aktivieren suche in den Einstellungen nach „Duress password“ und wähle das gewünschte Selbstzerstörungspasswort.

Schnelleinstellungen

GrapheneOS ermöglicht es, die Kamera und das Mikrofon auf Softwareebene zu deaktivieren. Wenn eine App Zugriff auf die Kamera oder das Mikrofon benötigt, erhältst du eine Benachrichtigung und kannst diese Funktionen aktivieren. Anschließend musst du die Kamera und das Mikrofon manuell wieder sperren. Um schnellen Zugriff auf diese Einstellungen zu haben und sie stets im Blick zu behalten, kannst du sie im Schnellzugriffsmenü hinterlegen.

Abbildung 8: Schnelleinstellungen

- Um das Schnellzugriffsmenü anzupassen, ziehe das Menü herunter und klicke auf das Stiftsymbol.
- Jetzt kannst du durch Halten und Verschieben das Menü so anpassen, wie es für dich am besten ist.
- Bei mir steht in der ersten Reihe „Internet“ und „Flugmodus“. In der zweiten Reihe befinden sich „Mikrofonzugriff“ und „Kamerazugriff“, damit ich schnell sehe, ob Kamera und Mikrofon blockiert sind.
- Darunter habe ich „Standort“, „Bluetooth“, „Taschenlampe“ und „Energiesparmodus“ angeordnet, da ich diese häufig verwende. Du kannst natürlich nach Belieben anpassen, was für dich am wichtigsten ist.

Nutzerprofile

Abbildung 9: GrapheneOS-Nutzer

Moderne Android-Geräte ermöglichen es, mehrere Nutzerprofile zu erstellen. Das ist besonders praktisch, um verschiedene Lebensbereiche, wie Arbeit und Privatleben, zu trennen oder Apps voneinander zu separieren. So können Apps in dem einen Profil nicht auf Apps oder Daten in anderen Profilen zugreifen. Jedes Profil hat also seine eigenen Einstellungen, Apps und Sicherheitsmaßnahmen. Während Android bis zu vier Profile unterstützt, erlaubt GrapheneOS die Erstellung von bis zu 32 Profilen.

Theoretisch kannst du für jede App ein eigenes Profil erstellen, um maximale Privatsphäre zu erreichen. Für die meisten von uns wäre das jedoch zu aufwendig und unnötig. Zusätzlich kannst du je nach Profil unterschiedliche Sicherheitsfunktionen aktivieren, z. B. Fingerabdruck, längere PINs oder PIN-Scrambling. Hier folgen einige empfohlene Profil-Typen.

Eigentümer (nur PIN): Dies ist das Standardprofil, das nicht gelöscht werden kann. Einige systemübergreifende Einstellungen lassen sich nur hier vornehmen. Ich halte dieses Profil möglichst leer und nutze es kaum. Die einzigen installierten Apps sind F-Droid, Aurora Store und eine VPN-App, um sie in andere Profile zu kopieren.

Privat (PIN und Fingerabdruck für schnellen Zugriff): Dieses Profil wrd am häufigsten genutzt. Hier mache ich Fotos, speichere meine Kontakte, installiere und verwende Apps und surfe im

Internet. Alle Messenger-Apps sind in diesem Profil, sodass ich die meiste Zeit hier verbringe.

Arbeit (PIN und Fingerabdruck): Um Arbeit und Privatleben zu trennen, nutze ich ein separates Arbeitsprofil. Hier sind alle Arbeits-E-Mails, Messenger und Apps, die ich ausschließlich beruflich benötige. Diese Trennung hilft mir, mich voll auf die Arbeit zu konzentrieren, ohne dass sich die Bereiche vermischen.

Finanzen (PIN und PIN-Scrambling für maximale Sicherheit): Viele Banken verlangen die Nutzung einer speziellen Banking-App für den Zugriff auf Konten und Transaktionen. Da Banken bekannt dafür sind, viele Nutzerdaten zu sammeln, ist es sinnvoll, ein separates Profil für solche Apps zu nutzen. So bleiben andere Profile vor Datenzugriffen geschützt, und meine Finanzdaten sind vor unerwünschtem Zugriff sicher.

Unsichere Apps (PIN und Fingerabdruck für schnellen Zugriff): In diesem Profil sollten alle Apps untergebracht werden, die möglicherweise unsicher sind und viele Daten sammeln – beispielsweise Google- und Facebook-Apps. Durch die Isolierung dieser Anwendungen kann ich die Menge an Daten minimieren, die solche Unternehmen sammeln.

Privacy (PIN und PIN-Scrambling für maximale Sicherheit): In diesem Profil strebe ich maximale Anonymität an. Hier nutze ich den Tor-Browser und Bitcoin-Apps, um sicher und privat zu surfen und zu bezahlen, ohne dass andere Profile davon Kenntnis erlangen.

Wenn du eine Identität vollständig von einem Alias trennen möchtest, kannst du für diesen Alias ein eigenes Profil mit speziellen Messenger- und E-Mail-Apps einrichten. Allerdings musst du jedes Profil manuell konfigurieren – das bedeutet, alle Apps neu herunterzuladen und die Einstellungen anzupassen, was zeitaufwendig sein kann. Es ist wichtig, im Voraus zu überlegen, welche Profile du wirklich benötigst. Eine weitere Idee wäre, ein eigenes Profil nur für die Navigation zu erstellen, sodass der Standort in den anderen Profilen immer deaktiviert bleibt. Es gibt viele Möglichkeiten, Profile individuell anzupassen.

Nutzerprofil erstellen

- Öffne die „Einstellungen“ und wähle „System“ und dann „Mehrere Nutzer“.
- Aktiviere die Option „Mehrere Nutzer“ und erstelle über „Nutzer hinzufügen“ ein neues Profil.
- Jetzt kannst du Berechtigungen festlegen. Deaktiviere „Im Hintergrund ausführen erlauben“, um die Akkulaufzeit zu schonen.
- Schalte „Telefonieren & SMS zulassen“ je nach Bedarf ein oder aus.
- Über „Verfügbare Apps installieren“ kannst du Apps aus dem Eigentümerprofil auf das neue Profil übertragen. Ich empfehle dies für den Aurora- und F-Droid-Store sowie für deine VPN-App, falls vorhanden. Das erspart dir Arbeit.
- Um zwischen Profilen zu wechseln, ziehe das Schnelleinstellungsmenü herunter und klicke auf das Benutzersymbol.
- Beende eine Sitzung, indem du auf das Ein-/Ausschalt-Symbol klickst und „Sitzung beenden“ auswählst. So wird verhindert, dass das Profil im Hintergrund weiterläuft und Ressourcen verbraucht.
- Es macht auch Sinn, das Telefon nach der Nutzung von Profilen komplett neu zu starten, um sicherzustellen, dass alles sauber beendet wird.

Im Eigentümerprofil kannst du deine Profile verwalten oder löschen – besonders nützlich, wenn du dein Gerät in Situationen verwendest, in denen es möglicherweise beschlagnahmt wird, beispielsweise bei Grenzkontrollen. So kannst du ungenutzte Profile löschen und später aus einem Backup wiederherstellen.

Es ist jedoch wichtig zu beachten, dass diese Profile auch Einschränkungen haben. Obwohl Apps und Daten in jedem Profil isoliert sind, teilen sie sich dennoch dieselben Standortdaten (sofern aktiviert), die Internetverbindung, die Telefonnummer sowie GPS, Bluetooth und die Hardware-Identifizierung. Nutzerprofile können somit zur Verbesserung der Privatsphäre beitragen, jedoch gibt es auch Grenzen.

Installieren von Apps

Im Unterschied zu anderen Betriebssystemen wirst du schnell feststellen, dass auf deinem Smartphone kein App-Store vorinstalliert ist – weder der Google Play Store noch eine Alternative. Das bedeutet, dass du selbst für die Installation von Apps verantwortlich bist. Den Google Play Store solltest du von Anfang an meiden, da er Unmengen an Daten über die von dir genutzten Apps sowie über die Zeiten und die Dauer ihrer Nutzung sammelt. Zudem benötigst du einen Google-Account, um Apps herunterzuladen oder zu aktualisieren. Obwohl der Google Play Store bei Android-Systemen weit verbreitet ist, gibt es bessere Alternativen, die wir uns näher ansehen werden.

Die erste Anlaufstelle ist der **F-Droid-Store**. F-Droid ist eine freie und Open-Source-Plattform für Android-Apps. Sie ist gemeinnützig, und alle Apps dort sind kostenlos, wobei die Möglichkeit besteht, den Entwicklern zu spenden. Du kannst Apps direkt über F-Droid suchen, herunterladen und installieren, ohne ein Konto erstellen zu müssen.

Der Vorteil: Rund 95 % der Apps im F-Droid-Store sind Open Source und enthalten keine Tracker. Das macht F-Droid zur besten Wahl für den Anfang. Lass uns also zuerst den F-Droid-Store herunterladen.

- Öffne den Vanadium-Browser und gehe auf die Webseite f-droid.org.
- Klicke auf „Download F-Droid“ und bestätige den Download im Pop-up mit „Herunterladen“.
- Öffne die heruntergeladene Datei. Nun erscheint ein Pop-up, das bestätigt, dass du Apps aus dem Vanadium-Browser installieren willst.
- Klicke auf „Einstellungen“ im Pop-up und aktiviere „Dieser Quelle vertrauen“.
- Klicke im nächsten Pop-up auf „Installieren“, um die Installation von F-Droid abzuschließen.
- Öffne die App. Sie aktualisiert sich kurz, und dann kannst du direkt mit dem Installieren von Apps loslegen.

- Um neue Apps zu installieren, suche sie in F-Droid (mit der Lupe unten links) und klicke auf „Installieren“, – und schon ist sie auf deinem Gerät.

Jetzt hast du einen App-Store, der vollständig ohne Google funktioniert und dir den Zugang zu zahlreichen Open-Source-Apps ermöglicht, ohne dass eine Anmeldung erforderlich ist. Allerdings wirst du schnell feststellen, dass einige gewünschte Apps fehlen. Dies liegt daran, dass F-Droid etwa 3.000 Apps anbietet, während der Google Play Store über 3 Millionen verfügt. Um dennoch Zugriff auf die meisten Apps zu erhalten, installieren wir zusätzlich den Aurora Store.

- Öffne den F-Droid-Store, klicke auf die Lupe unten links und suche nach „Aurora Store“.
- Wähle den Aurora Store aus und klicke auf „Installieren“.
- Wie zuvor musst du auch dem F-Droid-Store erlauben, Apps herunterzuladen. Klicke dafür auf „Einstellungen“ und aktiviere „Dieser Quelle vertrauen“.
- Klicke abschließend im Pop-up auf „Installieren“, um die Installation abzuschließen.

Der Aurora Store ist ein kostenloses, inoffizielles Front-End für den Google Play Store. Er ermöglicht es Nutzern, Apps aus dem Play Store herunterzuladen, ohne ein Google-Konto erstellen zu müssen und ohne dabei getrackt zu werden. Zudem informiert der Aurora Store darüber, welche Apps Tracker verwenden und welche nicht.

- Öffne nach der Installation den Aurora Store und klicke auf „Weiter“.
- Klicke bei „Installation unbekannter Apps.“ auf „Erlauben“ und aktiviere „Dieser Quelle vertrauen“.
- Klicke bei „Speicherverwaltung…“ auf „Erlauben“, wähle den „Aurora Store“ aus und aktiviere „Zugriff zum Verwalten aller Dateien zulassen“.
- Gehe zurück und klicke auf „Weiter“.
- Klicke bei „play.google.com“ auf „Aktivieren“, dann auf „Link hinzufügen“ und wähle „play.google.com“ aus und füge dies hinzu.

- Gehe zurück und klicke auf „Fertig“.
- Wähle „Anonym“ beim Öffnen der App, um Apps herunterzuladen, ohne dich mit einem Google-Account anzumelden.

Jetzt haben wir sowohl den F-Droid-Store als auch den Aurora Store installiert. Beide ermöglichen es uns, Apps ohne Anmeldung herunterzuladen. Zwar kann der Installationsprozess etwas Zeit in Anspruch nehmen, aber das musst du nur einmal machen.

Bei der Suche nach neuen Apps solltest du immer zuerst im F-Droid-Store nachsehen und den Aurora Store nur nutzen, wenn du dort nichts Passendes findest.

Die meisten Apps, die wir herunterladen, sind kostenlos und Open Source. Dennoch müssen Entwickler von etwas leben, daher sind Spenden eine Möglichkeit, ihre Arbeit zu unterstützen.

Wenn dir eine App gefällt und du sie regelmäßig nutzt, solltest du dem Entwicklerteam etwas spenden – es muss nicht viel sein, aber es zeigt Wertschätzung und hilft, Projekte zur Wahrung der Privatsphäre zu fördern.

Die Links zu den Spendenseiten von Apps, die hier empfohlen sind, findest du auf privatopia.de/open-source-spenden.

Apps

Es mag verlockend sein, sofort alle Apps herunterzuladen, die du zuvor auf deinem Smartphone hattest. Ich empfehle jedoch, dies zu vermeiden. Wer ernsthaft seine Privatsphäre schützen möchte, sollte sein Smartphone auf seine grundlegende Funktion – die Kommunikation – beschränken. Viele Menschen installieren Dutzende Apps, die sie nur einmal nutzen und dann vergessen. Diese Apps verfügen oft über umfangreiche Berechtigungen, sammeln Daten und sind häufig mit Trackern ausgestattet. Daher ist es ratsam, die Anzahl der installierten Apps auf ein Minimum zu reduzieren.

In den kommenden Kapiteln werde ich Empfehlungen für häufig genutzte Apps sowohl für Computer als auch für Smartphones geben. Jeder hat unterschiedliche Bedürfnisse und verwendet verschiedene Apps. Ich empfehle dir daher, regelmäßig alle installierten Apps zu überprüfen und diejenigen zu deinstallieren, die du nicht mehr nutzt.

Ein zusätzlicher Browser kann ebenfalls von Vorteil sein. GrapheneOS hat den Vanadium-Browser vorinstalliert, der bereits sehr gut ist, aber ich möchte dich dazu anregen, noch einen Schritt weiterzugehen.

- Installiere den „DuckDuckGo Browser“ über den F-Droid-Store.
- Nach dem Öffnen wirst du gebeten, DuckDuckGo als Standard-Browser festzulegen. Bestätige dieses Pop-up.
- Gehe in die Einstellungen, indem du auf die drei Punkte oben rechts klickst.
- Deaktiviere unter „Allgemeines“ und „Passwörter“ alle Optionen.
- Gehe zu „Fire Button“ und wähle bei „Automatisches Löschen von“ die Option „Tabs und Daten“. Stelle bei „Löschen“, „Beim Verlassen der App, 1 Stunde lang inaktiv“ ein.

DuckDuckGo löscht automatisch alle Browserdaten, Suchanfragen und Verläufe, sobald du die App schließt oder länger als eine Stunde inaktiv bist. Für schnelle Suchanfragen, z. B. zum Wetter oder zu Nachrichten, nutzen wir DuckDuckGo und können sicher sein, dass danach keine Daten gespeichert werden. Da DuckDuckGo unser Standardbrowser ist, werden alle Links darüber geöffnet und alle Daten anschließend gelöscht.

Ich persönlich verwende den DuckDuckGo-Browser für etwa 90 % meiner Internetnutzung. Für die verbleibenden 10 % nutze ich den Vanadium-Browser, und zwar ausschließlich für Seiten, auf denen ich meine Anmeldedaten speichern möchte – z. B. für den Zugriff auf ProtonMail, um meine E-Mails zu überprüfen. So kann ich sicherstellen, dass keine Verbindung zwischen den beiden Browsern besteht und meine Privatsphäre gewahrt bleibt.

Backups

Nachdem wir GrapheneOS eingerichtet haben, ist es wichtig, regelmäßig Backups zu erstellen. Dienste wie Google Drive und iCloud bieten zwar automatische Backup-Lösungen an, jedoch oft auf Kosten unserer Privatsphäre. Ich empfehle, einmal im Monat ein Backup deiner Einstellungen und Anpassungen auf einem USB-Stick zu erstellen. Ein SanDisk Dual Drive USB-Stick mit 128 GB ist dafür ideal und kostet etwa 15 €.

- Gehe dafür in die „Einstellungen“, wähle „System“ und dann „Sicherung“ aus.
- Wähle den USB-Stick aus und warte kurz, bis das Backup startet.
- Das Backup ist durch einen Wiederherstellungscode geschützt, den du benötigst, um darauf zugreifen zu können. Klicke deshalb auf „Wiederherstellungscode“ und speichere die Wörter sicher, z. B. in einem Passwortmanager.
- Aktiviere unter „Meine Apps sichern“ und „App-Sicherung“ beide Optionen.
- Jedes Mal, wenn du ein Backup machen möchtest, musst du den USB-Stick anschließen, oben rechts auf die drei Punkte tippen und „Jetzt sichern“ auswählen.

Solltest du dein Handy verlieren oder sollte es gestohlen werden, kannst du deine alten Daten problemlos auf einem neuen Gerät wiederherstellen.

Ich verwalte meine Fotos lieber auf dem Laptop und nutze das Handy hauptsächlich als Kamera. Daher übertrage ich meine Fotos und Videos monatlich auf den Laptop, wobei ich einen USB-Stick als Zwischenspeicher verwende.

- Öffne dafür die „Dateien-App“ und stecke den USB-Stick ins Handy.
- Tippe oben links auf die drei Striche und wähle „Bilder“ aus.
- Markiere alle Ordner durch längeres Drücken.
- Klicke oben rechts auf die drei Punkte und wähle „Kopieren nach …“ aus.

- Tippe wieder oben links auf die drei Striche, wähle den USB-Stick aus und klicke auf „KOPIEREN“.
- Wiederhole dieselben Schritte für die Videos.
- Verbinde danach den USB-Stick mit dem Laptop, um die Fotos zu übertragen.

Nach der Sicherung auf dem Laptop besteht die Möglichkeit, die Fotos vom Handy zu löschen, wobei dieser Schritt optional ist. So haben wir ein monatliches Backup unserer Fotos und Videos und verlieren im schlimmsten Fall nur die neuesten Aufnahmen.

Updates

Ein bedeutender Vorteil von GrapheneOS im Vergleich zu anderen Betriebssystemen sind die regelmäßigen Sicherheits- und Software-Updates, die etwa alle ein bis zwei Wochen bereitgestellt werden. Im Gegensatz dazu erhalten andere Systeme oft nur alle ein bis zwei Monate Updates. Dadurch bleibt dein Gerät stets auf dem neuesten Stand und optimal geschützt. Sobald ein Update verfügbar ist, erhältst du eine Benachrichtigung, um es herunterzuladen. Der anschließende Neustart des Handys verläuft reibungslos und unkompliziert.

Berechtigungen

Es ist ratsam, regelmäßig zu überprüfen, welche Berechtigungen du den Apps gewährt hast und ob diese tatsächlich erforderlich sind. Oftmals erteilen wir mehr Berechtigungen als nötig, da dies schnell über ein Pop-up erledigt wird. Daher nehme ich mir mindestens einmal im Monat die Zeit, um überflüssige Berechtigungen zu entziehen.

- Gehe in die „Einstellungen“ und suche nach „Berechtigungsmanager“.

Hier kannst du einsehen, welche Berechtigungen jede App benötigt, und diese nach Bedarf entziehen. Mit GrapheneOS hast du zudem

die Möglichkeit, Apps den Internetzugang vollständig zu verwehren, und zwar unter dem Punkt „Netzwerk“. So kannst du sicherstellen, dass die eigenständig gesammelten Daten nicht übertragen werden können.

Storage Scopes

GrapheneOS bietet eine praktische Funktion, mit der du den Zugriff von Apps auf Dateien gezielt einschränken kannst. So kannst du die App weiterhin nutzen, ohne dass sie Zugriff auf persönliche Daten erhält. Diese Funktion nennt sich Storage Scopes. Wenn eine App Zugriff auf Dateien anfordert, stehen dir drei Optionen zur Verfügung: „Erlauben“, „Nicht zulassen“ und „Storage Scopes einrichten“.

- Um Storage Scopes zu aktivieren, wähle „Setup Storage Scopes“ und dann „Enable Storage Scopes“.
- Jetzt kannst du einen Ordner, eine Datei oder ein Bild auswählen, auf die die App Zugriff erhalten soll.
- Ich wähle immer Ordner aus. Dafür auf „Add Folder“ klicken, einen neuen Ordner erstellen (idealerweise mit dem Namen der App) und auf „Diesen Ordner verwenden“ klicken.

Die App hat jetzt nur Zugriff auf einen spezifischen Ordner und kann dort Dateien lesen, bearbeiten oder speichern. Es wird der Eindruck erweckt, dass die App Zugriff auf alle Dateien hat, während deine Daten geschützt bleiben. Ich nutze Storage Scopes für fast alle Apps, die Speicherzugriff benötigen, z. B. für den E-Book-Reader Librera FD. Ich habe einen Ordner mit dem Namen „LibreraFD“ erstellt und alle meine E-Book-Dateien dort abgelegt. So kann ich die E-Books lesen, ohne dass die App über Zugriff auf meine anderen Daten hat.

Contact Scopes

Genau wie beim Speicher bietet GrapheneOS auch die Möglichkeit, den Zugriff auf Kontakte einzuschränken. Wenn eine App Zugriff auf deine Kontakte anfordert, kannst du mit Contact Scopes steuern,

welche Kontakte angezeigt werden. Da Kontakte äußerst sensible Informationen enthalten, verwende ich stets Contact Scopes.

- Um Contact Scopes zu aktivieren, wähle „Setup Contact Scopes“ und dann „Enable Contact Scopes“.
- Jetzt kannst du zwischen „Label“, „Contact“, „Number“ und „E-Mail“ auswählen.

Mit „Label“ kannst du Kontaktgruppen wie „privat“ oder „beruflich“ auswählen. Die App sieht dann nur die Kontakte dieser Gruppe, allerdings mit allen Informationen (Telefonnummer, Geburtstag, E-Mail usw.). Mit „Contact“ wählst du manuell einzelne Kontakte aus, allerdings werden auch hier alle Informationen angezeigt. Mit „Number“ sieht die App nur den Namen und die Telefonnummer, der Rest bleibt verborgen – meine bevorzugte Einstellung. Mit „E-Mail“ ist es ähnlich, hier werden nur der Name und die E-Mail-Adresse angezeigt.

WiFi Calling

Eine weitere Möglichkeit, deine Privatsphäre zu schützen, ist „WiFi Calling“. Viele Mobilfunkanbieter bieten diesen Service an. Anstatt ständig mit Mobilfunkmasten verbunden zu sein, kannst du im Flugmodus über WLAN telefonieren und SMS versenden. Dies schützt dich vor der kontinuierlichen Standortüberwachung durch Mobilfunkmasten.

- Gehe zum Aktivieren in die Einstellungen und wähle „Netzwerk & Internet“ aus.
- Wähle „SIM-Karten“ und dann deine gewünschte SIM-Karte.
- Scrolle bis zum Punkt „WLAN-Telefonie“.
- Aktiviere „WLAN-Telefonie verwenden“ und stelle bei „Bevorzugte Anrufeinstellung“ auf „Anruf über WLAN“ um.

Jetzt kannst du über WLAN telefonieren und SMS empfangen, ohne auf Mobilfunkmasten angewiesen zu sein. Der Flugmodus sorgt

nicht nur für mehr Privatsphäre, sondern schont auch den Akku, da das ständige Suchen nach Mobilfunkmasten entfällt. Ich habe festgestellt, dass mein Akku im Flugmodus zwei bis drei Tage hält, während er ohne diesen oft nur einen Tag durchhält.

VoIP

VoIP (Voice over IP) funktioniert ähnlich wie WiFi Calling, jedoch ist hierfür keine SIM-Karte erforderlich. Alle Anrufe und SMS werden über einen Anbieter abgewickelt und können über eine Open-Source-App verwaltet werden.

Der Vorteil von VoIP im Vergleich zu WiFi Calling liegt in der größeren Flexibilität. Du kannst mehrere kostengünstige Rufnummern einrichten, ähnlich wie bei E-Mail-Adressen, sodass du für unterschiedliche Zwecke verschiedene Nummern nutzen kannst. Zudem ist es möglich, Anrufe direkt über den Computer zu empfangen, sodass das Handy ausgeschaltet bleiben kann.

VoIP bietet ein hohes Maß an Privatsphäre, richtet sich jedoch eher an fortgeschrittene Nutzer. Da dies den Rahmen dieses Buches überschritte, werde ich hier nicht weiter darauf eingehen.

Faraday-Taschen

Früher war es einfach: Um sicherzustellen, dass das Handy weder zuhört noch geortet werden kann, genügte es, die Batterie zu entfernen. Heutzutage ist das bei den meisten Smartphones jedoch nicht mehr möglich, da die Rückseite nicht mehr geöffnet werden kann. Flugmodus und ähnliche Einstellungen versprechen zwar, die Verbindung zu kappen, doch letztlich handelt es sich dabei um Softwarelösungen.

Daher kann man nie zu 100 % sicher sein, dass das Gerät keine Daten sendet oder empfängt. Hier kommen Faraday-Taschen ins Spiel. Diese speziellen Taschen, benannt nach dem Wissenschaftler Michael Faraday, blockieren alle elektromagnetischen Wellen, sodass keine Signale hinein- oder hinausgelangen.

Das bedeutet: Du kannst dein Handy bei dir tragen, ohne befürchten zu müssen, getrackt zu werden. Zudem schützt du dich auch unterwegs oder zu Hause vor den potenziell schädlichen Strahlungen des Geräts.

Es gibt viele Anbieter von Faraday-Taschen in unterschiedlichen Designs und Größen. Allerdings solltest du sicherstellen, dass die Tasche auch tatsächlich funktioniert. Ich habe selbst schon Taschen gehabt, die Signale durchgelassen haben. Daher ist es ratsam, regelmäßig zu testen, ob deine Tasche ihren Zweck erfüllt.

Die einfachste Testmethode: Stecke dein Handy in die Faraday-Tasche und versuche dann, es mit einem anderen Gerät anzurufen. Diese Methode hat jedoch ihre Tücken: Geht der Anruf durch, funktioniert die Tasche definitiv nicht. Wenn der Anruf jedoch nicht durchkommt, könnte das auch an anderen Faktoren wie dem Mobilfunknetz oder deinem Standort liegen.

Eine bessere Testmethode besteht darin, zu überprüfen, ob die Tasche Bluetooth-Signale blockiert. Bluetooth ist stabiler und weniger fehleranfällig. Verbinde dein Handy mit einem Bluetooth-Lautsprecher, starte die Musik und stecke das Handy in die Faraday-Tasche. Stoppt die Musik, war der Test erfolgreich. Läuft die Musik weiter, blockiert die Tasche nicht richtig und sollte nicht verwendet werden.

Mikrofon und Kamera

Viele Apps verlangen Zugriff auf Mikrofon und Kamera, oft um ihre Funktionen überhaupt anbieten zu können. Leider nutzen viele von ihnen diese Berechtigungen auch, um Daten zu sammeln – beispielsweise für personalisierte Werbung. Zudem besteht immer das Risiko, dass Malware auf das Gerät gelangt und uns überwacht. Früher war es noch möglich, die Hardware selbst zu deaktivieren. Heute ist das, wie bereits erwähnt, leider nicht mehr möglich. Auf Geräten mit GrapheneOS kannst du Mikrofon und Kamera zwar auf Softwareebene blockieren, was besser ist als nichts, aber Software allein ist nie zu 100 % sicher. Daher empfehle ich, so weit wie möglich eine physische Deaktivierung vorzunehmen.

Die Kamera lässt sich relativ einfach absichern: Klebe einfach alle Kameras mit undurchsichtigen Stickern ab. Wenn du die Kamera dann doch einmal brauchst, kannst du die Abdeckung problemlos abnehmen und später wieder anbringen.

Beim Mikrofon gestaltet sich die Absicherung komplizierter. Früher reichte es, Mikrofone abzudecken, um Tonaufnahmen zu stören. Moderne Smartphones verfügen jedoch über mehrere Mikrofone an verschiedenen Stellen, sodass diese Methode nicht mehr effektiv ist. Doch genau dies können wir uns zunutze machen: Wenn das Smartphone erkennt, dass ein Mikrofon (z. B. der Kopfhörer) angeschlossen ist, nutzt es nur dieses. Funktioniert das angeschlossene Mikrofon nicht, kann das Handy keine Aufnahmen machen. Mikrofon-Blocker nutzen dieses Prinzip. Diese kleinen Geräte täuschen vor, ein Mikrofon zu sein, funktionieren jedoch nicht. Sie sorgen dafür, dass das Handy keine Aufnahmen machen kann. Mikrofon-Blocker sind für USB-C-, Lightning- und AUX-Anschlüsse erhältlich, sodass sie mit fast jedem Gerät kompatibel sind.

Perfekt sind diese Blocker allerdings nicht. Sollte Malware auf dein Gerät gelangen und alle Mikrofone nutzen, hilft der Blocker nicht. Daher habe ich zusätzlich auf Softwareebene alle Mikrofone deaktiviert und verwende den Blocker – so minimiere ich das Risiko.

Abbildung 10 Kamera- und Mikrofonblocker

Privacy Screen

Viele von uns möchten sich vor der Überwachung durch Unternehmen und den Staat schützen, übersehen jedoch oft, dass auch fremde Blicke auf unseren Bildschirm ein ernstzunehmendes Problem

darstellen können. In öffentlichen Verkehrsmitteln, Cafés oder anderen Orten kommt es häufig vor, dass Passanten unbewusst einen flüchtigen Blick auf das Handy ihres Nachbarn werfen. Dabei können sensible Informationen wie Nachrichten, Passwörter oder Codes mitgelesen werden. Auch wenn dies meist unbewusst geschieht – unser Gehirn ist ständig auf der Suche nach neuen Reizen. Wir sollten uns trotzdem aktiv davor schützen. Privacy-Displayschutzfolien sind hierfür eine ideale Lösung. Diese Folien werden auf den Bildschirm des Handys aufgebracht und stellen sicher, dass nur der Benutzer, der direkt auf den Bildschirm schaut, den Inhalt sehen kann. Aus seitlichem Blickwinkel erscheint der Bildschirm lediglich als schwarze Fläche. Darüber hinaus bieten diese Folien auch Schutz vor Kratzern und Stößen, sodass du deinen Bildschirm gleichzeitig vor unerwünschten Blicken und Beschädigungen bewahrst – so schlägst du zwei Fliegen mit einer Klappe.

Handy-Nutzung

Alle zuvor beschriebenen Maßnahmen können deine Privatsphäre erheblich optimieren, bringen jedoch wenig, wenn du dein Handy unachtsam nutzt. Hier sind einige wichtige Punkte, auf die du achten solltest:

WLAN und Bluetooth: Viele Menschen lassen WLAN und Bluetooth ständig aktiviert, weil es bequem ist, sich automatisch mit dem Heimnetzwerk oder dem Auto zu verbinden. Allerdings verbindet sich das Handy nicht nur mit diesen Netzwerken. Es sendet ständig Daten an WLAN-Netze in der Umgebung, um mögliche Verbindungen zu prüfen.

Einkaufszentren und Geschäfte nutzen dies, um die Bewegungen von Kunden zu verfolgen und analysieren. Über öffentliche WLANs kann auch Unternehmen und Insitutionen darauf zugreifen, um Analysen durchzuführen. Daher: Schalte WLAN und Bluetooth immer aus, wenn du sie nicht benötigst. Aktiviere am besten auch den Flugmodus, wenn möglich.

Flugmodus: Der Flugmodus blockiert alle Signale zu Mobilfunkmasten. Dies ist bei allen Smartphones weltweit möglich. Auch wenn diese Blockierung nur auf Softwareebene erfolgt, hilft sie enorm, um dich vor dem Tracking durch Mobilfunkanbieter zu schützen. Ich habe den Flugmodus zu Hause fast immer aktiviert (ich nutze stattdessen WLAN für Anrufe) und schalte ihn nur selten unterwegs aus, wenn ich Nachrichten lesen oder kommunizieren möchte.

Apps: Wie bereits erwähnt, solltest du dein Handy insgesamt weniger nutzen. Smartphones sind die am stärksten getrackten Geräte, und eine vollständige Vermeidung von Tracking ist kaum möglich. Der beste Schutz besteht darin, sie weniger zu nutzen und dem Tracking keine Gelegenheit zu geben.

Accounts: Ein großer Vorteil von GrapheneOS besteht darin, dass du keinen Account benötigst, um das Handy vollumfänglich zu nutzen. Das bedeutet, dass deine Daten nicht mehr einem zentralen Google- oder Apple-Konto zugeordnet werden. Nutze diese Freiheit und verknüpfe dein Handy niemals mit einem persönlichen Google- oder Apple-Konto.

• • •

In diesem Kapitel haben wir ein sicheres und privates Handy eingerichtet. Wir können jetzt alle Funktionen und Apps nutzen, ohne uns jemals mit einem Google- oder Apple-Konto verbinden zu müssen. Auch unser Betriebssystem sammelt keine Daten mehr über und gibt auch keine mehr weiter. Mit WiFi Calling können wir den Flugmodus dauerhaft aktivieren, wenn wir zu Hause sind, sodass auch die Mobilfunkmasten keine Informationen über uns erfassen. Zudem haben wir die Möglichkeit, sowohl softwareseitig als auch physisch das Mikrofon zu deaktivieren, Kameras auszuschalten und alle Signale zu blockieren. Jetzt sind wir bereit, im nächsten Kapitel zu entdecken, welche Apps wir benötigen, um das Beste aus unseren Geräten herauszuholen und dennoch gleichzeitig unsere Privatsphäre zu schützen.

Kapitel 3
Anonym surfen

„Wenn Privatsphäre zu einer knappen Ressource wird, wird die Überwachung zur Macht." ~ *Shoshana Zuboff*

Nachdem wir nun ein sicheres und privates Handy sowie einen geschützten Computer eingerichtet haben, sind wir bereits zwei wesentliche Schritte in Richtung Privatsphäre und Sicherheit gegangen. Um uns jedoch effektiv vor staatlicher Überwachung, Datensammlern und unerwünschtem Zugriff zu schützen, gibt es noch viel mehr zu beachten. Die nächsten Kapitel bieten eine detaillierte Anleitung, wie wir sicher und privat im Internet unterwegs sein und uns von Google sowie anderen Datenkraken lösen können. Diese Kapitel verdienen es deswegen, mehrfach durchgearbeitet zu werden.

Ich stelle hier verschiedene Tools und Softwarelösungen vor, von denen die meisten kostenfrei sind. Diese Empfehlungen sind jedoch nicht als endgültige Vorgaben zu verstehen – jeder sollte nach eigener Recherche entscheiden, welches Programm am besten den eigenen Anforderungen entspricht. Wichtig ist, dass die grundlegenden Prinzipien qualitativ hochwertiger Programme beachtet werden.

Open Source
Viele dieser Programme sind Open Source, was bedeutet, dass sie nicht von großen Unternehmen unterstützt werden, sondern meist freiwillig von Entwicklern aus der ganzen Welt betreut werden. Dies ist ein positiver Aspekt, da Open-Source-Software tendenziell transparenter ist und weniger kommerziellen Interessen unterliegt.

Da diese Entwickler oft nicht durch Sponsoren gefördert werden und auf Einnahmequellen wie den Verkauf von Daten oder Werbung verzichten, ist es sinnvoll, sie durch Spenden zu unterstützen. Damit fördern wir nicht nur das Entwicklerteam, sondern auch die gesamte Privacy-Bewegung, die auf solche finanzielle Unterstützung

angewiesen ist. Wenn dir ein Programm gefällt, du es nutzt und es kostenfrei ist, spende bitte an das Entwicklerteam. Links zu den Spendenseiten findest du auf privatopia.de/open-source-spenden.

Was macht ein gutes Programm aus?

Jeder hat individuelle Anforderungen an die Programme, die auf dem Computer oder Handy genutzt werden. Es ist unmöglich, auf alle Bedürfnisse einzugehen und für jedes Szenario eine Empfehlung auszusprechen. Daher ist es wichtiger, die Kriterien zu verstehen, die ein Programm erfüllen sollte, um Privatsphäre und Sicherheit zu gewährleisten.

Grundsätzlich sollten wir, wenn möglich, auf die Installation von Apps verzichten, sofern eine Webseite die gewünschten Funktionen bietet. Im nächsten Schritt richten wir einen sicheren und privaten Browser ein, der uns eine relativ hohe Sicherheit vor Tracking und Datensammlung durch Unternehmen bietet.

Wenn jedoch eine Anwendung heruntergeladen wird, sei es auf das Handy oder den Computer, erhält dieses Programm umfangreiche Rechte und Zugriff auf zahlreiche Daten. Daher sollten wir immer die Webseite bevorzugen, wenn diese die gleichen Funktionen bietet.

Es gibt beispielsweise keinen offensichtlichen Vorteil, Spotify als Anwendung zu nutzen, wenn es auch über den Browser funktioniert. Es gibt einige Kriterien, auf die man achten sollte bei der Auswahl eines Programms für unsere Privatsphäre.

Open Source: Der Quellcode sollte öffentlich zugänglich sein. Dies ist eines der wichtigsten Kriterien, da viele Menschen den Code auf Schwachstellen, Probleme und versteckte Tracking-Software überprüfen können. Selbst wenn wir den Code nicht vollständig verstehen, sorgt die Gemeinschaft für die notwendige Kontrolle und Transparenz.

Unternehmen: Wer steht hinter dem Produkt, und welche Philosophie verfolgt dieses Unternehmen? Handelt es sich um ein Unternehmen wie Google, dessen Hauptgeschäft das Sammeln von Daten und Werbung ist, oder um ProtonMail, das sich auf Datenschutz spezialisiert hat? Die Unternehmensethik spielt eine entscheidende Rolle.

Geschäftsmodell: Wie finanziert sich das Unternehmen? Wenn Werbung die Hauptquelle der Einnahmen ist, steigt das Risiko, dass Daten gesammelt werden, um gezielte Werbung effektiver zu gestalten. Idealerweise sollte sich das Produkt durch direkte Zahlungen der Nutzer finanzieren.

Erfahrungen und Vertrauenswürdigkeit: Programme, die bereits länger existieren, bieten mehr Sicherheit, da Schwachstellen eher entdeckt und behoben werden konnten. Ein Programm, das zwar Open Source ist, aber erst seit Kurzem existiert, ist möglicherweise noch nicht lange genug auf dem Markt, um umfassend geprüft zu werden.

Standort des Unternehmens: Wo ist das Unternehmen ansässig? Befindet es sich in den USA oder der EU, wo Regierungen und Gerichte über umfangreiche Zugriffsrechte auf Daten verfügen? Oder hat es seinen Sitz in einem Land, das neutral ist oder sogar in Gegensatz zu westlichen Regierungen steht, wie die Schweiz, Russland oder ein südamerikanisches Land? Dies könnte den Schutz der Daten vor staatlichem Zugriff erhöhen.

Nutzerkontrolle über Daten: Haben wir die Möglichkeit, selbst zu entscheiden, welche Daten geteilt werden und welche nicht? Beispielsweise bietet Apple viele Einstellungen, die es ermöglichen, wichtige Aspekte der Privatsphäre zu kontrollieren, während Windows von Microsoft in dieser Hinsicht kaum Wahlmöglichkeiten lässt.

Wenn du diese Punkte beachtest, kannst du selbst überprüfen, ob das gewünschte Programm deine Privatsphäre schützt oder eher von deinen Daten profitiert.

In diesem Kapitel schauen wir uns an, wie wir sicher und privat im Internet surfen können. Dazu richten wir gleich einen sicheren Browser ein und kümmern uns anschließend um eine sichere und private Verbindung durch ein VPN und ein DNS. Am Ende dieses Kapitels kannst du dann bedenkenlos im Internet surfen, ohne Werbung und ohne Tracking.

Webbrowser LibreWolf

Bevor du mit dem Surfen im Internet beginnst oder Software installierst, ist es wichtig, einen sicheren Browser zu verwenden. Ich empfehle dir den LibreWolf-Webbrowser, den ich selbst jederzeit nutze.

LibreWolf ist ein sogenannter Fork von Firefox. Das bedeutet einfach nur, dass ein Entwicklerteam den Code von Firefox genommen, ihn ein wenig modifiziert und dann unter einem anderen Namen veröffentlicht hat. Das ist bei Open-Source-Programmen üblich und passiert ziemlich oft.

Im ersten Entwurf des vorliegenden Buches hatte ich den Firefox Browser direkt empfohlen – mit angepassten Einstellungen für maximale Sicherheit und Privatsphäre.

Jedoch hat Firefox im Februar 2025 seine Nutzungsbedingungen geändert – zum Nachteil der Nutzer. Konkret ging es um eine Klausel, die Mozilla eine „nicht-exklusive, gebührenfreie, weltweite Lizenz“ zur Nutzung von Daten einräumte, die Nutzer in Firefox eingeben oder hochladen. Zwar würden laut Mozilla Firefox diese Daten nur für die Verbesserung von Firefox genutzt und die Klausel sei schlecht formuliert, das Vertrauen ist damit jedoch trotzdem in gewisser Weise gebrochen. Deswegen empfehle ich den LibreWolf-Browser, der genauso wie der Firefox-Browser aufgebaut ist, nur ohne diese Klausel und von Anfang an mit optimalen Einstellungen zum Schutz von Privatsphäre und Sicherheit.

Die Frage nach dem richtigen Browser nehmen manche sehr persönlich und man liest und hört ziemlich viele Empfehlungen im Internet

dazu – ein sehr häufig empfohlener Browser neben LibreWolf (Firefox) ist der Brave Browser.

Der Brave Browser verfügt über eine Menge Features und Optionen für Privatsphäre und Sicherheit – es gibt einen integrierten Werbeblocker, Schutz vor Tracking und vieles mehr. Der einzige Nachteil besteht darin, dass dieser auf Google Chrome aufbaut. Zwar hat man auch hier so gut wie möglich alle Tracker und Verbindungen zu Google entfernt, die Grundbasis bleibt jedoch trotzdem bei Google. Das ist aber nicht sehr gravierend, du kannst also durchaus den Brave Browser verwenden, wenn du diesen bevorzugst. Denn ein Vorteil ist sicherlich der, dass die Bedienung sehr derjenigen des Google-Chrome-Browsers ähnelt. Vorliegendes Buch fokussiert sich allerdings auf den LibreWolf-Browser, da dieser Firefox als Basis hat und wirklich überhaupt keine Verbindungen zu Google aufweist.

Bei allen Betriebssystemen ist ein Browser bereits vorinstalliert. Bei Linux ist es Firefox, bei Apple Safari und bei Windows Edge. Safari und Edge sind Teil des jeweiligen Ökosystems und tragen dazu bei, dass Unternehmen ein noch genaueres Profil von dir erstellen können – deswegen rate ich von deren Verwendung ab.

- Um LibreWolf zu installieren, rufe die Webseite librewolf.net/installation auf und installiere LibreWolf auf deinem Betriebssystem.
- Nach der Installation von LibreWolf solltest du dann alle Verknüpfungen und Referenzen zu Edge, Safari oder Firefox entfernen, um nicht versehentlich den „falschen“ Browser zu öffnen.
- LibreWolf ist von Grund auf sehr hinsichtlich Privatsphäre und Sicherheit optimiert, weswegen man hier Einstellungen nur noch minimal ändern muss. Klicke oben rechts auf das Menü (drei Striche) und wähle dort den Punkt „Einstellungen“ aus.
- Aktiviere unter „Allgemein den Punkt „Tab-Umgebungen aktivieren“. Klicke rechts auf „Einstellungen“ und aktiviere unten das Häkchen (dazu gleich mehr).

- Deaktiviere die Optionen „Erweiterungen während des Surfens empfehlen“ und „Funktionen während des Surfens empfehlen“, indem du die Häkchen entfernst.
- Wähle im Menü links „Startseite“. Und setzte bei „Startseite und neue Fenster“ sowie „Neue Tabs“ die Option auf „Leere Seite“.
- Deaktiviere alle Inhalte der Startseite.
- Wähle im Menü links „Suche“. Hier ist DuckDuckGo als Standartsuchmaschine festgelegt, diese kannst du nun ändern, falls du eine andere möchtest.
- Lege „DuckDuckGo“ als Standard-Suchmaschine fest.
- Deaktiviere alle Optionen unter „Suchvorschläge“ und „Adressleiste“, um zu verhindern, dass Anfragen direkt an Google weitergeleitet werden und um die Google-API für Suchvorschläge zu blockieren.
- Wähle im Menü links „Datenschutz & Sicherheit“:
- Aktiviere den Haken unter „Datenschutzeinstellungen für Websites“.
- Setzte ein Häkchen bei „Cookies und Website-Daten beim Beenden löschen“ (dies bewirkt, dass alle gespeicherten Daten beim Schließen von LibreWolf gelöscht werden; Ausnahmen kannst du unter „Ausnahmen verwalten“ hinzufügen, z. B. für proton.me, um eine erneute Anmeldung bei E-Mails zu vermeiden).
- Deaktiviere alle Optionen unter „Passwörter“ und „Automatisch ausfüllen“.
- Unter „Chronik“ deaktiviere alles außer „Die Chronik löschen, wenn Firefox geschlossen wird“.
- Aktiviere den „Nur-HTTPS-Modus in allen Fenstern“.

LibreWolf bietet bereits von Haus aus ein hohes Maß an Sicherheit und Privatsphäre. Im nächsten Abschnitt präsentiere ich Browser-Erweiterungen, die zusätzlichen Schutz und Komfort bieten.

uBlock Origin

Das erste unverzichtbare Add-on, das ich auf jedem Computer installiere, ist uBlock Origin. Dieses Tool blockiert nicht nur Werbung, sondern auch zahlreiche Tracking-Skripte sowie andere

potenziell schädliche Software. Es schützt dich effektiv vor Tracking, bösartigem Code und dem Senden von Standortdaten sowie vor vielen weiteren Prozessen, die deine Privatsphäre und Sicherheit gefährden könnten. uBlock Origin ist kostenlos, vollständig Open Source und bietet umfangreiche Anpassungsmöglichkeiten. Bereits mit den Standardeinstellungen gewährleistet es ein hohes Maß an Privatsphäre und Sicherheit. Es ist zwar möglich, erweiterte Funktionen zu deaktivieren, jedoch kann dies dazu führen, dass bestimmte Webseiten nicht mehr korrekt funktionieren.

Das gute bei LibreWolf ist, dass uBlockOrigin von Anfang an installiert ist, das heißt, du musst hier keine weiteren Einstellungen vornehmen.

Container Tabs

Ein weiteres unverzichtbares Plugin, das täglich nutzen solltest, ist Multi-Account Containers. Auch dieses Plugin ist LibreWolf von Anfang an installiert bei. Dieses Plugin ermöglicht es dir, Tabs im Browser zu isolieren, ohne den Browser neu starten oder alle Daten löschen zu müssen. Aber warum ist das wichtig?

Jedes Mal, wenn du eine Webseite öffnest und dich möglicherweise anmeldest, werden Daten gespeichert – häufig in Form von Cookies. Selbst wenn du alle Cookies ablehnst, sammeln Webseiten dennoch eine Vielzahl von Informationen.

Das größte Problem dabei ist, dass verschiedene Webseiten diese Daten untereinander austauschen, um dir gezielte Werbung anzuzeigen. So kann es beispielsweise passieren, dass du auf Facebook Werbung für Kaffeemaschinen siehst, nachdem du bei Amazon nach Kaffeemaschinen gesucht hast, ohne das es irgendeine Verbindung zwischen den Accounts gibt.

Multi-Account Containers löst dieses Problem, indem es dir ermöglicht, unterschiedliche Tab-Umgebungen zu erstellen, die nicht miteinander kommunizieren. So kannst du im „Shopping“-Tab nach Kaffeemaschinen suchen, ohne dass der im „SocialMedia-Container“ geöffnete Facebook-Tab davon Kenntnis erhält.

Dazu erlaubt dir das Plugin, verschiedene Konten in unterschiedlichen Containern gleichzeitig zu verwenden. So können z.B. die Anmeldedaten von Twitter-Account #1 im Container #1 gespeichert werden, während die Daten von Twitter-Account #2 in Container #2 abgelegt werden. Dies ermöglicht es dir, mit zwei Twitter-Tabs parallel zu arbeiten, ohne dich jedes Mal neu anmelden zu müssen.

Immer wenn du einen neuen Tab öffnen möchtest, wirst du gefragt, welche Umgebung du öffnen möchtest. Die Standardauswahl enthält Container wie Freizeit oder Arbeit, kann aber individuell angepasst werden. Ich selbst verwende zehn Tabs, die von 01 bis 10 nummeriert sind. In den Einstellungen unter „Allgemein“ und „Tab-Umgebungen aktivieren“ kannst du neue Container-Tabs erstellen, bearbeiten oder löschen.

Yandex

Nachdem wir nun einen sicheren Browser eingerichtet haben und DuckDuckGo als Suchmaschine verwenden, möchte ich dir eine weitere Option vorstellen: Yandex. Bei der Erwähnung von Yandex, oft als das „russische Google“ bezeichnet, denken viele möglicherweise sofort an potenzielle Risiken und schrecken zurück. Doch Yandex bietet einige interessante Vorteile – insbesondere, weil es in Russland ansässig ist. Im Gegensatz zu DuckDuckGo, das in den USA beheimatet ist, eröffnet Yandex den Zugang zu einer völlig anderen Informationswelt: Es zeigt Suchergebnisse an, die auf anderen Plattformen oft nicht zu finden sind.

Wie steht es jedoch um den Schutz der Privatsphäre bei Yandex? Yandex schützt unsere Privatsphäre nicht. Ähnlich wie Google und Meta sammelt auch Yandex Nutzerdaten und gibt diese weiter. Der Unterschied besteht jedoch darin, dass Yandex die Daten nicht mit westlichen Regierungen oder Geheimdiensten teilt, sondern mit russischen. In bestimmten Situationen kann dies ein akzeptabler Kompromiss sein, da eigene Regierungen unter Umständen mehr Schaden anrichten können als eine externe wie die russische. Zudem ist es wahrscheinlich, dass Yandex auf Anfragen westlicher Behörden nicht reagieren wird.

Dennoch würde ich nicht empfehlen, Yandex als tägliche Suchmaschine zu verwenden. Es kann jedoch sinnvoll sein, Yandex als zusätzliches Werkzeug zu nutzen, um Suchergebnisse zu finden, die andernorts möglicherweise blockiert sind.

Cookies

Cookies sind kleine Dateien, die auf deinem Gerät gespeichert werden, während du im Internet surfst. Sie sammeln Informationen über die besuchten Webseiten und deine Vorlieben und können ein digitales Profil von dir erstellen. Man könnte sie als einen Fingerabdruck betrachten, den du im Netz hinterlässt. Einerseits speichern Cookies nützliche Daten wie deine Anmeldedaten, sodass du dich nicht ständig neu anmelden musst. Andererseits ermöglichen sie es Webseiten, deine Surfgewohnheiten zu verfolgen und gezielte Werbung anzuzeigen.

Um deine Privatsphäre besser zu schützen, gibt es seitens der EU eine Regelung, die Webseiten verpflichtet, dich über die Verwendung von Cookies zu informieren. Allerdings ist diese Maßnahme oft weniger effektiv als erhofft. Viele Nutzer akzeptieren die Cookies einfach, ohne darüber nachzudenken. Selbst wenn man Cookies ablehnt, gibt es häufig „essenzielle“ Cookies, die dennoch Daten sammeln.

Um zu verhindern, dass diese Informationen dauerhaft auf deinen Geräten gespeichert bleiben, empfehle ich, den Browser auf deinem Handy (DuckDuckGo) und deinem PC (Librewolf) so einzustellen, dass alle Cookies beim Schließen automatisch gelöscht werden. Falls du dies nicht bereits getan hast, ist es sinnvoll, regelmäßig manuell die Cookies zu löschen. So verhinderst du, dass Webseiten langfristig detaillierte Profile über dich erstellen können.

Tor-Browser

Viele haben sicherlich schon vom „Darknet“ gehört, das oft mit dem Schutz der Privatsphäre und Anonymität in Verbindung gebracht wird. Der Tor-Browser ist ein hervorragendes Tool für unsere

Privatsphäre, auch wenn er einige Einschränkungen mit sich bringt. Besonders beliebt ist er bei politischen Aktivisten und Journalisten, die sich vor Überwachung durch autoritäre Regierungen schützen möchten. Generell nutzen ihn Menschen, die Zensur umgehen oder ihre Privatsphäre wahren wollen.

Um zu verstehen, wie der Tor-Browser funktioniert, schauen wir uns zunächst an, was er eigentlich ist. Der Tor-Browser leitet automatisch alle Anfragen durch das anonyme Tor-Netzwerk, das aus verschiedenen Knotenpunkten weltweit besteht – ähnlich dem Netzwerk von Bitcoin. Der Browser isoliert jede geöffnete Webseite, sodass kein Austausch von Cookies oder anderen Informationen zwischen gleichzeitig geöffneten Seiten möglich ist. Beim Schließen des Tor-Browsers werden alle Daten automatisch gelöscht. Darüber hinaus ermöglicht der Tor-Browser den Zugriff auf „Onion-Webseiten“, die nur über Tor erreichbar sind und als Teil des sogenannten „Darkweb“ gelten.

Im Kern ist der Tor-Browser eine angepasste Version von Mozilla Firefox, ähnlich zu LibreWolf. Er basiert auf einem speziellen Sicherheitssystem, das ursprünglich von der US Navy entwickelt wurde, um ihre Kommunikation zu schützen. Alle Daten, die über den Tor-Browser gesendet werden, sind verschlüsselt und werden mehrfach über das sogenannte „Onion-Router-Netzwerk“ aus Knotenpunkten geleitet, das aus Tausenden von freiwillig zur Verfügung gestellten Servern besteht. Diese Verschlüsselung und die Weiterleitung der Browserdaten sorgen dafür, dass niemand herausfinden kann, welche Webseiten besucht werden oder welche Aktivitäten dort stattfinden.

Ein weiterer Vorteil ist, dass alle Nutzer gleich aussehen, was eine Identifikation praktisch unmöglich macht. Das Einzige, was erkennbar ist, ist die Nutzung des Tor-Browsers. Zwischen unserem Computer und den Webseiten, die wir besuchen, liegen also mehrere Knotenpunkte. Um auch diesen nicht vertrauen zu müssen, verwendet Tor die „Onion-Strategie“. Dabei „schält“ jeder Knotenpunkt eine Schicht der Verschlüsselung ab, die nur den nächsten Knotenpunkt enthüllt. Wenn die letzte Schicht des Datenpakets erreicht wird, haben wir die Webseite erreicht. Dadurch bleibt der Absender

anonym, da jeder Knotenpunkt nur seinen Vorgänger und den Nachfolger kennt—dies wird auch als „Forward Privacy“ bezeichnet.

Das Ganze klingt vielleicht etwas kompliziert und führt auch zu einer Verlangsamung der Internetgeschwindigkeit, da alle Anfragen und Daten erst durch die Knotenpunkte geleitet sowie mehrfach verschlüsselt und entschlüsselt werden müssen. Daher ist die Geschwindigkeit eine der größten Herausforderungen. Jede neue Seite, die geladen wird, und jede Nutzeraktion, die wir normalerweise innerhalb von Millisekunden erwarten, kann Sekunden bis Minuten dauern. Aus diesem Grund ist Tor nicht als täglicher Browser geeignet.

Du solltest den Tor-Browser auch nicht ständig verwenden, da seine Nutzung Aufmerksamkeit erregen kann—sowohl von deinem Internetdienstanbieter (ISP-Internetserviceprovider) als auch von den Webseiten selbst. Obwohl der ISP nicht sehen kann, welche Webseiten du besucht hast, erkennt er die Nutzung des Tor-Browsers, was zu verstärkter Überwachung führen kann. Um dies zu vermeiden, ist es ratsam, vor der Nutzung des Tor-Browsers ein VPN zu verwenden. Auch Webseiten erkennen den Zugriff über den Tor-Browser und assoziieren das Tor-Netzwerk oft mit illegalen Aktivitäten. Das kann zu zusätzlichen Sicherheitsabfragen wie Google Captchas, zur Sperrung von Konten oder sogar zur Blockierung von Zahlungen führen. Deshalb solltest du den Tor-Browser nicht als alltäglichen Browser verwenden, sondern nur in bestimmten Situationen. Für den täglichen Gebrauch eignet sich LibreWolf besser.

Onion: Wie bereits erwähnt, ermöglicht der Tor-Browser den Zugriff auf „ .onion-Adressen“. Diese sind Webseiten, die nur im Darknet vorhanden sind. Um diese Seiten zu besuchen, ist die Nutzung des Tor-Browsers erforderlich.

Reisen: In einigen Ländern, in denen die Zensur strenger ist als in Deutschland, kann der Tor-Browser besonders hilfreich sein. Russland blockiert beispielsweise ProtonMail, und in anderen Ländern sind Verbindungen über VPNs generell nicht erlaubt. In solchen Fällen kann der Tor-Browser eine Lösung sein, um dennoch auf die gewünschten Seiten zugreifen zu können.

Öffentliche WLANs: Auch in Deutschland gibt es viele Orte, an denen der Zugriff auf bestimmte Webseiten eingeschränkt ist – z. B. bei öffentlichen Netzwerken von Bibliotheken, Universitäten oder Arbeitsplätzen. Hier bietet der Tor-Browser ebenfalls eine Möglichkeit, diese Beschränkungen zu umgehen.

Um den Tor-Browser für Mac und Windows zu installieren, folge einfach den Anweisungen auf www.torproject.org/download/.

Für Linux kannst du den Tor-Browser über das Terminal installieren, indem du die entsprechenden Befehle eingibst.

```
sudo add-apt-repository ppa:micahflee/ppa
sudo apt update
sudo apt install torbrowser-launcher
```

VPN

VPNs (Virtual Private Networks) stellen ein bedeutendes Thema im Internet dar, und viele Webseiten bieten Vergleiche an, um die besten Dienste zu empfehlen – jedoch nur mit dem Ziel, Provisionen zu verdienen. Viele VPN-Anbieter versprechen mehr, als sie tatsächlich halten können. Bevor du dich von solchen Versprechungen blenden lässt, ist es wichtig, zu verstehen, was ein VPN tatsächlich leistet.

Ein VPN ermöglicht eine sichere Verbindung zu einem anderen Netzwerk über das Internet. Vereinfacht gesagt: Es verbindet dein Gerät (z. B. Laptop) mit einem Server irgendwo auf der Welt und verbirgt somit deine Internetaktivitäten.

Statt deines Geräts wird der VPN-Server als Absender im Internet wahrgenommen. Wenn der Server sich in einem anderen Land befindet, scheint es, als würdest du dich von dort aus verbinden. Der VPN-Server fungiert also als Schutzschicht, die deine Online-Aktivitäten verschleiert.

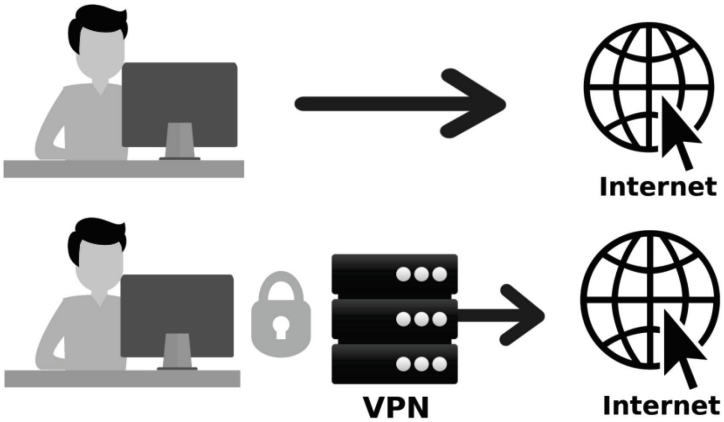

Abbildung 11VPN

Nachfolgend sind einige konkrete Vorteile von VPNs angeführt.

Schutz in öffentlichen WLANs: Ein VPN schützt deine Daten, wenn du öffentliche WLANs nutzt. Ohne VPN könnte der Betreiber des WLANs sehen, welche Webseiten du besuchst, was du herunterlädst und in einigen Fällen sogar deine Passwörter abfangen.

Privatsphäre im Heimnetzwerk: Auch zu Hause kann dein Internetanbieter (ISP = Internet Service Provider) nachvollziehen, welche Seiten du besuchst. Viele ISP speichern diese Informationen, um sie weiterzuverkaufen. Mit einem VPN sieht der ISP lediglich, dass du einen VPN verwendest – deine genauen Aktivitäten bleiben jedoch verschlüsselt.

Zensur umgehen: In Ländern mit strenger Internetzensur, wie China nutzen viele Menschen VPNs, um gesperrte Webseiten zu erreichen. Auch in anderen Ländern kannst du auf diese Weise blockierte Inhalte freischalten.

Anonymität: Deine IP-Adresse wird durch die Nutzung eines VPNs verschleiert. Diese Adresse verrät deinen ungefähren Standort und kann Hinweise auf dein Suchverhalten geben. Ein VPN sorgt dafür, dass deine IP-Adresse anonym bleibt.

Schutz vor Tracking: Webseiten können dich anhand deiner IP-Adresse identifizieren und personalisierte Werbung schalten. Ein VPN verbirgt deine IP, sodass Webseiten nur den VPN-Server sehen und du schwerer zu tracken bist.

Datenlecks: Bei Datenlecks von Webseiten oder Unternehmen wird oft auch die IP-Adresse der Nutzer veröffentlicht. Mit einem VPN bleibt deine tatsächliche IP geschützt, da nur die des VPN-Servers bekannt wird.

Geografische Beschränkungen umgehen: Mit einem VPN kannst du so tun, als würdest du dich aus einem anderen Land verbinden, um auf Dienste zuzugreifen, die nur in bestimmten Regionen verfügbar sind. Allerdings wird dies zunehmend schwieriger, da die meisten Webseiten solche Versuche blockieren (wie z.B. Netflix).

Du solltest ein ungefähres Bild davon haben, was ein VPN ist und warum es sinnvoll ist, eines zu nutzen. Für jeden, dem Privatsphäre und Sicherheit wichtig sind, ist ein VPN eine der besten ersten Investitionen. Ohne VPN ist es viel einfacher, von Unternehmen, Staaten oder anderen Parteien getrackt zu werden.

Nun stellt sich die Frage: Welcher VPN-Anbieter ist der richtige für dich? Ähnlich wie bei Passwortmanagern gibt es viele VPN-Anbieter, und es ist besser, irgendein VPN zu nutzen als gar keinen. Wenn du bereits ein VPN hast, den du magst, bleibe gerne dabei. Falls nicht, kannst du auch einen anderen Anbieter ausprobieren. Hier sind zwei VPN-Anbieter, die ich dir ans Herz legen möchte.

Mullvad VPN

Mullvad ist ein schwedischer Anbieter, der besonderen Wert auf Privatsphäre und Anonymität legt. Bei der Anmeldung erhälst du eine zufällig generierte Kontonummer – persönliche Daten oder E-Mail-Adressen sind nicht erforderlich. Mullvad verfolgt eine strikte No-Logs-Politik und speichert keine Nutzerdaten. Zudem bietet der Anbieter eine transparente und einfache Preisstruktur ohne versteckte Gebühren.

Es ist zu beachten, dass Mullvad weniger Server als andere Anbieter hat, was gelegentlich zu langsameren Verbindungen führen kann.

Kosten: 5 € pro Monat
Webseite: mullvad.net/de/vpn

ProtonVPN

ProtonVPN wurde von den Entwicklern von ProtonMail ins Leben gerufen und legt großen Wert auf Datenschutz. Der Dienst hat seinen Sitz in der Schweiz, was bedeutet, dass er strengen Datenschutzgesetzen unterliegt. ProtonVPN bietet zudem eine kostenlose Version ohne Datenlimit an, jedoch mit einer eingeschränkten Serverauswahl und nur für ein einzelnes Gerät.

Nutzer von ProtonMail, die Bedenken haben, all ihre Daten bei einem Anbieter zu speichern, sollten in Erwägung ziehen, für ProtonVPN einen separaten Account anzulegen.

Kosten: 3,99 € pro Monat bei einem Jahresvertrag
Webseite: protonvpn.com

Ein wesentlicher Aspekt beim Schutz deiner Privatsphäre ist die Wahl der Zahlungsmethode für deinen VPN-Dienst. Kreditkartenzahlungen sind nicht ideal, da dein Name direkt mit deinem VPN-Account verknüpft wird.

Eine bessere Option ist die Verwendung von Bitcoin oder einer anderen anonymen Zahlungsmethode. Einige VPN-Anbieter wie ProtonVPN und Mullvad akzeptieren sogar Barzahlungen per Post, was jedoch für die meisten Nutzer umständlich sein könnte. Ich persönlich empfehle die anonyme Zahlung mit Bitcoin oder Monero.

Wenn dir Privatsphäre und Anonymität wichtig sind, bieten diese beiden VPN-Dienste solide Optionen, je nachdem, welche Anforderungen du an Preis, Geschwindigkeit und Serververfügbarkeit hast. Ich nehme bewusst keine Affiliate-Deals an, um VPNs aufgrund ihrer Eigenschaften und nicht aus Profitinteresse zu empfehlen.

Affiliate Deals
Durch einen Affiliate Deal bekommt die Person, die ein VPN empfiehlt, eine kleine Provision. Das führt dazu, dass VPNs nicht wegen ihrer guten Eigenschaften empfohlen werden, sondern es wird oft das VPN empfohlen, das die höchste Provision zahlt.

DNS

Das Domain Name System (DNS) ist ein Dienst, der benutzerfreundliche Webadressen wie google.de in IP-Adressen übersetzt, die Computer verstehen (z. B. wird google.de in 173.194.10.100 umgewandelt). Ohne DNS müssten wir uns die IP-Adressen jeder Webseite merken, was kaum praktikabel wäre.

Jedes Mal, wenn du eine neue Webseite aufrufst, fragt dein Gerät beim DNS-Server nach der entsprechenden IP-Adresse, damit die Seite geladen werden kann. Standardmäßig wird der DNS-Server deines Internetanbieters verwendet, was jedoch einige Sicherheits- und Privatsphäreprobleme mit sich bringt.

DNS-Anfragen sind häufig unverschlüsselt und enthalten zusätzliche Metadaten. Das bedeutet, dass jeder, der Zugriff auf diese Daten hat – sei es dein Internetanbieter, Hacker oder staatliche Stellen – nachvollziehen kann, welche Seiten du besuchst, wann du sie besuchst und von welchem Gerät aus. Deine Internetaktivitäten können somit leicht überwacht werden, wenn du den Standard-DNS-Server nutzt. Daher ist es ratsam, einen alternativen DNS-Anbieter in Betracht zu ziehen.

Wenn du ein VPN (Virtuelles privates Netzwerk) verwendest, leitet dieses in der Regel alle DNS-Anfragen über seinen eigenen DNS-Server, was die Sicherheit im Vergleich zum Standard-DNS erhöht. Es ist jedoch hier wichtig, nicht alle Eier in einen Korb zu legen und dem VPN-Anbieter nicht komplett blind zu vertrauen. Daher empfiehlt es sich, einen unabhängigen DNS-Dienst zu nutzen und somit VPN und DNS voneinander zu trennen.

NextDNS

Ich empfehle NextDNS, da es einfach einzurichten ist, umfassenden Schutz bietet und sich individuell anpassen lässt.

Kosten: Kostenlos für bis zu 300.000 DNS-Anfragen pro Monat (genug für 99,9% der Benutzer), danach 20 € pro Jahr.

Einfache Konfiguration: NextDNS lässt sich schnell und unkompliziert einrichten.

Sicherheit und Privatsphäre: NextDNS unterstützt Technologien wie „DNS over TLS“ und „DNS over HTTPS“, die sichere DNS-Abfragen gewährleisten.

Zusätzliche Optionen: Du kannst Filterlisten anwenden, Tracker und Werbung blockieren sowie verschiedene Datenschutzeinstellungen konfigurieren.

Es gibt zwei Möglichkeiten, NextDNS zu nutzen: Die erste Möglichkeit besteht darin, einen öffentlichen NextDNS-Server zu verwenden, über den deine DNS-Anfragen geleitet werden. Deine Anfragen werden dabei nicht gespeichert und bleiben anonym. Alternativ kannst du ein eigenes Konto bei NextDNS erstellen. Dadurch erhältst du vollen Zugriff auf eine Vielzahl von Einstellungen, kannst Tracker blockieren und eigene Filterlisten konfigurieren.

- Besuche dafür die Webseite auf my.nextdns.io/signup und erstelle dir einen Account. Verwende am besten einen E-Mail-Alias (Kapitel 5), um anonym zu bleiben.
- Gehe auf den Reiter „Datenschutz“ und füge die „NextDNS Ads & Trackers Blockliste“ hinzu. Diese Liste blockiert Werbung und Tracker direkt beim Laden der Seite.
- Gehe auf den Reiter „Installation“ und kopiere den Link unter „DNS-over-HTTPS“ (der Link sieht etwa aus wie folgt: https://dns.nextdns.io/abc123).
- Öffne die Einstellungen von LibreWolf und wähle „Datenschutz & Sicherheit“ aus.

- Scrolle bis zu „DNS über HTTPS“ und aktiviere „Maximaler Schutz“.
- Wähle bei „Anbieter auswählen“, „Benutzerdefiniert“ und füge den kopierten Link ein.
- Jetzt kannst du eine Webseite aufrufen, z. B. die Tagesschau, und anschließend in NextDNS unter „Protokolle“ überprüfen, ob die DNS-Anfrage sichtbar ist.

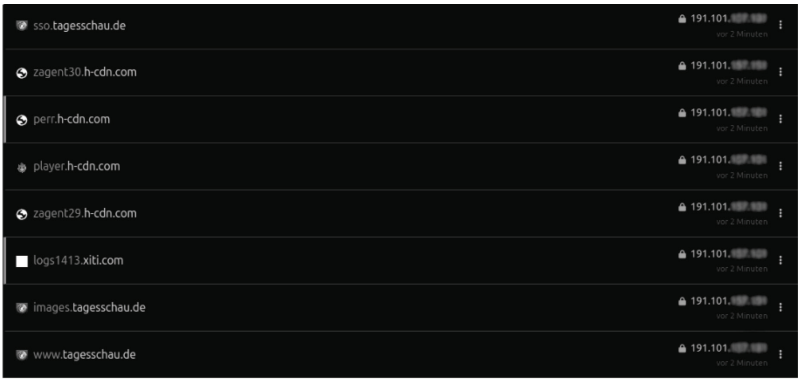

Abbildung 12 NextDNS Anfrage

Hier sind alle Anfragen aufgelistet, die in einem kurzen Zeitraum abgerufen wurden. Dazu gehören die aktiven Suchen bei DuckDuckGo und der Tagesschau, aber auch andere Webseiten und Tracker, die im Hintergrund liefen und blockiert wurden.

Um nicht nur die DNS-Anfragen deines Browsers, sondern die aller Apps über NextDNS zu leiten, kannst du den Dienst für das gesamte Gerät einrichten.

- Gehe auf den Reiter „Installation“ auf der NextDNS-Seite und kopiere die beiden IP-Adressen unter „Verknüpfte IP“ und „DNS-Server“.
- Wenn du ein VPN nutzt, öffne die VPN-Einstellungen und trage die IP-Adressen unter „Custom DNS“ ein.
- Falls du kein VPN verwendest, öffne die Netzwerkeinstellungen deines Computers und füge die IP-Adressen manuell in den DNS-Bereich ein. Detaillierte Anleitungen findest du auf der NextDNS-Seite unter „Installation“.

- Führe einen Test durch, indem du eine App mit Internetzugang öffnest (z. B. StandartNotes) und überprüfe, ob die Anfragen bei NextDNS unter „Protokolle“ angezeigt werden.

Wenn alle Tests erfolgreich abgeschlossen sind und alle Anfragen über NextDNS laufen, kann du sicherstellen, dass keine Daten gespeichert werden. Deaktiviere dazu die Protokollierung bei NextDNS.

- Gehe auf den Reiter „Einstellungen“ und schalte unter „Protokolle“ die Option „Protokolle aktivieren“ aus.

Öffentliche WLANs

Öffentliche WLAN-Netzwerke haben in der Privatsphäre-Community einen schlechten Ruf – und das nicht ohne Grund. In der Vergangenheit gab es ernstzunehmende Sicherheitsrisiken bei der Nutzung dieser Netzwerke, und auch heute sind sie nicht völlig risikofrei.

Früher waren Netzwerke generell unsicherer, und öffentliche WLANs wiesen besonders viele Schwachstellen auf. Oft waren sie gar nicht verschlüsselt, was bedeutete, dass alle Daten, die zwischen dir und dem Router übertragen wurden, ungeschützt waren. Jeder mit den passenden Werkzeugen konnte diese Daten abfangen. Selbst als die ersten Verschlüsselungsprotokolle eingeführt wurden, hatten sie viele Sicherheitslücken, die von Hackern ausgenutzt wurden. Dadurch kam es häufig zu sogenannten Man-in-the-Middle-Angriffen.

Man-in-the-Middle-Angriff
Bei einem Man-in-the-Middle-Angriff, schaltet sich ein Hacker zwischen dich und den Router und leitet den gesamten Datenverkehr über sich selbst. So kann er sensible Informationen wie Logins oder private Nachrichten mitlesen und abgreifen.

Zum Glück hat sich die Situation inzwischen verbessert. Die Verschlüsselung von öffentlichen WLANs ist heute deutlich sicherer und bietet ein ähnliches Sicherheitsniveau wie private WLANs zu Hause. Außerdem nutzen die meisten Webseiten mittlerweile HTTPS. Das bedeutet, dass der Datenverkehr zwischen deinem Browser und der Webseite verschlüsselt ist, was das Risiko senkt, dass jemand deine Daten abfängt.

Die Maßnahmen, die in diesem Buch vorgestellt werden, erhöhen deine Sicherheit erheblich. Mit sicheren Passwörtern und der Zwei-Faktor-Authentifizierung (Kapitel 4) wird der Schutz deiner Konten stark verbessert. Zudem nutzt du ein eigenes DNS, wodurch der Anbieter des öffentlichen WLANs nicht einmal mehr sehen kann, welche Webseiten du besuchst. Die Verwendung eines VPNs verstärkt diesen Schutz noch weiter. Deshalb sehe ich kein allzu großes Sicherheitsrisiko mehr bei der Nutzung öffentlicher WLANs.

Vielleicht hast du, wenn du schon länger ein VPN verwendest, festgestellt, dass es nicht immer problemlos funktioniert. Viele Webseiten blockieren den Zugang über VPNs komplett. Andere setzen endlose Captchas ein, die oft kaum lösbar sind. Manche Seiten verlangen wiederholt E-Mail- oder SMS-Codes zur Verifizierung und verweigern am Ende dennoch den Zugriff. Um unsere Sicherheit und Privatsphäre zu gewährleisten, wollen wir diese Seiten natürlich nicht ohne VPN besuchen. Hier kommen öffentliche WLANs ins Spiel. Wenn du von deinem Heimnetzwerk aus auf eine Webseite zugreifst, wird deine IP-Adresse – und damit dein ungefährer Standort – an die Seite übermittelt. Diese IP-Adresse wird gespeichert und oft mit deinem Account verknüpft. Nutzt du jedoch ein öffentliches WLAN, wird eine andere IP-Adresse verwendet – nämlich die des öffentlichen Netzwerks. Diese wird zwar ebenfalls gespeichert, zeigt aber lediglich auf das öffentliche WLAN. Wenn du also auf eine Webseite zugreifen musst, die VPN-Verbindungen blockiert, kannst du stattdessen öffentliche WLANs in Cafés, Hotels oder Bibliotheken nutzen, um trotzdem deine Privatsphäre zu wahren.

• • •

In diesem Kapitel hast du nun einen sicheren und privaten Browser eingerichtet, der deine Privatsphäre schützt. Dazu haben wir zwei Erweiterungen, die diesen Schutz weiter erhöhen. Außerdem haben wir den Tor-Browser eingerichtet, den du für sensible Angelegenheiten verwenden kannst. Zusätzlich dazu haben wir ein VPN eingerichtet, das unsere IP-Adresse vor den Webseiten und unsere Onlineaktivität vor unserem Internetserviceprovider schützt. Um nicht dem VPN-Anbieter zu viel Vertrauen zu schenken, haben wir NEXT DNS konfiguriert.

Jetzt bist du unabhängig vom DNS-Server deines Internetanbieters und kannst sicher und anonym surfen. NextDNS speichert keine Anfragen und hat nur Zugriff auf deine Alias-E-Mail-Adresse und die aufgerufenen Webseiten. Selbst dein VPN-Anbieter kann nicht mehr sehen, welche Webseiten du besuchst. Durch die Kombination von VPN und NextDNS verbesserst du deine Sicherheit und Privatsphäre erheblich, da du das Vertrauen auf mehrere Dienste verteilst und Überwachung sowie Tracking minimierst. Im nächsten Kapitel werden wir uns ansehen, wie wir unsere Onlineaktivität von den Passwörtern bis hin zur Verschlüsselung sichern können.

Kapitel 4
Passwörter und Verschlüsselung

„Jemand, der seine Daten schützen will, hat nichts zu verbergen. Er hat etwas zu bewahren.“ ~ *Max Schrems*

Konten und Passwörter sind aus unserer digitalen Welt nicht mehr wegzudenken – nahezu jede Anwendung und jeder Online-Dienst verlangt nach ihnen. Leider sind die meisten Passwörter, die von der breiten Bevölkerung verwendet werden, nicht sicher genug, was das Risiko eines Angriffs erheblich erhöht. Aus diesem Grund widme ich diesem Thema ein ganzes Kapitel.

Darüber hinaus werden wir einen Blick auf Verschlüsselungen und Backups werfen. Diese Themen werden oft ignoriert oder aufgeschoben, können jedoch erhebliche Probleme verursachen, wenn man plötzlich ein Backup benötigt.

Sichere Passwörter

Bevor wir uns damit beschäftigen, einen Passwortmanager zu verwenden und alle Passwörter zu ändern, ist es wichtig, zu verstehen, was ein sicheres Passwort ausmacht und auf welche Punkte man bei der Passwortauswahl achten muss.

Um diese Frage zu klären, sollten wir zunächst die Sicherheitsprobleme betrachten und verstehen, wie Passwörter in die Hände von Hackern oder unbefugten Dritten gelangen können. Der klassische Ansatz, um an ein Passwort zu gelangen, ist die Brute-Force-Attacke. Dabei versucht ein Computer in rasanter Geschwindigkeit, unzählige Passwortkombinationen auszuprobieren, bis das richtige gefunden ist. Ein leistungsstarker Computer kann dabei bis zu 10 Milliarden Passwörter pro Sekunde testen. Um uns vor solchen Angriffen zu schützen, sind zwei Faktoren entscheidend: die Länge des Passworts und die Vielfalt der verwendeten Zeichen.

Länge: Jedes zusätzliche Zeichen, das wir einem Passwort hinzufügen, erhöht die Dauer einer Brute-Force-Attacke exponentiell. Daher empfehle ich eine Mindestlänge von 16 Zeichen.

Variation: Je mehr unterschiedliche Zeichenarten in unserem Passwort enthalten sind, desto sicherer wird es. Statt allein Zahlen zu verwenden (die nur 10 verschiedene Möglichkeiten pro Stelle bieten), sollte eine Mischung aus Zahlen, Groß- und Kleinbuchstaben sowie Sonderzeichen verwendet werden, die mehr als 90 verschiedene Möglichkeiten pro Stelle bietet.

Eine weitere Möglichkeit, in einen Account einzudringen, besteht darin, dass das Passwort bereits bekannt ist. Wenn du für alle deine Accounts dasselbe Passwort verwendest und eines dieser Passwörter bei einem Datenleck offengelegt wird, können Angreifer problemlos auch auf alle anderen Accounts zugreifen. Daher ist es wichtig, für jeden Account ein einzigartiges, noch nie verwendetes und nicht ähnliches Passwort zu wählen.

Viele Menschen, die sich dieses Problems bewusst sind, verwenden für jede Webseite ein ähnliches Passwort, das sie nur geringfügig abändern. Diese Methode scheint zunächst praktisch, da sie leicht umzusetzen ist und für jeden Account ein anderes Passwort bereitstellt. Allerdings ist diese Vorgehensweise nicht optimal. Bei Datenlecks versuchen Angreifer nicht nur, alle bekannten Passwörter für andere Accounts zu verwenden, sondern setzen auch Algorithmen ein, um solche Variationen zu erkennen. So können sie die Regel, nach der du deine Passwörter erstellst, entschlüsseln und damit Zugang zu all deinen Accounts erlangen.

Achtung: Ein schlechtes Beispiel
Wenn als Hauptpasswort „privacy!“ gewählt wird und für jede Webseite drei Zeichen angehängt werden, die von der jeweiligen Seite abhängen, z. B. „goo“ für Google oder „you“ für YouTube, entstehen Passwörter wie „privacy!you“ oder „privacy!goo“. Diese Methode ist jedoch schnell durchschaubar und daher unsicher.

Die sichere Verwaltung der zahlreichen Passwörter, die wir heute benötigen, ist nahezu unmöglich, wenn man sich auf das eigene Gedächtnis verlässt. Die beste Möglichkeit hier ist ein Passwortmanager der sichere Passwörter erstellt und diese dann sicher abspeichert. Solltest du bei Passwortmanagern ein schlechtes Gefühl haben kannst du auch physisch du alle Passwörter in einem analogen Notizbuch notieren (Ich empfehle eins mit A-Z Sortierung zum einfachen Wiederfinden.) für maximalen Schutz sollte ein Passwortmanger jedoch die erste Wahl sein.

Passwortmanager

Jedes Jahr gibt es Hunderte von Datenlecks, durch die Milliarden von Passwörtern in die Hände von Hackern gelangen. Viele Menschen verwenden dasselbe Passwort für verschiedene Konten oder haben ihre Passwörter seit Jahren nicht geändert. Daher ist es ratsam, davon auszugehen, dass alle deine Passwörter potenziell kompromittiert sind und aktualisiert werden müssen. Der erste Schritt besteht darin, die wichtigsten Konten zu identifizieren und sichere, einzigartige Passwörter für jedes einzelne zu erstellen. Ein Passwortmanager ist hierfür die beste Lösung.

Man unterscheidet allgemein zwischen Online- und Offline-Passwortmanagern. Bei Online-Managern werden die Daten verschlüsselt auf Servern gespeichert, was den Vorteil bietet, dass du von überall auf deine Passwörter zugreifen kannst. Offline-Passwortmanager hingegen erfordern eine manuelle Synchronisation zwischen den Geräten und regelmäßige Backups. Der Vorteil dieser Variante liegt in der erhöhten Sicherheit, da die Passwörter ausschließlich auf deinem eigenen Gerät gespeichert werden. Wenn du diese Option bevorzugst, empfehle ich KeePassXC.

Es gibt viele Diskussionen darüber, welcher Passwortmanager der beste ist, und ich möchte diese hier vermeiden. Ich präsentiere dir Bitwarden, da es sich hervorragend für den Einstieger eignet. Natürlich steht es dir frei, ein anderes Programm zu nutzen, wenn du bereits eines im Einsatz hast oder ein anderes bevorzugst.

Bitwarden

Bitwarden ist ein Open-Source-Online-Passwortmanager, der für alle Betriebssysteme verfügbar ist. Die kostenlose Version bietet bereits für die meisten Nutzer umfassende Funktionen, kann jedoch bei Bedarf durch die kostenpflichtige Version für 10 € pro Jahr erweitert werden. Bitwarden kannst du unter bitwarden.com/download/ installieren.

- Öffne die Anwendung und klicke unten in der Mitte auf „Create Account".
- Gib deine E-Mail-Adresse ein (falls du noch keine sichere private E-Mail-Adresse habt, kannst du im Kapitel 5 nachschlagen) und lege ein Masterpasswort fest.

Das Masterpasswort fungiert als Schlüssel für den Zugriff auf den Passwortmanager. Jeder, der dieses Passwort kennt, hat uneingeschränkten Zugriff auf alle gespeicherten Passwörter – sofern keine Zwei-Faktor-Authentifizierung (2FA) eingerichtet ist. Daher sollte das Masterpasswort besonders sicher sein und aus mindestens 16 Zeichen bestehen, wobei es noch nie zuvor verwendet worden sein darf. Sollte der Zugriff auf dieses Passwort verloren gehen, ist auch der Zugang zu den gespeicherten Passwörtern und damit zu den entsprechenden Konten nicht mehr möglich. Es ist daher von größter Bedeutung, das Masterpasswort sicher aufzubewahren.

- Du kannst optional einen Hinweis für das Masterpasswort hinterlassen, der bei Bedarf an die angegebene E-Mail-Adresse gesendet wird. Ich würde diese Funktion überspringen.
- Setzte das Häkchen bei den Nutzungsbedingungen („TOS") und klicke auf „Submit".

Der Passwortmanager ist nun einsatzbereit. Um den Zugriff auf die Passwörter während des Surfens im Internet zu erleichtern, kann später eine Browser-Erweiterung installiert werden. Als Nächstes erstellen wir einen neuen Testeintrag um zu sehen wie der Passwortmanager funktioniert und wie man neue Einträge zu Webseiten und Passwörtern erstellen kann.

- Gib auf der Anmeldeseite deine E-Mail-Adresse ein und klicke auf „Continue“. Optional kannst du das Häkchen bei „Remember E-Mail“ setzen, um bei zukünftigen Anmeldungen nur noch das Passwort eingeben zu müssen.
- Gib dann dein Passwort ein und klicke auf „Log in with“.
- Um einen neuen Eintrag zu erstellen, klicke oben links auf „File“ und anschließend auf „New Login“.
- Bei „Name“ kannst du einen Namen für den Eintrag angeben, meistens eignet sich hier der Name der Webseite.
- Gebe bei „Username“ den Benutzernamen für die Anmeldung ein, häufig ist das die E-Mail-Adresse.
- Bei „Password“ wird das Passwort gespeichert. Da davon ausgegangen wird, dass bisherige Passwörter unsicher sind, sollte immer ein neues Passwort erstellt werden.
- Klicke dazu auf die zwei Pfeile, die im Kreis aufeinander zeigen, wodurch der Passwortgenerator geöffnet wird. Ein Passwort wird direkt vorgeschlagen, es lohnt sich jedoch, einige Anpassungen vorzunehmen, um die Sicherheit zu erhöhen.
- Durch Klicken auf „Options“ kannst du weitere Einstellungen vornehmen.
- Wähle bei „Length“ die Länge auf 20 Zeichen fest.
- Setzte das Häkchen für Sonderzeichen.
- Gebe unten bei „Minimum numbers“ und „Minimum special“ jeweils „3“ ein, um sicherzustellen, dass mindestens drei Zahlen und drei Sonderzeichen im generierten Passwort enthalten sind.
- Bestätige die Auswahl mit dem Haken unten links, und schon ist ein neues sicheres Passwort für den Account erstellt.
- Weiter unten besteht die Möglichkeit, durch Klicken auf „New URI“ eine Webseite hinzuzufügen. Dies ist nur nützlich, wenn eine Browser-Erweiterung verwendet wird, da die Anmeldedaten (Benutzername und Passwort) dann automatisch für diese Seite ausgefüllt werden können.

Jetzt wurde ein sicheres, zufälliges und einzigartiges Passwort für den ersten Account erstellt. Es mag zwar schwer zu merken sein, aber genau dafür ist der Passwortmanager da – zur sicheren

Aufbewahrung aller Passwörter. Es wäre unrealistisch, alle Passwörter auf einmal zu ändern. Daher empfiehlt es sich, immer dann, wenn du eine Webseite besuchst, bei der ein altes Passwort verwendet wird, dieses zu aktualisieren. So wird schrittweise jedes Passwort gesichert, ohne dass du stundenlang daran arbeiten musst. Bei jeder Anmeldung mit einem neuen Passwort sollte der Passwortmanager verwendet werden. Auf diese Weise bleiben die Accounts auch dann geschützt, wenn eines der Passwörter durch ein Datenleck veröffentlicht wird.

Da Bitwarden ein Online-Passwortmanager ist, sind regelmäßige Backups unerlässlich. Sollte es jemals zu einer Abschaltung der Bitwarden-Server, einer Kontosperrung oder einem blockierten Zugriff kommen, könnten alle Passwörter verloren gehen. Ein Backup, beispielsweise alle zwei Wochen, ist daher sehr empfehlenswert.

- Klicke dafür oben links auf „File“ und anschließend auf „Export Vault“.
- Wähle unter „File-Format“ die Option „json (Encrypted)“ und „Passwortgeschützt“ aus und gib das Passwort ein, das diese Datei verschlüsseln soll.
- Bestätige den Vorgang mit dem Masterpasswort.
- Wähle den Speicherort aus und speichere die Datei ab.

Es ist wichtig zu beachten, dass Browsererweiterungen und mobile Apps optional sind und stets ein gewisses Risiko mit sich bringen. Bitwarden ist zwar ein leistungsstarker Passwortmanager, jedoch werden die Passwörter in der Cloud gespeichert, was ein Restrisiko mit sich bringt. Die Passwörter werden zwar auf dem Gerät des Nutzers verschlüsselt und entschlüsselt, sodass Bitwarden-Mitarbeiter keinen Zugriff darauf haben, dennoch bleibt die Gefahr eines Hacks höher als bei einem Offline-Passwortmanager wie KeePassXC. Jeder sollte individuell abwägen, welches Abwägung von Sicherheit und Benutzerfreundlichkeit für ihn angemessen ist. Mit Sicherheit ist jeder Passwortmanager besser als keiner. Es ist ratsam, alle Passwörter schrittweise durch sichere, neu generierte Passwörter zu ersetzen. Dabei sollte man mit den wichtigsten Konten beginnen, beispielsweise mit dem E-Mail-Konto oder Bankkonten. Zudem ist es entscheidend, einen sicheren Computer zu verwenden, denn wenn

auf einem älteren Windows-PC ein Keylogger installiert ist, nützt die Änderung der Passwörter wenig, da diese sofort ausgelesen und gespeichert werden könnten. Auch sollte das Netzwerk sicher sein; daher niemals in einem öffentlichen WLAN.

2FA (Zwei-Faktor-Authentifizierung)

Mit der Erstellung sicherer und einzigartiger Passwörter für alle Konten haben wir bereits ein hohes Maß an Sicherheit erreicht. Dennoch schützt dies unsere Konten nicht vollständig. Wie bereits erwähnt, werden jährlich Millionen von Daten geleakt, und es ist unmöglich zu wissen, ob jemand eines unserer Passwörter besitzt und nur darauf wartet, sich damit anzumelden.

- Persönliche Informationen zu verkaufen,
- Zugang zu Geldkonten zu erhalten oder
- unsere allgemeine Sicherheit zu gefährden.

Um unbefugten Zugriff zu verhindern, sind zwei wesentliche Maßnahmen zu beachten: die Zwei-Faktor-Authentifizierung (2FA) und Benachrichtigungen über Account-Zugriff.

Die 2FA hast du sicherlich schon einmal genutzt, beispielsweise wenn deine Bank nach den Anmeldedaten einen sechsstelligen Code anfordert hat, der dir per E-Mail oder SMS zugesendet worden ist. Das ist die Zwei-Faktor-Authentifizierung. Überall, wo es möglich ist, solltest du 2FA aktivieren.

Mit aktivierter 2FA verlangt das System zusätzlich zu deinen Anmeldedaten eine weitere Verifizierung. Es gibt verschiedene Formen der 2FA, etwa SMS-Benachrichtigungen, Apps auf deinem Smartphone oder spezielle USB-Sticks. In der Regel wird ein zeitlich begrenzter Code (One-Time-Password) bei der Anmeldung zusammen mit deinen Anmeldedaten eingegeben. Dies erhöht die Sicherheit erheblich. Selbst wenn ein Angreifer deine Anmeldedaten erlangt hat, benötigt er zusätzlich den Code, der nur dir (z. B. auf deinem Handy) zugänglich ist. Der Prozess funktioniert wie folgt.

- Der Benutzer gibt seinen Benutzernamen und sein Passwort ein.
- Die Plattform fordert zur Eingabe eines Einmalpasswortes (z. B. den an das Handy gesendeten Code) auf.
- Nach Eingabe dieses Codes erhält der Benutzer Zugang zu seinem Account.

Verschiedene Arten von 2FA

SMS- oder E-Mail-2FA: Diese Methode ist zwar die am häufigsten verwendete, jedoch auch die unsicherste. Wenn ein Programm nur SMS oder E-Mail als 2FA-Option anbietet (wie es bei vielen Bankanwendungen der Fall ist), solltest du diese Methode dennoch nutzen, auch wenn das Sicherheitsrisiko höher ist als bei anderen Varianten. In diesem Fall kann es sinnvoll sein, eine separate Telefonnummer (siehe Kapitel 5, „Telefonnummern“) ausschließlich für diesen Zweck zu verwenden, um dich gegen SIM-Swapping-Angriffe abzusichern.

Hardware-Token: Dies ist ein kleines Gerät in Form eines USB-Sticks, das als 2FA-Methode dient. Bei der Anmeldung muss der Stick physisch berührt werden, um die Authentifizierung zu bestätigen. Ohne Zugriff auf dieses Gerät kann sich niemand in die geschützten Konten einloggen. Diese Methode bietet die höchste Sicherheit, erfordert jedoch, dass das Gerät immer griffbereit ist. Wenn du es vergisst, kann der Zugriff auf dein Konto gesperrt sein. Die genaue Anleitung zur Einrichtung eines YubiKey (einem gängigen Hardware-Token) variiert je nach Programm und wird regelmäßig aktualisiert. Eine Anleitung findest du auf der Yubico-Website: www.yubico.com

Software-Token: Wenn ein Hardware-Token nicht gewünscht ist oder ein Programm es nicht unterstützt, ist dies die zweite Option. Ich empfehle die App EnteAuth. Unabhängig davon, welche 2FA-App du wählst, ist diese Option besser als keine, da auch hier der physische Zugriff auf das Gerät erforderlich und das Auslesen des Codes durch Malware wesentlich schwieriger ist als bei der Verwendung einer E-Mail oder SMS. Die App zeigt dir dann einen

sechsstelligen Code an, der sich alle 30 Sekunden ändert und den du bei der Anmeldung manuell eingeben musst.

EnteAuth

EnteAuth ist eine Open-Source-2-Faktor-Authentifizierungs-App, die für alle Betriebssysteme verfügbar ist und auf der Webseite ente.io/auth heruntergeladen werden kann. Nach dem Download hast du die Möglichkeit, dich anzumelden. Mit einer Anmeldung kannst du deine 2FA-Codes verschlüsselt zwischen verschiedenen Geräten synchronisieren. Ich bevorzuge jedoch die lokale Variante. Klicke dafür auf „Use without backups“. Anschließend kannst du sofort mit dem Hinzufügen neuer Codes beginnen.

Da sich bei jedem Accouunt die Einstellung von 2FA ein wenig unterscheidet, werde ich beispielhaft Bitwarden und ProtonMail aufzeigen. Die Einstellungen werden zwar in Abhängigkeit von den verschiedenen Programmen variieren, der grundlegende Prozess bleibt jedoch gleich.

ProtonMail:

- Wähle in den Einstellungen links „Konto und Passwort“ aus.
- Aktiviere das Häckchen bei „Authenticator app“, scanne mit der EnteAuth App den QR-Code und gib den sechsstelligen Code ein, der in der App angezeigt wird.

Bitwarden:

- Klicke auf der Webseite auf „Einstellungen“, dann auf „Security“ und oben auf „Two-Step login“ oder öffne diesen Link: vault.bitwarden.com/#/settings/security/two-factor
- Wähle die „Authenticator app“ aus und klicke auf „Manage“.
- Scanne den QR-Code mit der App und gib den sechsstelligen Code ein, der in EnteAuth angezeigt wird.

EnteAuth generiert für jeden Account alle 30 Sekunden einen neuen sechsstelligen Code. Bei der Anmeldung bei ProtonMail oder anderen Programmen mit aktivierter Zwei-Faktor-Authentifizierung

(2FA) wird neben dem Benutzernamen und Passwort auch dieser Code abgefragt. Ohne diesen Code hast du keinen Zugriff auf deinen Account.

EnteAuth speichert keine Account-Details der jeweiligen Programme, sondern lediglich die zufällig generierten Codes. Um den Zugang zu deinen Accounts nicht zu verlieren, sind regelmäßige Backups besonders wichtig. Ich empfehle, nach jedem neuen Eintrag ein Backup zu erstellen, um sicherzustellen, dass du bei Verlust des Geräts weiterhin Zugriff auf deine 2FA-Codes hast.

- Öffne dafür EnteAuth, klicke oben links auf die drei Striche und wähle „Datei“ aus.
- Wähle den Unterpunkt „Codes exportieren“ und klicke auf „Verschlüsselt“.
- Gebe in das Pop-up-Fenster das Passwort, ein mit dem diese Datei verschlüsselt werden soll und bestätige mit „Export“
- Klicke auf „Speichern“ – kannst du den Speicherort auswählen. Ich speichere die Datei direkt auf einen USB-Stick, um sie auf meinen Laptop zu übertragen.

Diese Datei wird mit dem von dir gewählten Passwort verschlüsselt, sodass du damit alle deine 2FA-Codes wiederherstellen kannst.

Probleme ohne 2FA

Neben den Sicherheitsrisiken, die ohne 2FA bestehen, gibt es auch ein weiteres Problem, das von den Unternehmen selbst ausgehen kann. Im Jahr 2021 führten viele Online-Dienste die verpflichtende Nutzung von 2FA für ihre Kunden ein. Auf den ersten Blick mag dies sinnvoll erscheinen, doch oft verbirgt sich dahinter das Bestreben, noch mehr Kundendaten zu sammeln.

Ich hatte einen anonymen Google-Account, den ich häufig nutzte. Eines Tages, als ich mich anmelden wollte, forderte Google einen Einmalcode per SMS an. Da ich nie eine Telefonnummer angegeben hatte, verlangte Google, dass ich eine Nummer hinzufüge; andere Optionen gab es nicht. Andernfalls würde der Zugriff auf meinen Account komplett blockiert.

Hier kommt die proaktive 2FA ins Spiel. Hätte ich bei diesem Account einen 2FA-Code über eine Authentifizierungs-App wie EnteAuth verwendet, hätte Google niemals nach einer Telefonnummer gefragt. Daher empfehle ich, jeden Account, der 2FA anbietet, damit zu sichern. Dies erhöht nicht nur die Sicherheit erheblich, sondern verhindert auch, dass man von seinen Accounts ausgeschlossen wird, wenn man keine Telefonnummer angeben möchte.

Benachrichtigungen für Account-Zugriff

Seit 2016 hat Google eine Funktion eingeführt, die bei jeder Anmeldung eine E-Mail und eine Push-Benachrichtigung versendet. Diese Maßnahme dient dazu, die Nutzer darüber zu informieren, wer sich wann und wo in ihrem Konto anmeldet. Obwohl ich Google wegen seiner Eingriffe in die Privatsphäre kritisch betrachte, muss man ihre Sicherheitsvorkehrungen als erstklassig anerkennen.

Diese Funktion ist besonders wichtig, um zu überwachen, ob Konten gehackt wurden. Viele Online-Dienste haben dies mittlerweile als Standard übernommen, während andere es als optionale Einstellung anbieten. Auch wenn diese Benachrichtigungen manchmal lästig sein können, erhöhen sie die Sicherheit erheblich, da man sofort auf unautorisierte Logins reagieren kann, indem man das Passwort und die 2FA-Einstellungen ändert. Daher sollten Login-Benachrichtigungen immer aktiviert sein, wenn der Dienst dies ermöglicht. Überprüfe dazu die entsprechenden Sicherheitseinstellungen.

Verschlüsselte Backups und USB-Sticks

Die effektivste Methode, um sensible Daten vor unerwünschtem Zugriff zu schützen, ist die Verschlüsselung. Dabei werden deine Daten mithilfe eines geheimen Schlüssels in unleserlichen „Datenmüll" umgewandelt. Nur mit diesem Schlüssel können sie wieder in lesbare Informationen zurückverwandelt werden.

Ein bewährtes Tool zur Verschlüsselung ist VeraCrypt, ein Open-Source-Programm, das Festplatten, USB-Sticks und einzelne Dateien schützt. VeraCrypt basiert auf dem früheren Programm

TrueCrypt, das auch von Edward Snowden verwendet wurde. Die Verschlüsselung erfolgt ohne spürbare Verzögerung und ist benutzerfreundlich.

VeraCrypt ist für die Betriebssysteme Linux, Windows und MacOS verfügbar. Diese kannst du unter veracrypt.eu/en/Downloads.html herunterladen (Siehe Kapitel 1 für die Linux-Installation).

- Öffne VeraCrypt nach dem Herunterladen. Danach kannst du direkt mit der Verschlüsselung beginnen.
- Klicke auf „Create Volume“ in der Mitte links.
- Nun stehen dir zwei Optionen zur Verfügung:
- „Create an encrypted file container“: Erstelle einen verschlüsselten Container, der als virtueller Ordner genutzt werden kann.
- „Encrypt a non-system partition/drive“ verschlüsselt eine gesamte Partition, z. B. einen USB-Stick.
- Für dieses Tutorial wählen wir die erste Option.
- Wähle im nächsten Schritt „Standard VeraCrypt volume“ aus.
- Lege bei „Select File“ den Speicherort fest, beispielsweise den Desktop oder einen USB-Stick, und gib dem Container einen Namen wie „Backup“ oder „VeraCrypt“.
- Bei den „Encryption Options“ kannst du die Standardeinstellungen beibehalten.
- Lege unter „Volume Size“ die gewünschte Größe des verschlüsselten Containers fest. Für Textdokumente sind oft 5 GB ausreichend; für vollständige Backups deines Computers oder Handys benötigst du jedoch mehr Speicherplatz.
- Wenn der USB-Stick ausschließlich für die Verschlüsselung verwendet werden soll, kannst du einen Container in voller Größe erstellen.
- Gib im nächsten Schritt ein sicheres, langes Passwort ein. Hierfür kannst du den zuvor eingerichteten Passwortmanager nutzen. Klicke danach auf „Next“.
- Überspringe die nächsten drei Seiten jeweils mit „Next“.
- Bewege die Maus innerhalb des Fensters auf der Seite „Volume Format“, um die Verschlüsselung weiter zu verstärken. Deine manuell hinzugefügten Bewegungen werden genutzt,

um die Zufälligkeit zu erhöhen und somit die Sicherheit der Verschlüsselung zu verbessern.
- Sobald die Anzeige „Randomness collected from mouse movements“ voll ist, klicke auf „Format“, um den Container zu verschlüsseln.
- Nach erfolgreicher Verschlüsselung kannst du das Fenster schließen.

Nun hast du einen verschlüsselten Container auf deinem Computer oder USB-Stick erstellt, auf den ohne das Passwort kein Zugriff möglich ist. Um den Container zu verwenden, muss er zunächst gemountet werden. Hierfür brauchst du dann dein zuvor ausgewähltes Passwort.

Mounten
Bei VeraCrypt bedeutet „Mounten“, dass das verschlüsselte Volumen (die zuvor erstellte Datei) in das System eingebunden wird, um auf die darin gespeicherten Daten zugreifen zu können. Erst nach dem Mounten und der Eingabe des richtigen Passworts wird das Volume wie ein normaler Datenträger angezeigt und kann genutzt werden.

- Öffne dafür VeraCrypt, klicke auf „Select File“ in der Mitte rechts und wähle den zuvor erstellten Container aus.
- Klicke unten links auf „Mount“, gib das Passwort ein und bestätige, falls gefragt, auch das Passwort des Computers.
- Der Container wird nun gemountet und als zusätzliches Laufwerk angezeigt. Du kannst Dateien nach Belieben hinein- oder herauskopieren. Um den Container wieder zu verschlüsseln, klicke einfach auf „Dismount All“.

Welche Daten sollten verschlüsselt werden?

Sensible Informationen: Dazu zählen Kontaktdaten, Dokumente wie Ausweise und Pässe sowie alles, was nicht für die Öffentlichkeit bestimmt ist. Ein kleiner Container mit 10 GB auf dem Laptop ist oft ausreichend, um diese Daten sicher zu speichern.

Backups: Eine zuverlässige Backup-Strategie sollte immer eine Verschlüsselung beinhalten. Zwar bieten Microsoft, Apple und Linux eigene Backup-Programme an, ich empfehle jedoch eine Open-Source-Lösung wie FreeFileSync. Dieses Programm unterstützt dich dabei, Dateien, die noch nicht gesichert wurden, zu identifizieren und in den erstellten verschlüsselten Container zu kopieren.

- Lade dafür FreeFileSync von der Webseite freefilesync.org/ herunter und öffne es.
- Wähle links deinen Home-Ordner aus und rechts den VeraCrypt-Ordner auf dem USB-Stick. (1)
- Klicke oben rechts auf das Zahnrad und wähle „Update“ aus. (2)
- Klicke oben links auf „Compare“. (3)
- Nach Abschluss des Vergleichs klicke oben rechts auf „Synchronize“. (4)
- Bestätige im Popup-Fenster mit „Start“.

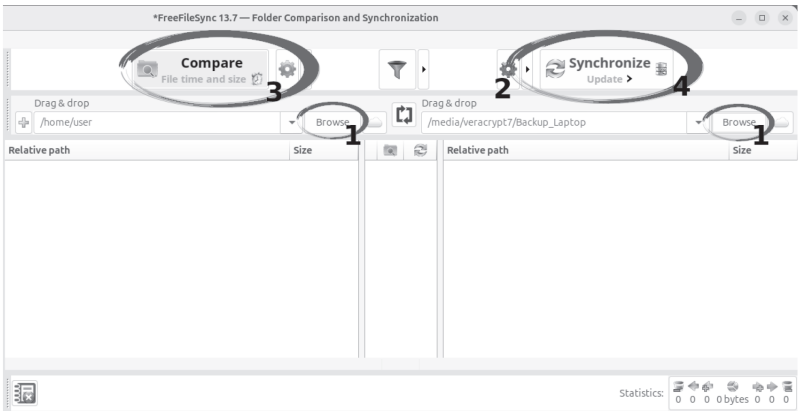

Abbildung 13FreeFileSync-Synchronisation

Jetzt beginnt die Synchronisation. Zu Beginn kann es etwas länger dauern, da alle Dateien gesichert werden müssen. Bei zukünftigen Backups erfolgt die Übertragung schneller, da nur noch neue und geänderte Dateien gesichert werden.

Es ist empfehlenswert, regelmäßige Backups auf einem verschlüsselten USB-Stick zu erstellen. Sollte dieser verloren gehen oder

gestohlen werden, brauchst du dir keine Sorgen zu machen, da der Inhalt durch die Verschlüsselung unzugänglich bleibt. Eine effektive Backup-Strategie lässt sich mithilfe der 3-2-1-Regel umsetzen:

- **3 Kopien:** Du solltest mindestens drei Backups deiner Daten haben.
- **2 verschiedene Speichermedien:** Nutzte mindestens zwei unterschiedliche Speichermedien, z. B. USB-Sticks und externe Festplatten.
- **1 Kopie an einem anderen Ort:** Bewahre eine Kopie an einem anderen Ort auf.

Sollte ein Backup verloren gehen, gestohlen oder zerstört werden, bleiben die anderen beiden verfügbar. Selbst im schlimmsten Fall, wenn dein Haus abbrennt, hast du immer noch ein Backup an einem anderen Ort.

Das erste der drei Backups befindet sich auf deinem verschlüsselten Computer. Für die anderen beiden Backups eignen sich USB-Sticks mit jeweils 512 GB (je nach Bedarf auch mehr oder weniger) und einem VeraCrypt-Container. Backups sollten in Abhängigkeit davon erstellt werden, wie viele neue Dateien seit dem letzten Backup hinzugekommen sind – mindestens jedoch einmal im Monat. Auf Reisen, wenn das Risiko eines Diebstahls höher ist, sind häufigere Backups sinnvoll.

Einer der beiden USB-Sticks sollte zu Hause aufbewahrt werden, um regelmäßig Backups erstellen zu können. Den zweiten Stick kannst du sicher bei Freunden oder Familienmitgliedern aufbewahren. Sollten dein Laptop und der erste USB-Stick gestohlen werden, kannst du durch einen kurzen Anruf darum bitten, dass dir die Daten vom zweiten USB-Stick geschickt werden. So kannst du auf einem anderen Gerät deine Daten entschlüsseln und weiterhin darauf zugreifen.

Da du nicht immer Zugriff auf diesen Stick hast, sind Backups nicht so oft möglich wie auf dem ersten. Dennoch sollte dieser Stick mindestens alle zwei Monate aktualisiert werden.

Backups in der Cloud, wie sie von OneDrive oder Apple iCloud angeboten werden, solltest du vermeiden. Da sie jedoch einfacher zu handhaben sind, wäre ein Kompromiss, dein Backup in einem VeraCrypt-Container zu verschlüsseln und dann nur diesen hochzuladen. Am besten verwendest du dafür die ProtonCloud.

• • •

In diesem Kapitel haben wir unsere Accounts mit sicheren Passwörtern sowie der Zwei-Faktor-Authentifizierung (2FA) gesichert. Das heißt das vor jedem Account ein einzigartiges, zufällig generiertes Passwort ist sowie eine 2FA durch EnteAuth. Damit ist die Angriffsfläche enorm minimiert. Darüber hinaus haben wie verschiedene verschlüsselte Backups wichtiger Daten erstellt, auf dem Computer sowie auch auf anderen Speichermedien. Im Notfall können wir darauf zugreifen, während sie gleichzeitig vor unbefugtem Zugriff geschützt sind. Im nächsten Kapitel geht es dann um einen weiteren unverzichtbaren Bereich in unserem digitalen Alltag sichere und private Kommunikation.

Kapitel 5
Private Kommunikation

„In der digitalen Welt sind wir alle nur einen Klick voneinander entfernt." ~ *James H. Fowler*

In den letzten Jahren haben wir einen erheblichen Wandel in unserer Kommunikation erlebt – weg von persönlichen Gesprächen hin zur digitalen Welt. Dies führt dazu, dass auch unsere privaten, sensiblen Unterhaltungen mit Freunden, Anwälten und Ärzten zunehmend auf Online-Kommunikationsdiensten stattfinden.

Insbesondere im Jahr 2020, beeinflusst durch die Lockdowns, stieg die Nutzung von Online- und Videokommunikationssoftware signifikant an. Beispielsweise erhöhte sich die Nutzung von Zoom von 16 % im Februar 2020 innerhalb von nur sieben Monaten auf 49 %. Eine weitere Studie aus demselben Jahr ergab, dass 43 % der Befragten digitale Treffen mit Freunden und Familie als festes Ritual etabliert haben. [7]

Diese Entwicklung geschieht nicht ohne Grund, denn digitale Kommunikation ist deutlich schneller, effizienter und einfacher als persönliche Treffen. Doch damit einher geht das Problem, dass das gesamte Internetzugang zu unseren privaten Gesprächsinformationen erhalten könnte. Um sicherzustellen, dass deine sensiblen Gespräche trotz digitaler Kommunikation geschützt bleiben, werden wir in diesem Kapitel sichere und private E-Mail-Dienste, Telefonnummern und Messengerdienste näher betrachten.

E-Mail

E-Mails sind heutzutage ein unverzichtbarer Bestandteil unseres Alltags. Daher ist es umso wichtiger, einen sicheren und datenschutzfreundlichen Anbieter zu wählen. Viele der großen, bekannten E-Mail-Dienste wie Google, Yahoo oder Microsoft bieten ihre Dienste zwar kostenlos an, doch wie das Sprichwort sagt: „Wenn

etwas kostenlos ist, bist du das Produkt.“ Das bedeutet, dass wir im Gegenzug zur kostenlosen Nutzung den Unternehmen erlauben, unsere persönlichen Daten zu sammeln und diese für gezielte Werbung oder sogar den Weiterverkauf an Dritte zu verwenden. Nachfolgend werden einige Beispiele angeführt.

- Google integriert zunehmend mehr Werbung in die Postfächer – teils ohne klare Kennzeichnung als solche.
- Gmail gewährte Unternehmen und Regierungen Zugriff auf die E-Mails von Nutzern.
- Google speichert Kaufdaten aus E-Mails, um gezielte Werbung zu schalten.
- Yahoo erlaubt Werbefirmen, E-Mails algorithmisch zu scannen, um potenzielle Kunden anhand ihrer Kaufgewohnheiten zu finden.
- Yahoo scannt E-Mails in Echtzeit für US-Geheimdienste.
- Bei Datenleaks wurden 500 Millionen Yahoo-Accounts veröffentlicht.
- Ein Yahoo-Mitarbeiter wurde erwischt, als er Nutzerkonten an Kriminelle verkaufte.

Da der durchschnittliche Mensch mehr als 15 Stunden pro Woche mit der Verwaltung von privaten und beruflichen E-Mails verbringt, ist es umso wichtiger, einen sicheren und datenschutzfreundlichen E-Mail-Anbieter zu wählen. In den folgenden Abschnitten präsentiere ich eine E-Mail-Strategie, die ich selbst anwende und auch meinen Kunden empfehle. Diese Strategie ist selbstverständlich nicht verpflichtend, und es gibt zahlreiche Ansätze, um den E-Mail-Verkehr sicherer zu gestalten. Dennoch ist es entscheidend, die grundlegenden Prinzipien im Blick zu behalten.

ProtonMail

ProtonMail ist ein in der Schweiz ansässiger E-Mail-Dienst, der sich in der Datenschutz-Community einen hervorragenden Ruf erarbeitet hat. Nach der Gründung 2014 wurde Proton schnell als der einzige E-Mail-Anbieter, auf den die NSA keinen Zugriff hat, bekannt. [8]

Was ProtonMail besonders macht, ist seine offene und transparente Plattform (Open Source). Das bedeutet, dass der Programmcode öffentlich einsehbar ist und von unabhängigen Experten geprüft wurde. ProtonMail verwendet standardmäßig starke Verschlüsselungstechniken, sodass alle Nachrichten und Anhänge verschlüsselt auf Servern in der Schweiz gespeichert werden. Einfach gesagt: Selbst wenn jemand Zugang zu den Servern hätte, könnte er ohne den passenden Schlüssel nichts lesen. Zudem bietet ProtonMail eine Ende-zu-Ende-Verschlüsselung an. Das bedeutet, dass nur Sender und Empfänger die Nachrichten lesen können – keine Mitarbeiter, Dritte und nicht einmal ProtonMail selbst hat Zugriff darauf. Für alle, die Wert auf Privatsphäre legen und sicherstellen möchten, dass ihre Kommunikation vertraulich bleibt, ist das ein entscheidendes Merkmal. Selbst bei Gerichtsbeschlüssen können keine persönlichen Daten preisgegeben werden, und im Falle eines Datenlecks bleibt nur unleserlicher, verschlüsselter Datenmüll zurück.

ProtonMail bietet einen kostenlosen Account an, der eine E-Mail-Adresse, 1 GB Speicherplatz und den Versand von maximal 150 E-Mails pro Tag umfasst. Darüber hinaus gibt es kostenpflichtige Tarife: „Mail Plus“ für 3,99 € pro Monat (10 E-Mail-Adressen, 15 GB Speicherplatz, 10 E-Mail-Aliase und die Nutzung einer eigenen Domain) sowie „Unlimited“ mit noch mehr Optionen für 9,99 € monatlich. Für die meisten Nutzer dürfte „Mail Plus“ vollkommen ausreichend sein.

Es ist ratsam, ProtonMail nicht lediglich mit einem Alias zu nutzen, da dein echter Name irgendwann mit dem Account verknüpft wird – sei es im beruflichen Kontext oder im Austausch mit Freunden und Familie. Deshalb empfehle ich, gleich eine neue „echte“ E-Mail-Adresse bei ProtonMail anzulegen, z. B. max.mustermann@protonmail.com.

Ein kostenloser ProtonMail-Account stellt bereits eine deutliche Verbesserung im Vergleich zu Google, Microsoft und Co. dar. Wenn du jedoch maximale Sicherheit und Privatsphäre wünschst, solltest du auf einen kostenpflichtigen Account zurückgreifen. Es besteht auch die Möglichkeit, mehrere kostenlose Proton-Accounts für verschiedene Zwecke zu erstellen. Allerdings muss man sich für jedes

Konto separat anmelden, und dies verstößt gegen die Nutzungsbedingungen von ProtonMail. Daher empfehle ich, die 48 € pro Jahr zu investieren, um die empfohlene E-Mail-Strategie zu implementieren:

vorname.nachname@protonmail.com: Diese E-Mail-Adresse, die deinen Klarnamen enthält, ist für die Kommunikation mit engen Kontakten gedacht, die dich persönlich kennen – also Familie, Freunde und andere Vertraute. Früher oder später wird diese Adresse auch in den Datenbanken von Unternehmen landen, die Datamining betreiben. Das lässt sich leider nicht verhindern, wenn wir E-Mail nutzen. Diese Adresse verwenden wir auch für die Anmeldung bei ProtonMail.

- Besuche dafür die Webseite von ProtonMail unter mail.proton.me und klicke auf „Create a free account“. Hier kannst du einen Tarif auswählen.
- Gebe nach der Tarifauswahl eine E-Mail-Adresse und ein sicheres Passwort ein. Es macht Sinn, hier eine Adresse mit deinem Klarnamen zu verwenden, etwa max.mustermann@protonmail.com. Proton schlägt standardmäßig die Domain @proton.me vor, doch ich empfehle, rechts neben dem Benutzernamen auf @protonmail.com zu wechseln, da .com-Adressen weniger Aufsehen erregen als .me. Generiere das Passwort am besten von einem Passwortmanager.
- Jetzt musst du eine E-Mail-Adresse zur Verifizierung angeben. Hide-my-E-mail-Aliase funktionieren hier nicht, also gebe einfach deine bisherige E-Mail-Adresse an, z. B. die von Google. Es mag widersprüchlich klingen, mehr Daten anzugeben, um ein privates E-Mail-Konto zu erhalten, aber das betrachte ich als unbedenklich. ProtonMail wird ohnehin deinen echten Namen erhalten, und da wir später alle alten E-Mails in das neue ProtonMail-Konto weiterleiten, hat es keine Nachteile, diese E-Mail für die Verifizierung zu nutzen.
- Gib den Code ein, der dir per E-Mail zugesandt wird, und klicke auf „Verify“.
- Jetzt kannst du den Namen festlegen, der den Empfängern deiner E-Mails angezeigt wird. Da diese Adresse für

Personen gedacht ist, die dich persönlich kennen, trage hier bitte deinen Klarnamen (Vorname und Nachname) ein und klicke anschließend auf „Continue“.
- Im nächsten Schritt hast du die Möglichkeit, optional eine Telefonnummer oder eine E-Mail-Adresse anzugeben, um die Sicherheit deines Accounts zusätzlich zu erhöhen.
- Überspringe diesen Schritt, indem du auf „Maybe later“ und dann „Confirm“ klickst.

Du hast jetzt einen sicheren neuen E-Mail-Account mit deinem Klarnamen, wie beispielsweise *max.mustermann@protonmail.com*, und dem Anzeigenamen *Max Mustermann*. ProtonMail bietet von Anfang an ein hohes Maß an Sicherheit und Datenschutz. Mit einigen zusätzlichen Einstellungen können wir diese jedoch noch weiter optimieren.

- Klicke oben rechts auf das Zahnradsymbol und wähle „Alle Einstellungen“.
- Klicke im Menü auf „Wiederherstellung“ und aktiviere unter „Datenwiederherstellung“ die Option „Wiederherstellung per Wiederherstellungsphrase zulassen“.
- Dadurch werden dir 12 Wörter generiert, mit denen du deinen Account wiederherstellen kannst, falls du dein Passwort oder den Zugang zur Zwei-Faktor-Authentifizierung (2FA) verlierst.
- Bewahre diese Wörter sicher auf, denn jeder, der sie besitzt, hat vollen Zugriff auf deinen Account.
- Wähle im linken Menü den Punkt „Konto und Passwort“ aus und aktiviere entweder die „Authenticator-App“, falls du eine 2FA-App wie EnteAuth nutzt, oder den „Sicherheitsschlüssel“, wenn du beispielsweise einen YubiKey verwendest. Gib dein Passwort erneut ein, klicke auf „Weiter“, scanne den QR-Code mit der Authenticator-App und gib den generierten Code ein.
- Gehe weiter zu „Sicherheit und Datenschutz“ und deaktiviere unten bei „Privatsphäre und Datenerfassung“ beide Optionen.

- Deaktiviere unter „Nachrichten und verfassen“ die Option „Eingebettete Bilder automatisch anzeigen“ und aktiviere die Funktion „Link-URLs bestätigen“.
- Gehe als Nächstes zu „E-Mail Datenschutz“ und deaktiviere dort „Bilder aus externen Quellen automatisch anzeigen“.

Mit diesen Schritten sind deine Sicherheits- und Datenschutzeinstellungen optimiert und wir können nun mit der Umsetzung unserer E-Mail-Strategie beginnen.

Weitere E-Mail-Adressen

Anstatt jedem deine persönliche E-Mail-Adresse zu geben, werden wir als Nächstes verschiedene E-Mail-Adressen für unterschiedliche Zwecke einrichten. Das erhöht nicht nur deine Privatsphäre, sondern auch deine Sicherheit.

- Wähle links den Menüpunkt „Identität und E-Mail-Adressen“. Wenn du einen kostenpflichtigen Plan hast, kannst du hier neue E-Mail-Adressen hinzufügen.
- Klicke dafür auf „Add address“ und trage eine neue E-Mail-Adresse sowie den gewünschten Anzeigenamen ein.
- Auch hier empfehle ich, für alle neuen Adressen die Domain @protonmail.com an Stelle der anderen Optionen zu verwenden.
- Der Anzeigename unter „Display name“ wird denjenigen angezeigt, die an diese E-Mail-Adresse schreiben oder von ihr Nachrichten erhalten. Den Anzeigenamen solltest du passend zur jeweiligen Adresse wählen.

name.xxx@protonmail.com: Diese E-Mail-Adresse, die ebenfalls deinen Klarnamen enthalten kann, eignet sich für den Kontakt mit Personen oder Institutionen, die deinen Namen kennen, aber zu denen du keine so enge Beziehung hast, dass du deine „Haupt-E-Mail-Adresse“ verwenden möchtest. Dazu zählen beispielsweise Arbeitskollegen, staatliche Stellen oder Dienstleister, die eine offizielle E-Mail-Adresse mit Klarnamen benötigen. Diese E-Mail bietet eine gute Balance hinsichtlich Privatsphäre und Formalität. Als Anzeigename ist ebenfalls der volle Vor- und Nachname zu empfehlen, um

Glaubwürdigkeit zu vermitteln – etwa mustermann.this@protonmail.com mit dem Anzeigenamen „Max Mustermann“.

aliasname@protonmail.com: Diese E-Mail-Adresse basiert auf einem Alias, also einer angenommenen Identität. Sie dient dazu, deine wahre Identität zu schützen, während du dennoch seriös und formell auftreten kannst. Mehr zu dieser Strategie findest du in Kapitel 7, „Aliase“. Der Anzeigename sollte natürlich zur Alias-Persönlichkeit passen. Ein Beispiel wäre *max.maier@protonmail.com* mit dem Anzeigenamen *Max Maier*.

wort.123@protonmail.com: Diese E-Mail-Adresse hat keinerlei Verbindung zu deinem Klarnamen und kann für vielfältige Zwecke genutzt werden, bei denen du deine echte Identität nicht preisgeben möchtest. Ich nutze diese Art von Adresse vor allem für Online-Konten, die häufig verwendet werden, aber nicht mit meinem echten Namen in Verbindung stehen sollen. Achte darauf, dass der Anzeigename nicht auf deine echte Identität hinweist. Ein Beispiel für die E-Mail ist ananas9821@protonmail.com mit dem Anzeigenamen „Ananas“ sein.

bestellungen@protonmail.com: Diese E-Mail-Adresse, ebenfalls ohne Bezug zu deinem echten Namen, wird ausschließlich für Online-Käufe und Bestellungen genutzt. Sie wird höchstwahrscheinlich in Datenbanken landen und möglicherweise auch Spam oder Werbung erhalten – genau dafür ist sie gedacht. Deine „echte“ E-Mail-Adresse und dein Klarname werden dadurch nicht mit den Einkäufen verknüpft. Auch hier sollte der Anzeigename allgemein gehalten sein, um keine Rückschlüsse auf deine Identität zuzulassen. Ein Beispiel wäre bestellungen9821@protonmail.com mit dem Anzeigenamen „Purchases“ oder „Käufe und Bestellungen“.

nachname.finanzen@protonmail.com: Diese E-Mail-Adresse, die deinen Klarnamen enthält, ist, wie der Name schon sagt, ausschließlich für den Kontakt mit Finanzdienstleistern vorgesehen. Dazu zählen Banken, Kreditkartenanbieter und Broker – alles, was mit Geld zu tun hat. Der Vorteil dieser separaten E-Mail ist, dass selbst im Falle eines Leaks deiner anderen E-Mail-Adressen keine Verbindung zu deinen Finanzkonten hergestellt werden kann. Diese

Adresse wird nicht für den allgemeinen E-Mail-Verkehr genutzt, sondern nur für wichtige Finanzgeschäfte. Auch hier ist es ratsam, den vollen Klarnamen als Anzeigenamen zu verwenden, um eventuelle Rückfragen der Banken zu vermeiden – etwa mustermann.finanzen@protonmail.com mit dem Anzeigenamen „Max Mustermann".

Wir sollten ab sofort die neuen E-Mail-Adressen für die Erstellung neuer Konten verwenden. Gleichzeitig ist es sinnvoll, unsere alten Accounts schrittweise von den bisherigen E-Mail-Adressen auf die neuen Adressen umzustellen. Ähnlich wie bei Passwörtern wäre es zu aufwendig, alle Adressen auf einmal zu ändern. Daher empfehle ich, die E-Mail-Adresse immer dann zu aktualisieren, wenn du dich bei einer Seite oder einem Konto mit der alten E-Mail-Adresse anmeldest – ändere die Adresse dann direkt auf eine der neu erstellten, die für diesen Zweck vorgesehen sind.

Alternativen zu ProtonMail

Natürlich gibt es auch andere Anbieter neben ProtonMail. Persönlich bevorzuge ich ProtonMail, da viele meiner Kontakte diesen Dienst nutzen und ich bei meinen Kunden die beste Akzeptanzrate erlebe, da die Benutzerfreundlichkeit außergewöhnlich gut ist. Andere Dienste scheinen in Bezug auf Benutzerfreundlichkeit und Design etwas hinter ProtonMail zurückzubleiben. Allerdings gibt es auch in der Privacy-Community Stimmen, die ProtonMail kritisch betrachten und aufgrund seiner weiten Verbreitung als potenziellen „Honeypot" ansehen – also einen Dienst, bei dem es viel zu gewinnen gäbe, sollte er gehackt werden. Wenn du eine Alternative suchst, kann ich Tutanota empfehlen.

Tuta Mail (tuta.com) ist ein in Hannover ansässiger, datenschutzorientierter E-Mail-Anbieter, der ähnliche Funktionen wie ProtonMail bietet. Dazu gehören Ende-zu-Ende-Verschlüsselung für E-Mails zwischen Nutzern, die Möglichkeit, verschlüsselte E-Mails auch an andere Empfänger zu senden, Open-Source-Software, keine Datensammlung oder -weitergabe, sowohl kostenlose als auch kostenpflichtige Tarife, die Nutzung eigener Domains sowie Zwei-Faktor-Authentifizierung (2FA) und Zero-Knowledge-Sicherheit. Im Grunde bietet Tuta auch alle Vorteile von ProtonMail.

Die meisten in diesem Kapitel beschriebenen Schritte zur Erstellung und Sicherung von E-Mail-Adressen können auch bei Tuta Mail angewendet werden.

E-Mail-Import und Weiterleitung

Viele Menschen machen beim Umstieg auf einen sicheren E-Mail-Anbieter wie ProtonMail denselben Fehler: Sie installieren ProtonMail und nutzen es für neue E-Mails, greifen jedoch immer wieder auf ihr altes Postfach zurück, um wichtige Nachrichten zu lesen oder neue E-Mails zu sehen, die weiterhin an die alte Adresse gesendet werden.

Um genau das zu vermeiden, zeige ich dir, wie du eine Weiterleitung einrichtest, sodass neue E-Mails von deinem alten Anbieter direkt in dein ProtonMail-Postfach weitergeleitet werden. Außerdem erkläre ich dir, wie du alle bisherigen E-Mails vom alten Anbieter nach ProtonMail importieren kannst, damit du sie an einem sicheren Ort gesammelt einsehen kannst.

E-Mail-Weiterleitung: Ähnlich wie beim Wechsel einer Telefonnummer ist es oft schwierig, alle Personen sofort über die neue E-Mail-Adresse zu informieren. Daher kann es vorkommen, dass du auch Jahre später noch E-Mails an die alte Adresse erhältst. Aus diesem Grund empfehle ich, alte E-Mail-Accounts niemals zu löschen. Stattdessen richten wir eine automatische Weiterleitung ein, sodass neue E-Mails direkt in dein ProtonMail-Postfach gelangen.

Nach der Einrichtung musst du dich um den alten Account nicht mehr kümmern. Die meisten großen Anbieter ermöglichen eine solche Weiterleitung, sodass du dich nicht mehr in deinen alten Account einloggen musst. Du kannst zwar keine E-Mails vom alten Account aus senden, aber das ist auch nicht das Ziel – ab jetzt soll die gesamte Kommunikation über ProtonMail erfolgen.

Hier sind die Schritte für die bekanntesten E-Mail-Anbieter. Falls dein Anbieter nicht aufgeführt ist, findest du im Internet durch eine kurze Suche eine passende Anleitung.

Gmail:

- Öffne dein Gmail-Postfach und klicke auf das Zahnrad-Symbol, dann auf „Alle Einstellungen anzeigen“.
- Unter dem Punkt „Weiterleitung und POP/IMAP“ findest du den Abschnitt „Weiterleitung“ und klicke dort auf „Weiterleitungsadresse hinzufügen“.
- Gib deine ProtonMail-Adresse ein.
- Es wird eine Bestätigungsmail an ProtonMail geschickt, der du durch Klicken auf den Link entsprechen musst.
- Gehe danach zurück zu Gmail und wähle die Option „Weiterleitung einer Kopie eingehender Nachrichten an …“.
- Stelle ein, dass keine Kopie im Gmail-Postfach verbleiben soll.

Outlook/Hotmail:

- Öffne dein Outlook-Postfach, klicke auf das Zahnrad und wähle „Alle Outlook-Einstellungen anzeigen“.
- Navigiere unter „E-Mail“ zum Abschnitt „Weiterleitung“.
- Aktiviere „Meine E-Mails weiterleiten an“ und gib deine ProtonMail-Adresse ein.
- Wähle aus, dass keine Kopie behalten werden soll, und klicke auf „Speichern“.

GMX:

- Gehe in dein GMX-Postfach, klicke auf das Zahnrad-Symbol und wähle „Einstellungen“.
- Wähle unter „E-Mail“ den Punkt „Filterregeln“ und erstelle eine „Neue Filterregel“.
- Wähle bei „Bedingung“ den Punkt „Alle neuen E-Mails“.
- Wähle unter „Aktion“ die Option „Weiterleiten an“ und gebe deine ProtonMail-Adresse ein.
- Speichere die Einstellung.

E-Mail-Archiv: Wahrscheinlich hast du im Laufe der Jahre viele wichtige E-Mails in deinem alten Postfach gesammelt – Nachrichten mit bedeutenden Daten, wertvollen Bildern oder Bestätigungen von erstellten Konten. All dies sollte sicher an einem Ort gespeichert werden. Daher ist es wichtig, deine bisherigen E-Mails nach ProtonMail zu importieren.

- Gehe dazu in deine ProtonMail-Einstellungen und wähle den Punkt „Import via Easy Switch“ aus.
- Wähle dort deinen E-Mail-Anbieter aus und befolge die Schritte.

Sobald du alle Mails erfolgreich importiert hast, kannst du die Nachrichten beim alten Anbieter löschen, um sie vor Datenlecks zu schützen.

E-Mail-Backups

Backups sind in jedem Bereich von großer Bedeutung – besonders wenn es um E-Mails geht. Denk einmal darüber nach, wie viele wichtige Dinge mit deiner E-Mail-Adresse verknüpft sind: unzählige Konten, wichtige Konversationen und Dateien. Du solltest dich niemals ausschließlich auf den Anbieter verlassen, sondern immer einen Plan B haben. Auch wenn viele nicht daran denken, ist es unerlässlich, regelmäßig die eigenen E-Mails zu sichern. ProtonMail bietet hierfür ein spezielles Export-Tool an.

- Lade dieses von der ProtonMail-Webseite herunter: proton.me/support/export-emails-import-export-app
- Öffne die Import und Export-App und logge dich mit deinem ProtonMail-Account ein.
- Jetzt solltest du deine E-Mail-Konten sehen. Du kannst entweder alle Mails zusammen exportieren oder nur einzelne Mails auswählen.
- Um alle Mails zu exportieren, klicke auf „Export all“ bei deiner Hauptadresse.
- Auf der nächsten Seite kannst du angeben, was genau exportiert werden soll. Die Standardeinstellungen sind meistens ausreichend.
- Ändere noch das Dateiformat auf „EML“ und wähle den Ordner aus, in dem das Backup gespeichert werden soll (z.B. auf einem USB-Stick).
- Bestätige mit „Export“. Beim ersten Mal kann das etwas dauern, aber bei regelmäßigen, monatlichen Backups geht es deutlich schneller.

Ab sofort sollte dein ProtonMail-Account als primärer und einziger E-Mail-Account verwendet werden. Alle ausgehenden Kommunikationen sowie eingehenden Mails laufen über diesen Account. Den alten Account (egal ob Gmail, Outlook usw.) solltest du zwar nicht löschen, aber es besteht kein Grund mehr, dich dort einzuloggen – bereits beim Einloggen sammeln diese Anbieter viele Daten wie deine IP-Adresse oder deinen Standort.

E-Mail-Aliase

Eine effektive Methode, um deine E-Mails zu schützen, besteht darin, für jeden neuen Account eine eigene E-Mail-Adresse zu verwenden. So wird bei einem Datenleck nicht deine Hauptadresse kompromittiert, sondern nur eine einmalig genutzte Adresse, die speziell für diesen einen Account erstellt wurde.

Jedes Mal, wenn du dich auf einer neuen Webseite anmeldest und eine E-Mail-Adresse angeben musst, verwendest du einfach eine neu erstellte Adresse, die beispielsweise den Namen der Seite enthält. Wichtig ist, dass du diese Adresse mit niemandem teilst und ausschließlich für diesen spezifischen Account verwendest. Falls du dann unerwünschte E-Mails an diese Adresse erhältst, weißt du, dass das Unternehmen, dem du die Adresse gegeben hast, entweder deine Daten weitergegeben hat oder gehackt wurde. Ein weiterer Vorteil ist, dass Hacker oft den Versand von Spam an Alias-E-Mails vermeiden, da diese Nutzer in der Regel mehr über Datenschutz wissen und Spam daher eher melden.

Das klingt vielleicht komplizierter, als es ist. Du musst nicht jedes Mal einen komplett neuen Account erstellen. Es gibt einfache und praktische Möglichkeiten, E-Mail-Aliase zu nutzen.

Plus-Alias (emailadresse+wort@protonmail.com): Diese Methode ist kostenlos und sehr einfach, jedoch nicht die effektivste. Du kannst durch Anhängen von „+wort“ vor dem „@protonmail.com“ unendlich viele Aliase erstellen. Dabei musst du nichts in den Einstellungen ändern und kannst direkt loslegen. Allerdings sehen sowohl Unternehmen als auch Hacker, dass du ein Alias verwendest,

und könnten einfach das „+wort“ entfernen, um auf deine eigentliche E-Mail-Adresse zuzugreifen.

Daher bietet diese Variante nur begrenzten Schutz und wird oft ignoriert. Tatsächlich waren laut einer Analyse von „Have I Been Pwned“ nur 0,03 % der über eine Milliarde durchgesickerten Datensätze mit Plus-Aliassen verknüpft. Ich empfehle daher, die folgende Methode zu wählen.

Hide-my-E-mail-Alias: Diese Methode verbirgt deine E-Mail-Adresse vollständig. Unternehmen und Hacker sehen lediglich eine zufällig generierte Adresse wie „amazon.4jb55@passmail.com“, die alle Nachrichten an deine eigentliche Adresse weiterleitet, ohne dass das Unternehmen weiß, welche das ist. Hacker haben somit keine Möglichkeit, die wahre Adresse zu erfahren. Ein Dienst wie SimpleLogin bietet dir 10 kostenlose Alias-Adressen an. Das kannst du wie folgt einrichten.

- Besuche die Webseite simplelogin.io und registriere dich über die Funktion „Signup“. Nutze am besten eine anonyme E-Mail-Adresse, z. B. „wort.123@protonmail.com“. Vermeide es, deinen Hauptaccount bei ProtonMail zu verwenden, um SimpleLogin keine Informationen über deine tatsächliche Identität zu geben.
- Nach der Anmeldung solltest du umgehend die Zwei-Faktor-Authentifizierung (2FA) aktivieren. Klicke dazu oben links auf dein Kontosymbol und wähle „Kontoeinstellungen“. Dort hast du die Möglichkeit, die 2FA zu aktivieren.
- Klicke dann auf „+ New Custom Alias“. Im Feld „Alias Prefix“ kannst du beispielsweise „amazon“ eintragen, wenn diese E-Mail nur für deinen Amazon-Account gedacht ist. Alternativ kannst du eine zufällige Zeichenfolge wählen, um noch anonymer zu bleiben.
- Neben den 10 Alias-Adressen von SimpleLogin bietet auch ProtonMail in seinem Mail Plus-Abonnement 10 weitere Aliase an und im Unlimited-Abonnement sogar unbegrenzt viele.
- Öffne dafür die Seite mail.proton.me/u/0/inbox.

- Klicke rechts in der Seitenleiste auf das lilafarbene Schildsymbol.
- Wähle unter dem Reiter „Hide-my-E-Mail alias“, den Punkt „New Alias“ aus.
- Hier kannst du einen Namen wie „amazon“ eintragen, um den Überblick zu behalten.

Achtung
Verwende Alias-E-Mails ausschließlich für weniger wichtige Accounts, etwa für Newsletter oder weniger sensible Anmeldungen. Für wichtige Angelegenheiten, wie Bankkonten oder geschäftliche Kontakte, solltest du immer deine Hauptadresse verwenden.

Sollte ein Dienst wie SimpleLogin eines Tages eingestellt werden, verlierst du den Zugang zu allen mit den Alias-Adressen verknüpften Accounts. Wenn du feststellst, dass Anbieter wie Amazon oder Google SimpleLogin-Aliase blockieren, kannst du auf ProtonMail-Aliase zurückgreifen, die nach meiner Erfahrung stets akzeptiert wurden.

Wegwerf-E-Mail-Adressen: Wegwerf-E-Mails sind eine effektive Methode, deine Privatsphäre zu schützen und Spam zu vermeiden.

Diese Adressen werden temporär erstellt und nach kurzer Zeit wieder gelöscht. Sie sind nützlich, wenn du beispielsweise einen Bestätigungscode erhalten musst, um einen Blogartikel zu lesen, oder dich einmalig irgendwo anmelden möchtest, ohne deine echte Adresse anzugeben.

Gehe dafür auf eine der folgenden Seiten und lasse dir eine temporäre Adresse generieren.

- tempmail.email
- www.throwawaymail.com
- temp-mail.io/de

Achtung
Wenn du das Fenster mit der Wegwerf-E-Mail schließt, verlierst du den Zugang zu dieser Adresse. Verwende solche E-Mails daher nur für einmalige Zwecke und niemals für Accounts, auf die du später noch zugreifen möchtest.

Viele Anbieter blockieren außerdem Wegwerf-E-Mails, aber mit etwas Ausprobieren findest du oft eine, die funktioniert.

Weitere Ideen

Wir verlassen uns derzeit vollständig auf ProtonMail. Sollte jedoch dein Account gesperrt oder gelöscht werden, ginge der Zugang zu deiner gesamten E-Mail-Kommunikation verloren. Auch wenn ich dieses Risiko als gering einschätze, gibt es viele, die auf Nummer sicher gehen möchten. Hier kommt eine eigene Domain ins Spiel.

Mit einem kostenpflichtigen ProtonMail-Abo kannst du deine eigene Domain einrichten. Diese ermöglicht es dir, unabhängig von ProtonMail zu sein. Du kaufst einfach eine eigene Domain, registrierst sie bei ProtonMail und verwendest sie, um E-Mails zu senden und zu empfangen. Anstelle von @protonmail.com nutzt du dann @meinedomain.de.

Der Vorteil: Solltest du den Zugang zu deinem ProtonMail-Account verlieren, kannst du deine Domain problemlos mit einem anderen E-Mail-Anbieter verbinden und behältst weiterhin Zugriff auf deine E-Mails. So schaffst du nicht nur eine sichere und anonyme E-Mail-Strategie, sondern hast auch einen zusätzlichen Plan B, um deine Kommunikation langfristig abzusichern.

Fassen wir unsere E-Mail-Strategie noch einmal zusammen: Wir haben nun persönliche und anonyme E-Mails in unserem ProtonMail-Account. Insgesamt verfügen wir über sechs verschiedene E-Mail-Adressen, die jeweils für einen bestimmten Zweck gedacht sind. Dadurch können wir unser digitales Leben besser organisieren und unsere Sicherheit erhöhen.

Zusätzlich nutzen wir E-Mail-Aliase und Wegwerf-Adressen. Mit diesen Methoden verfügst du über verschiedene Möglichkeiten, deine Privatsphäre im Umgang mit E-Mails zu wahren und dich vor Datenlecks zu schützen. Ein cleverer Mix aus anonymen Alias-Adressen, temporären Wegwerf-E-Mails und deinen Hauptadressen sorgt dafür, dass du die Kontrolle über deine Daten behältst und nur so viel preisgibst, wie du möchtest.

Neben E-Mails sind für uns auch Telefonate von hoher Relevanz. Ohne eine Telefonnummer wäre man aufgeschmissen. Im nächsten Abschnitt schauen wir uns an, wie wir diese so sicher und privat wie möglich nutzen können.

Telefonnummern und SMS

Ähnlich wie bei E-Mail-Adressen ist es auch bei Telefonnummern vorteilhaft, mehrere zu besitzen. Dies gestaltet sich jedoch nicht so einfach wie bei ProtonMail, da du für jede neue Nummer eine separate SIM-Karte benötigst. In den USA sind VoIP-Dienste (Voice-over-IP) sehr verbreitet. Diese ermöglichen es, ganz ohne SIM-Karte auszukommen, denn alles basiert, wie der Name schon sagt, auf der Internetverbindung. Dadurch kannst du mehrere Telefonnummern erstellen und auf verschiedenen Geräten nutzen.

Leider gibt es in Deutschland nicht viele Anbieter, die solche Dienste anbieten. Ohne VoIP wird es etwas aufwendiger, da jede zusätzliche Nummer eine eigene SIM-Karte erfordert, die du dann auch häufig benötigst. Ich empfehle, mindestens zwei verschiedene Nummern zu haben, aber je nach Bedarf können auch mehr Nummern für unterschiedliche Zwecke sinnvoll sein.

Persönliche Nummer: Diese Nummer wird für die tägliche Kommunikation mit deinen Kontakten verwendet. Die zugehörige SIM-Karte befindet sich im Handy, sodass du jederzeit Anrufe und SMS empfangen kannst. Diese Nummer hast du wahrscheinlich schon lange und sie ist vermutlich in mehreren Datenbanken mit deinem echten Namen verknüpft – bei Freunden, am Arbeitsplatz und bei

verschiedenen Institutionen. Daher ist es gut möglich, dass auch persönliche Daten damit verbunden sind.

Account-Nummer: Die zweite Nummer, die ich empfehle, dient der Sicherung wichtiger Konten. Hierfür eignet sich eine kostengünstige Prepaid-Karte, die alle sechs Monate mit einem kleinen Betrag aufgeladen wird, um aktiv zu bleiben. Diese Nummer wird nicht für die Kommunikation genutzt, sondern ausschließlich für sicherheitsrelevante Konten, z. B. bei Banken oder wichtigen Online-Diensten. Die SIM-Karte wird nur ins Handy eingelegt, wenn ein Bestätigungscode benötigt wird. Der Grund für diese Vorsichtsmaßnahme ist die Gefahr von Betrugsversuchen wie SIM-Swapping, bei dem Kriminelle versuchen, die Kontrolle über deine Telefonnummer zu erlangen. Wenn niemand diese Nummer kennt, erhöht das die Sicherheit erheblich.

Optional: Wegwerfnummer: Dies ist eine wichtige Sicherheitsmaßnahme, die viel Ärger ersparen kann. Früher oder später wird ein Unternehmen deine Telefonnummer weitergeben oder es kommt zu einem Datenleck, wodurch deine Nummer in Werbe- oder Spamdatenbanken landet. Um dem vorzubeugen, gibt es die Möglichkeit, eine Wegwerfnummer zu verwenden, die ähnlich wie eine Wegwerf-E-Mail funktioniert. Diese wird für unwichtige Online-Konten oder Bestellungen genutzt, sodass Werbung und Spam auf die Wegwerfnummer reduziert werden, während deine persönliche Nummer unberührt bleibt.

Optional: Alias-Nummer: Für diejenigen, die einen Schritt weiter gehen möchten, kann es sinnvoll sein, eine zusätzliche Nummer für den Alias (siehe Kapitel 7, „Aliase“) zu verwenden. Dadurch lässt sich die Kommunikation klarer trennen: Freunde und Familie haben die echte Nummer, während für alle anderen der Alias genutzt wird.

Optional: Arbeitsnummer: Eine Arbeitsnummer ist weit verbreitet und wird häufig zusammen mit einem Diensthandy genutzt. Der Vorteil ist, dass Arbeitgeber und Kollegen nicht die private Nummer kennen, was es erleichtert, Berufliches und Privates voneinander zu trennen.

Allerdings benötigen die meisten von uns keine so detaillierte Aufteilung und können Zeit und Geld in andere Sicherheitsmaßnahmen investieren. Wichtig ist, sich zu überlegen, vor welchen Bedrohungen man sich schützen möchte und wie viel Aufwand man dafür zu betreiben bereit ist.

Anonyme Nummern

KYC (Know Your Customer)
KYC ist der Prozess zur Überprüfung der Identität von Kunden, um Betrug und Geldwäsche zu verhindern. Dieser Prozess umfasst die Prüfung von Ausweisdokumenten sowie persönlichen Daten.

In Deutschland ist es erforderlich, sich bei der Registrierung einer SIM-Karte vollständig zu identifizieren (KYC-Verfahren). Dies bringt einige Nachteile mit sich.

- Alle Anrufe und Nachrichten sind mit deiner eigenen Identität verknüpft.
- Die gesamte Nutzungshistorie der Nummer kann bei rechtlichen Anfragen oder durch Mitarbeiter des Anbieters abgerufen werden.
- Jedes Gerät, das mit dieser SIM-Karte verwendet wird, ist ebenfalls an deine Identität gebunden.
- Accounts, die mit dieser Nummer erstellt werden, sind ebenfalls mit deiner persönlichen Identität verknüpft.
- Der Standort des Geräts wird durch die Verbindung zu Mobilfunkmasten erfasst und gespeichert; diese Daten können ebenfalls bei einer Anfrage von Gerichten offengelegt werden.

Deshalb wäre es ideal, eine Telefonnummer zu verwenden, bei deren Registrierung keine vollständige Identifizierung erforderlich ist – eine sogenannte anonyme Nummer.

Es gibt Anbieter, die bereits vorregistrierte deutsche SIM-Karten verkaufen, die auf fiktive Personen wie „Max Huber“ ausgestellt

sind. Der Erwerb solcher Prepaid-SIM-Karten bietet anonyme deutsche Nummern und mobile Daten, verstößt jedoch gegen geltendes Recht und sollte daher vermieden werden.

Eine legale Alternative ist der Kauf einer SIM-Karte im Ausland, vorzugsweise innerhalb der EU. In einigen Ländern sind die Vorschriften weniger streng, sodass dort noch anonyme Prepaid-SIM-Karten erhältlich sind. Ich empfehle EU-Länder, da du dank der EU-Roaming-Verordnung diese Karten auch in Deutschland nutzen kannst, ohne zusätzliche Gebühren für Anrufe, SMS oder Daten zu zahlen. Folgende Länder bieten noch anonyme SIM-Karten an.

- Island
- Irland
- Dänemark
- Finnland
- Estland
- Tschechien
- Slowenien

Für die meisten Menschen wird Tschechien geografisch am nächsten liegen. Falls es nicht möglich ist, persönlich in eines dieser Länder zu reisen, bieten einige Webseiten den Verkauf ausländischer Prepaid-Karten an, bei denen keine Registrierung erforderlich ist.

Überlegungen zu anonymen SIM-Karten

Es ist wichtig, realistisch zu bleiben: Viele Menschen glauben, dass sie durch den Kauf einer anonymen SIM-Karte automatisch anonym bleiben – das ist jedoch nur bedingt der Fall. SIM-Karten können sehr präzise nachverfolgt werden, und dies gilt nicht nur für registrierte SIM-Karten, sondern auch für anonyme Karten.

Wenn du die anonyme Karte regelmäßig an Orten wie zu Hause oder am Arbeitsplatz verwendest, wird es nicht lange dauern, bis Algorithmen diese mit deiner Identität in Verbindung bringen. Auch Bewegungsmuster können analysiert werden. Wenn du beispielsweise in einer Tasche dein Handy mit der persönlichen SIM-Karte und in der anderen Tasche ein Gerät mit der anonymen Karte hast, und sich

diese über längere Zeit parallel bewegen, könnten die Karten von Algorithmen als zusammengehörig erkannt und miteinander verknüpft werden. Selbst im Auto besteht dieses Risiko, da moderne Fahrzeuge verpflichtend mit einer eigenen SIM-Karte ausgestattet sind. Die Bewegungen des Fahrzeugs und der anonymen SIM-Karte können ebenfalls analysiert werden, und wenn sie identisch sind, besteht die Möglichkeit einer Verknüpfung.

Selbst wenn du die Karte vorsichtig verwendest und darauf achtest, dass sie nicht direkt mit deiner Identität verbunden wird, können deine Kontakte ein Problem darstellen. Wenn jemand deine anonyme Nummer mit deinem echten Namen speichert und später eine App mit weitreichenden Berechtigungen auf seine Kontakte zugreifen lässt, könnte die Verbindung zu deiner Identität schnell hergestellt werden. Geschieht dies häufiger, ist die Anonymität dieser Nummer rasch verloren. Aus diesen Gründen bleibt es schwierig, dauerhaft anonyme SIM-Karten zu nutzen. Wer diesen Aufwand scheut, kann also auch gleich auf registrierte KYC-Karten zurückgreifen.

SMS und der Schutz vor Spam

Eine einfache Möglichkeit, um die Anzahl der Telefonnummern zu reduzieren und gleichzeitig Spam zu minimieren, ist die Nutzung eines Dienstes wie SMSforSats (sms4sats.com).

Viele Unternehmen verlangen eine Telefonnummer, um sicherzustellen, dass es sich nicht um Bots handelt, oder um eine Account-Bestätigung durchzuführen. Oftmals ist dies nur einmalig erforderlich, während die Nummer von den Unternehmen weiterverwendet, geteilt oder sogar verkauft werden kann.

Mit SMSforSats hast du die Möglichkeit, eine Nummer aus dem gewünschten Land auszuwählen und den entsprechenden Dienst anzugeben, um den Bestätigungscode zu erhalten – ganz ohne deine eigene Nummer preiszugeben. Dieser Dienst kostet eine kleine Gebühr von etwa 1 €, die du mit Lightning bezahlen musst (siehe Kapitel 8, „Das Lightning Netzwerk“).

Allerdings solltest du diese Option nicht für Accounts verwenden, die dir wichtig sind. Denn auf diese Nummer kannst du in Zukunft nicht mehr zugreifen – ähnlich wie bei Wegwerf-E-Mail-Adressen.

Messenger

E-Mails und das Telefonnetz sind leider sehr unsichere Technologien – sie sind unverschlüsselt und können leicht angegriffen sowie manipuliert werden. Messenger, die ausschließlich auf dem Internet basieren, bieten hier eine weitaus bessere Alternative.

Messenger-Apps haben unsere Art zu kommunizieren revolutioniert. Früher nutzten wir SMS, heute sind es Messenger-Apps, die Textnachrichten, Sprachnachrichten und sogar Videos unterstützen. Da wir diese Apps häufig für persönliche Gespräche verwenden, ist es von entscheidender Bedeutung, dass sie sicher und privat sind. Leider erfüllen viele gängige Messenger diese Anforderungen nicht. Glücklicherweise gibt es Alternativen, die unsere Privatsphäre respektieren und unsere Kommunikation mit modernster Technologie schützen.

Was ist Ende-zu-Ende-Verschlüsselung (E2EE)?

Ende-zu-Ende-Verschlüsselung (E2EE) ist eine Verschlüsselungsmethode, bei der ausschließlich der Sender und der Empfänger die Nachrichten entschlüsseln und lesen können. Diese Technologie schützt die Kommunikation vor dem Zugriff unbefugter Dritter, darunter Regierungen, Unternehmen und Kriminelle.

Ursprünglich wurde Verschlüsselung vor allem von großen Unternehmen und staatlichen Institutionen eingesetzt, um sensible Daten zu sichern. Auch Aktivisten und Politiker griffen auf Verschlüsselung zurück, wenn es um besonders hohe Sicherheitsanforderungen ging. Das allgemeine Bewusstsein für den Schutz privater Kommunikation durch Verschlüsselung wuchs jedoch erst nach den Enthüllungen von Edward Snowden, die die Überwachung der Bevölkerung durch die NSA offenlegten. Dank E2EE ist es äußerst

schwierig, auf den Inhalt einer Nachricht zuzugreifen. Dennoch sammeln viele Unternehmen weiterhin Metadaten ihrer Nutzer.

Was sind Metadaten?

Metadaten umfassen alle Informationen, die im Zusammenhang mit einer Nachricht entstehen, abgesehen vom Inhalt der Nachricht selbst. Man kann sich Metadaten wie einen elektronischen Fingerabdruck vorstellen: Sie geben Aufschluss darüber, wer mit wem kommuniziert, wann dies geschieht, wie lange die Kommunikation dauert, von welchem Gerät, aus welcher Zeitzone und vieles mehr.

Selbst ohne den genauen Inhalt zu kennen, lassen sich durch die Analyse von Metadaten Muster und Beziehungen erkennen. So kann man herausfinden, wer häufig miteinander spricht, und daraus persönliche oder berufliche Verbindungen ableiten. Aus diesem Grund ist es wichtig, einen Messenger zu wählen, der nicht nur die Nachrichten verschlüsselt mit E2EE, sondern auch möglichst wenige Metadaten sammelt. Einen Messenger zu finden, der kostenlos, sicher und privat ist und gleichzeitig von vielen Menschen genutzt wird, erweist sich jedoch oft als schwierig. Dennoch gibt es einige empfehlenswerte Optionen.

Signal

Signal ist bereits seit einiger Zeit verfügbar und hat besonders viel Aufmerksamkeit erlangt, nachdem WhatsApp seine Datenschutzrichtlinien mehrfach geändert hatte und zunehmend Daten von Nutzern sammeln wollte. Mittlerweile hat Signal nicht nur in der Privacy-Community, sondern auch im Mainstream an Bedeutung gewonnen, was bedeutet, dass wir immer mehr Kontakte über Signal erreichen können.

Alle Nachrichten bei Signal sind Ende-zu-Ende-verschlüsselt, was bedeutet, dass nur der Empfänger und wir selbst den Inhalt sehen können. Niemand sonst hat die Möglichkeit, die Nachrichten abzufangen oder mitzulesen. Die Verschlüsselung ist so sicher, dass sogar andere Plattformen wie Skype und WhatsApp darauf basieren. Zusätzlich sind Gruppenchats, Anrufe und Videoanrufe ebenfalls

geschützt. Wir können selbstlöschende Nachrichten einstellen, die nach einer bestimmten Zeit automatisch verschwinden. Signal ist Open Source, sodass der Quellcode von jedem überprüft werden kann.

Molly

Molly ist eine auf Privatsphäre fokussierte Abwandlung von Signal. Das bedeutet, dass Molly auf der gleichen Technologie wie Signal basiert, jedoch zusätzliche Funktionen für einen verbesserten Datenschutz bietet. Mit Molly können wir mit Signal-Nutzern kommunizieren und verschlüsselte Nachrichten, Anrufe sowie Dateien austauschen, ohne die offizielle Signal-App verwenden zu müssen. Ein wesentlicher Vorteil von Molly ist die Möglichkeit, mehrere „Signal-Konten" zu nutzen, was mit der offiziellen Signal-App nicht möglich ist. So können wir beispielsweise ein separates Konto für Freunde und eines für berufliche Kontakte anlegen.

SimpleX

SimpleX ist eine der neuesten sicheren und privaten Messenger-Apps auf dem Markt. Im Gegensatz zu vielen anderen Apps erfordert SimpleX keine Nutzer-IDs. Das bedeutet, dass wir keine Telefonnummer oder E-Mail-Adresse angeben müssen, um die App zu nutzen. Dadurch bleibt unsere Identität vollständig anonym. SimpleX bietet Ende-zu-Ende-Verschlüsselung und ermöglicht es uns, mehrere Profile zu erstellen, darunter sogar vollkommen zufällig generierte Profile. Dies erhöht unsere Privatsphäre und Sicherheit erheblich.

Da SimpleX jedoch ein relativ neues Projekt ist, gibt es bislang noch nicht viele Nutzer, und die App kann gelegentlich Fehler oder Bugs aufweisen.

Wire

Wire ist eine sichere Messaging-App, die Ende-zu-Ende-Verschlüsselung für Nachrichten, Audio- und Videoanrufe sowie für geteilte Bilder, Videos und Dateien bietet. Da Wire Open Source ist, kann der Quellcode von jedem überprüft werden. Für die Anmeldung

benötigst du lediglich eine E-Mail-Adresse. Du hast die Möglichkeit, verschiedene Accounts zu erstellen und somit unterschiedliche Profile zu nutzen, die über mehrere Geräte synchronisiert werden können. Dies ist besonders praktisch, wenn du beispielsweise ein Profil für Freunde und ein anderes für die Arbeit anlegen möchtest. Allerdings ist Wire in Deutschland noch nicht sehr verbreitet, sodass du möglicherweise nicht viele deiner Kontakte dort antreffen wirst.

Matrix

Matrix ist ein dezentrales Kommunikationsprotokoll für sichere Nachrichten sowie für Audio- und Videoanrufe mit Ende-zu-Ende-Verschlüsselung. Das dezentrale Konzept bedeutet, dass es keinen zentralen Server gibt, über den alle Daten geleitet werden. Stattdessen werden die Daten über verschiedene Server verteilt, was die Privatsphäre der Nutzer erhöht. Matrix ist Open Source, sodass jeder den Code einsehen und zur Verbesserung beitragen kann. Die hohe Sicherheit und der Schutz der Privatsphäre machen Matrix zu einer ausgezeichneten Wahl für Personen, die besonderen Wert auf Datenschutz legen. Allerdings kann die Nutzung von Matrix anfangs etwas komplex erscheinen, und die Nutzerbasis ist im Vergleich zu anderen Plattformen kleiner und eher technisch orientiert.

Threema

Threema ist eine äußerst sichere Messaging-App, die Ende-zu-Ende-Verschlüsselung bietet. Beim ersten Start der App erhalten Nutzer eine Threema-ID, sodass keine Telefonnummer oder E-Mail-Adresse angegeben werden muss. Dies ermöglicht eine vollständige Anonymität bei der Nutzung der App. Threema ist jedoch kostenpflichtig und kostet etwa 3 €, was dazu führt, dass die Nutzerbasis im Vergleich zu kostenlosen Alternativen relativ klein ist.

Jitsi

Jitsi ist eine Open-Source-Videoplattform, die mit dem Fokus auf Privatsphäre entwickelt wurde. Mit Jitsi kannst du Videoanrufe und Videokonferenzen durchführen, ohne dass deine Daten von Dritten gesammelt werden. Allerdings ist es erforderlich, sich bei der

offiziellen Jitsi-Plattform zu registrieren, um einen Videoraum zu erstellen, und dies ist nur über Google, Facebook oder GitHub möglich, was für unsere Privatsphäre nicht ideal ist. Es gibt jedoch alternative Dienste, die auf Jitsi basieren und keine Anmeldung erfordern. Ein Beispiel dafür ist Freifunk Meet (ffmeet.net). Dort kannst du einfach einen Videoraum erstellen und deine Freunde einladen, ohne persönliche Daten anzugeben.

WhatsApp

WhatsApp ist zwar sehr weit verbreitet, jedoch empfehle ich es nicht denjenigen, die Wert auf Privatsphäre legen. Obwohl WhatsApp eine Ende-zu-Ende-Verschlüsselung anbietet, sammelt es eine Vielzahl von Metadaten, die viel über uns verraten können. Zudem sind die Chat-Backups häufig nicht verschlüsselt und werden in der Google Cloud gespeichert, was bedeutet, dass unsere Nachrichten dort ungeschützt liegen. Da WhatsApp zu Facebook (jetzt Meta) gehört, sollten Bedenken hinsichtlich der Privatsphäre und Sicherheit besonders ernst genommen werden.

Telegram

Telegram wurde lange Zeit als sichere und private Kommunikationsplattform geschätzt. Auch ich habe in der ersten Version dieses Buches positiv über Telegram berichtet. Allerdings gab es kürzlich besorgniserregende Entwicklungen, weshalb ich Telegram nicht mehr empfehle. In der Vergangenheit sprach vieles für Telegram. Russland versuchte, die Plattform zu verbieten, nachdem CEO Pavel Durov sich weigerte, Daten der Nutzer an die russische Regierung weiterzugeben. Auch westliche Länder hatten Haftbefehle gegen ihn erlassen, weil er nicht kooperieren wollte. Viele Kriminelle und Terrorgruppen nutzten Telegram als ihr Hauptkommunikationsmedium. Die Organisation hinter Telegram weigerte sich, Informationen zu zensieren oder Daten über ihre Kunden preiszugeben. Dies sprach für die Privatsphäre und Sicherheit von Telegram.

Leider hat sich dies im Sommer 2024 geändert. Pavel Durov wurde in Frankreich festgenommen, und nach einer gewissen Zeit der Ungewissheit änderte Telegram seine Nutzungsbedingungen sowie die

Datenschutzrichtlinien. Früher stand dort, dass sie keine Daten an andere Unternehmen oder Regierungen weitergeben und dies auch nie getan haben. Jetzt ist das Gegenteil der Fall: Nach bestem Wissen und Gewissen können sie nun Daten weitergeben, und es ist anzunehmen, dass sie dies auch tun werden. Aus diesem Grund empfehle ich Telegram nicht mehr.

Persönlich nutze ich die meisten Apps je nach den Vorlieben meiner Kontakte und Kunden. Oft haben Menschen Vorurteile gegenüber bestimmten Apps. Es kann hilfreich sein, mehrere Alternativen anzubieten, um sie von einer privateren Lösung zu überzeugen. Allerdings wird es schnell unübersichtlich, wenn wir in jeder App nach neuen Nachrichten suchen müssen. Auch den Überblick zu behalten, welcher Kontakt über welches Medium kommunizieren möchte, kann herausfordernd sein. Daher empfehle ich allgemein Signal für die meisten Nutzer und SimpleX für maximale Privatsphäre.

Selbstlöschende Nachrichten

Egal welchen Messenger du verwendest, eine Funktion sollte immer aktiviert sein: selbstlöschende Nachrichten. Stell dir vor, ein Hacker könnte jede Konversation, die du je hattest, online veröffentlichen. Das wäre ein Albtraum und sollte auf jeden Fall vermieden werden. Jede Nachricht, jeder Gedanke wäre dann öffentlich zugänglich. Es muss nicht immer ein Hacker sein; auch ein Fehler im Programm oder eine Gerichtsverhandlung könnten dazu führen. Dennoch speichern die meisten ihren gesamten digitalen Kommunikationsverlauf auf ihrem Handy oder sogar in der Cloud. Um sich zu schützen, können wir einstellen, dass sich Nachrichten nach einem Tag, einer Woche oder sogar einem Jahr automatisch von beiden Geräten löschen. Die meisten Dienste bieten diese Option an. Für viele ist ein Tag oder eine Woche zu kurz, da wir zumindest die letzten Nachrichten in der Konversation nachvollziehen möchten. Aber eine monatliche oder jährliche Löschung macht Sinn.

- Gehe dafür in der jeweiligen App in die Einstellungen und suche nach einer Option wie „Verschwindende Nachrichten“ oder „Selbstlöschende Nachrichten“. Meistens ist diese Option unter dem Punkt „Datenschutz“ zu finden.

• • •

In diesem Kapitel haben wir unsere digitale Kommunikation so sicher und privat wie möglich gestaltet. Angefangen bei den E-Mails haben wir eine Strategie umgesetzt, bei der wir mehrere E-Mail-Adressen für verschiedene Zwecke haben, um Bereiche in unserem Leben auch hier klarer zu trennen. Dazu benutzen wir E-Mail-Aliase sowie Temporäre E-Mail-Adressen damit wir nichtmehr unsere echte E-Mail-Adresse an aufdringliche Online-Anbieter weitergeben müssen.

Auch bei Telefonnummern haben wir uns verschiedene Optionen angeschaut, um auch hier das höchste Maß an Privatsphäre und Sicherheit rauszuschlagen. Für maximale Sicherheit und Privatsphäre bei digitaler Kommunikation haben wir uns daraufhin verschiedene Messenger angeschaut, die Ende-zu-Ende Verschlüsselung anbieten, was bei E-Mails und Telefon leider nicht der Fall ist. Kurzum, unsere digitale Kommunikation ist größtmöglich abgesichert.

Durch die letzten Kapitel haben wir schon fast alle Bereiche unseres digitalen Lebens sicher und privat gestaltet von Computer und Handys, sicherem Browser bis hin zu Passwörtern und Verschlüsselung sowie sichere Kommunikation. Jedoch gibt es noch viel mehr Apps, Anwendungen und Dienste, die immer noch ein in unsere Privatsphäre eingreifen. Im nächsten Kapitel tauschen wir diese zu Privatsphäre freundlichen Alternativen aus und schauen, was es für weitere Werkzeuge gibt um unsere Privatsphäre zu erhöhen.

Kapitel 6
Digitale Werkzeuge und Alternativen

„Ohne Privatsphäre gibt es keinen Sinn, ein Individuum zu sein."
~ *Jonathan Franzen*

Mit diesem Ratgeber haben wir zunächst einen sicheren und privaten Computer sowie ein Handy eingerichtet, um eine solide Grundlage für die Nutzung des Betriebssystems zu schaffen. Anschließend haben wir einen sicheren und anonymen Browser konfiguriert, um anonym zu surfen und mithilfe eines VPNs sowie DNS unsere Internetaktivitäten zu schützen. Wir verfügen nun über sichere Passwörter und verschlüsselte Backups. Im letzten Kapitel haben wir uns mit sicherer und privater Kommunikation beschäftigt. Kurz gesagt, wir sind bereits sehr gut aufgestellt. Dennoch gibt es weitere zahlreiche Apps und Tools, die wir nutzen können, um noch unabhängiger von großen Unternehmen zu werden und unsere Privatsphäre weiter zu schützen.

Kalender

Ein sicherer und privater Kalender hat oberste Priorität, da er viele sensible Informationen speichert: Arbeitstermine, Arztbesuche, private Veranstaltungen, Geburtstage, Reisen und vieles mehr. Oft enthalten die Notizen zu den Terminen zusätzliche Details wie Adressen, Arbeitgeber oder Gesundheitsdaten. Dein Kalender spiegelt somit dein gesamtes Leben wider. Es ist daher nachvollziehbar, dass man nicht möchte, dass Unternehmen wie Google oder Microsoft Zugriff auf diese Daten erhalten. Diese Firmen nutzen solche Informationen nicht nur für personalisierte Werbung, sondern verkaufen sie auch an Dritte, wie beispielsweise an diverse Versicherungsunternehmen.

Wenn du eine Synchronisation von deinem Kalender zwischen verschiedenen Geräten wünschst, empfiehlt sich der **Proton Kalender**. Dieser ist für Android und IOS sowie unter calendar.proton.me

verfügbar. Seit seiner Einführung im Jahr 2020 hat er zahlreiche Verbesserungen und neue Funktionen erhalten und kann problemlos mit den Kalendern großer Anbieter wie Google und Microsoft konkurrieren. Die Synchronisation ist Ende-zu-Ende-verschlüsselt, sodass deine Termine sicher sind.

Für diejenigen, die ihre Daten lokal auf dem Handy behalten möchten, eignet sich der **Fossify Kalender**, ein Open-Source-Programm, das im F-Droid-Store verfügbar ist. Mit dieser Lösung bleiben deine Termine ausschließlich lokal auf dem Gerät und gelangen nicht ins Internet. Solltest du dennoch eine Synchronisation wünschen, ist **EteSync** eine empfehlenswerte Option. Mit EteSync kannst du auch deine Termine Ende-zu-Ende-verschlüsselt synchronisieren, unabhängig davon, welche App du auf dem Handy oder Computer verwendest. In beiden Fällen ist es ratsam, regelmäßig Backups zu erstellen, um im Falle eines Problems immer eine Kopie der Kalenderdaten zur Hand zu haben.

Kontakte

Genauso wie dein Kalender enthalten auch deine Kontaktlisten sensible Informationen über Menschen, die im Laufe der Jahre in dein Leben getreten und wieder daraus verschwunden sind. Sie spiegeln verschiedene Arten von Beziehungen wider, sowohl berufliche als auch private. Viele nutzen die Kontaktliste auf ihrem Handy als praktischen Ort, um persönliche Daten zu speichern – darunter Geburtstage, physische Adressen, IBAN-Nummern und sogar Türcodes.

Trotzdem geben viele ihre Kontaktlisten bedenkenlos an Apps weiter, darunter soziale Netzwerke wie Facebook, Zahlungsdienste und sogar Anwendungen, die solche Daten überhaupt nicht benötigen, wie Handyspiele oder smarte Haushaltsgeräte. Dies geschieht oft unbemerkt, indem man einfach ein Pop-up während der Installation bestätigt, wodurch deine Kontaktinformationen auf den Servern der Unternehmen landen. Diese Daten werden dann verwendet, um gezielte Werbung für dich und deine gespeicherten Kontakte zu schalten, und sie werden häufig auch weiterverkauft.

Leider wird dem Thema der gesammelten Kontaktlisten oft weniger Beachtung geschenkt als anderen privaten Daten wie dem Standortverlauf oder der Suchhistorie. Dabei enthalten Kontaktlisten wertvolle Informationen über dein persönliches Umfeld und über dich selbst. Daher solltest du diesen Aspekt keinesfalls vernachlässigen, um deine Privatsphäre und die deiner Kontakte zu schützen.

Wenn du deine Kontakte auf einem Android- oder Apple-Gerät speicherst, hast du bisher nur über wenige Möglichkeiten verfügt, deine Privatsphäre zu wahren. Das Gleiche gilt für Kontakte, die über Dienste wie Outlook oder Google verwaltet werden. Selbst wenn du nun die Berechtigungen für diese Apps zurückziehst und die Kontakte an einen sicheren Ort exportierst, bleiben die bereits geteilten Informationen bei den Unternehmen. Um diese Daten löschen zu lassen, müsstest du dich direkt an die entsprechenden Firmen wenden und auf eine Reaktion hoffen. Ein guter erster Schritt ist, alle Kontakte als .vcf-Datei zu exportieren und anschließend den Apps den Zugriff auf die Kontaktliste zu entziehen. Danach gibt es verschiedene sichere Optionen, um Kontakte zu verwalten.

.vcf-Dateien
.vcf-Dateien (Virtual Contact File) sind Dateien, die Kontaktinformationen wie Namen, Adressen, Telefonnummern und E-Mail-Adressen enthalten. Sie werden häufig verwendet, um Kontakte zwischen verschiedenen Anwendungen und Geräten auszutauschen.

Um eine .vcf-Datei zu exportieren, kannst du folgende Schritte ausführen:

- Öffne die Einstellungen in deinem E-Mail-Programm oder deinem Smartphone.
- Suche nach einer Option wie „Kontakt exportieren“ oder „Als VCF exportieren“.
- Wähle diese Optionen und speichere die Datei auf deinem Computer oder Smartphone.

ProtonMail: Diese Lösung bietet sich vor allem für diejenigen an, die Wert auf Privatsphäre legen, ohne auf Benutzerfreundlichkeit zu verzichten. ProtonMail verschlüsselt außerdem sämtliche sensiblen Kontaktinformationen, sodass weder Mitarbeiter noch Dritte darauf zugreifen können.

- Öffne mail.proton.me und klicke in der rechten Seitenleiste auf das Kontakt-Symbol.
- Klicke auf „Import contacts“ und wähle die zuvor erstellte .vcf-Datei aus.

Linux: Unter Linux gibt es keine native Anwendung für Kontakte, weshalb du auf alternative Programme zurückgreifen musst. Während Thunderbird lediglich Namen und E-Mail-Adressen importiert, ist Evolution eine empfehlenswerte Alternative, die umfangreichere Funktionen bietet.

- Installation über das Terminal:
  `sudo apt-get install evolution`
- Klicke auf „Datei“ und dann auf „Importieren“.

MacOS: Auch auf einem Mac kannst du deine Kontakte sicher und privat verwalten. Es ist wichtig, dass der Computer nicht mit einer Apple-ID verknüpft ist und keine iCloud verwendet wird. Wenn dies der Fall ist, kannst du die Standard-Kontakt-App problemlos nutzen.

- Klicke auf „Ablage“ und dann auf „Importieren“

Bei iPhones und iPads ist eine Apple-ID erforderlich, um das Gerät nutzen zu können. Daher empfiehlt es sich in diesem Fall, entweder ProtonMail zu verwenden oder die Daten offline zu speichern.

GrapheneOS Kontakte: GrapheneOS bietet fortschrittliche Datenschutzoptionen für Kontakte. Hier können Kontakte im internen Speicher des Geräts als Datei gespeichert werden, sodass Apps, die Zugriff auf die Kontaktliste anfordern, lediglich eine leere Liste sehen. Zudem gibt es die Funktion „Contact Scopes“ (siehe Kapitel 2, „Contact Scopes“). Im Unterschied zu herkömmlichen Android-Geräten, bei denen die Berechtigung für Kontakte eine Alles-oder-

nichts-Einstellung ist, ermöglicht es GrapheneOS, gezielt einzelne Kontakte sowie spezifische Informationen wie Namen, Telefonnummern oder E-Mail-Adressen zu teilen. Darüber hinaus verfügen Apps nur über die Berechtigung „nur lesen", was bedeutet, dass sie keine Kontakte bearbeiten können.

- Um Kontakte zu importieren, klicke in der Kontakt-App auf „Einstellungen“ und dann auf „Importieren“.

Offline-Speicherung: Für noch mehr Sicherheit und Privatsphäre kannst du deine Kontakte vollständig offline speichern, unabhängig vom Betriebssystem. Dies lässt sich einfach in einer Excel-Tabelle oder mit einem Passwortmanager wie **KeePassXC** realisieren, in dem alle Kontaktinformationen sicher abgelegt werden. Alternativ kannst du die .vcf-Datei in einer Textbearbeitungs-App speichern und bearbeiten.

Synchronisation: Wenn du deine Kontakte zwischen verschiedenen Geräten synchronisieren möchtest, ist **Etesync** eine ausgezeichnete Wahl. Damit kannst du deine Kontakte sicher und verschlüsselt sowohl auf deinem Handy als auch auf deinem Computer speichern und bearbeiten. Etesync bietet zudem eine Ende-zu-Ende-Verschlüsselung, die deine Daten schützt.

Es ist wichtig, dass du alle Kontakte aus der bisher genutzten App – sei es Google Kontakte, iOS, Android oder eine andere – löschst, da sonst weiterhin auf diese zugegriffen werden kann.

Notizen

Unsere Notizen bestehen aus persönlichen Gedanken und Ideen, die unser Leben, unsere Arbeit und unsere Beziehungen betreffen. Daher ist es wichtig, sie sicher und privat zu speichern. Programme wie Evernote, OneNote und Apples iCloud Notes sind zwar benutzerfreundlich und bieten viele nützliche Funktionen, speichern jedoch sensible Daten unverschlüsselt und in der Regel online. Das bedeutet, dass Mitarbeiter, Hacker oder andere Unternehmen potenziell

auf diese Daten zugreifen und sie für verschiedene Zwecke nutzen könnten. Aus diesem Grund ist es ratsam, solche Dienste zu meiden.

Es ist natürlich nicht einfach, sich von einer gewohnten Plattform zu trennen, insbesondere wenn man jahrelang damit gearbeitet hat. Auch ich stand vor dieser Herausforderung und habe zahlreiche Programme für sichere Notizen ausprobiert. Zwei davon kann ich besonders empfehlen.

Standard Notes: Standard Notes (standardnotes.com) ist eine benutzerfreundliche und sichere Notizen-App, die Ende-zu-Ende-Verschlüsselung bietet und es ermöglicht, Notizen nahtlos zwischen verschiedenen Geräten zu synchronisieren. Die App ist für alle gängigen Betriebssysteme verfügbar und bietet sowohl kostenlose als auch kostenpflichtige Pläne an. Alle Notizen sind durchgängig verschlüsselt, sodass weder das Unternehmen noch Dritte auf die Inhalte zugreifen können. Für die meisten Nutzer reicht die kostenlose Version vollkommen aus. Ich verwende Standard Notes, um meine Notizen zwischen meinem Handy, Laptop und PC zu synchronisieren. Wenn dir diese Funktion wichtig ist, kann ich Standard Notes wärmstens empfehlen. Aktiviere direkt nach der Erstellung deines Kontos die Zwei-Faktor-Authentifizierung (2FA), um die Sicherheit weiter zu erhöhen.

Obsidian: Im Vergleich dazu bietet Obsidian (obsidian.md) eine Vielzahl an Funktionen und ist äußerst anpassbar. Die Notizen werden lokal als Markdown-Dateien auf deinem Computer gespeichert, wodurch Obsidian für diese Dateien „nur“ als leistungsstarker Editor fungiert. Deine Notizen verlassen somit nie deinen Computer. Auch Obsidian bietet eine kostenpflichtige Synchronisationsfunktion an, aber wenn du diese nicht benötigst, hast du mit der kostenlosen Version vollen Zugriff auf alle Funktionen.

Obsidian stellt zudem zahlreiche Plug-ins zur Verfügung, die die Funktionalität erweitern. Für diejenigen, die von Evernote, OneNote oder Apple Notes wechseln möchten, ist Obsidian eine hervorragende Alternative, die nur minimale Kompromisse erfordert. Ich selbst nutze Obsidian zu 90 % und habe alle Notizen und Entwürfe für dieses Buch damit erstellt.

Microsoft-Office-Alternative

Zusätzlich zu einfachen Notizen benötigt man eine Office-Anwendung. Eine häufig empfohlene Lösung ist LibreOffice, eine Open-Source-Anwendung. Allerdings hinkt LibreOffice in den Bereichen Design und Funktionen leicht hinter Microsoft Office hinterher und kann etwas veraltet wirken. Daher empfehle ich LibreOffice nicht.

Eine der besten Alternativen zu Microsoft Office ist **OnlyOffice** (www.onlyoffice.com). OnlyOffice ist Open-Source und vollständig kostenlos, während Microsoft für die Nutzung seiner Produkte Gebühren erhebt und zudem persönliche Nutzerdaten sammelt, um sie zu monetarisieren. Aus diesem Grund ist es ratsam, auf Microsoft zu verzichten. Der Vorteil von OnlyOffice liegt darin, dass es bei den meisten Funktionen Microsoft Office in nichts nachsteht. Es bietet Anwendungen für Textdokumente, Tabellenkalkulationen und Präsentationen, die denjenigen von Microsoft sehr ähneln. Somit ist es eine hervorragende Alternative, bei der man keine Kompromisse eingehen muss.

Musik, Podcasts und YouTube

Viele Menschen sind daran gewöhnt, stundenlang Unterhaltungsmedien wie YouTube oder Spotify zu konsumieren. Dabei wird oft übersehen, dass diese Unternehmen umfangreiche Nutzerdaten sammeln und weitergeben. Glücklicherweise gibt es auch hier einige privatere Alternativen.

YouTube: Beginnen wir mit YouTube. Google sammelt erhebliche Mengen an Daten über uns, insbesondere wenn wir uns mit unserem Google-Konto anmelden. Unsere Vorlieben und Interessen werden direkt mit diesem Konto verknüpft. Wenn man einen VPN verwendet, fordert YouTube dazu auf, sich mit einem Konto anzumelden, und blockiert sonst die Videos. Um dies zu umgehen, gibt es zwei Alternativen.

Odysee (odysee.com) ist eine unabhängige Plattform, die als Alternative zu YouTube entwickelt wurde. Sie bietet Nutzern und

Videoerstellern mehr Freiheit und Unabhängigkeit. Auf Odysee können Videos zu fast jedem Thema hochgeladen werden, solange sie keine pornografischen Inhalte oder Gewalt darstellen. Im Gegensatz zu YouTube können hier politische Ansichten frei geäußert werden, ohne Angst haben zu müssen vor einer Sperrung des Kanals. Während der Corona-Pandemie gewann Odysee durch diese Meinungsfreiheit an Popularität. Ein Nachteil ist, dass Videoersteller ihre Inhalte manuell hochladen müssen, sodass nur ein kleiner Teil der YouTube-Videos auch auf Odysee verfügbar ist. Dieser Anteil wächst jedoch stetig.

Wenn du jedoch auf das gesamte YouTube-Archiv zugreifen möchtest, ohne deine Privatsphäre zu opfern, kannst du ein alternatives Front-End für YouTube nutzen. Statt die YouTube-App oder Website zu verwenden, greifen wir auf eine Open-Source-Alternative zurück, die das YouTube-Backend verwendet, aber unsere Daten schützt. Das heißt dass man Zugriff auf alle YouTube-Videos hat, ohne die offizielle Seite dafür zu benutzen.

Für Mobilgeräte empfiehlt sich **NewPipe**, erhältlich im F-Droid-Store. Auf dem Computer kannst du **Invidious** (invidious.io) nutzen.

Bei Invidious wählt man aus verschiedenen Instanzen, die von Freiwilligen gehostet werden. Diese Instanzen kann YouTube sperren, aber in diesem Fall wechselt man einfach zu einer anderen. Abgesehen davon gibt es keine wesentlichen Einschränkungen im Vergleich zur YouTube-App: Man kann Kanäle abonnieren und alle Videos werbefrei anschauen.

Der einzige Unterschied betrifft das Fehlen einer „For-You-Seite“, da Invidious keine Daten sammelt und daher keine personalisierten Empfehlungen gibt. Manche sehen das als Nachteil, aber es kann auch befreiend sein, nur die Inhalte zu sehen, die man wirklich sehen möchte, ohne von zahlreichen empfohlenen Videos abgelenkt zu werden.

Podcasts und Musik: Viele möchten nicht auf ihre aktuellen Musik- und Podcast-Dienste wie Spotify oder Deezer verzichten, vor allem, weil Open-Source-Programme in diesem Bereich noch nicht

so weit entwickelt sind. Wenn du diese Dienste weiterhin nutzt, solltest du zumindest einen Alias-Namen und eine separate E-Mail-Adresse verwenden, um die gesammelten Daten nicht direkt mit deiner Identität zu verknüpfen. Von den großen Plattformen respektiert Apple Music die Privatsphäre am meisten. Wenn du jedoch maximale Privatsphäre möchtest, sind auch hier Open-Source-Programme die beste Wahl.

Ich empfehle **RiMusic** (erhältlich im F-Droid-Store). Diese App basiert ähnlich wie Invidious auf dem YouTube-Music-Archiv und greift auf diese Titel zu, wenn du einen Song auswählst. Hier gibt es viele voreingestellte Playlisten, und du kannst Musik auch herunterladen.

Für Podcasts empfehle ich **AntennaPod** (ebenfalls im F-Droid-Store erhältlich). Hier hast du Zugriff auf alle Podcast-Episoden, genauso wie es bei Spotify der Fall ist. Du kannst diese Episoden streamen oder herunterladen.

Beide Apps sind kostenlos und open-source. Wenn ich auf dem Computer Musik oder Podcasts hören möchte, greife ich auf Invidious zurück, da nahezu alle Musik und Podcasts auch auf YouTube verfügbar sind.

Social Media

Diesen Punkt habe ich bereits mehrfach angesprochen und möchte ihn hier erneut betonen: Wenn dir deine Privatsphäre am Herzen liegt, solltest du in Erwägung ziehen, Social-Media-Plattformen zu verlassen und deine Accounts dort zu löschen. Diese Unternehmen bieten ihre Dienste völlig kostenlos an, ohne kostenpflichtige Funktionen einzuführen, weil sie das auch nicht müssen. Durch die gesammelten Daten können sie Milliarden an Gewinnen erzielen. Jeder Like, jeder Follower und jeder Post wird mithilfe modernster Algorithmen analysiert, wodurch erschreckend präzise Benutzerprofile erstellt werden, die genutzt werden, um gezielte Werbung zu schalten. Darüber hinaus beeinflussen diese Netzwerke dein Verhalten, um sicherzustellen, dass du möglichst viel Zeit auf der Plattform

verbringst. Je mehr Zeit du investierst, desto mehr Daten werden gesammelt, und desto genauer wird dein Profil. Es ist eine gefährliche Spirale, die nur zu mehr Konsum führt.

Nostr

Wie bereits erwähnt, respektieren große Social-Media-Plattformen wie Instagram, Facebook, Twitter und YouTube oft nicht die Privatsphäre der Nutzer. Um die eigene Privatsphäre zu schützen, sollte die Nutzung dieser Dienste entweder vollständig eingestellt oder zumindest auf ein Minimum reduziert werden.

Eine vielversprechende Alternative aus der Bitcoin-Community ist Nostr. Nostr ist jedoch keine herkömmliche Social-Media-App, sondern eine offene Technologie, die es ermöglicht, digitale Nachrichten ohne zentrale Instanz zu senden und zu empfangen. Es handelt sich um ein dezentrales Netzwerk, das keine Unternehmen oder Institutionen zur Verwaltung benötigt. Jeder kann sich diesem Netzwerk anschließen, es nutzen und weiterentwickeln.

Das Netzwerk basiert auf sogenannten Relays, also Knotenpunkten, über die Daten verschickt werden. Im Unterschied zu herkömmlichen Plattformen, die von zentralen Unternehmen betrieben werden und Nutzerdaten sammeln, um gezielte Werbung zu schalten, gibt es bei Nostr keine zentrale Instanz. Der Zugang zum Netzwerk erfolgt über einen privaten Schlüssel, der wie ein Passwort funktioniert. Dieser private Schlüssel wird zufällig generiert und ermöglicht den Zugriff auf verschiedene Nostr-Apps – alles funktioniert ohne E-Mail-Adresse oder Telefonnummer. Mit diesem Schlüssel kann man Inhalte veröffentlichen, Bitcoin senden, eine Webseite erstellen oder Social Media im Stil von Twitter nutzen.

Da keine zentrale Kontrolle stattfindet, gibt es keine Zensur, und niemand kann Nachrichten oder Konten einfach löschen. Um Nostr zu nutzen, empfehle ich die App Primal (primal.net), die sowohl im Browser als auch für Android und iOS verfügbar ist.

- Klicke dafür nach dem Öffnen auf „Get Started“, um einen Account zu erstellen.
- Wähle dann „Create Account“ und gebe einen Alias als „Username“ und „Display Name“ ein, der nicht auf deine wahre Identität schließen lässt.
- Überspringe die weiteren Felder mit „Next“ und schließe die Einrichtung mit „Finish“ ab.

Um deinen Account zu sichern, ist es wichtig, deinen privaten Schlüssel zu speichern. So kannst du auch in anderen Anwendungen auf deinen Nostr-Account zugreifen. Kopiere außerdem den öffentlichen Schlüssel, den du mit anderen teilen kannst, ähnlich wie einen Benutzernamen.

- Klicke links in der Seitenleiste auf das Zahnrad und dann auf „Account“.
- Kopiere den Public Key unter „Your public key“ und speichere ihn sicher.
- Mache dasselbe mit dem „Your private key“. Zum Speichern verwende ich einen Passwortmanager.

Jetzt kannst du mit Nostr durchstarten. Während des Setups wurden dir automatisch einige Accounts zum Folgen vorgeschlagen. Du hast jedoch die Möglichkeit, dies beim Start zu deaktivieren oder später anzupassen. Den Public Key, den du zuvor kopiert hast, kannst du nun an Freunde weitergeben, die bereits Nostr nutzen, oder in deine Bio einfügen, um auf dein Profil aufmerksam zu machen.

Obwohl Nostr zum Zeitpunkt dieses Schreibens noch etwas unter dem Radar liegt, zeigt die wachsende Nutzerzahl, dass das Interesse an einer privaten und dezentralen Plattform steigt. Wenn du also nicht vollständig auf soziale Netzwerke verzichten möchtest, ist Nostr derzeit die beste Wahl.

Künstliche Intelligenz

Mit der Veröffentlichung von ChatGPT im Jahr 2022 hat Künstliche Intelligenz (KI) einen bedeutenden Schritt in den Mainstream

gemacht. Seitdem haben viele Unternehmen ihre eigenen Versionen dieser Technologie entwickelt und vermarktet, mit dem Versprechen, unser Leben grundlegend zu verändern – von der Art und Weise wie wir arbeiten bis hin zu unserem Alltag. Trotz der zahlreichen Vorteile birgt diese Technologie jedoch erhebliche Risiken für unsere Privatsphäre. Daher ist es wichtig, einige grundlegende Punkte zu beachten, um uns besser zu schützen.

Zunächst sollten wir uns darüber im Klaren sein, dass KI ähnliche Risiken für unsere Privatsphäre mit sich bringt wie frühere Technologien – jedoch in einem viel größeren Ausmaß, da nun riesige Mengen an persönlichen Daten „intelligent" verarbeitet werden können. Diese KI-Systeme sind oft datenhungrig und intransparent, was bedeutet, dass wir noch weniger Kontrolle über unsere eigenen Daten erhalten. Wie bereits in den vorherigen Kapiteln beschrieben, ist es bereits jetzt schwierig, der digitalen Überwachung zu entkommen – und der Einsatz von KI macht dies noch komplizierter.

Nahezu jedes große Technologieunternehmen nutzt mittlerweile KI – von Microsoft über Apple bis Google. Diese Unternehmen setzen KI in ihren Betriebssystemen ein, angeblich um das Nutzererlebnis zu verbessern. Doch werfen wir einen genaueren Blick auf das, was wirklich passiert. Ein Beispiel dafür ist Windows Recall: Dieser Dienst macht alle 30 Sekunden einen Screenshot deines Bildschirms, um später das Nutzungsverhalten zu analysieren. Eine KI wird dabei eingesetzt, um diese Daten zu verarbeiten. Das bedeutet, dass alles, was du auf einem Microsoft-Computer machst, in diese KI eingespeist wird.

Ähnliche Mechanismen werden auch von Betriebssystemen wie iOS, MacOS und Android verwendet. KI wird genutzt, um immer mehr Daten zu sammeln und zu analysieren. Was genau mit diesen Daten geschieht, bleibt oft unklar, da die Systeme komplett abgeschottet sind. Der einzige wirkliche Schutz vor dieser Art von Überwachung sind Open-Source-Systeme wie Linux und GrapheneOS, die in den ersten Kapiteln vorgestellt wurden. Mit Linux und GrapheneOS kannst du dich also vor der Überwachung durch die KI großer Firmen schützen.

Aber wie können wir KI sicher und privat nutzen? Es wäre zwar möglich, komplett auf Künstliche Intelligenz zu verzichten, aber das würde bedeuten, eine Technologie zu ignorieren, die in Zukunft nicht mehr wegzudenken ist. Wie also können wir KI nutzen, ohne unsere Privatsphäre zu opfern? Um das zu verstehen, müssen wir zunächst wissen, wie KI funktioniert. Vereinfacht gesagt, wird Künstliche Intelligenz hauptsächlich auf zwei Arten trainiert.

Grundlegendes Training: Zu Beginn wird die KI mit enormen Datenmengen trainiert, die sie verarbeitet und analysiert. Dabei kommen sämtliche öffentlich im Internet zugänglichen Informationen zum Einsatz. Das bedeutet, dass alles, was wir online veröffentlichen, potenziell von KI-Systemen erfasst und verarbeitet werden kann. Darauf haben wir nur einen begrenzten Einfluss.

Feinabstimmung durch Feedback: Im nächsten Schritt erfolgt eine Feinabstimmung der KI durch das Feedback der Nutzer. Alles, was wir eingeben – seien es persönliche Nachrichten oder allgemeine Anfragen – wird genutzt, um die KI weiterzuentwickeln. Dies ist ein kritischer Punkt: Unsere Eingaben fließen in das Trainingsmaterial ein und helfen der KI, besser zu werden.

Wenn wir also eine Online KI wie ChatGPT nutzen, stimmen wir zu, dass unsere Eingaben vom Unternehmen verarbeitet werden, um die KI zu trainieren. Diese Daten werden zwar nicht direkt an andere Nutzer weitergegeben, jedoch lernt die KI daraus und verwendet dieses Wissen, um Antworten für andere zu generieren. Eine vollständige Kontrolle über unsere Daten haben wir dabei nicht.

Eine Möglichkeit, die wir haben ist unsere Eigene KI lokal und offline zu nutzen, sodass unsere Daten bei uns bleiben und nicht für das Training anderer KI-Modelle verwendet werden. Eine KI von Grund auf zu trainieren ist jedoch so gut wie unmöglich als Privatperson, da dies oft tausende von Grafikkarten und enorme Datenmengen erfordert. Glücklicherweise müssen wir dies nicht selbst tun, da viele KI-Modelle bereits von großen Unternehmen trainiert wurden. Wir können diese Modelle herunterladen und lokal nutzen, ohne sie neu trainieren oder anpassen zu müssen. Das Modell selbst ist in der

Regel nicht besonders groß, und wir können es nach unseren Bedürfnissen einsetzen.

Ein Beispiel dafür ist **JanAI** (jan.ai). JanAI bietet eine benutzerfreundliche Schnittstelle, um mit KIs zu arbeiten. Nach dem Öffnen wählen wir ein KI-Modell aus, das wir herunterladen und dann auf unserem Gerät betreiben können.

Neben dem Namen der KI wird angezeigt, ob dein Gerät zu langsam ist und wie viele GB das KI-Modell verbraucht. Anstatt uns über die Cloud mit Servern von Unternehmen zu verbinden, nutzen wir die KI vollständig lokal, müssen dafür jedoch die erforderliche Hardware bereitstellen. Am besten geeignet sind Computer, die für Gaming oder Videoschnitt ausgelegt sind, da diese in der Regel über viel Arbeitsspeicher (RAM) und leistungsstarke Grafikkarten verfügen. Kleinere Modelle (wie Llama 3.2 1B) laufen jedoch auch problemlos auf Laptops.

Nachdem wir das Modell heruntergeladen haben, können wir die KI für verschiedene Aufgaben im Chatfenster nutzen. Zwar ist sie etwas weniger leistungsfähig als ChatGPT, aber für einfache Aufgaben reicht sie aus. Da wir Jan lokal nutzen, bleiben unsere Anfragen und Gedanken so sicher und privat wie unser Computer selbst. Wenn wir in Kapitel 1 einen Linux-Computer eingerichtet haben, können wir hier maximale Sicherheit und Privatsphäre gewährleisten. In vielen Fällen kommen wir um Cloud-Dienste nicht herum. Diese sind zwar sicher, jedoch besteht immer das Risiko, dass die eingegebenen Daten gespeichert und möglicherweise für andere Zwecke verwendet werden. Auch wenn Unternehmen wie OpenAI, die hinter ChatGPT stehen, derzeit verantwortungsvoll mit Nutzerdaten umgehen, könnte sich ihre Haltung in Zukunft ändern. Um unsere Privatsphäre bei der Nutzung von Cloud-KIs zu schützen, sollten wir folgende Punkte beachten.

Getrennte Accounts nutzen: Verwende unterschiedliche Konten für private und berufliche Zwecke, um sicherzustellen, dass keine Verknüpfung zwischen diesen Bereichen hergestellt werden kann. Diese Trennung kannst du weiter ausbauen, indem du für verschiedene Themen oder Aufgaben separate Konten erstellst. Nutze eine

Alias-E-Mail-Adresse und vermeide es, echte persönliche Daten anzugeben. Meiner Erfahrung nach sind ProtonMail-Aliase zuverlässig und werden von den meisten Diensten akzeptiert, während SimpleLogin gelegentlich Probleme bereitet.

Generische Angaben: Verwenden Sie keine echten Namen oder spezifischen Informationen in den Anfragen. Statt „Sehr geehrter Timo Volkov“ sollte man einfach „Sehr geehrter XXXX“ schreiben. Auch technische Details wie Server- oder IP-Adressen sollten anonymisiert oder vollständig weggelassen werden.

Einstellungen überprüfen: Bei ChatGPT und anderen Diensten gibt es oft die Möglichkeit, die Verwendung deiner Daten zur Verbesserung der KI zu deaktivieren. Es ist ratsam, diese Einstellung auszuschalten. Zudem solltest du Funktionen deaktivieren, die Daten zwischen verschiedenen Chats speichern und verknüpfen, um zu verhindern, dass die KI-Informationen aus dem einen Chat im nächsten verwendet.

Um deine Daten zu schützen, ist eine lokal gespeicherte und offline genutzte KI die beste Option. Auf diese Weise werden keine Daten ins Internet gesendet, und du behältst die vollständige Kontrolle über deine Eingaben und Informationen.

Einige Unternehmen bieten genau das an. Sie verfügen über die notwendige Hardware und laden diese KI-Modelle herunter, sodass du die KI genauso nutzen kannst wie bei anderen Online-Dienstleistern, ohne dass deine Daten für das Training verwendet werden. Zwar musst du diesen Unternehmen ein gewisses Vertrauen entgegenbringen, aber sie haben in der Regel strenge No-Log-Richtlinien. Das bedeutet, dass deine Chats direkt nach der Nutzung gelöscht werden. **Venice-AI** (venice.ai) und **DuckDuckGo-AI** (duck.ai) sind derzeit die besten Optionen dafür.

PGP

PGP (Pretty Good Privacy) ist eine Software zur Verschlüsselung und Signierung von Nachrichten und Daten. In diesem Abschnitt

konzentrieren wir uns auf eine besonders nützliche Funktion: die Überprüfung und Verifizierung von Dateien.

Die Überprüfung von Signaturen ist entscheidend, um sicherzustellen, dass die Daten sowohl unversehrt als auch authentisch sind. Authentizität bedeutet, dass die Datei tatsächlich von der angegebenen Quelle stammt und nicht von Dritten verändert wurde. Es wäre riskant, Webseiten oder Downloads blind zu vertrauen. Mit PGP-Signaturen kannst du sicherstellen, dass eine Datei von einer vertrauenswürdigen Quelle stammt, da sie signiert wurde.

Don't trust, verify
„Don't trust, verify" bedeutet, dass man sich nicht allein auf Vertrauen zu anderen verlassen sollte, sondern Informationen oder Systeme immer selbst überprüfen muss. Dies unterstreicht die Wichtigkeit, alles eigenständig zu verifizieren, um Sicherheit und Zuverlässigkeit zu gewährleisten.

Um PGP-Signaturen zu überprüfen, verwenden wir die Software Kleopatra.

- www.gpg4win.org (für Windows)
- apps.kde.org/kleopatra (für Linux)
- gpgtools.org (für MacOS)

Bevor wir beginnen können, benötigen wir ein Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht.

- Klicke in Kleopatra auf „New Key Pair".
- Gib einen beliebigen Namen ein und aktiviere das Kästchen „Protect the generated key".
- Bestätige mit „OK" und lege ein sicheres Passwort fest, vorzugsweise im Passwortmanager.

Abbildung 14 Kleopatra

Nun hast du ein eigenes Schlüsselpaar und kannst Dateien überprüfen. Zum Verifizieren eines Downloads benötigst du drei Dinge.

1. Die heruntergeladene Datei.
2. Die zugehörige PGP-Signatur der Datei.
3. Den öffentlichen Schlüssel des Entwicklers.

Um den Prozess zu veranschaulichen, werde ich ihn anhand des Tools VeraCrypt erläutern. Der Ablauf ist bei anderen Programmen ähnlich und wird in der Regel auf den jeweiligen Webseiten ausführlich erklärt.

- Auf der VeraCrypt-Webseite findest du links die Downloads und rechts die PGP-Signatur. Lade beide Dateien herunter. Achte darauf, dass die Signatur zur passenden Datei gehört.
- Nun benötigst du noch den öffentlichen Schlüssel des Entwicklers, um die Signatur zu überprüfen. Es gibt zwei Möglichkeiten, diesen zu erhalten.
- Möglichkeit 1: Manche Webseiten, wie auch VeraCrypt, bieten einen direkten Link zum öffentlichen Schlüssel an (z. B. am Ende der Download-Seite unter „PGP Public Key“). Kopiere den Schlüssel und gehe in Kleopatra auf „Notepad“. Füge den Schlüssel ein und klicke auf „Import Notepad“. Bestätige den importierten Schlüssel zwei Mal

mit „Certify“ und gib das von dir erstellte Passwort ein, falls erforderlich.

- Möglichkeit 2: Alternativ wird der öffentliche Schlüssel manchmal als Datei (.key oder .asc) angeboten. Lade diese Datei herunter, gehe in Kleopatra auf „Certificates“, ziehe die Datei per Drag-and-Drop hinein und klicke auf „Import Certificates“. Bestätige danach ebenfalls zweimal mit „Certify“.

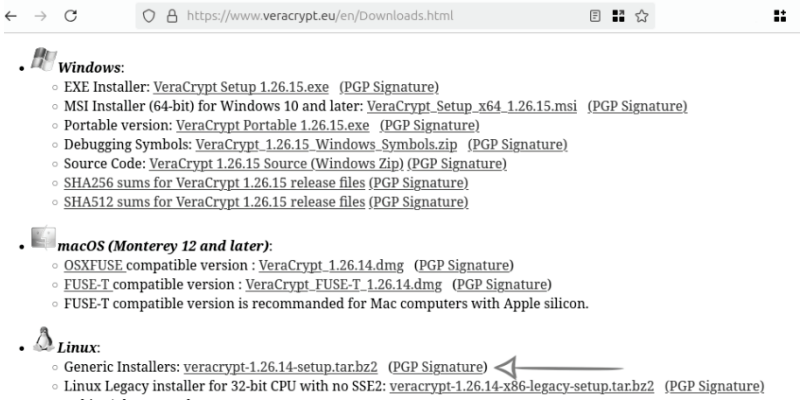

Abbildung 15Kleopatra Webseite

Der Public Key sieht dann so ähnlich aus:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFOts5YBEADqLnI89/N1VrlSHzUyDyFlzjPawPLjUD896TTc+3
2r5sGwTu9K+MRZBlitEDMdBIZYkT1HfOSTx4CUSofmyL/H9YpjssHa
RQ+47eSjl/KmFGaR31ZWNbFJQ95P5LvLSzMWJEVppIfLsDq3JJVW83
kyRkNSgtFnK+36hWloC9Xk9mX0/fyEbUf8MTFJhVOg+GtSLp2fzZTw
znKfO7ompmSJhK6Va9E6D+XkONY5boEcBl/l7qi0R8IKrWl3m6WyAV
qRooiSf/Dyg0UzQ1dljoJyOivMhShxqtOzcJTidFidQrjOGjeCtfYD
Kv1sMLaFxLBqQOmoNRJqu6MHtt6Jz0UISX/V+j4mm7DyPr9hb9HslT
mdM+ZloDdRKsDjI5o2wpkzjPx4fRprBOAhcOHhSGH0ZNaKlh2ZwT0R
/6E4jwIbj3/I5wh4Vzwct8g+TWGjovyzEq3sd5lWVBanoiXdPzuKuF

-----END PGP PUBLIC KEY BLOCK-----
```

Wenn du dann die Datei, die Signatur und den öffentlichen Schlüssel hast, kannst du den Download verifizieren.

- Klicke in Kleopatra auf „Decrypt/Verify“.
- Wähle die heruntergeladene Datei aus und klicke auf „Open“.
- Wenn alles korrekt ist, erscheint die Nachricht „Valid signature“, was bedeutet, dass die Datei unverändert und echt ist.

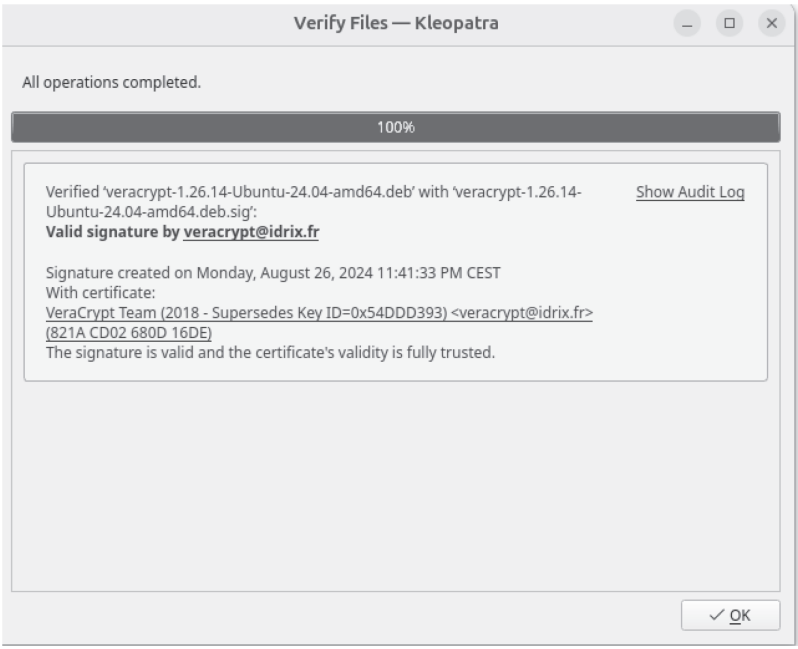

Abbildung 16 Kleopatra Verifikation

Nun kannst du die Datei sicher installieren.

Insbesondere bei Software, die sensible Daten verwaltet – wie Bitcoin-Wallets, die in Kapitel 8 behandelt werden – ist es entscheidend, diesen Schritt durchzuführen. Es dauert nur wenige Minuten und kann dich vor erheblichen Sicherheitsrisiken bewahren. Es ist besser, jetzt kurz zu verifizieren, als später durch manipulierte Software finanzielle Verluste oder Datenlecks zu erleiden.

Finanzmanagement

Ein finanziell stabiles Leben zu führen, ist herausfordernd, wenn man keine klare Vorstellung davon hat, wie viel Geld man verdient, ausgibt und spart. Viele Menschen nutzen verschiedene Tools zur Verwaltung ihrer Finanzen, doch man sollte sorgfältig abwägen, welchem Anbieter man seine sensiblen Daten anvertraut. Denn das Risiko besteht, dass Dritte Zugang zu diesen Daten erhalten.

Icogni, ein Dienstleister, der persönliche Daten im Internet sucht und löscht, hat herausgefunden, dass viele Budget-Apps äußerst großzügig mit den Daten ihrer Nutzer umgehen. In einer im Jahr 2023 durchgeführten Studie stellte das Unternehmen fest, dass 60 % der 20 beliebtesten Apps Nutzerdaten weitergeben. Dazu zählen Informationen wie Kreditscores, Einkommen und detaillierte Ausgaben, die an alle verkauft werden, die bereit sind, dafür zu zahlen – darunter Banken, Versicherungsunternehmen und Werbeagenturen. Bereits ein kurzer Blick auf diese Daten reicht aus, um viel über das Leben und die finanzielle Situation der Nutzer zu erfahren. Um dies zu vermeiden, möchte ich drei privatere Alternativen vorstellen.

Analog: Zurück zu Papier und Stift: Diese Methode ist die sicherste und privateste Variante, besonders geeignet für Personen, die einem hohen Risiko ausgesetzt sind. Es geht nicht nur darum, Einnahmen und Ausgaben zu verfolgen, sondern auch alle Ersparnisse zu verwalten. Besonders im Fall von Bitcoin oder Gold oder Bargeld-Beständen, über die niemand etwas wissen sollte, ist diese Vorgehensweise sinnvoll.

Eine alternative Methode – wenn auch nicht vollständig analog – besteht in der Nutzung eines Air-Gapped-Computers. Das bedeutet, dass dieser Computer keine Verbindung zu Internet, Bluetooth oder ähnlichen Netzwerken herstellt. Dadurch wird das Risiko, mit Viren infiziert zu werden, auf nahezu null reduziert, während du dennoch über die nötige Rechenleistung verfügst. Denn das manuelle Zusammenrechnen aller Transaktionen und das Vornehmen der notwendigen Abzüge können auf Dauer zeitaufwendig sein. Ein Spreadsheet eignet sich hier hervorragend.

Spreadsheet: Viele assoziieren mit einem Spreadsheet sofort Excel. Doch wir möchten uns von Microsoft abgrenzen und stattdessen die Open-Source-Alternative ONLYOFFICE nutzen. Diese Software bietet die gleichen Funktionen wie Excel, erfordert jedoch kein Benutzerkonto, und es werden keine Nutzerdaten erfasst oder weitergegeben. Du kannst eine Budget- und Finanztracking-Tabelle nach deinen eigenen Vorstellungen erstellen oder eine Vorlage herunterladen. Dort musst du nur noch die Tabelle öffnen, alle neuen Daten eintragen, und die Ergebnisse werden automatisch berechnet.

Softwareoptionen: Wenn die beiden oben genannten Optionen für dich zu aufwendig sind und du eine einfachere Lösung bevorzugst, empfehle ich **MoneyManagerEx** (moneymanagerex.org), erhältlich für alle Betriebssysteme. Dieses kostenfreie Open-Source-Programm ist für Mac, Windows, Linux und Android verfügbar. Es bietet eine umfassende Verschlüsselung deiner Daten auf dem Gerät und alle Funktionen, die von einer solchen Software erwartet werden: verschiedene Konten, Währungen, Kategorien, wiederkehrende Transaktionen, Aktien und mehr. Denke daran, regelmäßig deine Daten als CSV-Datei zu sichern, um deine Transaktionshistorie im Notfall nicht zu verlieren.

Für Personen, die einem sehr hohen Risiko ausgesetzt sind oder über beträchtliche Vermögen verfügen, kann es sinnvoll sein, nur einen Teil des tatsächlichen Besitzes anzugeben (z. B. 10 % oder 1 %). So könntest du angeben, nur 10 oder 1 Bitcoin zu besitzen, anstatt die tatsächlichen 100. Für das Hochrechnen musst du dann lediglich eine bzw. zwei Nullen anhängen. Besonders bei Bitcoin solltest du NIEMALS preisgeben, wo diese genau liegen (ob in einer Software- oder Hardware-Wallet, in welcher App oder bei welchem Dienstleister), da ein Datenleck sonst zu einem erheblichen physischen Sicherheitsrisiko führen kann.

Karten und Navigation

Google Maps wird jeden Monat von über einer Milliarde Menschen genutzt, und täglich senden mehr als 20 Millionen Nutzer Vorschläge für Kartenaktualisierungen. Dies führt zu einer verbesserten

Navigation, bedeutet jedoch auch, dass Google eine enorme Menge an Daten sammelt.

Ein Grund für die Popularität von Google Maps ist die benutzerfreundliche Oberfläche, die im Vergleich zu Alternativen deutlich mehr Informationen bietet, etwa Öffnungszeiten, Verkehrslage oder Baustellen. Der Netzwerkeffekt verstärkt diesen Vorteil, wodurch es für Konkurrenten schwierig wird, mitzuhalten.

Der Netzwerkeffekt bedeutet, dass die Plattform wertvoller wird, je mehr Menschen sie nutzen. Nutzer tragen kontinuierlich durch Bewertungen, Fotos und Daten zu Verkehr und Routen bei, wodurch Google Maps immer genauer und hilfreicher wird. Dieser zusätzliche Input verbessert die Qualität für alle anderen Nutzer, was wiederum mehr Menschen anzieht und den Dienst weiter optimiert.

Doch die scheinbar kostenlose Navigation hat ihren Preis: Google sammelt umfangreiche Daten über uns, einschließlich unseres genauen Standorts, der gefahrenen Routen, der Geschwindigkeit und sogar der Aufenthaltsdauer an bestimmten Orten. Das ist auch der Grund, warum Google Maps so bequem zu nutzen ist. Wenn dir deine Privatsphäre jedoch am Herzen liegt, solltest du Alternativen in Betracht ziehen. Ich empfehle jedem, verschiedene Optionen eine Zeit lang auszuprobieren, um die passende Lösung für die eigenen Bedürfnisse zu finden, denn die Ansprüche sind oft sehr unterschiedlich.

OpenStreetMap

OpenStreetMap ist das Wikipedia der Karten. Es handelt sich um eine Open-Source-Plattform, auf der Nutzer selbständig Informationen wie Baustellen oder Öffnungszeiten hinzufügen können. Eine Anmeldung ist nicht erforderlich, und es werden keine personenbezogenen Daten erfasst. Die Webversion ist unter www.openstreetmap.org verfügbar, und die App **OsmAnd~** kann für Android sowie IOS heruntergeladen werden. Daraufhin kannst du dann die benötigten Kartenbereiche herunterladen.

Organic Maps

Organic Maps ist eine Open-Source-Plattform, die ähnliche Funktionen wie OpenStreetMap bietet. Auch hier werden keine persönlichen Daten gesammelt, und eine Anmeldung ist nicht erforderlich. Die App ist sowohl im F-Droid-Store als auch im Apple Store erhältlich. Ich nutze diese Option am häufigsten, da hier die meisten Unternehmen mit ihren Öffnungszeiten verzeichnet sind.

Magic Earth

Magic Earth ist zwar kostenlos, jedoch nicht Open-Source. Die App sammelt keine personenbezogenen Daten und erfordert keinen Account. Im Vergleich zu anderen Alternativen bietet Magic Earth zusätzliche Funktionen wie Stauwarnungen sowie Informationen zu Baustellen und Öffnungszeiten, wobei diese Informationen jedoch nicht immer so aktuell sind wie bei Google Maps.

Alle drei Alternativen ermöglichen Autofahrern, Radfahrern und Fußgängern die Navigation. Zudem kannst du Karten für die Offline-Nutzung herunterladen. Um maximale Privatsphäre zu gewährleisten, empfiehlt es sich, die benötigten Karten (z. B. für Deutschland) herunterzuladen und den Internetzugriff für die App in GrapheneOS zu deaktivieren. So wird sichergestellt, dass keine Daten geteilt werden.

Google Maps

Es ist nachvollziehbar, dass du möglicherweise nicht vollständig auf Google Maps verzichten möchtest oder eine Umstellungsphase benötigst. Es gibt jedoch Möglichkeiten, Google Maps zu nutzen, ohne dabei zu viele Daten preiszugeben.

Wenn du schnell nach einem Geschäft oder Restaurant suchen möchtest, kannst du den zuvor eingerichteten DuckDuckGo-Browser verwenden. Öffne darin Google Maps, suche die benötigten Informationen, ohne dich anzumelden oder den Standort zu aktivieren. Nach dem Schließen des Browsers werden daraufhin alle zwischengespeicherten Daten gelöscht, sodass Google keine Informationen

speichern kann. Hast du die Adresse gefunden, kannst du einen der oben genannten Dienste zur Navigation nutzen.

Solltest du feststellen, dass du Google Maps regelmäßig benötigst, kannst du die App in einem separaten Profil unter GrapheneOS verwenden. Dadurch bleibt sie isoliert und hat keinen Zugriff auf deine Hauptdaten. Wichtig ist, sich niemals mit einem Google-Konto anzumelden und die App ohne Account zu nutzen. So wird die Datenweitergabe auf ein Minimum beschränkt.

• • •

Inzwischen haben wir einen sicheren und privaten Computer sowie ein geschütztes Smartphone eingerichtet, um unsere Internetaktivitäten sicher und anonym fortzusetzen. Anstatt uns auf die Dienste großer Monopole zu verlassen und unsere Daten preiszugeben, setzen wir in vielen Bereichen auf Open-Source-Alternativen, die unsere Privatsphäre schützen.

Dank der Nutzung von Firefox, VPNs und sicheren DNS-Diensten können wir nun privat im Internet surfen. Unsere Daten und Konten sind durch einen Passwortmanager, eine Zwei-Faktor-Authentifizierung und verschlüsselte Backups gut gesichert. Wir haben gelernt, wie wir Technologie sicher und privat nutzen können, ohne dass unsere Identität leicht zurückverfolgt werden kann.

Allerdings hinterlassen wir bis zu diesem Punkt immer noch Spuren unserer Daten, die wir nun beseitigen sollten. Darüber hinaus werden wir im nächsten Kapitel unsere privaten Informationen durch gezielte Desinformation verschleiern. Um weiterhin anonym im Netz unterwegs zu sein, richten wir uns im nächsten Schritt einen Alias ein, der unsere wahre Identität schützt.

Kapitel 7
Unsichtbar werden

„Anonymität ist nicht nur für Kriminelle. Jeder verdient das Recht, sich hinter einem Pseudonym zu verstecken, wenn dies seine Sicherheit oder Freiheit schützt.“ ~ *Bruce Schneier*

Jetzt hast du deinen Computer, dein Handy und deine Apps sicher eingerichtet und könntest theoretisch anonym durchs Leben gehen. Aber das ist erst der Anfang. Selbst wenn du Programme sicher und privat nutzt, kommt irgendwann der Moment, an dem eine Webseite nach deinen echten Daten fragt – was machst du dann?

Außerdem existieren viele Informationen über dich bereits online, und sie verschwinden nicht einfach, nur weil du neue Geräte verwendest. In diesem Kapitel werden wir uns diesen Herausforderungen stellen.

Vermutlich bist du in der Vergangenheit etwas großzügig mit deinen Daten umgegangen. Ob du deine E-Mail-Adresse und deinen Namen zu oft für Newsletter weitergegeben hast, unzählige Online-Konten mit privaten Informationen erstellt oder regelmäßig an deine private Adresse bestellt hast – eines ist sicher: Diese Daten sind jetzt irgendwo in Datenbanken gespeichert und sollten entfernt werden. Im ersten Teil dieses Kapitels werden wir versuchen, so viele Informationen wie möglich zu löschen, damit es keine vollständigen Profile über uns im Internet gibt.

Anschließend erstellen wir eine Alias-Identität. Das bedeutet, ein Profil, mit dem du weiterhin im Internet aktiv sein kannst, ohne deine echten Informationen preiszugeben. So kannst du dich künftig hinter einer fiktiven Person verstecken und bleibst persönlich geschützt. Zuletzt legen wir falsche Fährten zu deiner echten Identität. Dabei nutzen wir falsche Adressen, Telefonnummern und mehr, um es potenziellen Angreifern schwer zu machen und die großen Datensammler in die Irre zu führen.

Informationen löschen

Es ist nahezu unmöglich, sämtliche Daten aus dem Internet zu entfernen, aber wir können sie zumindest auf ein Minimum reduzieren. In den ersten Kapiteln hast du bereits dafür gesorgt, dass möglichst wenige neue Informationen ins Netz gelangen. Jetzt konzentrieren wir uns darauf, die bisher gesammelten Daten zu löschen oder zumindest zu minimieren.

Methoden

Viele Webseiten und Dienste bieten eine unkomplizierte Möglichkeit, deine Konten in wenigen Minuten zu löschen. Die Webseite **JustDeleteMe** (backgroundchecks.org/justdeleteme) ist dabei eine hilfreiche Ressource. Dort findest du die notwendigen Schritte, um deine Accounts bei verschiedenen Anbietern zu löschen. Alternativ kannst du auch einfach nach „[Webseitenname] Account löschen" oder „[Webseitenname] Daten löschen" im Internet suchen, um direkt zur entsprechenden Seite zu gelangen und unnötiges Herumklicken zu vermeiden. Bei etwa 90 % aller Anbieter und Dienstleister ist der Prozess relativ einfach und schnell.

Einige Seiten oder Institutionen erschweren es jedoch, Konten zu löschen. In solchen Fällen habe ich gute Erfahrungen damit gemacht, eine E-Mail zu schreiben. Im Folgenden findest du einen Textvorschlag, den du kopieren und verwenden kannst.

Deutsch:

> Betreff: Antrag auf Löschung meines Accounts und meiner personenbezogenen Daten
>
> Sehr geehrte Damen und Herren,
> ich habe versucht, meine persönlichen Informationen über Ihre Webseite zu entfernen, jedoch ohne Erfolg. Daher bitte ich hiermit um die vollständige Löschung meines Accounts sowie aller personenbezogenen Daten gemäß Art. 17 DSGVO und den Angaben in Ihrer Datenschutzerklärung.
> Meine Kontodaten lauten:

- Benutzername: (falls vorhanden)
- Name: (falls vorhanden)
- E-Mail-Adresse: (falls vorhanden)
- Account-ID: (falls vorhanden)
- Telefonnummer: (falls vorhanden)
- Adresse: (falls vorhanden)

Bitte bestätigen Sie mir die Löschung meines Accounts sowie aller damit verbundenen personenbezogenen Daten innerhalb der gesetzlich vorgeschriebenen Fristen.
Vielen Dank im Voraus für Ihre Unterstützung. Ich erwarte eine Bestätigung der Löschung innerhalb der gesetzlich festgelegten Frist. Vielen Dank für Ihre Unterstützung.
[Name]

Englisch:

Subject: Request for Account Deletion and Removal of Personal Data
Dear Sir or Madam,

I was unable to remove my personal information through your website. Therefore, I formally request the deletion of my account and all personal data in accordance with Article 17 of the GDPR and as stated in your privacy policy.
My account details are as follows:

- Username: (falls vorhanden)
- Email Address: (falls vorhanden)
- Account ID: (falls vorhanden)
- Phone Number: (falls vorhanden)
- Address: (falls vorhanden)

Please confirm that my account and all associated personal data have been permanently deleted from your system.
I would appreciate your confirmation of the account deletion within the legally mandated timeframe. Thank you,
[Name]

GDPR und DSGVO
Die GDPR (General Data Protection Regulation) entspricht der Datenschutz-Grundverordnung (DSGVO) der Europäischen Union. Beide Begriffe beziehen sich auf dieselbe Verordnung, die seit Mai 2018 in Kraft ist. Sie schützt die Privatsphäre von EU-Bürgern, indem sie Unternehmen strenge Vorgaben zur Verarbeitung personenbezogener Daten auferlegt. Nutzer erhalten mehr Kontrolle über ihre Daten, während Unternehmen bei Verstößen hohe Strafen riskieren.

Solltest du nach der E-Mail keine Rückmeldung erhalten, empfiehlt es sich, das Unternehmen telefonisch zu kontaktieren. Oft lassen sich Informationen schneller und unkomplizierter löschen, wenn man direkt mit einem Mitarbeiter spricht. Die meisten sind in solchen Fällen sehr hilfsbereit und entfernen deine Daten ohne weitere Rückfragen.

Wer hat alles deine Daten?

Um herauszufinden, wer unsere Daten gespeichert hat und wo wir überall Konten besitzen, sollten wir die gleiche Vorgehensweise wählen wie ein Angreifer, der mehr über uns erfahren möchte.

Der erste und offensichtlichste Schritt besteht darin, deinen eigenen Namen in den großen Suchmaschinen einzugeben. Ergänze deine Suche mit der Stadt oder dem Land, in dem du aktuell lebst oder in der Vergangenheit gelebt hast. Suche auf Plattformen wie Google, Bing, DuckDuckGo und Yandex, da jede Suchmaschine unterschiedliche Ergebnisse liefert. Wenn du ein Konto oder eine Webseite findest, auf der deine Daten auftauchen, notiere diese, um später die entsprechenden Konten und Daten zu löschen. Es ist ratsam, mindestens die ersten drei Seiten der Suchergebnisse zu durchforsten.

Solltest du keine relevanten Ergebnisse finden oder alle identifizierten Daten entfernt haben, geht es im zweiten Schritt darum, tiefer zu graben – nämlich mit OSINT (Open Source Intelligence). Ein

Angreifer hört nach einer einfachen Suchmaschinensuche nicht auf, sondern nutzt spezielle Tools, um noch mehr Informationen über deine E-Mail-Adresse, Telefonnummer, Adresse und andere Daten zu sammeln. Eine Übersicht solcher Tools und Datenbanken findest du auf osintframework.com.

OSINT (Open Source Intelligence)
OSINT bezeichnet die Sammlung und Auswertung öffentlich zugänglicher Informationen, etwa aus dem Internet, sozialen Medien oder Nachrichten. Es wird genutzt, um Trends zu erkennen, um Risiken zu bewerten und Recherchen durchzuführen – alles legal und ohne spezielle Zugriffsrechte.

Auf dieser Webseite kannst du gezielt nach spezifischen Informationen wie deiner Adresse, deinem Namen, deiner Telefonnummer, E-Mail oder deinem Benutzernamen suchen. Solltest du etwas finden, notiere dir die Funde, um diese später zu entfernen. Eine weitere Möglichkeit besteht darin, dein eigenes E-Mail-Postfach zu durchforsten.

Dies kann jedoch zeitaufwendig sein, da viele von uns Tausende von E-Mails mit Hunderten von Kontoerstellungen in ihren Postfächern haben. Ich empfehle, nach Schlüsselwörtern wie „Account“, „Verify“ (die meisten Konten müssen bestätigt werden), „Welcome“, „Sign up“ oder „Registration“ zu suchen. Alle Konten, die du auf diese Weise findest, solltest du ebenfalls notieren und die entsprechenden E-Mails mit einem Label wie „Löschung gestartet“ markieren.

Ich bin ein Fan davon, alles schriftlich festzuhalten. Dieser Prozess des Suchens und Löschens von Konten kann sich über Tage oder sogar Wochen hinziehen. Daher führe ich eine Liste mit all meinen Konten, die ich löschen möchte oder bei denen ich bereits eine Anfrage gestellt habe, samt aktuellem Status.

Nachfolgend ist ein Beispiel zu sehen (mit Beispieldaten nicht meine echten).

Firma	Account	Status
Google	timo.v@gmail.com	Nicht angefangen
Twitter	TimoV	Gelöscht
Facebook	timo.v	E-Mail gesendet
Apple	timo.v@icloud.com	Anfrage gesendet,

So behält man den Überblick und weiß genau, wo man weitermachen kann, wenn man sich wieder diesem Thema widmet. Zudem ist es motivierend zu sehen, wie die Liste der gelöschten Konten wächst und der Fortschritt sichtbar wird.

Google

Beginnen wir mit einem der größten Datensammler: Google. Glücklicherweise bietet Google eine relativ einfache Möglichkeit, deine Daten oder sogar den gesamten Account zu löschen. Achte jedoch darauf, deinen Google-Account nicht vollständig zu löschen, wenn du die zugehörige E-Mail-Adresse weiterhin benötigst, da sonst alle Nachrichten verloren gehen. Stattdessen kannst du die Menge an Informationen, die Google über dich sammelt, erheblich reduzieren.

- Unter „myaccount.google.com“ hast du Zugriff auf alle Einstellungen deines Google-Kontos. Wenn du mehrere Konten hast, solltest du die folgenden Schritte für jedes Konto wiederholen.
- Falls noch nicht geschehen, richte unter „Sicherheit“ die Zwei-Faktor-Authentifizierung (2FA) ein.
- Gehe zum Reiter „Persönliche Daten“, entferne dein Profilbild und ändere deinen Namen sowie das Geburtsdatum (z. B. „Name“ und „01.01.2000“).
- Entferne, falls vorhanden, deine Telefonnummer und Adresse.
- Gehe auf „Profile ansehen“, durchsuche alle Profile (z. B. Google Maps, YouTube) und entferne, wo möglich, alle persönlichen Informationen oder lösche die Profile komplett.
- Unter „Über mich“ solltest du alle Optionen entweder löschen oder auf privat stellen.
- Wechsel nun zum Reiter „Daten und Datenschutz“.

- Deaktiviere unter „Einstellungen für den Verlauf“ alle Punkte und stelle das automatische Löschen auf 3 Monate ein.
- Deaktiviere „Personalisierte Werbung“ und die „Personalisierung der Suche“.
- Solltest du „Google Fit“ verwendet haben, lösche auch hier alle Daten.
- Entferne unter „Daten aus Apps und Diensten, die du nutzt“ alle Verbindungen und Dienste und lösche die entsprechenden Daten. Je nachdem, wie häufig du Google-Dienste verwendet hast, kann dieser Schritt länger dauern.
- Exportiere unter dem Reiter „Sicherheit“ alle Passwörter aus dem Passwortmanager (falls verwendet) und entferne diese dann.
- Gehe zum Reiter „Kontakte und Teilen“, entferne alle Kontakte (nachdem diese gespeichert wurden) und deaktiviere alle weiteren Optionen.
- Entferne unter „Zahlungen & Abos“ alle hinterlegten Zahlungsdaten.

Da Google das Layout seiner Seite regelmäßig aktualisiert, können die Schritte leicht variieren. Es ist jedoch wichtig, dass du alles deaktivierst und löschst, was möglich ist gehe dafür durch alle Einstellungen und wähle entfernen bzw. löschen aus. Nun entfernen wir endgültig alle bei Google gespeicherten Daten. Speichere zuvor wichtige Daten aus der Cloud offline, da du später keinen Zugriff mehr darauf haben wirst. Dies kannst du unter takeout.google.com umsetzen. Dort kannst du auswählen, welche Daten du exportieren möchtest – vieles davon benötigst du wahrscheinlich nicht mehr. Stelle sicher, dass du alle Daten sicher gespeichert hast. Die nächsten Schritte können nicht rückgängig gemacht werden.

- Um alle Fotos zu löschen, gehe auf photos.google.com, wähle das erste Bild aus, scrolle nach unten und halte die Umschalttaste (Shift) gedrückt, während du das letzte Bild auswählst. Klicke anschließend auf das Papierkorbsymbol, um alle Bilder zu löschen. Vergiss nicht, den Papierkorb anschließend zu leeren.

- Um alle Dateien in Google Drive zu löschen, gehe auf drive.google.com, wähle mit „Strg + A“ alle Dateien aus und klicke anschließend auf „Löschen“.
- Für alle weiteren Google-Dienste besuche die Webseite about.google/products/#all-products, wähle die genutzten Dienste aus und lösche nach einem Backup alle Informationen und Dateien.

Je nachdem, wie intensiv du Google genutzt hast, können diese Schritte unterschiedlich viel Zeit in Anspruch nehmen. Am Ende wirst du jedoch fast alle Informationen, die Google über dich gesammelt hat, gelöscht und deine Einstellungen so angepasst haben, dass deine Privatsphäre geschützt bleibt. Idealerweise musst du dich nun nicht mehr bei diesem Google-Konto anmelden, da alle Daten gesichert und alle E-Mails an einen sicheren E-Mail-Dienst wie Proton-Mail weitergeleitet werden.

Wenn du dir sicher bist, dass du dieses Google-Konto nicht mehr benötigst und die dazugehörige E-Mail-Adresse nicht mehr verwenden möchtest, kannst du das Konto unter „Daten und Datenschutz“ im Bereich „Mein Google-Konto löschen“ endgültig entfernen. Dieser Schritt ist jedoch nicht umkehrbar, gehe also mit Vorsicht vor.

Social Media

Dieser Schritt mag für viele besonders herausfordernd sein. Doch wer ernsthaft seine Online-Präsenz reduzieren will und ein Leben mit mehr Privatsphäre anstrebt, kommt um ihn nicht herum: das Löschen aller Social-Media-Accounts. Durch deine Social-Media-Profile sammeln nicht nur Unternehmen, sondern auch Privatpersonen und Institutionen wertvolle Informationen über dich. Dies gilt nicht nur für aktuelle und häufig genutzte Konten, sondern auch für alte, möglicherweise längst vergessene Profile, die sich im Laufe der Jahre angesammelt haben.

Solltest du diesen Schritt nicht wagen wollen, ist es zumindest ratsam, die Privatsphäre-Einstellungen deiner Profile anzupassen, um den öffentlichen Zugriff zu erschweren. Lösche alte Beiträge, die nicht mehr relevant sind, und entferne Freunde und Follower, die du

nicht mehr benötigst. Jede Person weniger, die dein Profil sehen kann, verringert ein potenzielles Risiko.

Weitere Accounts

Neben den Social-Media-Profilen haben sich im Laufe der Jahre wahrscheinlich zahlreiche andere Online-Konten oder persönliche Blogs angesammelt, von denen viele längst ungenutzt oder vergessen sind. Diese Konten solltest du ebenfalls löschen.

Im Abschnitt „Methoden“ haben wir bereits besprochen, wie du deine Accounts findest. Jetzt geht es darum, die Arbeit zu erledigen: Durchsuche deine Liste, finde die ungenutzten Konten und lösche sie entweder direkt auf der Webseite oder per E-Mail-Anfrage. Auch wenn es Zeit kostet, bringt dir jede gelöschte Information ein Stück mehr Sicherheit und Privatsphäre zurück. Manche Webseiten erschweren das Löschen oder Deaktivieren von Accounts. Auch wenn es mühsam ist, sollte der Schutz deiner Privatsphäre den Aufwand rechtfertigen.

Da du in Zukunft wahrscheinlich neue Online-Konten erstellen wirst, ist es ratsam, dabei auf E-Mail-Aliase und fiktive Informationen zurückzugreifen. Wenn ein Name erforderlich ist, denke dir einen aus oder nutze einen Alias. Für die Adresse könntest du eine nahegelegene, aber nicht deine eigene angeben. Das Geburtsdatum? Einfach das heutige Datum plus/minus 10 Jahre. Und ganz wichtig: Notiere dir, wo und wann du einen Account erstellt hast. So kannst du ihn später leichter wiederfinden und löschen.

Alte Geräte

Falls du in den ersten Kapiteln des Ratgebers die Empfehlung befolgt und dir neue Geräte angeschafft hast, stehen nun wahrscheinlich deine alten Geräte ungenutzt herum. Es ist wichtig, diese alten Geräte, die du nicht mehr verwendest, auf die Werkseinstellungen zurückzusetzen, nachdem du alle wichtigen Daten gesichert hast.

Danach hast du zwei Möglichkeiten:

Verkaufen: Du kannst die Geräte verkaufen, um einen Teil deiner Investition zurückzuerhalten. Gleichzeitig sorgst du damit für Verwirrung bei den Netzbetreibern, da sie nun eine neue Person mit anderen Standortdaten registrieren müssen. Allerdings ist dies nicht ganz optimal, da das Gerät jetzt einer anderen Person gehört, was immer ein gewisses Risiko mit sich bringt.

Ausschalten und aufbewahren: Wenn du mehr Kontrolle über deine alten Geräte behalten möchtest, schalte sie vollständig aus und bewahre sie in einer Faraday-Tasche bei dir zu Hause auf. So kannst du sicherstellen, dass sie nicht mehr getrackt werden und niemand unbefugt darauf zugreifen kann.

Google-Suchergebnisse aktualisieren

Nachdem du wichtige Konten und persönliche Daten gelöscht hast, kann es sein, dass diese Informationen weiterhin in den Google-Suchergebnissen angezeigt werden. Dies geschieht, weil Google die betreffenden Seiten in seinen Suchergebnissen noch nicht aktualisiert hat. Selbst wenn die sensiblen Informationen bereits entfernt wurden, können sie nach wie vor in den Suchergebnissen sichtbar sein.

Um dies zu ändern, kannst du Google auffordern, die veralteten Inhalte zu aktualisieren. Dieses Tool löscht die betroffenen Seiten nicht, sondern aktualisiert nur die Suchergebnisse. Die sensiblen Informationen musst du zuvor selbst entfernt haben.

- Melde dich mit einem Google-Konto an – ich benutze dafür ein anonymes Konto, das ich nur für solche Zwecke habe.
- Öffne die Webseite search.google.com/search-console/remove-outdated-content und klicke auf „Neuer Antrag“.
- Wähle „Ein veraltetes Ergebnis in der Google-Suche…“ aus und gib die genaue URL der Seite ein, z. B. nicht nur https://www.linkedin.com, sondern die genaue URL deines Profils, die du entfernt haben möchtest, wie z.B. https://www.linkedin.com/in/DeinName.
- Sende den Antrag ab.

Nach etwa 24 Stunden sollte das Suchergebnis aktualisiert und deine Informationen müssten aus den Google-Ergebnissen verschwunden sein. Diesen Schritt ist in der Regel durchzuführen, wenn du Accounts oder persönliche Daten gelöscht hast, die zuvor über Google-Suchanfragen auffindbar waren.

Google-Suchergebnisse entfernen

Wie bereits erwähnt, kannst du Google nicht direkt auffordern, beliebige Seiten zu löschen. Es gibt jedoch Ausnahmen für besonders sensible Informationen, die Google unter bestimmten Umständen entfernen kann. Dazu zählen:

- Adressen, Telefonnummern oder E-Mail-Adressen
- Vertrauliche staatliche Identifikationsnummern
- Bankkonto- oder Kreditkartennummern
- Handschriftliche Unterschriften oder Ausweisdokumente
- Vertrauliche persönliche und offizielle Unterlagen (z. B. medizinische Daten)
- Vertrauliche Anmeldedaten
- Inhalte, die Minderjährige zeigen
- Inhalte mit Nacktheit oder sexuellen Darstellungen
- Inhalte, deren Entfernung auf der Webseite kostenpflichtig ist

Es gibt zahlreiche Gründe, die Google akzeptiert, um Informationen aus den Suchergebnissen zu entfernen. Dabei werden die Informationen jedoch nicht von der Webseite selbst gelöscht, sondern lediglich aus den Google-Suchergebnissen entfernt. Daher ist es ratsam, auch den Webseitenbetreiber zu kontaktieren, um eine vollständige Löschung der Daten zu veranlassen.

- Besuche die Webseite support.google.com/websearch/contact/content_removal_form und folge den Anweisungen.
- Gib deinen Namen und eine E-Mail-Adresse an – hier kannst du wieder eine anonyme E-Mail-Adresse verwenden.
- Die weiteren Informationen, die Google benötigt, um die Anfrage durchzuführen, werden auf der Seite gut erklärt.

Auch Bing bietet einen ähnlichen Dienst an, den du unter der Webseite microsoft.com/de-de/concern/bing findest.

Regelmäßige Überprüfung persönlicher Daten

Um sicherzustellen, dass keine persönlichen Daten ungewollt veröffentlicht werden, solltest du regelmäßig in verschiedenen Suchmaschinen nach deinen Informationen suchen. Ich empfehle dir, Google, Bing und DuckDuckGo zu nutzen. Achte dabei nicht nur auf deinen Namen, sondern auch auf andere sensible Daten, die du privat halten möchtest.

- E-Mail-Adressen
- Telefonnummern
- Adressen
- Medizinische Daten in Verbindung mit deinem Namen
- Informationen über Familienmitglieder

Bitte beachte, dass Suchergebnisse nur angezeigt werden, wenn sie exakt mit deiner Anfrage übereinstimmen. Experimentiere daher mit verschiedenen Schreibweisen, beispielsweise bei Identifikationsnummern oder Bankdaten, indem du Leerzeichen, Groß- und Kleinschreibung sowie unterschiedliche Formatierungen ausprobierst. Führe solche Suchanfragen zudem nur in einer sicheren Internetumgebung durch, um zu verhindern, dass sensible Daten in die falschen Hände geraten.

Datenbroker

Datenbroker, auch bekannt als Informationshändler, sind genau die Unternehmen, vor denen wir uns schützen möchten. Firmen wie Google oder Microsoft sammeln riesige Mengen an Daten, die dann an Datenbroker weitergegeben werden, die im Hintergrund agieren. Diese erstellen detaillierte Benutzerprofile und verkaufen diese an den Höchstbietenden oder stellen sie sogar auf Personensuchmaschinen zur Verfügung. Diese Profile enthalten eine Vielzahl von Informationen, die Datenbroker über uns finden oder erwerben können. Dazu zählen nicht nur persönliche Daten wie Namen, Adressen oder Telefonnummern, sondern auch Annahmen über unsere Interessen.

Diese Annahmen entstehen durch die Auswertung von Suchverläufen, Konten, Kaufverhalten, Treuekarten oder sozialen Medien. So wird ein umfassendes Bild unserer Identität geschaffen, um gezielte Werbung an uns zu richten. Datenbroker sammeln unsere Informationen nicht nur online, etwa durch Webtracking, sondern auch offline. Viele öffentliche Dokumente wie Heiratsurkunden, Immobilienverzeichnisse, geschäftliche Lizenzen oder Kraftfahrzeugregister liefern ihnen ebenfalls wertvolle Daten.

Es ist zwar schwierig, sich vollständig und dauerhaft von den Listen dieser Datenbroker fernzuhalten, doch es gibt zwei Ansätze, um die Kontrolle zurückzugewinnen. Es ist ein ständiges Katz-und-Maus-Spiel.

Option 1: Selbstständig vorgehen: Diese Methode erweist sich oft als effektiver, da du dich gezielt auf die großen Datenbroker konzentrieren kannst, die die meisten Informationen sammeln. Es gibt zahlreiche Webseiten, die den Prozess Schritt für Schritt erläutern, beispielsweise privacyrights.org/data-brokers.

Dort findest du eine umfassende Liste der gängigen Datenbroker sowie präzise Anleitungen, wie du deine Daten entfernen lassen kannst. Allerdings erfordert diese Option Geduld und regelmäßige Überprüfungen, um wirklich effektiv zu sein. Da es Dutzende solcher Unternehmen gibt, kann dieser Prozess zeitaufwendig werden.

Option 2: Eine spezialisierte Firma beauftragen: Diese Option spart viel Zeit, da eine Firma die mühsame Arbeit für dich übernimmt. Allerdings bleibt oft unklar, ob tatsächlich alle Daten bei sämtlichen Brokern gelöscht wurden. Diese Unternehmen suchen nach deinen persönlichen Daten und reichen dann, basierend auf der Vollmacht, die du ihnen erteilt, Löschanträge bei den entsprechenden Brokern ein.

Es könnte sein, dass hier deutlich weniger Informationen über uns im Umlauf sind – insbesondere, wenn man in der Vergangenheit bereits darauf geachtet hat, wie man sich im Internet bewegt. Die Sorgen, die in der amerikanischen Privatsphäre-Community bestehen, sind jedoch berechtigt, denn in den USA ist die Situation wesentlich

schlimmer. Das liegt vor allem daran, dass der Markt für Datenbroker dort deutlich profitabler ist, da Europa, insbesondere Deutschland, mit der DSGVO viel strengere Datenschutzrichtlinien hat. Die Erhebung, Speicherung und Verarbeitung personenbezogener Daten unterliegt hier klaren Regeln, die den Markt weniger attraktiv machen.

In Deutschland sind viele Unternehmen kleiner und spezialisiert auf Kreditinformationen, Bonitätsprüfungen und Adresshandel. Viele dieser Firmen stehen in engem Zusammenhang mit staatlichen Stellen, weshalb es hier schwieriger ist, Daten löschen zu lassen.

Dennoch haben wir das Recht auf Auskunft darüber, welche Daten diese Unternehmen über uns speichern. Folgende Unternehmen spielen dabei eine Rolle:

Schufa Holding AG

- Webseite: www.schufa.de
- E-Mail Kontakt: datenschutz@schufa.de

Creditreform

- Webseite: www.creditreform.de
- E-Mail Kontakt: datenschutz@creditreform.de

Bürgel Wirtschaftsinformationen

- Webseite: www.buergel.de
- E-Mail Kontakt: datenschutz@buergel.de

Acxiom Deutschland GmbH

- Webseite: www.acxiom.de
- E-Mail Kontakt: datenschutz@acxiom.com

Um Informationen über die gespeicherten Daten zu erhalten, kannst du den Unternehmen eine E-Mail senden. Dafür kannst du z. B. folgende Vorlagen verwenden.

Betreff: Datenauskunft gemäß Art. 15 DSGVO

Sehr geehrte Damen und Herren,

ich bitte um eine Auskunft gemäß Artikel 15 der Datenschutz-Grundverordnung (DSGVO) darüber, welche personenbezogenen Daten Sie über mich gespeichert haben.
Zu meiner Identifikation:

- Name:
- Anschrift:
- Geburtsdatum:

Bitte senden Sie mir die Informationen kostenlos und fristgerecht innerhalb eines Monats an diese E-Mail-Adresse.

Mit freundlichen Grüßen,
[Name]

Sobald du die angeforderten Daten erhalten hast, besteht die Möglichkeit, bestimmte Informationen löschen zu lassen. Allerdings schränkt die Gesetzeslage unsere Optionen in diesem Bereich ein, denn:

- Daten, die zur Erfüllung gesetzlicher Pflichten (z. B. steuerliche Aufbewahrungspflichten) oder zur Geltendmachung und Verteidigung von Rechtsansprüchen benötigt werden, dürfen nicht gelöscht werden.
- Auch Daten, die im öffentlichen Interesse oder zur Wahrnehmung des Rechts auf freie Meinungsäußerung verarbeitet werden, können unter Umständen weiterhin gespeichert werden.

Dies ist sehr vage formuliert und kann nahezu immer als Argument verwendet werden. Trotz dieser Einschränkungen gibt es jedoch zahlreiche Fälle, in denen Daten gelöscht werden können, z. B.:

- Wenn die Daten für den ursprünglichen Zweck nicht mehr notwendig sind.
- Wenn die Einwilligung widerrufen wird oder der Verarbeitung widersprochen wird.
- Wenn die Daten unrechtmäßig verarbeitet wurden.

Um die Löschung von Daten zu beantragen, solltest du eine formelle Anfrage über die Webseite des betreffenden Unternehmens einreichen und den Prozess zur Prüfung der Löschung in Gang setzen.

Unbenutzte Apps entfernen

Genauso wie sich Online-Accounts ansammeln, häufen sich bei vielen von uns auch Apps an, die kaum oder gar nicht genutzt werden. Oft laden wir eine App herunter, verwenden sie ein oder zwei Mal und lassen sie dann einfach auf dem Smartphone zurück, während sie weiterhin Daten sammelt. Es ist daher ratsam, regelmäßig alle Apps und Anwendungen zu überprüfen und diejenigen zu löschen, die du nicht mehr benötigst. Durch das Entfernen dieser Apps werden auch viele gespeicherte Nutzerdaten gelöscht, was deine Privatsphäre erheblich verbessert.

Freunde und Familie

Auch Freunde und Familie können ein Risiko für deine Privatsphäre darstellen. Viele von ihnen nutzen Social Media und laden im Laufe der Zeit möglicherweise das eine oder andere Foto hoch, auf dem du zu sehen bist. Diese Bilder enthalten oft auch Standortinformationen oder genaue Beschreibungen, wann und wo sie aufgenommen wurden – Informationen, die problematisch sein könnten.

In den meisten Fällen genügt es, deine Freunde oder Familienmitglieder höflich zu bitten, diese Fotos zu entfernen oder zumindest die Einstellungen so anzupassen, dass sie nicht öffentlich sichtbar sind. Einige werden deine Einstellung zur Privatsphäre mehr respektieren als andere. Ein nachvollziehbarer Grund, der oft auf Verständnis stößt, ist: „Ich möchte nicht, dass meine Arbeit oder mein Chef sieht, was ich in meiner Freizeit mache.“ Damit können sich nähmlich viele identifizieren.

Newsletter abbestellen

Falls du auf ProtonMail umgestiegen bist, ist dieser Schritt besonders einfach: Alle Newsletter, die du nicht mehr benötigst, kannst du mit nur einem Klick auf „Abbestellen“ oder „Unsubscribe“

deaktivieren. Die meisten Newsletter sind ohnehin nur Werbekampagnen, die dein Postfach unnötig füllen. Durch das Abbestellen entziehst du diesen Unternehmen den Zugriff auf deine E-Mail-Adresse.

Idealerweise solltest du dich von allen Newslettern, die an deine primäre E-Mail-Adresse gesendet werden, abmelden. Wenn es dennoch Newsletter gibt, die du lesen möchtest, empfiehlt es sich, eine Alias-E-Mail-Adresse ausschließlich für diesen Zweck zu verwenden.

Newsletter
Wenn dir dieses Buch gefällt und du mehr Informationen zu Privatsphäre und Sicherheit wünschst, kannst du dich auf gerne mit deiner Alias Adresse auf privatopia.de/newsletter anmelden.

Achte bei zukünftigen Anmeldungen darauf, Unternehmen nicht zu erlauben, dir Werbung und Informationsmaterial zuzusenden. Oft versteckt sich diese Zustimmung in einem kleinen Kästchen, das du bei der Registrierung eines Kontos ankreuzen musst. Wenn du dem Unternehmen die Erlaubnis gibst, dich zu kontaktieren, öffnest du Tür und Tor für unerwünschte Werbenachrichten. Noch schlimmer: Deine E-Mail-Adresse kann weiterverkauft werden – für 3 bis 30 Euro pro Monat – nur weil du dieses Kästchen angekreuzt hast.

Bei physischen Werbesendungen ist die Situation etwas komplizierter. Hier gelten andere Regelungen, und es gibt keine einfache Möglichkeit, diese durch einen Klick auf „Abbestellen“ zu stoppen. Wenn du jedoch die vorherigen Schritte befolgt hast, solltest du bereits eine Verbesserung feststellen, da deine Adresse aus den meisten Datenbanken entfernt wurde.

Bei der Post, die du weiterhin erhältst, gibt es zwei Szenarien: Entweder sie kommt immer von derselben Firma oder von verschiedenen. Wenn es unterschiedliche Absender sind, bedeutet dies, dass deine Adresse noch irgendwo bei einem Datenbroker im Umlauf ist. In diesem Fall solltest du dort nachhaken und deine Daten löschen lassen. Handelt es sich hingegen um denselben Anbieter, reicht

meist ein kurzer Anruf, um die Abbestellung vorzunehmen. Eine einfache Erklärung wie „Das Familienmitglied, das Interesse hatte, ist weggezogen“ und der Hinweis, dass diese Werbesendungen nur unnötigen Papiermüll verursachen, sind oft ausreichend.

Es ist nahezu unmöglich, alle Spuren persönlicher Daten vollständig zu beseitigen. Doch die richtige Kombination aus einem auf Privatsphäre ausgerichteten Computer, sicheren Apps und regelmäßigen „Aufräumarbeiten“ kann dazu beitragen, unsere digitale Spur so klein wie möglich zu halten. Ich weiß, dass dies der langweiligste und oft undankbarste Teil unserer Bemühungen für mehr Privatsphäre ist, doch er ist von entscheidender Bedeutung und sollte auf keinen Fall vernachlässigt werden.

Aliase (Pseudonyme)

Stell dir vor, du könntest sowohl online als auch im echten Leben in eine alternative Identität zu schlüpfen, ohne dabei ständig deine wahre Person preiszugeben. Ein Alias oder Pseudonym ermöglicht genau das und bietet zahlreiche Vorteile für deine Privatsphäre und Sicherheit. Während jemand mit einem gängigen Namen wie Lukas Müller möglicherweise weniger Bedarf für ein Pseudonym hat, kann es für Personen mit selteneren Namen durchaus sinnvoll sein, sich eine alternative Identität zuzulegen. Denk darüber nach, wer alles an deinem echten Namen interessiert sein könnte und welche Informationen du dadurch preisgibst.

Online-Konten: Bei der Erstellung von Online-Konten werden häufig der Name und weitere persönliche Daten abgefragt. Ein Pseudonym kann in dem Fall helfen, deine wahre Identität zu schützen.

Geschäfte und Restaurants: Ob bei einer Tischreservierung im Restaurant oder bei der Bestellung maßgeschneiderter Kleidung – häufig werden Name und Kontaktinformationen abgefragt. Es gibt jedoch oft keinen echten Vorteil, den eigenen Namen anzugeben.

Rabattaktionen: Viele Geschäfte bieten Rabatte über Apps oder Newsletter an, sammeln dabei jedoch umfangreiche Informationen

über uns. Die Verwendung eines Pseudonyms kann verhindern, dass dein Einkaufsverhalten mit deiner echten Identität verknüpft wird.

Online-Kommunikation: In Foren, beim Spielen von Online-Videospielen oder in Webinaren genügt es oft, wenn andere ein Pseudonym kennen. Ob dieses mit deinem echten Namen übereinstimmt, ist dabei irrelevant.

Trennung von Berufs und Privatleben: Im beruflichen Umfeld kann es eine Herausforderung sein, ein Pseudonym zu verwenden. Im privaten Bereich hingegen ist es gegebenenfalls sehr hilfreich, um sich vor neugierigen Kollegen oder Vorgesetzten zu schützen.

Meinungsfreiheit: Wer sich in Online-Debatten engagiert oder kritische Meinungen äußern möchte, kann durch die Verwendung eines Pseudonyms verhindern, dass diese Äußerungen direkt mit seiner eigenen Identität verknüpft werden. Dies ist besonders wichtig im Hinblick auf mögliche Konsequenzen im Berufsleben oder im sozialen Umfeld, aber auch in Anbetracht der jüngsten Fälle von Hausdurchsuchungen.

Identitätsdiebstahl: Identitätsdiebstahl kann schneller geschehen, als man denkt. Sei es durch einen gefälschten Ausweis oder durch jemanden, der online deine Identität übernimmt – beides lässt sich durch die Verwendung eines Pseudonyms vermeiden.

Schutz vor Stalking: Ein Pseudonym schützt nicht nur vor Stalkern, sondern auch vor neugierigen Menschen, die sich in dein Privatleben einmischen möchten.

Sicherheit: Viele Bitcoin-Core-Entwickler nutzen Pseudonyme, um sich vor unerwünschter Aufmerksamkeit durch Staaten oder Kriminelle zu schützen, die möglicherweise Interesse an ihrer Identität haben. Ein Pseudonym bietet ihnen eine gewisse Anonymität und Sicherheit.

Berühmtheit: Egal ob durch soziale Medien, eine Buchveröffentlichung oder eine hohe Position in einem Unternehmen – ein Pseudonym ermöglicht es, das Privatleben weitgehend ungestört zu führen.

Zukünftige Entwicklungen: Auch wenn deine Online-Präsenz derzeit noch gering ist, kann sich das schnell ändern. Vielleicht wirst du in Zukunft im Journalismus tätig oder gewinnst im Lotto. Ein Pseudonym bietet dir bereits jetzt einen gewissen Schutz für solche Eventualitäten.

Anonymität vs. Pseudonymität

Pseudonyme bieten zwar ein gewisses Maß an Anonymität, garantieren jedoch keine vollständige Anonymität. Es bestehen Unterschiede zwischen diesen beiden Konzepten, die jeweils ihre eigenen Vor- und Nachteile mit sich bringen.

Anonymität: Bei vollständiger Anonymität bist du nicht mehr rückverfolgbar. Unterschiedliche Benutzernamen für verschiedene Konten verhindern jegliche Verknüpfung deiner Identitäten. Dies stellt den größten Vorteil der Anonymität dar, doch sie ist auch schwieriger aufrechtzuerhalten.

Pseudonymität: Ein Pseudonym bietet hingegen eine gewisse Kontinuität. Vollständig anonyme Zeichenfolgen wirken oft verdächtig und ziehen Aufmerksamkeit auf sich. Ein gut gewähltes Pseudonym hingegen fällt nicht auf und wird in der Regel nicht hinterfragt.

Der richtige Ansatz hängt von deinen Zielen ab: Anonymität bietet den höchsten Schutz, während Pseudonymität es ermöglicht, sich diskret im digitalen Raum zu bewegen, ohne dabei verdächtig zu wirken.

Das Pseudonym erstellen

Der erste Schritt zur Erstellung eines Pseudonyms ist die Wahl eines Namens. Dies ist der wichtigste und oft auch schwierigste Teil des Prozesses. Es gilt, einen Namen zu finden, der deine wahre Identität verbirgt und gleichzeitig natürlich wirkt. Überlege dir dabei: Wovor möchtest du dich schützen? Wie hoch ist dein Sicherheitsbedarf? Ein völlig zufälliger Alias bietet zwar einen höheren Schutz, kann sich jedoch ungewohnt anfühlen. Viele möchten auch nicht den Eindruck erwecken, zu lügen. Daher gibt es verschiedene Optionen, die von

einfachen bis hin zu komplexen Pseudonymen reichen. Unabhängig davon, für welche Variante du dich entscheidest – ein Alias ist immer besser als keiner.

Option 1: Vorname + Zweitname oder Geburtsname
Dies ist die einfachste Möglichkeit und erfordert nur wenig Aufwand. Du verwendest deinen echten Vornamen und kombinierst ihn mit deinem Zweitnamen oder einem früheren Nachnamen, z. B. deinem Geburtsnamen vor einer Heirat. Ein Beispiel: Lukas Alexander Müller wird zu Lukas Alexander, oder Jonas Bauer nutzt seinen Geburtsnamen „Schmidt". Der Vorteil dieser Methode ist, dass der Name leicht zu merken ist und sich in alltäglichen Situationen, etwa beim Check-in im Hotel, unkompliziert verwenden lässt. Der Nachteil besteht darin, dass lediglich der Nachname geschützt wird.

Option 2: Vorname + ausgedachter Nachname
Diese Variante wird am häufigsten genutzt. Der Vorname bleibt unverändert, während der Nachname vollständig ausgetauscht wird. So kannst du in Gesprächen weiterhin auf deinen Vornamen reagieren, während der neue Nachname deine Identität schützt. Z. B. wird Maximilian Becker zu Maximilian Wagner. Wenn du deine Identität noch weiter verschleiern möchtest, kannst du den Vornamen abkürzen oder einen Spitznamen verwenden, beispielsweise Maximilian für „Max" oder Leonardo für „Leo". Diese Option bietet eine gute Balance zwischen Schutz und Alltagstauglichkeit.

Option 3: Ausgedachter Vorname + ausgedachter Nachname
Dies ist die sicherste Option. Hier wählst du sowohl einen neuen Vor- als auch Nachnamen, die keinerlei Bezug zu deiner echten Identität haben. Diese Wahl bietet maximalen Schutz, erfordert jedoch, dass du dich an den neuen Namen gewöhnst und in Gesprächen darauf reagierst. Für die meisten Menschen reicht Option 2 aus, aber wenn du den höchsten Schutz benötigst, ist dies die beste Wahl.

Beginne einfach und taste dich Schritt für Schritt zu einem Pseudonym vor, das zu dir passt. Ein gut gewähltes Pseudonym schützt deine Privatsphäre, ohne dass du dich verstellen musst. Die Auswahl kann herausfordernd sein, aber es gibt Online-Dienste, die dir dabei helfen können (z. B randomwordgenerator.com/name.php). Achte

darauf, dass der Name leicht auszusprechen, zu buchstabieren und zu verstehen ist. Vermeide sehr gängige Nachnamen, da manche Dienstleister bei häufigen Namen misstrauisch werden könnten.

Pseudonym anwenden

Ein Pseudonym kann ein effektives Werkzeug sein, um deine Privatsphäre zu wahren. Sobald du dich für einen passenden Alias entschieden hast, kannst du beginnen, ihn in deinen Alltag zu integrieren. Für manche Menschen reicht es aus, den Alias nur in bestimmten Situationen zu verwenden. Wenn du jedoch planst, das Pseudonym häufiger – sowohl online als auch offline – zu nutzen, gibt es einige wichtige Schritte, die du beachten solltest.

Nehmen wir „Paul Huber" als Beispiel. Führe die folgenden Schritte in einer sicheren Umgebung durch, beispielsweise an einem vertrauenswürdigen Computer, und nutze idealerweise ein VPN, um die Verbindungen zwischen deiner echten Identität und dem Pseudonym zu minimieren.

Geburtsdatum: Viele Anmeldungen, ob online oder offline, verlangen nach einem Geburtsdatum. Wähle ein Datum, das maximal drei Jahre von deinem echten Geburtsdatum abweicht und einen anderen Tag oder Monat hat. Sei darauf vorbereitet, eventuell Geburtstagsglückwünsche zu erhalten, und sei bereit, Fragen zu deinem Alter oder Sternzeichen zu beantworten.

Bild: Die Wahl des Bildes hängt davon ab, wie anonym du bleiben möchtest. Optionen sind kein Bild, dein eigenes Bild oder ein generiertes Bild (z. B. von thispersondoesnotexist.com). Wenn du ein eigenes Bild nutzt, stelle sicher, dass keine Metadaten enthalten sind und dass das Bild nicht mit deiner echten Identität verknüpft ist. Verwendest du nämlich dasselbe Bild für deine echte und deine Alias-Identität, kann eine einfache Bildersuche die Verbindung herstellen. Eine weitere Möglichkeit ist, ein eigenes Bild in niedrigerer Qualität zu verwenden, sodass dein Gesicht nicht klar erkennbar ist.

Hintergrundinformationen: Smalltalk ist oft unvermeidlich, sei es online oder im realen Leben. Du kannst eine komplett neue

Berufsbiografie und Lebensgeschichte für deinen Alias erstellen oder nur kleine Anpassungen an deinem echten Lebenslauf vornehmen. Achte darauf, dass Widersprüche schnell auffallen können und deinen Alias gefährden. Bei zu persönlichen Fragen kannst du höflich darauf hinweisen, dass diese Informationen nicht relevant sind.

E-Mail: Es ist unerlässlich, eine eigene E-Mail-Adresse für den Alias zu verwenden. Wenn du einen Alias-Namen angibst, aber deine echte oder anonyme E-Mail-Adresse nutzt, kann das Misstrauen hervorrufen. Am besten erstellst du eine separate E-Mail-Adresse, z. B. paul.huber@protonmail.com.

Telefonnummer: Eine zusätzliche Telefonnummer für den Alias ist sinnvoll. Wenn du dieselbe Nummer für deine private und deine Alias-Identität verwendest, wird der Alias mit deiner echten Nummer verknüpft. Eine neue Nummer, die auf deinen echten Namen registriert ist, bietet ebenfalls wenig Anonymität. Hier können anonyme Prepaid-Karten oder VoIP-Nummern hilfreich sein.

Website und Domain: Für besondere Anlässe ist es ratsam, eine eigene Website mit einer passenden Domain für deinen Alias zu erstellen. Dies steigert die Glaubwürdigkeit erheblich. Beispielsweise könntest du die Domain paul-huber.de registrieren und die E-Mail-Adresse huber@paul-huber.de verwenden. Dies vermittelt einen professionellen Eindruck und kann mögliche Bedenken zerstreuen.

Soziale Netzwerke: Obwohl ich die Nutzung sozialer Netzwerke nicht empfehle, verstehe ich, dass sie für viele Menschen unverzichtbar sind. Du kannst einen Account unter einem Alias-Namen erstellen, um deine Privatsphäre zu wahren und dennoch Zugang zu sozialen Medien zu erhalten. Dies steigert auch die Glaubwürdigkeit deines Pseudonyms.

Visitenkarten: Im realen Leben kann eine Visitenkarte dazu beitragen, deine Identität zu bestätigen, insbesondere wenn jemand skeptisch ist. Es gibt zahlreiche kostenlose Designs, die du online erstellen und kostengünstig drucken lassen kannst. Das Hinzufügen eines Fotos verleiht der Karte zusätzlich Glaubwürdigkeit. Achte jedoch darauf, keine großen Unternehmen als Arbeitgeber anzugeben,

sondern wähle stattdessen eine erfundene oder eigene Firma, z. B. „PH IT-Services“.

Bezahlen: All diese Bemühungen sind vergeblich, wenn du mit deiner herkömmlichen Kreditkarte bezahlst. Der Name auf der Karte wird mit dem Alias verknüpft. Versuche daher, wann immer möglich, bar oder mit anonymen Zahlungsmethoden zu bezahlen.

Konsistenz: Das A und O beim Alias ist Konsistenz. Überlege dir genau, wie weit du mit dem Alias gehen möchtest, und halte dich strikt an diesen Plan. Nichts gefährdet die Glaubwürdigkeit eines Alias mehr als Unstimmigkeiten in den Angaben.

Alles dokumentieren: Ein Alias kann viele unterschiedliche Informationen und Verbindungen enthalten. Daher ist es wichtig, den Überblick zu behalten. Es empfiehlt sich, ein Textdokument zu erstellen (z. B. in Standard Notes oder Obsidian), in dem du alle Anmeldungen und wichtigen Details festhältst. Auch wenn du die meisten Informationen auswendig weißt, dient dieses Dokument als nützliches Backup.

Tipp
Frage dich immer: „Braucht die Institution, mit der ich kommuniziere, wirklich meine echten Daten?“ Ein Polizist bei einer Befragung benötigt in der Regel deinen echten Namen, und es ist illegal, in solchen Situationen falsche Angaben zu machen. Ein Arzt muss deine korrekten Daten haben, um dich kontaktieren und behandeln zu können. Der Staat benötigt deine echten Informationen, um Steuern einzuziehen. Aber braucht Facebook wirklich deinen Namen und dein Geburtsdatum? Die Antwort hier ist eindeutig „nein“.

Das waren viele Informationen und Optionen, wie du einen Alias erstellen und anwenden kannst. Für manche wird der Alias zum alltäglichen Begleiter, den sie häufiger nutzen als ihren echten Namen. Für andere ist er lediglich eine praktische Maßnahme für Online-Accounts. Wichtig ist, dass du auch mit einem Alias ethische Standards und Gesetze einhältst. Ein Pseudonym ist nicht dazu gedacht,

anderen zu schaden oder sich vor rechtlichen Konsequenzen zu verstecken. Das Ziel ist, unsere Privatsphäre und persönliche Daten zu schützen. Nochmals: In der Kommunikation mit staatlichen Stellen darf ein Alias niemals verwendet werden. Dies kann zu ernsthaften rechtlichen Konsequenzen führen und sollte unbedingt vermieden werden.

Falschinformationen gezielt einsetzen

In den vorherigen Schritten haben wir bereits umfassende Maßnahmen ergriffen, um unsere privaten Informationen vor Unternehmen und Privatpersonen zu schützen, die zu viel über uns erfahren möchten. Obwohl wir viele unserer Daten gelöscht haben und künftig vermehrt mit Pseudonymen arbeiten, ist es nahezu unmöglich, alle Spuren im Internet vollständig zu beseitigen. Es ist wahrscheinlich, dass weiterhin persönliche Informationen in den Tiefen des Internets vorhanden sind, die wir schützen möchten. Hier kommt der gezielte Einsatz von Falschinformationen ins Spiel. Durch das bewusste Streuen von falschen Daten können wir Datenbroker und potenzielle Angreifer in die Irre führen. Das Ziel ist es, unsere echten Daten weniger auffindbar zu machen, indem die falschen Informationen relevanter und sichtbarer erscheinen. Diese Strategie kann sehr effektiv sein, birgt jedoch auch einige Nachteile. Je mehr Falschinformationen mit unserem Namen verknüpft sind, desto größer wird unsere allgemeine Internetpräsenz. Zudem könnte es in Zukunft schwieriger werden, diese falschen Angaben zu entfernen, falls wir dies irgendwann wünschen. Daher ist es wichtig, genau zu überlegen, vor wem oder was du dich schützen möchtest und wie weit du zu gehen bereit bist.

Achtung
Die Verbreitung von Falschinformationen im Zusammenhang mit staatlichen Behörden ist illegal und kann zu erheblichen Problemen führen. Diese Maßnahmen zielen ausschließlich darauf ab, unsere Privatsphäre gegenüber Angreifern zu wahren, nicht um gesetzliche Institutionen zu täuschen.

Es gibt verschiedene Arten von Falschinformationen, die wir kombinieren können.

Adresse: Durch das Erstellen mehrerer fiktiver Adressen oder Aufenthaltsorte, die mit deinem echten Namen verknüpft sind, entsteht der Eindruck, dass du an verschiedenen Orten lebst. Dies erschwert es, deine tatsächliche Adresse herauszufinden. Zudem kann es hilfreich sein, den Anschein zu erwecken, dass an deiner echten Adresse mehrere Personen wohnen, um Verwirrung zu stiften.

Geburtsdatum: Du kannst deinem Namen mehrere verschiedene Geburtsdaten hinzufügen oder zusätzliche Identitäten mit deinem echten Geburtsdatum, aber unter einem anderen Namen erstellen.

Telefonnummern: Um die echte Telefonnummer zu schützen, können wir mehrere fiktive Nummern mit unserem Namen verknüpfen, sodass es schwerer wird, die echte herauszufinden.

Beruf: Indem wir unserem echten Namen falsche Berufsbezeichnungen zuweisen, erschweren wir es Angreifern, unseren tatsächlichen Arbeitsplatz zu identifizieren.

Lebenslauf: Ähnlich wie im Berufsleben können wir alternative Karrierewege und Qualifikationen entwickeln, um Verwirrung zu stiften und es schwieriger zu machen, den tatsächlichen Werdegang nachzuvollziehen.

Familie: Durch das Erstellen fiktiver Familienbäume oder Verbindungen schützen wir sowohl uns selbst als auch unsere Familie.

Die Strategie besteht darin, mit unserem eigenen Namen möglichst viele falsche Informationen zu verknüpfen.

Es empfiehlt sich, Profile zu erstellen, die all diese Falschinformationen zusammenführen, sodass sie bei einer Suche nach dir ganz oben erscheinen. So können wir auf einen Schlag viele Fehlinformationen streuen.

Profil erstellen

Je nach deinen Bedürfnissen kannst du im Internet verschiedene Fake-Profile – also Identitäten – erstellen. Angenommen, ich möchte meine echten Daten schützen. Dafür verwende ich den Namen „Timo Volkov“ und erstelle ein Profil, das mit gezielten Falschinformationen gefüllt ist. Bevor wir beginnen, sollten wir überlegen, welche Informationen wir verwenden möchten. Starten wir mit der Adresse.

Adresse: Zuerst sollten wir ein Land und eine Stadt auswählen. Es ist ratsam, in demselben Land zu bleiben und für mindestens ein Profil auch die gleiche Stadt zu wählen, da häufig zuerst nach Stadt und Land gesucht wird. Die Wahl der richtigen Adresse gestaltet sich als schwierig: Eine fiktive Adresse funktioniert nicht, da viele Online-Dienste automatisch überprüfen, ob eine Adresse existiert, und nichtexistierende Hausnummern erkennen. Wir müssen also eine reale Adresse verwenden. Das Problem dabei ist, dass es unethisch wäre, die Adresse einer realen Person anzugeben, da wir diese in eine unangenehme Lage bringen könnten. Theoretisch könnten wir öffentliche Institutionen nutzen, aber das fällt schnell auf. Eine clevere Lösung besteht darin, die Adresse eines Apartmentkomplexes zu verwenden. Dort leben viele Menschen unter einer Adresse, sodass es unwahrscheinlicher ist, jemanden zu stören. Wenn gewünscht, können wir eine Apartmentnummer hinzufügen, sollten jedoch am besten eine wählen, die im Gebäude nicht existiert, auch aus Respekt zum Bewohner dieses Hauses.

Nachdem die Adresse feststeht, ist der wichtigste Schritt sind bereits erledigt. Jetzt fügen wir noch ein Geburtsdatum, eine Telefonnummer sowie einen Beruf und Lebenslauf hinzu.

Telefonnummer: Bitte verwende keine echten Telefonnummern, die bereits jemand anderem gehören, um ungewollte Anrufe zu vermeiden. In Deutschland gibt es Telefonnummern, die mit +49 11 beginnen – diese sind nicht in Gebrauch und können daher problemlos angegeben werden, klingeln aber trotzdem und werden als „echte“ Telefonnummer anerkannt.

Lebenslauf, Beruf und Geburtsdatum: Hier kann eine KI (siehe Kapitel 6, „Künstliche Intelligenz“) nützlich sein, um eine glaubwürdige Identität zu erstellen. Ein Beispiel für eine fiktive Person könnte folgendermaßen aussehen.

> *Beruf: Softwareentwickler*
>
> *Geburtsdatum: 15. April 1990*
>
> *Ausbildung:*
>
> *Bachelor of Science in Informatik, Technische Universität Berlin (2010–2014)*
>
> *Master of Science in Künstliche Intelligenz, Universität Heidelberg (2014–2016)*
>
> *Berufserfahrung:*
>
> *Junior Softwareentwickler, Digital Solutions GmbH, Berlin (2016–2028)*
>
> *Entwicklung und Implementierung von Webanwendungen*
>
> *Senior Softwareentwickler, FutureSoft Technologies, Stuttgart (2022–heute)*
>
> > *Projektleitung in der Entwicklung von Cloud-basierten Plattformen*

Diese Informationen stammen aus der Anfrage: „Stelle mir einen Lebenslauf und ein Geburtsdatum für eine fiktive Person zusammen.“

Nun fügen wir eine fiktive Adresse und Telefonnummer hinzu, und schon haben wir eine vollständige Identität. Der nächste Schritt besteht darin, diese Identität im Internet zu präsentieren.

Falschinformationen als falsche Fährte

Ein hervorragender Ausgangspunkt ist LinkedIn. Diese Plattform verfügt über eine starke Suchmaschinenoptimierung (SEO), wodurch das Profil bei einer Google-Suche nach dem Namen weit oben angezeigt wird. Außerdem muss das Profil nur einmal erstellt

werden und bleibt dann gut sichtbar, während es im Laufe der Zeit an Glaubwürdigkeit gewinnt.

SEO (Search Engine Optimization)
SEO oder Suchmaschinenoptimierung bezeichnet Maßnahmen, welche die Platzierung einer Website in Suchmaschinen verbessern. Durch gezielte Anpassungen von Inhalten und Technik wird die Sichtbarkeit erhöht, um mehr Besucher auf die Website zu lenken.

- Um einen LinkedIn-Account zu erstellen, gehe zu linkedin.com/login. Hier benötigst du eine E-Mail-Adresse oder Telefonnummer – ich empfehle, eine E-Mail-Adresse zu verwenden.
- Eine neue E-Mail-Adresse mit dem Geburtsdatum für dieses Profil kann zusätzlich für Authentizität sorgen (z. B. timo.volkov1990@gmail.com).

Nachdem du das LinkedIn-Profil erstellt hast, kannst du dieselbe Strategie auf weiteren Plattformen anwenden, um dem Profil mehr Glaubwürdigkeit zu verleihen. Melde dich in Foren an und teile dort „zufällig" Informationen über dieses Profil oder registriere dich auf Jobportalen und mache deinen Lebenslauf öffentlich zugänglich. Zudem kannst du den fiktiven Namen in Unternehmensverzeichnissen eintragen, damit diese Seiten ebenfalls bei der Suche nach deinem Namen angezeigt werden.

Eine weitere Möglichkeit besteht darin, eine einfache Webseite mit **Carrd** (carrd.co) zu erstellen, um alle relevanten Informationen zu verlinken. Diese Seite kannst du dann auch mit deinem LinkedIn-Profil, Forenbeiträgen und anderen Plattformen verbinden, um die Sichtbarkeit im SEO-Algorithmus zu erhöhen. Für einen noch radikaleren Schritt könntest du eine eigene Domain mit einem fiktiven Namen erwerben, auf der die falschen Informationen platziert werden, und diese Domain auch für eine fiktive E-Mail-Adresse nutzen. Die Idee hinter dieser Strategie ist klar: Du erstellst ein Profil mit zahlreichen falschen Informationen und verbreitest diese gezielt im Internet, sodass jemand, der nach dir sucht, ausschließlich auf diese

Informationen stößt. Durch die Verknüpfung dieser Daten über verschiedene Plattformen erscheint die „Person“ glaubwürdiger. Je mehr verschiedene Profile (also fiktive Identitäten) du erstellst, desto besser werden deine echten Informationen im Hintergrund verborgen, und potenzielle Angreifer werden in die falsche Richtung geleitet.

Ein weiterer Vorteil: Mit der Zeit gelangen diese Falschinformationen auch in die Datenbanken von Datenhändlern, was deren Algorithmen zusätzlich verwirren kann. Es ist jedoch wichtig, dass du während des Prozesses fokussiert und gewissenhaft vorgehst. Ein kleiner Fehler, wie das versehentliche Einfügen echter Daten, kann den gesamten Plan zunichtemachen und möglicherweise negative Konsequenzen für dich haben. Deshalb solltest du diese Schritte immer auf einem sicheren Computer durchführen und hinter einem VPN arbeiten, um so wenige echte Informationen wie möglich preiszugeben.

Außerdem solltest du vermeiden, Profile zu erstellen, die deinen echten Informationen zu ähnlich sind. Das könnte ein Sicherheitsrisiko darstellen, da man so leichter auf deine wahren Daten schließen könnte. Denke auch an die Zukunft: Wenn du dich irgendwo bewirbst, wird ein Arbeitgeber mit hoher Wahrscheinlichkeit deinen Namen im Internet suchen. Wenn die falschen Informationen sehr unterschiedlich sind, kannst du glaubhaft machen, dass es sich um eine andere Person handelt. Dies wird schwieriger, wenn echte und falsche Daten zu ähnlich aussehen. Solche Situationen wollen wir vermeiden.

Diese Strategie, die auf Falschinformationen setzt, ist eher für Fortgeschrittene geeignet. Wenn du gerade erst beginnst, deine Privatsphäre zurückzugewinnen, könnte dieser Schritt möglicherweise zu früh sein. Kleine Fehler oder ungenaue Angaben können zu großen Problemen führen und deine Privatsphäre gefährden. Du kannst später immer wieder zu dieser Methode zurückkehren, wenn du dich sicherer fühlst und mehr Erfahrung im Umgang mit Datenschutz gesammelt hast.

• • •

Lassen wir kurz Revue passieren, was wir bisher erreicht haben. In den ersten Kapiteln haben wir gelernt, wie wir Smartphones und Computer privat und sicher nutzen können, ohne dabei ständig Daten an Unternehmen weiterzugeben. Wir haben Programme kennengelernt, die uns helfen, unsere Privatsphäre und Sicherheit zu wahren, und Alternativen zu Anwendungen gefunden, die unsere Daten nicht respektieren. In diesem Kapitel haben wir uns darauf konzentriert, unsere Informationen aus dem Internet zu entfernen und sie besser zu schützen. Wir haben alle vorhandenen Daten gelöscht, die noch aus Zeiten stammen, als wir sorgloser mit unseren Informationen umgegangen sind. Anschließend haben wir eine pseudonyme Identität erstellt, um auch in Zukunft das Internet nutzen zu können, ohne unsere echten Daten preiszugeben. Zuletzt haben wir durch den Einsatz gezielter Falschinformationen weitere Schritte unternommen, um unsere privaten Daten zu schützen und potenzielle Angreifer mit falschen Fährten in die Irre zu führen.

Im nächsten Kapitel wenden wir uns der finanziellen Privatsphäre zu. Geld und Zahlungen sind ein zentraler Bestandteil unseres Lebens, ohne die wir nicht auskommen können. Wir werden uns anschauen, welche Möglichkeiten es gibt, so privat wie möglich zu zahlen und zu investieren. Leider ist dies im Bankensystem nicht wirklich möglich, da es vor allem um Überwachung und Macht geht. Daher wird auch Bitcoin einen großen Teil des nächsten Kapitels einnehmen, denn Bitcoin bietet eine freie Alternative zum Fiat-Bankensystem.

Kapitel 8
Zahlungen, Finanzen und Bitcoin

„Als ich jung war, dachte ich, dass Geld das Wichtigste im Leben ist; jetzt, wo ich alt bin, weiß ich, dass es das ist."
~ Oscar Wilde

In den bisherigen Kapiteln haben wir eine Vielzahl an Hilfen und Maßnahmen angesprochen, welche die digitale Welt absichert, sodass du dich dort sicher und privat bewegen kannst – vom Computer über das Handy bis hin zu Software und verschiedenen Tarnmechanismen. Nun ist es an der Zeit, uns dem Thema finanzieller Privatsphäre und Bitcoin umfassend zu widmen.

Ziel dieses Kapitels ist es, dir Ideen und Werkzeuge an die Hand zu geben, mit denen du wirklich privat bleiben kannst – sei es bei Zahlungen, Investitionen oder im Umgang mit Bitcoin. Insbesondere die Privatsphäre im Zusammenhang mit Bitcoin ist ein tiefer Kaninchenbau und ein Thema, über das bereits umfangreiche Bücher geschrieben wurden.

Dieses Buch ist bewusst so gestaltet, dass die finanziellen Aspekte erst am Schluss behandelt werden. Denn finanzielle Sicherheit und Privatsphäre setzen ein geschütztes und privates Umfeld voraus.

Wenn du beispielsweise einen Windows-PC mit Standardsoftware oder einen Chrome-Browser nutzt, sind deine Aktivitäten beim möglichen Bitcoin-Kauf nachverfolgbar, und jegliche Viren stellen ein Sicherheitsrisiko für dein Banking dar. Der App Store auf deinem Android- oder Apple-Gerät zeichnet alles über die heruntergeladenen Finanz-Apps auf. Ohne geschützte Geräte ist wahre finanzielle Privatsphäre nicht möglich – und genau deshalb ist das Verständnis der vorherigen Kapitel der Schlüssel dazu. Lass uns mit den täglichen Zahlungen beginnen, gefolgt von Investitionen und schließlich dem Thema Bitcoin.

Zahlungen

Seit der Corona-Pandemie sind die Umsätze im Onlinehandel im Vergleich zum Einzelhandel stark angestiegen und haben sich auf einem hohen Niveau stabilisiert. Dies liegt nicht nur an der Bequemlichkeit, von zu Hause aus alles bestellen zu können, was man benötigt. Staaten und Unternehmen haben diese Einkaufsform zudem intensiv propagiert. Während der Lockdowns wurde Online-Shopping als sichere Alternative beworben, da kein direkter Kontakt zu anderen Menschen erforderlich ist. Darüber hinaus bieten Online-Shops oft eine größere Auswahl, und die Einkäufe lassen sich schneller abwickeln. Hinter dieser Entwicklung steht jedoch vor allem ein Ziel: mehr Daten zu sammeln und Monopole zu fördern. Denn anonym online einzukaufen, ist schwierig, da alle Bestellungen bezahlt werden müssen – und die gängigen Zahlungsmethoden ermöglichen es, diese direkt mit einer Person zu verknüpfen. Dabei bleibt die Privatsphäre oft auf der Strecke. Mit der Einführung von CBDC könnte sich die Situation noch verschärfen, da alle Transaktionen bei einer einzigen Institution, der Zentralbank, erfasst würden. Es gibt jedoch Möglichkeiten, auch beim Bezahlen die eigene Privatsphäre zu wahren.

CBDC (Central Bank Digital Currency)
CBDC ist eine digitale Währung, die von der Zentralbank ausgegeben und kontrolliert wird. CBDCs ermöglichen eine umfassende Überwachung, da jede Transaktion zentral erfasst wird. Dadurch könnte der Staat das Zahlungsverhalten der Bürger genau verfolgen und gegebenenfalls einschränken.

Bargeld

Bargeld bleibt nach wie vor der Goldstandard unter den anonymen Zahlungsmethoden. Man kann im Geschäft einfach bar bezahlen, ohne persönliche Daten preiszugeben. Jeder Einkauf ist unabhängig vom anderen, sodass kein detailliertes Nutzerprofil erstellt werden kann. Da Bargeld nahezu überall akzeptiert wird, ist es die beste Option, wann immer es möglich ist.

Der einzige Nachteil: Online ist diese Zahlungsmethode nicht direkt anwendbar. Wer also online einkaufen möchte, muss auf Bargeld verzichten – es sei denn, man nutzt eine hybride Lösung. Einige Händler bieten die Möglichkeit, online zu bestellen und den Artikel dann im Geschäft abzuholen und bar zu bezahlen. Dies erfordert zwar einen kleinen Umweg, ermöglicht jedoch, die Anonymität von Bargeld mit dem Komfort des Online-Shoppings zu kombinieren.

Eine weitere besorgniserregende Entwicklung ist, dass Banken in einigen Fällen beginnen, die Seriennummern von Banknoten bei Abhebungen oder Einzahlungen zu erfassen. Zwar ist dies derzeit noch nicht weit verbreitet und liefert nur begrenzte Informationen, doch sollte man diese Praxis im Auge behalten. Sollte sie sich ausweiten, könnte die Anonymität, die Bargeld ermöglicht, ernsthaft gefährdet werden.

Mit Bargeld online bezahlen
Es gibt auch Online-Dienstleister, die Bargeld akzeptieren, z. B. ProtonMail oder Mullvad VPN. Dies funktioniert über das sogenannte „Cash by Mail“ (Bargeld per Post) und stellt eine der anonymsten Möglichkeiten dar, online zu bezahlen. Das Versenden von Geld, birgt jedoch ein gewisses Risiko.

Gutscheine

Gutscheine bieten eine nahezu ebenso anonyme Zahlungsmöglichkeit wie Bargeld, jedoch mit dem zusätzlichen Vorteil, dass sie auch online verwendet werden können. Diese Gutscheine sind in vielen Supermärkten oder Tankstellen erhältlich und können direkt bar bezahlt werden. Sie sind für nahezu jeden Online-Shop verfügbar, oft unter dem Begriff „Geschenkgutschein“. Wenn du online bezahlen möchtest, wählst du einfach die Option „Gutschein einlösen“ und gibst den aufgedruckten Code ein.

Es sind jedoch zwei wichtige Punkte zu beachten. Jeder Gutschein verfügt über eine individuelle Identifikationsnummer, die vom Unternehmen gespeichert wird. Wenn derselbe Gutschein mehrfach verwendet wird, besteht die Möglichkeit, dass das Unternehmen ein

Nutzerprofil erstellt. Es kann nachvollzogen werden, wo du den Gutschein gekauft und welche Waren du damit bestellt hast. Daher ist es ratsam, Gutscheine nicht wieder aufzuladen und keine hohen Beträge darauf zu laden. Mehrfach aufgeladene Gutscheine oder große Summen könnten mehr Informationen preisgeben, als es der Fall ist, wenn bei jedem Einkauf einen Gutschein verwendet wird.

Ein weiteres Hindernis kann auftreten, wenn du mit einem Gutschein auf einem neuen Konto bestellst – insbesondere, wenn die Lieferadresse eine Postbox ist. Viele Unternehmen lehnen solche Bestellungen aus Betrugspräventionsgründen direkt ab. Da das Bestellen ohne persönliche Zahlungsinformationen und ohne eigene Adresse eine optimale Möglichkeit darstellt, solltest du hier nicht sofort aufgeben.

Um deine Privatsphäre bei Onlinekäufen bestmöglich zu schützen, empfiehlt es sich, ein neues Konto zu erstellen, das nicht mit deiner Heim-IP-Adresse verknüpft ist. Dieses Konto sollte unter einem Alias geführt und mit einem sicheren Browser auf einem entsprechend geschützten Gerät eingerichtet werden; ferner sollte die Lieferung der Ware nicht an deine echte Adresse gehen. Natürlich erfolgt die Bezahlung mit einem Gutschein. Allerdings kann die Kombination all dieser Maßnahmen Misstrauen verursachen und zur Sperrung des Kontos führen, da auch Kriminelle genau diese Vorgehensweisen nutzen, um Geld zu waschen. Mit etwas Geduld und Vorsicht kannst du jedoch einen solchen Account einrichten, ohne Verdacht zu erregen. Beachte dabei die folgenden Punkte.

Gerät: Linux-Betriebssysteme werden gelegentlich als auffällig eingestuft. Im Gegensatz dazu erscheinen Android-Geräte, selbst wenn sie mit einem sicheren System wie GrapheneOS betrieben werden, unauffälliger. Daher ist es ratsam, Bestellungen zunächst über das Handy aufzugeben.

Browser: Sichere Browser wie LibreWolf können Misstrauen hervorrufen. Eine unauffälligere Alternative wie der DuckDuckGo-Browser oder der Brave Browser eignet sich gut für die Nutzung auf dem Handy.

Netzwerk: VPNs werden häufig als verdächtig wahrgenommen. Daher solltest du vorerst auf deren Nutzung verzichten. Anstelle deines Heimnetzwerks kannst du mobile Daten oder ein öffentliches WLAN verwenden. Mit einem sicheren DNS kannst du dich dennoch ein Stück weit schützen, ohne dabei aufzufallen.

Gutscheine: Für anonyme Zahlungen sind Gutscheine eine ausgezeichnete Wahl. Es könnte jedoch auffällig wirken, gleich 500 € auf einen neuen Account einzuzahlen. Beginne stattdessen mit kleineren Beträgen wie 10 € und steigere dich allmählich, um das Vertrauen in den Account zu erhöhen.

Account: Ein neuer Account ist erforderlich, um künftig sicher und anonym online einkaufen zu können. Neue Accounts können jedoch verdächtig erscheinen, weshalb es wichtig ist, die Reputation des Kontos schrittweise aufzubauen. Beginne mit kleinen Einkäufen und steigere dich allmählich. Starte mit dem Kauf eines digitalen Artikels wie einem Film oder einem Song für etwa 2 €. Solche Käufe stellen ein geringes Risiko für das Unternehmen dar und werden in der Regel problemlos akzeptiert. Nach ein oder zwei Wochen kannst du ein günstiges physisches Produkt für unter 5 € bestellen. Wenn auch dieser Kauf reibungslos verläuft, kannst du nach und nach teurere Produkte erwerben – aber achte darauf, dies langsam zu tun, um nicht aufzufallen.

Name: Nutze ein Pseudonym, um anonym zu bleiben. Achte darauf, dass der Name nicht zu generisch ist (vermeide z. B. „Max Müller“).

E-Mail: Private E-Mail-Anbieter wie ProtonMail oder TutaMail können bei manchen Nutzern Misstrauen erwecken. Daher kann es sinnvoll sein, für diesen Zweck eine E-Mail-Adresse bei einem etablierten Anbieter wie Google zu erstellen.

Adresse: Eine Postbox wirkt verdächtiger als eine echte Adresse. Wenn du mit kleinen Einkäufen beginnst, kannst du möglicherweise dennoch erfolgreich bestellen zu einer Postbox bestellen. Eine weitere Möglichkeit wäre, an einen Bekannten oder an die Arbeit liefern zu lassen, um zunächst eine positive Reputation aufzubauen.

Nach einiger Zeit solltest du einen sicheren Online-Account haben, mit dem du anonym und ohne Sperrungen einkaufen kannst. Auch in stationären Geschäften können Gutscheine genutzt werden, allerdings bieten sie dort keinen nennenswerten Vorteil gegenüber Bargeld.

Kreditkarten und Banküberweisungen

Kreditkarten und Banküberweisungen sind nicht privat. Bei jeder Zahlung mit diesen Methoden solltest du dir bewusst sein, dass sowohl die Bank als auch das Unternehmen, bei dem du einkaufst, Zugriff auf deine Transaktionsdaten haben. Daher sollten diese Zahlungsmethoden, wenn möglich, vermieden werden. Leider lässt sich dies nicht immer umgehen. Anders als in einigen anderen Ländern ist es hier aufgrund von Regulierungen nicht möglich, anonyme Kreditkarten zu nutzen. Somit sind solche Zahlungen grundsätzlich nicht privat.

Es gibt jedoch Möglichkeiten, die Sicherheit zu erhöhen. Einige Finanzdienstleister wie Revolut bieten virtuelle Einmalkreditkarten an. Diese kann nur einmal benutzt werden, danach verfällt die Karte. Diese Karten sind zwar weiterhin mit deinem Namen verbunden, bieten jedoch einen erhöhten Schutz. Sollte es zu einem Datenleck kommen und deine Zahlungsinformationen veröffentlicht werden, kann von dieser Kreditkarte nichts mehr abgebucht werden, da sie nur einmalig verwendet werden kann. Dies schützt auch vor unerwünschten Abbuchungen, beispielsweise bei ungewollten Abonnements. Wenn eine Kreditkartenzahlung unumgänglich ist, empfiehlt sich daher die Nutzung einer virtuellen Einmalkarte.

Oft stellt sich die Frage, wie es mit PayPal oder anderen Fintech-Banken aussieht. Leider ist die Situation bei diesen Diensten nicht besser – in vielen Fällen sogar schlechter. Unternehmen wie PayPal bieten sehr günstige oder sogar kostenlose Tarife an, die es ermöglichen, ohne Gebühren Geld zu überweisen oder zu bezahlen. Diese Transaktionen erfolgen oft in Echtzeit und bieten ein hohes Maß an Sicherheit. Genau aus diesem Grund ist PayPal so beliebt: es ist bequem, kostenlos und bietet viele praktische Optionen.

Doch auch hier gilt das Sprichwort: „Wenn das Produkt kostenlos ist, bist du das Produkt.“ PayPal sammelt umfangreiche Daten darüber, an wen Geld gesendet wird, von wem man es erhält, wo man einkauft und was in den Notizen zu den Transaktionen steht. Hinzu kommt, dass Fintech-Banken meist auf den Netzwerken von Mastercard und Visa basieren, die ebenfalls Daten sammeln. Somit sind mindestens zwei Parteien an der Datensammlung beteiligt. Diese Daten werden nicht nur gesammelt, sondern auch verkauft. Ja, PayPal ist sehr bequem, aber wenn dir deine Privatsphäre wichtig ist, solltest du diese Bequemlichkeit vielleicht hinterfragen.

Banküberweisungen, Kreditkartenzahlungen und kontaktloses Bezahlen per Handy sind zweifellos einfach und praktisch – man muss nicht viel darüber nachdenken. Doch diese Bequemlichkeit hat ihren Preis: die eigene Privatsphäre. Es lohnt sich daher, abzuwägen, ob der zusätzliche Aufwand anderer Zahlungsmethoden diesen Preis wert ist.

Bitcoin

Bitcoin und andere Kryptowährungen bieten eine potenziell anonyme Möglichkeit für Online-Zahlungen. Es sind jedoch einige wichtige Aspekte zu beachten, um sicherzustellen, dass die Zahlungen nicht mit deiner Identität verknüpft werden können. Diese Bezahlmethode ist jedoch nur in einer sehr begrenzten Anzahl von Shops möglich.

Privat Investieren

Sparen und Anonymität miteinander zu vereinbaren, ist eine Herausforderung. Zwar kannst du Geld in bar aufbewahren, jedoch birgt dies Sicherheitsrisiken, und durch Inflation verliert Fiat-Geld im Laufe der Zeit an Wert. Naheliegende Optionen wie Aktien und ETFs bieten zwar einen gewissen Schutz vor Inflation, doch jede deiner Transaktionen wird aufgezeichnet und in zentralen Datenbanken gespeichert. Zudem musst du den Banken vertrauen, dass sie nicht insolvent werden und dein Geld nicht riskieren – was in der Vergangenheit immer wieder zu Bankruns geführt hat, bei denen

viele Menschen ihr Geld nicht zurückerhalten konnten. Auch Immobilien sind in dieser Hinsicht nicht privat, da dein Name immer mit dem Objekt verknüpft ist und du diese nicht einfach an einen anderen Ort mitnehmen kannst. Diese Anlageformen haben zwar ihre Vorteile, dennoch ist es wichtig, sich auch der damit verbundenen Nachteile bewusst zu sein.

Fiatgeld
„Fiatgeld“ bezeichnet Geld, dessen Wert nicht durch physische Güter wie Gold gedeckt ist, sondern ausschließlich auf dem Vertrauen in den ausgebenden Staat basiert. Der Wert von Fiatgeld wird durch staatliche Regulierung sowie das Vertrauen der Nutzer bestimmt. Beispiele für Fiatgeld sind der Euro, der US-Dollar und der japanische Yen.

Edelmetalle

Eine gute Möglichkeit, anonym Werte zu speichern, sind Edelmetalle. In Deutschland können bis zu einer Grenze von 2.000 Euro Edelmetalle anonym in bar erworben werden. Wenn du größere Summen anlegen möchtest, kannst du mit mehreren Personen verschiedene Geschäfte aufsuchen, um größere Mengen zu kaufen. Diese musst du dann sicher verwahren, aber zumindest hast du dich damit gegen Inflation geschützt und trägst kein Risiko einer Drittpartei.

Allerdings gibt es Import- und Exportregulierungen für Gold, die bei einer Auswanderung problematisch sein könnten, da es schwierig ist, größere Mengen an Goldbarren oder -münzen durch den Zoll am Flughafen zu bringen.

Die Grenze liegt derzeit bei Gold im Gegenwert von 10.000 Euro. Goldschmuck hingegen ist von dieser Regelung ausgeschlossen. Das bedeutet, dass du so viel Goldschmuck tragen kannst, wie du möchtest, ohne Probleme am Flughafen zu bekommen. In der Vergangenheit war Schmuckgold ebenfalls nicht betroffen, als Länder wie die USA und Indien den Besitz von Gold verbaten. Bürger, die Goldbarren und -münzen besaßen, waren verpflichtet, diese

abzugeben – wer jedoch Schmuck hatte, war auf der sicheren Seite und durfte ihn behalten. Daher macht es Sinn, bei Edelmetallen zu diversifizieren, sowohl in Form von Münzen und Barren als auch durch Schmuck und andere Edelmetalle wie Silber.

Sammlerstücke

Es lohnt sich, auch einen Blick auf Sammlerstücke wie Diamanten oder Luxusuhren zu werfen. Beide können anonym mit Bargeld erworben werden, sind relativ wertstabil und lassen sich sehr einfach ins Ausland transportieren. Diamanten bieten einen hohen Wert bei geringem Gewicht und Platzbedarf und fallen bei Zollkontrollen nicht auf. Eine Uhr am Handgelenk ermöglicht es, einen Gegenwert von mehreren tausend Euro diskret zu transportieren. Selbstverständlich fallen auch andere Sammlerstücke wie Kunstwerke, Spielkarten oder Vintage-Konsolen wie Gameboys in diese Kategorie.

Bitcoin

Die beste Option für Privatsphäre und finanzielle Freiheit ist Bitcoin. Wenn man einige grundlegende Sicherheitsmaßnahmen beachtet, kann man Bitcoin anonym erwerben und sicher digital aufbewahren. Dadurch minimiert man das Risiko physischer Verluste, wie es bei Bargeld oder Edelmetallen vorkommen kann. Zudem lässt sich Bitcoin einfach und sicher über große Entfernungen transferieren.

Bitcoin sicher und privat nutzen

„Bitcoin gibt uns, den Menschen, die Macht zurück aber bringt die Verantwortung, die mit Freiheit einhergeht."
~ Andreas M. Antonopoulos

Ziel dieses Kapitels ist es, dir zu zeigen, wie du Bitcoin sicher, privat und ganz nach deinen eigenen Bedingungen kaufen, aufbewahren und verwenden kannst.

Anstelle von Schritt-für-Schritt-Anleitungen werde ich mich hier eher auf Grundprinzipien konzentrieren, denn der Bitcoin ist ein

umfangreiches Thema. Nutze die hier präsentierten Ideen als Ansatzpunkte, um weitere Möglichkeiten zur sicheren und privaten Verwahrung von Bitcoin zu entdecken.

Mehr zu Bitcoin
Detaillierte Schritt-für-Schritt Anleitungen zu allen hier besprochenen Punkten findest du unter privatopia.de/bitcoin

Warum Bitcoin?

Was hat Bitcoin mit dem Ziel dieses Buches – unserer Privatsphäre – zu tun? Privatsphäre und Freiheit sind eng miteinander verknüpft. Doch wie gestaltet sich finanzielle Freiheit konkret? Viele verbinden diesen Begriff mit dem Gedanken, genug Geld zu besitzen, um sich keine Sorgen mehr machen zu müssen. Lass uns jedoch einen anderen Blickwinkel einnehmen.

- Ist man finanziell frei, wenn Banken sehen, was wir genau mit unserem Geld machen?
- Ist man finanziell frei, wenn Banken oder Regierungen Transaktionen blockieren können? [9]
- Ist man finanziell frei, wenn das eigene Geld bei den Banken nicht mehr uns selbst gehört?
- Ist man finanziell frei, wenn man nicht mehr als 5.000 € von seinen Ersparnissen bei der Bank abheben kann? [10]
- Ist man finanziell frei, wenn digitale Zahlungen jederzeit von Dritten überwacht oder nachverfolgt werden können?
- Ist man finanziell frei, wenn der Zugriff auf das eigene Konto durch Sanktionen oder politische Entscheidungen eingeschränkt wird?

Das staatliche Finanzsystem weist zahlreiche Probleme auf: Es kontrolliert nicht nur unser Geld, den Wert davon durch Inflation, sondern nutzt es auch zur Überwachung und Steuerung unserer Aktivitäten. Eine mögliche Lösung hierfür ist Bitcoin denn dahinter steht keine zentrale Instanz die Macht ausüben kann.

Hinweis
Ich gehe davon aus, dass du bereits eine grundlegende Vorstellung vom Bitcoin hast. Falls das nicht der Fall ist, kannst du in der Tool-Sammlung (privatopia.de/buch oder hintem im Buch) weitere Informationen dazu finden und später zu diesem Kapitel zurückkehren.

Bitcoin ist ein dezentrales Netzwerk, das ohne zentrale Autorität operiert. Dein Konto kann nicht gesperrt, und Transaktionen können nicht blockiert werden. Es gibt keine Einschränkungen, an wen du Geld senden kannst oder wie viel du senden möchtest. Politische Vorgaben spielen keine Rolle; jeder ist gleichberechtigt, unabhängig von seinem Herkunftsland. Bitcoin ermöglicht zensurfreie Zahlungen.

Bitcoin ist ein vollständig freies und unabhängiges System, dem jeder beitreten und teilnehmen kann. Du verwaltest dein Geld selbst, ohne die Kontrolle von Banken. Bitcoin bietet eine der besten Möglichkeiten, deine eigene Bank zu sein – sowohl für private Transaktionen als auch für die echte Vermögensverwaltung.

Einfach erklärt ist Bitcoin ein Stück Computercode, das von einer weltweiten Gemeinschaft von Computern, den sogenannten Bitcoin-Nodes, überprüft und validiert wird. Ein zentraler Bestandteil dieses Codes ist die Blockchain – ein öffentliches Kassenbuch, das alle Bitcoin-Transaktionen seit Beginn aufzeichnet. Die Blockchain wird von Minern, die durch Rechenleistung das Netzwerk sichern, und von Nodes, die die Blockchain speichern, aktualisiert und überprüft.

Der Bitcoin-Code basiert auf soliden ökonomischen Modellen, darunter eine maximale Menge von 21 Millionen Bitcoin. Aufgrund dieser festen Obergrenze sehen viele in Bitcoin die einzige und beste Möglichkeit, sich vor inflationären staatlichen Systemen zu schützen. Um Bitcoin nutzen zu können, musst du lediglich eine App, eine Bitcoin-Wallet, herunterladen, die deine privaten Schlüssel verwahrt. Wenn du Bitcoin besitzt, benötigst du einen privaten Schlüssel, um auf deine Bitcoin zuzugreifen und sie zu versenden.

Von dieser Wallet aus kannst du Bitcoin weltweit problemlos versenden, und das gegen eine geringe Gebühr, die an die Miner geht. Mit Bitcoin kannst du große Transaktionen innerhalb von Minuten über die ganze Welt senden. Dazu musst du nur einen Knopf drücken – ohne jemanden um Erlaubnis fragen und dich verifizieren zu müssen. Versuche das mal mit einem Bankkonto. Unabhängig davon, wie du zu Bitcoin stehst, muss man zugeben, dass es eine Revolution in Bezug auf Unabhängigkeit und finanzielle Freiheit darstellt.

Bitcoin und Privatsphäre

Man hört oft, dass Bitcoin ein anonymes Netzwerk sei. Tatsächlich ist es jedoch eines der transparentesten Zahlungssysteme, die es gibt. Mit geschicktem Einsatz kann es jedoch auch eine beachtliche Privatsphäre bieten.

Die Bitcoin-Privatsphäre ist komplex, insbesondere für Einsteiger. Es gibt viele Fehler, die man begehen kann. Dieses Thema ist so umfangreich, dass es nicht möglich ist, alle Aspekte und Schritt-für-Schritt-Anleitungen in einem Kapitel abzudecken. Daher werde ich eher Ideen vorstellen, die du nutzen kannst, um dich weiter mit dem Thema zu beschäftigen. Ich habe versucht, alle wichtigen Punkte zumindest anzusprechen.

Die Bitcoin-Privatsphäre umfasst ein breites Spektrum. Verschiedene Protokoll-Updates, Wallet- und Node-Funktionen sowie gesetzliche Regelungen sorgen dafür, dass sich vieles ständig verändert. Dennoch gibt es Grundprinzipien, die konstant bleiben, und diese werde ich dir vorstellen. Egal, ob du gerade bei Null anfängst oder bereits Erfahrung hast – du musst nicht alles sofort umsetzen. Betrachte dieses Kapitel als Leitfaden, den du schrittweise anwenden kannst. Lese die Vorschläge am besten zuerst komplett durch, bevor du startest, damit du die Schritte findest, die am besten zu dir passen und mit denen du beginnen möchtest.

Es gibt gute Gründe, bei Bitcoin auf Privatsphäre zu achten. Denn jede Transaktion ist öffentlich einsehbar, was gewisse Risiken birgt. Wenn man Bitcoin über eine KYC-Börse kauft, werden diese Käufe

mit der eigenen Identität verknüpft – und damit auch alle zukünftigen Transaktionen.

KYC (Know Your Customer)
KYC bezeichnet die Identitätsprüfung durch Unternehmen bezüglich ihrer Kunden, meist im Finanzbereich. Es dient dazu, Betrug, Geldwäsche und andere illegale Aktivitäten zu verhindern, indem Kunden ihre Identität nachweisen müssen.

Das bedeutet, dass diese Börsen, Blockchain-Überwachungsfirmen oder sogar Regierungen

- deine Ausgabegewohnheiten verfolgen können,
- dich davon ausschließen können, andere Dienste zu nutzen,
- deine Bitcoin beschlagnahmen können,
- von dir gegebenenfalls zusätzliche Steuern verlangen,
- und generell mehr über dich wissen, als sie sollten.

Diese Entwicklungen stehen im Widerspruch zu dem ursprünglichen Gedanken des Entwicklers von Bitcoin, Satoshi Nakamoto, der ein freies Peer-to-Peer-System konzipierte. Dieses Kapitel führt dich durch Schritte, die dich vor diesen Risiken schützen können. Viele Leser des vorliegenden Buches sind technisch nicht versiert, doch das ist kein Hindernis. Während wir die verschiedenen Punkte durchgehen, werde ich dir ein grundlegendes Verständnis hinsichtlich Bitcoin und seiner Funktionsweise vermitteln. Sollten Unklarheiten bleiben, findest du in der Tool-Sektion zusätzliche Informationen.

Bitcoin sicher und privat aufbewahren

Bevor du Bitcoin kaufst, solltest du dir Gedanken darüber machen, wie du sie sicher und privat aufbewahren kannst. In der Bitcoin-Welt gibt es das Sprichwort: „Not your keys, not your coins“. Das bedeutet, dass du nur dann wirklich im Besitz deiner Bitcoin bist, wenn du den privaten Schlüssel (die sogenannten 24 Wörter) selbst verwahrst. Fehlt dieser Schlüssel, gehören die Bitcoin technisch gesehen nicht dir. Diese Erfahrung haben wir in der Geschichte von

Bitcoin bereits mehrfach gemacht – beispielsweise bei den Vorfällen von Mt. Gox (2014) [11] und FTX (2022) [12], als Bitcoin über Nacht verschwanden, weil sie in der Verwahrung dieser Unternehmen waren.

Für deine Privatsphäre ist es zudem wesentlich besser, eine eigene Wallet zu nutzen. Wenn du die Verwahrung jemand anderem überlässt, hat diese Person oder Institution Einsicht in all deine Transaktionen, Bestände und Adressen. Deine Bitcoin-Aktivitäten sind dann wie ein offenes Buch.

Wallets

Bevor du eine Wallet herunterlädst und nutzt, ist es wichtig, die Funktionsweise zu verstehen. Bei Bitcoin bist du deine eigene Bank. Das bietet dir Unabhängigkeit, bringt jedoch auch die Verantwortung mit sich, deine Bitcoin sicher zu verwahren. Grundsätzlich unterscheidet man Hardware-Wallets und Software-Wallets:

Hardware-Wallets (HWW) sind physische Geräte, die du benötigst, um Bitcoin sicher zu senden und zu empfangen. Sie bieten ein hohes Maß an Sicherheit, da du das Gerät physisch besitzen musst, um Transaktionen durchzuführen.

Software-Wallets (SWW) hingegen sind Anwendungen auf deinem Computer oder Smartphone, in denen die Daten digital gespeichert werden. Diese Wallets sind anfälliger für Cyberangriffe, da sie mit dem Internet verbunden sind und somit potenziellen Bedrohungen ausgesetzt sind.

Besonders für Einsteiger ist oft unklar, was eine Wallet eigentlich ist und wie sie funktioniert. Viele Menschen glauben, dass die Bitcoin direkt auf einer Hardware- oder Software-Wallet gespeichert sind. Tatsächlich ist das jedoch nicht der Fall. Eine Wallet – egal ob HWW oder SWW – speichert nicht deine Bitcoin, sondern lediglich den privaten Schlüssel. Ihre Hauptaufgabe besteht darin, diesen Schlüssel sicher zu verwahren.

Stell dir vor, du schreibst einen Scheck mit dem Namen des Absenders und des Empfängers, deiner Bankverbindung, dem Betrag und, am wichtigsten, deiner Unterschrift. Nachdem die Bank den Scheck geprüft hat, wird die Zahlung ausgeführt. Ähnlich funktioniert es bei Bitcoin-Transaktionen: Es gibt einen Absender, einen Empfänger, den Betrag und eine Signatur – wobei diese Signatur digital ist und mit dem privaten Schlüssel erzeugt wird.

Dieser private Schlüssel ist also notwendig, um Bitcoin zu senden. Eine Wallet speichert diesen Schlüssel und signiert die Transaktionen, die du damit durchführst. Die Software-Wallet speichert den Schlüssel digital auf deinem Gerät, was ein höheres Risiko für Cyberangriffe mit sich bringt. Die Hardware-Wallet hingegen speichert den Schlüssel physisch und sicher auf dem Gerät selbst. Dieser Schlüssel verlässt das Gerät niemals; es wird nur die Signatur gesendet, um die Transaktion zu autorisieren. Dadurch ist eine Hardware-Wallet erheblich sicherer, weshalb ich für größere Summen immer eine Hardware-Wallet empfehle.

Privater Schlüssel

Der private Schlüssel ist das Herzstück deiner Bitcoin-Sicherheit. Nur mit ihm kannst du Bitcoin versenden – und leider auch jeder, der ihn besitzt. Wenn jemand Zugang zu deinem privaten Schlüssel (in Form von 12 oder 24 Wörtern) hat, kann diese Person uneingeschränkt über deine Bitcoin verfügen. Solltest du deine Hardware-Wallet und das Backup (diese Wörter auf Papier) verlieren, gibt es keinen Weg, deine Bitcoin wiederherzustellen.

Jede Wallet erstellt für dich einen privaten Schlüssel (die 24 Wörter), den du unbedingt aufschreiben und sicher aufbewahren musst. Wenn du deine Hardware-Wallet verlierst oder sie beschädigt wird, kannst du mit diesen Wörtern von jeder anderen Wallet auf deine Bitcoin zugreifen.

Jetzt stellt sich die Frage, wie und wo du diese 24 Wörter am besten verwahrst. Es gibt viele Ideen aus der Bitcoin-Community, doch drei Aspekte sind dabei besonders wichtig:

- Schutz vor Verlust oder Diebstahl
- Schutz vor Feuer, Wasser oder anderen Umwelteinflüssen
- Langlebigkeit für die Zukunft

Ein bewährtes Konzept ist die 3-2-1-Backup-Regel: Erstelle drei Kopien deines privaten Schlüssels, verwende dabei zwei verschiedene Formate (die Hardwarewallet, Papier oder Stahl) und bewahre eine Kopie an einem anderen Ort auf. Sichere Verstecke und ein Safe bieten Schutz vor Diebstahl, während unterschiedliche Standorte vor Umwelteinflüssen schützen. Verschiedene Materialien – wie Papier, Hardware-Wallets und Metall – gewährleisten, dass der Schlüssel beständig bleibt.

Passphrase

Ein nützliches Tool für zusätzliche Sicherheit und Privatsphäre ist die Passphrase.

Die Passphrase
Eine Passphrase ist nicht mit dem Passwort zu verwechseln, das zum Sperren von Wallets oder Geräten verwendet wird. Eine Passphrase (das 25. Wort) ist eine zusätzliche Zeichenkette, die du an deine 24 Wörter anhängst.

Du kannst frei entscheiden, welche Passphrase du verwenden möchtest. Es wird empfohlen, mindestens 15 Zeichen zu wählen – sie sollte nicht zu einfach sein, aber dennoch etwas, das du dir merken kannst. Jedes Mal, wenn du deine Hardware-Wallet verwendest, musst du diese Passphrase angeben.

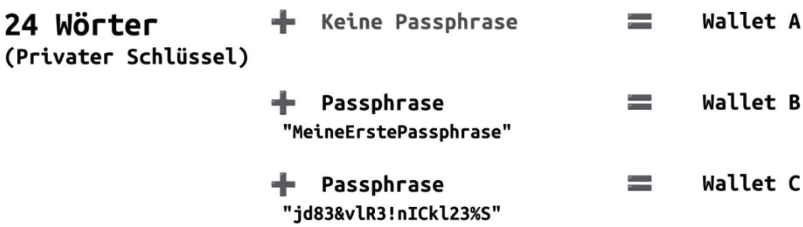

Abbildung 17: Bitcoin-Passphrasen

Ich empfehle zunächst mit einer Passphrase zu beginnen. Wenn du dich sicher fühlst, kannst du weitere hinzufügen. Wenn du mehrere Passphrasen hast und somit mehrere Wallets, ergeben sich verschiedene Vorteile:

Sicherheit bei Übergriffen: Im Bitcoin-Bereich gibt es das Konzept der „5-Dollar-Schraubenschlüssel-Attacke", es handelt sich um Angriffe, bei denen physische Gewalt angewendet wird, um an Bitcoin zu gelangen. In solchen Situationen kannst du eine Passphrase herausgeben, die den Zugriff auf einen kleinen Betrag an Bitcoin ermöglicht, während deine tatsächlichen Ersparnisse sicher bleiben.

Staatliche Zugriffe: Sollte der Staat jemals gewaltsam auf dein Vermögen zugreifen wollen, könntest du eine Passphrase für kleinere Beträge verwenden und den Rest sicher schützen. Nutze daher eine Passphrase für deine KYC-Bitcoin und eine andere Passphrase für deine no-KYC-Bitcoin.

Privatsphäre: Durch die Verwendung mehrerer Passphrasen kannst du separate Wallets einrichten, um deine Bitcoin besser zu trennen. So lässt sich eine klare Unterscheidung zwischen KYC-gekauften und No-KYC-gekauften Bitcoin gewährleisten, wodurch Verwechslungen vermieden werden.

Vererbung: Auch beim Vererben kann die Passphrase von großem Nutzen sein. Indem du mehrere Empfänger einbeziehst, kannst du die 24 Wörter allen zugänglich machen und jedem eine individuelle Passphrase zuweisen, sodass jeder nur seinen eigenen Teil erhält.

Software-Wallets

Eine Software-Wallet ist in der Regel nicht so sicher wie eine Hardware-Wallet. Daher verwende ich eine Software-Wallet ausschließlich auf meinem Handy, in der ich nur einen kleinen Betrag aufbewahre – so viel, wie ich bereit wäre zu verlieren. Ich betrachte sie als Geldbörse für unterwegs, während die Hardware-Wallet als Konto oder Safe fungiert. Der Großteil deiner Bitcoin sollte sicher auf einer Hardware-Wallet aufbewahrt werden.

Besonders für Anfänger und bei kleinen Beträgen ist eine Software-Wallet oft sinnvoller, da Hardware-Wallets schnell über 100 € kosten können. Meine Empfehlung in diesem Fall ist die **BlueWallet**, die im Aurora Store und auf iOS erhältlich ist.

Satoshi
Ein Satoshi ist die kleinste Einheit von Bitcoin und entspricht 0,00000001 Bitcoin (BTC). Der Name „Satoshi" ehrt den Schöpfer von Bitcoin, Satoshi Nakamoto. Während Bitcoin als Ganzes die Kryptowährung beschreibt, ist ein Satoshi lediglich ein Bruchteil davon, ähnlich wie Cent bei einem Euro.

Hardware-Wallets

Es gibt zahlreiche Hardware-Wallets auf dem Markt, und ebenso viele Meinungen dazu. Für Anfänger empfehle ich die **BitBox02 Bitcoin-only Edition**, da sie:

- vollständig Open Source ist,
- einen Secure Chip für zusätzliche Sicherheit enthält,
- nur Bitcoin unterstützt (weniger Angriffsfläche),

Wenn du etwas fortgeschrittener bist, kannst du auch eine Hardware-Wallet wählen, die noch mehr Funktionen bietet und die du selbst zusammenbauen kannst. Der **SpecterDIY** lässt sich für etwa 185 € zusammenstellen und zeichnet sich durch eine Vielzahl fortschrittlicher Funktionen sowie ein großes Touchdisplay aus. **Seedsigner** ist die kompakte Variante des Specters und kostet nur etwa 50 €, bietet jedoch einen kleineren Bildschirm.

Sparrow

Die meisten Wallets werden mit einer eigenen Software geliefert: die BitBox02 mit der BitBox App, Trezor mit Trezor Suite und Ledger mit Ledger Life. Statt diese proprietären Anwendungen zu verwenden, solltest du zu einer Open-Source-Lösung wie Sparrow wechseln.

Diese bietet nicht nur erweiterte Funktionen, sondern es ist auch sinnvoll, nicht alles auf einen einzigen Hersteller zu setzen. Berichten zufolge haben auch einige dieser Wallet-Apps, z. B. Ledger Live, Nutzerdaten erfasst – möglicherweise sogar unter Druck von Regierungen oder Geheimdiensten. Darüber hinaus ermöglicht dir Sparrow, ein tieferes Verständnis für Bitcoin zu entwickeln, da du Zugriff auf eine Vielzahl von Funktionen hast.

- Sparrow kannst du unter sparrowwallet.com herunterladen.

Test-Transaktion

Nachdem du deine Hardware-Wallet eingerichtet hast, solltest du nicht sofort deine gesamten Ersparnisse dorthin transferieren. Zunächst ist es wichtig, sicherzustellen, dass alles einwandfrei funktioniert. Daher empfiehlt es sich, einige Test-Transaktionen mit einem Betrag von etwa 50 € durchzuführen.

Ich würde empfehlen, zunächst 50 € an die Wallet zu senden und zu überprüfen, ob der Betrag erfolgreich angekommen ist. Anschließend solltest du eine Transaktion von dieser Wallet an eine andere durchführen, um sicherzustellen, dass du Transaktionen senden und signieren kannst. Diese beiden Tests sind in der Regel ausreichend. Wenn du auf Nummer sicher gehen möchtest, kannst du die Wallet auf die Werkseinstellungen zurücksetzen und dann deine 24 Wörter erneut eingeben. Wenn die beiden Transaktionen danach korrekt angezeigt werden, kannst du beginnen, größere Beträge zu transferieren.

Coin Control und Labeling

Die gesamte Transaktionshistorie von Bitcoin ist öffentlich einsehbar. Jede Transaktion, einschließlich der Senderadresse, der Empfangsadresse und des Betrags, kann von jedem eingesehen werden. Überwachungsunternehmen, die die Blockchain analysieren und möglicherweise Zugriff auf direkte Informationen von Börsen haben, könnten in der Lage sein, zu erkennen, dass zwei deiner Adressen miteinander verbunden sind.

Man könnte daraus ableiten, wie viele Bitcoin dir gehören, und diese Informationen an den Staat oder andere Institutionen weitergeben. Ein zuverlässiger Schutz beginnt damit, dass du genau weißt, woher deine Bitcoin stammen: Ob sie von einer Börse mit KYC-Verfahren („Know Your Customer"), einer anderen Person oder aus einem anonymen Kauf stammen. Da dies mit einer zunehmenden Anzahl an Transaktionen komplex werden kann, ist die „Labeling"-Funktion äußerst hilfreich. Markiere jeden empfangenen und gesendeten Bitcoin-Transaktion mit relevanten Informationen, beispielsweise dem Kaufort oder dem Empfänger. Dieser Prozess dauert paar Sekunden und verbessert sowohl deine Privatsphäre als auch die Übersicht erheblich.

Bitcoin anonym erhalten

Nachdem du eine sichere Wallet eingerichtet hast, geht es nun darum, Bitcoin zu erhalten. Es gibt verschiedene Möglichkeiten, dies zu tun, aber der einfachste Weg ist der Kauf über eine lizenzierte Börse. Viele Börsen bieten einen praktischen, automatisierten Sparplan an, mit dem du regelmäßig Bitcoin erwerben kannst. Das klingt doch sehr bequem, oder?

Ein Unternehmen, das Tausende sensible Kundendaten wie Namen, Adressen und Kaufinformationen speichert, ist ein attraktives Ziel für Hacker. Die Gefahr besteht darin, dass genau diese Informationen in die falschen Hände geraten. Datenlecks im Finanzbereich sind besonders heikel: Stell dir vor, deine persönlichen Daten, die Menge an Bitcoin und deine Adresse gelangen in die Hände von Kriminellen und werden im Darknet meistbietend verkauft. Das betrifft nicht nur deine Privatsphäre, sondern könnte sogar deine persönliche Sicherheit gefährden. Zum Glück gibt es Möglichkeiten, No-KYC-Bitcoin zu erhalten, die keine Verbindung zu deiner Identität haben.

Bitcoin verdienen: Diese Methode eignet sich hervorragend, um Bitcoin zu fördern und gleichzeitig deinen Bestand zu vermehren. Bietest du eine Dienstleistung oder ein Produkt an? Dann kannst du Zahlungen oder Spenden in Bitcoin akzeptieren und so schrittweise deinen Bestand aufbauen.

Bitcoin von Freunden oder auf Meetups gegen Bargeld kaufen: Dieser Weg ermöglicht es, anonym zu bleiben. Das größte Hindernis besteht darin, jemanden zu finden, der bereit ist, zu verkaufen, da viele ihre Bitcoin behalten möchten. Mit etwas Geduld kann dies jedoch eine optimale Möglichkeit sein, Bitcoin zu erwerben.

Bitcoin online auf einer Peer-to-Peer-Börse kaufen: Eine Peer-to-Peer-Börse ist keine traditionelle Börse, sondern ein Online-Vermittlungsdienst, der Käufer und Verkäufer von Bitcoin direkt miteinander verbindet und dafür sorgt, dass alle Transaktionen fair und sicher ablaufen. Im Gegensatz zu einer herkömmlichen Börse kaufst du hier von einer anderen Person, während die Börse lediglich als vertrauenswürdiger Mittelsmann fungiert.

Die folgenden Plattformen bieten die Möglichkeit, Bitcoin anonym zu kaufen und zu verkaufen. Angegeben sind die wesentlichen Funktionen und beispielhafte Gebühren für einen Kauf über 200 € (Stand April 2025).

PeachBitcoin (peachbitcoin.com): Peach Bitcoin ist eine ausgezeichnete Wahl für Einsteiger, die anonym Bitcoin erwerben möchten. Das in der Schweiz ansässige Unternehmen bietet eine benutzerfreundliche Open-Source-App für Mobilgeräte. Bei einem Kauf von über 200 € fallen lediglich 2,00 € Gebühren an.

RoboSats (robosats.com): RoboSats ist derzeit eine der besten Optionen für den anonymen Kauf von Bitcoin und bietet zahlreiche Vorteile, z. B. vollständig anonyme Konten, äußerst geringe Gebühren und Ende-zu-Ende–Verschlüsselung. RoboSats funktioniert über das Tor-Netzwerk und das Lightning-Netzwerk, was ein Höchstmaß an Privatsphäre gewährleistet. Bei einem Kauf über 200 € fallen lediglich 0,05 € Gebühren an.

Bisq (bisq.network): Bisq ist eine dezentrale, quelloffene P2P-Plattform für den Kauf von Bitcoin ohne zentrale Instanz. Die Benutzeroberfläche kann etwas unübersichtlich erscheinen. Bei Käufen über 200 € fallen Gebühren in Höhe von 2,30 € an, zusätzlich zu den variablen Bitcoin-Transaktionskosten.

HodlHodl (hodlhodl.com): HodlHodl ist eine etablierte P2P-Börse, die eine Vielzahl von Zahlungsoptionen anbietet. Allerdings steht die Plattform in der Kritik, da sie unter bestimmten Umständen Zahlungs- und Transaktionsdaten weitergibt, beispielsweise zur Bekämpfung von Geldwäsche. Bei Käufen über 200 € fallen Gebühren in Höhe von 1,20 € an.

Ein wichtiger Hinweis für Peer-to-Peer-Käufe von Bitcoin: Zahlungsmethoden über Fintech-Banken, die oft mit Kürzeln (z. B. Benutzername statt IBAN) arbeiten, sind in der Regel vorteilhafter als klassische Banküberweisungen. Bei einer IBAN-Überweisung sind mehr persönliche Informationen einsehbar, die der Verkaufspartner theoretisch ausnutzen könnte. Bei Fintech-Kürzeln bleibt in der Regel nur der Name sichtbar, was die Privatsphäre zusätzlich schützt.

Es ist zu beachten, dass nahezu alle Verkäufer einen Aufschlag auf den aktuellen Marktpreis verlangen, typischerweise etwa 5 % über dem Marktpreis. Dies liegt zum einen daran, dass es weniger No-KYC-Angebote gibt, und zum anderen daran, dass No-KYC Bitcoin momentan einen höheren Wert haben als solche von regulären Börsen. Man zahlt diesen Aufschlag also nicht direkt dem Verkäufer, sondern vielmehr für den Erhalt von No-KYC-Bitcoin. Mit etwas Geduld lassen sich jedoch auch Angebote finden, die nur 1–3 % über dem Marktpreis liegen.

Bitcoin Node

Wenn du keine eigene Node (Bitcoin Knotenpunkt) besitzt, wird dir eine öffentliche Node zugewiesen, die du momentan nutzen kannst.

- Eine Bitcoin Node verifiziert alle empfangenen Transaktionen auf Gültigkeit,
- übermittelt die von dir versendeten Transaktionen an das Netzwerk von den anderen Nodes,
- liefert der Wallet genaue Informationen zu Kontoständen und Transaktionen,
- Verhindert, dass die Wallet mit bösartigen Nodes interagiert oder gefälschte Transaktionen akzeptiert.

Solange deine Wallet nicht mit deiner eigenen Node verbunden ist, vertraust du einer fremden Node. Da alle Transaktionen, die du sendest oder empfängst, über diese Node laufen, kann der Betreiber einerseits ausgehende Transaktionen blockieren und auch eingehende Transaktionen nicht anzeigen. Zwar gibt es bislang keine öffentlich bekannten Vorfälle, dass so etwas geschehen ist, jedoch besteht diese Möglichkeit. Wenn wir ins Bankensystem schauen, sehen wir, dass dort bereits Entitäten blockiert werden. Es ist nur eine Frage der Zeit, bis dies auch bei Bitcoin der Fall sein könnte.

Ein wahrscheinlicheres Szenario, das bereits praktiziert wird, ist die Überwachung durch Nodes. Das Unternehmen, das die Node betreibt, hat Zugang zu all deinen Kontoständen und Transaktionen. Diese Daten können gespeichert und an den Staat, Werbeunternehmen oder andere Institutionen weitergegeben werden.

Es gibt verschiedene Möglichkeiten, eine Node zu betreiben. Im Grunde musst du die gesamte Bitcoin-Blockchain herunterladen (ca. 700 GB, Stand 2025) und eine Software verwenden, die alle Transaktionen und Blöcke verifiziert. Theoretisch kannst du das auch auf deinem eigenen Rechner machen, jedoch bringt das einige Nachteile mit sich. Der Computer müsste ständig eingeschaltet sein, und die Software müsste durchgehend laufen, um alle Transaktionen und Blöcke zu validieren. Ein normaler Computer würde dabei viel Strom verbrauchen und könnte langsamer werden.

Daher empfiehlt es sich, spezielle Hardware zu nutzen. Die günstigste und einfachste Variante ist die Verwendung eines Raspberry Pi. Eine Anleitung für den Betrieb einer solchen Node findest du unter privatopia.de/node. Eine andere Möglichkeit ist der Kauf eines Mini-PCs, der dafür verwendet wird. Dies ist jedoch etwas teurer und verbraucht mehr Strom. Neben der Hardware musst du auch eine Software herunterladen, um eine Benutzeroberfläche zu haben und die Bitcoin-Blockchain herunterzuladen. Für Anfänger empfehle ich UmbrelOS, da es quelloffen ist und sich durch eine sehr benutzerfreundliche Oberfläche auszeichnet. Wenn du technisch versierter bist, kannst du auch Betriebssysteme wie RaspiBlitz oder Start9OS verwenden.

Spuren verwischen

Jeder kann einen Blockexplorer (Eine sogenannte Suchmaschine für Bitcoin) wie mempool.space nutzen, um alle Transaktionen der letzten Stunde oder sogar der letzten zehn Jahre einzusehen. Abhängig von den verfügbaren Tools und dem eigenen Fachwissen kann man diese Transaktionen analysieren und ein Bild zu den Ausgabegewohnheiten einer Person erstellen. Genau das tun Blockchain-Überwachungsfirmen. Sie können aus den Transaktionen ableiten, wem was gehört. Wenn man über eine Börse mit KYC Bitcoin kauft, lassen sich diese Informationen direkt der Identität zuordnen. Bei No-KYC-Bitcoin kennt der Verkäufer oft die Zahlungsmethode. Sollte dieser Verkäufer einem Geheimdienst oder einem Blockchain-Überwachungsunternehmen angehören, kann auch hier viel über dich herausgefunden werden.

Das Ziel ist es also, nach einer Transaktion die deterministische Verbindung zur Vergangenheit zu unterbrechen. Wenn jemand versucht, diese Transaktion nachzuvollziehen, soll er oder sie an einem Punkt festhängen, an dem es dann unzählige Möglichkeiten gibt, wie und wohin diese Bitcoin gegangen sein könnten.

Hier sind einige Ideen, wie du deine finanzielle Privatsphäre erhöhen kannst, um nicht von Blockchain-Überwachungsfirmen oder anderen böswilligen Akteuren überwacht zu werden. Bitcoin ist ein freies System, bei dem dir niemand helfen wird. Man spricht auch nicht laut darüber, wie viel Bargeld man hat und wo es aufbewahrt wird – aus gesundem Menschenverstand. Genau dieses Ziel wollen wir in diesem Kapitel für Bitcoin erreichen. Dieses Buch richtet sich an Menschen, die ihre Privatsphäre zurückgewinnen möchten, und ist keine Anleitung zur Geldwäsche.

Coinjoin

CoinJoin ist eines der ersten und bekanntesten Privacy-Tools im Bitcoin-Bereich. Dabei schließen sich mehrere Personen zusammen, um eine gemeinsame Transaktion zu erstellen, bei der jeder Teilnehmer seinen Betrag zurückerhält. Durch die Vielzahl an Eingängen (Inputs) und Ausgängen (Outputs) in einer solchen Transaktion wird

es äußerst schwierig, den Zusammenhang zwischen einem bestimmten Input und dem entsprechenden Output herzustellen. Man kann lediglich verschiedene Möglichkeiten in Betracht ziehen, doch eine eindeutige Zuordnung ist nicht möglich.

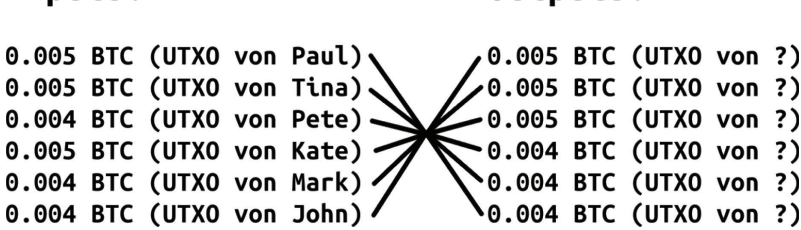

Abbildung 18Bitcoin Coinjoin

Die CoinJoin-Technologie geriet im Jahr 2024 stark ins Visier der Behörden. Die auf Privatsphäre ausgerichtete Samourai Wallet, bekannt für ihren CoinJoin-Service, wurde in diesem Jahr geschlossen. Es kam zu Verhaftungen und rechtlichen Schritten gegen die Gründer, die beschuldigt wurden, ein nicht lizenziertes Geldtransaktionsgeschäft zu betreiben und Geldwäsche ermöglicht zu haben. Kurz darauf blockierte die Wasabi Wallet, eine weitere beliebte CoinJoin-Plattform, den Zugang für US-Nutzer. Diese Maßnahme folgte unmittelbar auf die behördlichen Aktionen gegen Samourai Wallet, während sich der Gründer von Wasabi gegen ähnliche Vorwürfe zu schützen versuchte. Schließlich wurde Wasabi vom Gründer vollständig geschlossen.

CoinJoins stehen somit im Fokus von Regierungen und Behörden. Es gibt wachsende Spannungen und einen Kampf gegen dieses Privatsphäre-Tool. Obwohl CoinJoins an sich nicht illegal sind, können sie bei manchen Institutionen Misstrauen erregen. Daher sollte man sich der Konsequenzen bewusst sein, wenn man CoinJoins verwendet.

Bitcoin Sidechains

CoinJoins basieren vollständig auf dem Bitcoin-Hauptnetzwerk. Darüber hinaus existieren jedoch weitere Netzwerke wie Lightning

und Liquid, die auf dem Bitcoin-Hauptnetzwerk aufbauen, aber unabhängig davon operieren und dadurch zusätzliche Möglichkeiten bieten.

Das **Lightning Network** ermöglicht schnelle und kostengünstige Bitcoin-Transaktionen. Diese Transaktionen werden off-chain, also außerhalb der Blockchain, abgewickelt, was die Privatsphäre der Nutzer erhöht. Zahlungen werden ähnlich wie im Tor-Netzwerk weitergeleitet, sodass die verschiedenen Nutzer des Netzwerks nur schwer überwacht werden können. Diese erhöhte Privatsphäre können wir uns zunutze machen. **Liquid** wurde speziell für größere Transaktionen entwickelt und bietet vertrauliche Transaktionen, die den Betrag einer Transaktion für Dritte verschleiern. Nur die beiden beteiligten Parteien kennen den Wert der Transaktion. Zudem sind die Transaktionen schnell und kostengünstig.

Durch die Nutzung dieser beiden Netzwerke kann man kostengünstig, ähnlich wie bei CoinJoins, seine Spuren verwischen. Dafür „wechselt" man, seine On-Chain-Bitcoin ins Lightning Network oder das Liquid Network. Dadurch wird der Transaktionsfluss von außen nicht mehr nachvollziehbar. Man versendet die Bitcoin durch die verschiedenen Netzwerke und verschleiert somit, wohin sie gehen. Dafür stehen verschiedene Anbieter zur Verfügung, die man nutzen kann.

Boltz (boltz.exchange): Ein nicht-kustodialer Dienst, der den Austausch von Swaps zwischen dem Lightning Network, Liquid und der Bitcoin-Blockchain ermöglicht. Boltz unterstützt private und schnelle Swaps zwischen verschiedenen Netzwerken.

FixedFloat (ff.io): Ein Instant-Tauschdienst, der schnelle und anonyme Swaps zwischen Lightning- und On-Chain-Bitcoin ermöglicht. Der Dienst zeichnet sich durch eine benutzerfreundliche Oberfläche aus und bietet eine unkomplizierte Handhabung.

Aqua Wallet (Handy-App): Eine non-custodial Wallet, die speziell für das Liquid Network entwickelt wurde. Sie unterstützt Liquid-Bitcoin sowie Bitcoin-Lightning.

Diese Swaps verfolgen das gleiche Ziel wie CoinJoins, wirken jedoch wie gewöhnliche Transaktionen. Auch gebührenmäßig gibt es im Vergleich zu CoinJoins keine nennenswerten Unterschiede. Daher empfehle ich, verstärkt auf Swaps zu setzen, um sich vor Überwachungsfirmen zu schützen.

Bitcoin ausgeben

Beim Ausgeben und Versenden von Bitcoin ist es wichtig, bei Transaktionen darauf zu achten, verschiedene Transaktionen nicht miteinander zu mischen, die nicht zusammengehören. Besonders beim Ausgeben ist dies von großer Bedeutung. Nachfolgend werden nochmals die wichtigsten Punkte zusammengefasst.

- Alle Labels (Beschriftungen) beim Senden beachten.
- Immer bei der Transaktion notieren, wohin sie geht, an wen und zu welchem Zweck.
- Auch beim Wechselgeld (der zurückgesendeten Transaktion) vermerken, aus welcher Transaktion diese stammt.
- Bevorzugt keine vorherigen Transaktionen miteinander verbinden.
- Steuerangelegenheiten beachten.
- Bevorzugt Lightning für Zahlungen nutzen.

Steuern

Derzeit bist du nicht verpflichtet, deine Bitcoin-Bestände dem Staat zu melden, es sei denn, du musst Steuern auf die erzielten Gewinne zahlen. Daher ist es wichtig zu wissen, wann eine Steuerpflicht besteht und wann nicht. Glücklicherweise sind die steuerlichen Regelungen in Deutschland relativ großzügig.

Hinweis
Ich bin kein Steuer- oder Finanzberater. Die Informationen hier dienen lediglich allgemeinen Informationszwecken. Bitte konsultiere einen Steuerberater für deine individuelle Situation.

Wenn du eine Vermögensposition länger als ein Jahr hältst, sind die Gewinne beim Verkauf steuerfrei, unabhängig von der Höhe des Gewinns.

Wenn du innerhalb eines Jahres Gewinne erzielst, musst du diese mit deinem persönlichen Einkommensteuersatz versteuern. Liegt der Gewinn (nicht die Verkaufssumme) innerhalb eines Jahres unter 600 €, ist dieser steuerfrei. Überschreitest du diese Grenze, muss der gesamte Gewinn versteuert werden.

Zur Bestimmung der einjährigen Haltefrist wird die FIFO-Methode (First In, First Out) angewendet. Dabei wird angenommen, dass stets die zuerst erworbenen Coins auch zuerst verkauft werden, unabhängig davon, welche Coins tatsächlich veräußert werden.

Ein Verkauf im Zusammenhang mit Bitcoin umfasst grundsätzlich jede Transaktion, bei der du Bitcoin abgibst oder gegen einen Gegenwert tauschst. Dazu zählt der Verkauf von Bitcoin gegen Fiatgeld ebenso wie der Kauf eines Kaffees mit Bitcoin – in diesem Fall tauschst du deine Bitcoin gegen einen Gegenwert (Kaffee). Eine Transaktion zwischen deinen eigenen Wallets hingegen stellt jedoch keine Veräußerung dar.

Mit Bitcoin bezahlen

Derzeit ist die Akzeptanz von Bitcoin noch gering, und es gestaltet sich oft schwierig, jemanden zu finden, der für seine Dienstleistungen oder Produkte Bitcoin akzeptiert. Hier sind einige Ansätze.

Online-Privatsphäre-Dienste: Hier ist Bitcoin wahrscheinlich die am weitesten verbreitete Zahlungsmethode. Egal ob für VPN-Dienste, ProtonMail oder Spenden für Open-Source-Projekte – die meisten akzeptieren Bitcoin als Zahlungsmittel.

Online-Stores: Auch Online-Stores bieten Bitcoin als Zahlungsmethode anbieten. Ein bedeutender Anbieter in diesem Bereich ist shopinbit.com, der sich gezielt auf Zahlungen mit Bitcoin spezialisiert hat.

BTC Maps: Wenn du nach einem Restaurant, Café oder Geschäft suchst, kannst du auf btcmaps.org schauen. Dort findest du eine Übersicht zu allen physischen Standorten, an denen du mit Bitcoin bezahlen kannst.

Gutscheine: Wenn ein Geschäft nicht direkt Bitcoin akzeptiert, kann man über Umwege mit Bitcoin bezahlen, indem man eine Geschenkkarte kauft. Bitrefill ermöglicht es, Geschenkkarten für eine Vielzahl von Händlern mit Bitcoin zu kaufen.

Das Lightning-Netzwerk

Bitcoin verarbeitet etwa 7 Transaktionen pro Sekunde, während Zahlungsnetzwerke wie Mastercard und Visa bis zu 40.000 Transaktionen pro Sekunde bewältigen können. Um dennoch schnelle, kostengünstige und private Transaktionen zu ermöglichen, ist es nicht mehr notwendig, diese auf dem Bitcoin-Hauptnetzwerk durchzuführen, vielmehr kann dies über ein Neben-Netzwerk geschehen.

Hier kommt das Lightning-Netzwerk (LN) ins Spiel. Es ermöglicht Transaktionen, ohne dass diese auf der Bitcoin-Blockchain gespeichert werden müssen. Das Netzwerk funktioniert sozusagen offchain, als zweite Schicht. Es gibt zahlreiche Lightning-Nodes (Knotenpunkte), über die Zahlungen geleitet werden. Das bedeutet, dass das Netzwerk so aufgebaut ist, dass Geld den Weg über mehrere Nodes finden kann, ähnlich wie Nachrichten im Internet von einem Punkt zum anderen geleitet werden, was oft ohne direkte Verbindung geschieht. Da nicht mehr jede Transaktion für alle zugänglich gespeichert werden muss und auf einer zweiten Ebene basiert, sind Zahlungen extrem schnell und die Gebühren sehr gering. Zudem bietet das Lightning-Netzwerk eine hohe Privatsphäre. Durch die Nutzung des Lightning-Netzwerks kann man seine Spuren effektiv verwischen.

Weniger Transparenz für Außenstehende: Da der Zahlungskanal ausschließlich zwischen zwei Entitäten besteht, sind alle Transaktionen innerhalb dieses Kanals für Außenstehende unsichtbar. Dritte können einzelne Zahlung nicht nachvollziehen.

Routen über mehrere Knotenpunkte: Im Bitcoin-Netzwerk gibt es Nodes, die im Lightning-Netzwerk Zahlungskanäle untereinander eröffnen und schließen. Da Zahlungen über mehrere Kanäle und Nodes geleitet werden, bis sie beim Empfänger ankommen, wissen nur der Sender und der Empfänger genau, wer das Geld erhält. Die Nodes, die Teil der Route sind, erkennen lediglich, dass sie an der Transaktion beteiligt sind, kennen jedoch weder den ursprünglichen Sender noch den endgültigen Empfänger.

Kein dauerhaftes Aufzeichnen: Im Gegensatz zu Bitcoin-Transaktionen, die dauerhaft auf der Blockchain gespeichert werden, gibt es im Lightning-Netzwerk keine dauerhaften Aufzeichnungen der einzelnen Zahlungen innerhalb des Kanals. Diese Details „verschwinden", wenn der Zahlungskanal geschlossen wird.

Es ist daher schwierig, nachzuvollziehen, welche und wie viele Transaktionen im Lightning-Netzwerk stattfinden. Zudem kennen die Lightning-Nodes, die diese Zahlungen weiterleiten, weder den Sender noch den Empfänger. Dies macht das Lightning-Netzwerk zu einer optimalen Alternative für Zahlungen. Die Vorteile in Bezug auf Privatsphäre, niedrige Kosten und Schnelligkeit sprechen eindeutig dafür.

Custodial Lighting Wallets

Um das Lightning-Netzwerk zu nutzen, benötigst du eine spezielle Art von Wallet. Hier wird zwischen custodial und non-custodial Wallets unterschieden.

Bei custodial Lightning-Wallets übernimmt ein Unternehmen die Verwahrung deiner Bitcoin. Viele Nutzer zögern hier und ziehen oft die non-custodial Variante vor. Im Lightning-Netzwerk ist es jedoch nicht so einfach wie im Bitcoin-Netzwerk, alles selbst zu verwalten. Wenn du dich entscheidest, musst du dich, kurz gesagt, um sehr viel kümmern und erfordert viel Zeit, Wissen und Energie. Wenn dir dieser Aufwand zu groß ist, kannst du dich auf einen custodial Anbieter verlassen. Hierbei handelt es sich meist um kleinere Beträge, die es dir ermöglichen, schnell mit Bitcoin zu bezahlen. Betrachte es als

deine Geldbörse, während deine Hardware-Wallet wie ein Konto oder Safe fungiert.

Als custodial Wallet empfehle ich die **Blink Wallet**, die im Aurora Store oder im App Store verfügbar ist. Für die Anmeldung kannst du entweder eine E-Mail-Adresse oder eine Telefonnummer verwenden.

Non-custodial Lightning Wallets

Wie bereits erwähnt, erfordert die Nutzung einer non-custodial Lightning-Wallet, dass du dich selbst um alle Aspekte kümmerst. Du musst eine eigene Lightning-Node betreiben, die kontinuierlich online ist. Zudem ist es notwendig, manuell Kanäle zu anderen Knotenpunkten im Netzwerk zu erstellen und sicherzustellen, dass diese Kanäle jederzeit verfügbar sind. Auch die Ausbalancierung der Kanäle ist entscheidend, da unbalancierte Kanäle dazu führen können, dass Transaktionen fehlschlagen. Du kannst diese Node auf demselben Gerät wie die Bitcoin-Node betreiben, beispielsweise auf einem Raspberry Pi oder einem Mini-PC.

Zusammenfassend erfordert der Betrieb einer eigenen Lightning-Node erheblichen Aufwand und Fachwissen. Dies geht leider über den Rahmen dieses Buches hinaus. In der Tool-Sektion findest du jedoch Links, die dir helfen, dich intensiver mit dem Thema auseinanderzusetzen.

Altcoins

Seit der Einführung von Bitcoin haben Viele versucht, die Idee zu adaptieren und die vermeintlichen „Probleme“ von Bitcoin zu lösen. So gibt es mittlerweile über 2,4 Millionen verschiedene Altcoins. Die als problematisch angesehenen Aspekte von Bitcoin sind jedoch oft keine echten Probleme, sondern Merkmale, die Bitcoin die Sicherheit und Dezentralität verleihen, die es heute auszeichnen. Die begrenzte Anzahl und die Langsamkeit der Transaktionen ermöglichen es jedem, die Blockchain herunterzuladen und zu validieren. Die öffentlichen Transaktionen erlauben es allen Nutzern, die Blockchain zu validieren und sicherzustellen, dass im Netzwerk

niemand betrügt. Eine Änderung dieser Variablen, um andere Funktionen zu ermöglichen, würde die gesamte Netzwerkstruktur beeinflussen und könnte schnell zu einem zentralen System führen, das mehr auf Vertrauen als auf echtem Verifizieren basiert.

Das ist das Hauptproblem bei den meisten Altcoins: Sie sind zentralisiert, und das Vertrauen, dass die richtigen Entscheidungen getroffen werden und alles richtig validiert wird, liegt beim Unternehmen, das hinter dem jeweiligen Altcoin steht. Ethereum wird von der Ethereum Foundation kontrolliert, Solana von Solana Labs und Cardano von IOHK sowie der Cardano Foundation. Es ist wichtig zu unterscheiden, ob es sich um einen Altcoin handelt, der von einem Unternehmen kontrolliert wird, oder um wirklich dezentrales Geld wie Bitcoin. Wer langfristig sparen möchte, sollte sich auf Bitcoin konzentrieren. Wer hingegen mit NFTs oder neuen „Features“ spekulieren möchte, kann Altcoins in Betracht ziehen. Die Entscheidung liegt bei jedem selbst.

Eines bleibt jedoch klar: Bitcoin ist und bleibt das einzige wirklich dezentrale Geld. Wer echte Freiheit anstrebt und niemandem vertrauen möchte, hat nur Bitcoin als Option. Dennoch gibt es auch Vorteile bei anderen Coins wie beispielsweise Monero. Besonders in der Privatsphäre-Community wird Monero hochgeschätzt, da es im Vergleich zu Bitcoin eine extrem hohe Privatsphäre bei einfacher Nutzung bietet.

Alles, was wir in diesem Kapitel über den privaten Kauf, die Verwahrung und den Versand von Bitcoin besprochen haben, bietet Monero grundsätzlich. Bei einer Transaktion werden Sender, Empfänger und Betrag verborgen. Für Zahlungen, die wirklich privat sein sollen, eignet sich Monero gut, weshalb es Bitcoin bei Darknet-Geschäften übertroffen hat. Allerdings würde ich nicht empfehlen, Monero zum Sparen zu verwenden, da die Sicherheit von Monero im Gegensatz zu Bitcoin anfälliger für Angriffe von außen ist. Daher sollte Monero eher als Werkzeug für anonyme Zahlungen betrachtet werden, das bei Bedarf gegen Bitcoin eingetauscht werden kann.

Bitcoin Privacy Guide
Die Schritte aus diesem Kapitel findest du noch ausführlicher und mit detailierten Anleitungen auf der Seite privatopia.de/bitcoin.

„The nature of Bitcoin is such that once version 0.1 was released, the core design was set in stone for the rest of its lifetime."
~ Satoshi Nakamoto

Bitcoin ist eine Technologie und ein Zahlungsmittel, das nicht so schnell verschwinden wird. Obwohl es viele kleine Änderungen und Verbesserungen gegeben hat, bleibt das Grundkonzept fest verankert. Dieses Kapitel hat dir wichtige Bausteine vorgestellt, mit denen du Bitcoin sicher und privat nutzen kannst. Doch damit endet es nicht.

Bitcoin ist wie ein Kaninchenbau, der immer tiefer führt – besonders wenn es um Sicherheit und Privatsphäre geht. Bitcoin erfordert ständiges Lernen und kontinuierliche Weiterentwicklung. Um die Vorteile von Bitcoin voll auszuschöpfen und deine Privatsphäre zu schützen, ist es wichtig, sich ständig weiterzubilden und die neuesten Entwicklungen zu verfolgen.

• • •

Mit all diesen Maßnahmen haben wir die entscheidenden Schritte unternommen, um unsere Privatsphäre und Sicherheit wiederherzustellen. Wir können also zu Recht sagen, dass wir so unsere Privatsphäre zurückgewinnen können. Doch auch in Zukunft lauern weitere Herausforderungen, und es ist wichtig, wachsam zu bleiben und keine Fehler zu begehen. Im nächsten Kapitel geht es darum, wie wir langfristig mit möglichst geringem Aufwand privat und sicher bleiben können.

Kapitel 9
Sicher und privat bleiben

„Du kannst dich nie zu 100% schützen. Was du tun kannst, ist, dich so gut wie möglich vorzubereiten und das Risiko auf ein akzeptables Maß reduzieren. Du kannst das Risiko niemals vollständig beseitigen“ ~ *Kevin Mitnick*

Wenn du den bisherigen Schritten gefolgt bist, hast du dein digitales Leben bereits auf ein neues Level der Privatsphäre gehoben. Dein Smartphone und Computer laufen nun auf sicheren, datenschutzfreundlichen Betriebssystemen. Die Programme, die du verwendest, sind Open Source, respektieren deine Privatsphäre und bieten höchste Sicherheit. Deine digitale Präsenz ist auf ein Minimum reduziert, alte Spuren sind gelöscht, und durch den Einsatz von Aliasnamen und Desinformationen schützt du deine Identität im Netz. Auch deine finanzielle Privatsphäre und Sicherheit sind gewährleistet.

Doch der Weg zur vollständigen Privatsphäre ist noch nicht vollständig begangen. Jeden Tag treffen wir Entscheidungen, die unsere Sicherheit und Privatsphäre beeinflussen können. Unternehmen lauern überall darauf, persönliche Daten zu sammeln. Ein kleiner Fehler kann ausreichen, um die hart erarbeitete Privatsphäre zu gefährden. Deshalb ist es entscheidend, vorbereitet zu sein und zu wissen, wie du auch im Alltag sicher und privat bleiben kannst.

To-dos

Mit deinem sicheren Smartphone und Computer hast du die Kontrolle über deine Daten übernommen. Diese Freiheit bringt jedoch auch Verantwortung mit sich. Wenn du etwas verlierst, kannst du dich nicht mehr uneingeschränkt auf Unternehmen verlassen, die alles für dich wiederherstellen. Daher ist es wichtig, selbst gut vorbereitet zu sein. In den vorherigen Kapiteln habe ich bereits über Backups und regelmäßige Aufgaben gesprochen. Diese lassen sich

in wöchentliche und monatliche To-dos unterteilen. Um sicherzustellen, dass du sie nicht vergisst, empfiehlt es sich, wiederkehrende Termine in deinen Kalender einzutragen. Schon nach kurzer Zeit wird dies zur Routine: Wöchentliche Aufgaben nehmen nicht mehr als 10 Minuten in Anspruch, während monatliche etwa 30 Minuten benötigen. Nutze folgende Liste als Checkliste; die genauen Anleitungen findest du in den jeweiligen Kapiteln. Unter jeder To-do-Liste gibt es Platz für eigene Notizen, z. B. zu zusätzlichen Backups für spezielle Apps oder andere Ideen.

Wöchentliche To-dos

- PC aktualisieren: Bei Linux das erforderliche Skript im Terminal ausführen (siehe Seite: 33)
- PC-Apps aktualisieren: Benötigte Updates im Softwarestore herunterladen (siehe Seite: 34)
- PC mit Bleachbit säubern: Nicht mehr benötigte zwischengespeicherte Dateien löschen lassen (siehe Seite: 39).
- ClamAV: Wöchentlichen Virenscan mit ClamAV durchführen (siehe Seite: 40).
- Browserdaten löschen (Handy + PC): Solltest du die automatische Speicherung von Cookies nicht deaktiviert haben, einmal manuell alle Daten in den Einstellungen löschen.
- Dateien aufräumen: Im Laufe der Woche sammeln sich viele neue Dateien an, z. B. Downloads oder selbst erstellte Dokumente. Wöchentlich solltest du hier Ordnung schaffen.
- Handy-Apps aktualisieren: F-Droid und Aurora öffnen und die erforderlichen Updates herunterladen (siehe Seite: 62).
- Handy neu starten: Ein regelmäßiger Neustart schadet nicht und kann die Sicherheit erhöhen (siehe Seite: 56).

_____

_____

_____

_____

Die wöchentlichen Aufgaben verfolgen hauptsächlich das Ziel, dein System und deine Software auf dem neuesten Stand zu halten sowie für Ordnung zu sorgen. Diese Schritte nehmen nicht viel Zeit in Anspruch und sollten einmal pro Woche gegangen werden.

Monatliche To-dos:

- Fotos sichern: Bilder vom Handy auf den PC und einen Backup-USB-Stick kopieren (siehe Seite: 66).
- Passwortmanager sichern: Alle Passwörter vom Passwortmanager auf PC und USB-Stick speichern (siehe Seite: 104).
- 2FA-Codes sichern: Alle 2FA-Codes aus EnteAuth auf PC und USB-Stick sichern (siehe Seite: 108).
- E-Mails sichern: Neue E-Mails auf PC und USB-Stick speichern (siehe Seite: 127).
- Finanz-App-Daten sichern: Daten der Finanz-App auf PC und USB-Stick speichern (siehe Seite: 164).
- Handy-Dateien sichern: Wichtige Dateien vom Handy auf den PC kopieren.
- PC-Dateien sichern: Dateien auf dem PC mit einem USB-Stick synchronisieren (siehe Seite: 112).
- Kontakte sichern: Neue Kontakte auf PC und USB-Stick sichern (siehe Seite: 146).
- Kalender sichern: Kalender auf PC und USB-Stick sichern (siehe Seite: 145).
- Daten überprüfen und löschen: Internet nach neuen, ungewollten Informationen durchsuchen und diese löschen (siehe Seite: 172).
- Apps/Accounts überprüfen und löschen: Nicht genutzte Apps und Accounts auf Handy und PC entfernen.
- Dritter Speichertort**:** Daten vom USB-Stick mit dem extern gelagerten Speichermedium synchronisieren.

_____

_____

_____

Die monatlichen Aufgaben, insbesondere die Backups, erfordern einen gewissen Zeitaufwand. Wenn du dein digitales Leben jedoch stark vereinfacht hast, könntest du in der Lage sein, die Backups nur alle zwei Monate durchzuführen. Je weniger du Daten doppelt sicherst, desto höher ist das Risiko, diese zu verlieren. Während einige wöchentliche Backups bevorzugen, empfinden andere es als ausreichend, diese alle zwei Monate durchzuführen.

Metadaten

Metadaten werden oft als „Daten über Daten" beschrieben. Bei dem Inhalt einer Textnachricht handelt es sich nicht um Metadaten. Informationen darüber, wer die Nachricht gesendet hat, an wen sie ging, zu welcher Uhrzeit und die Größe der Nachricht – das sind Metadaten. Auf den ersten Blick mag das vielleicht nicht als ein großer Eingriff in unsere Privatsphäre erscheinen. Doch betrachten wir einige Beispiele, um zu verstehen, wie aufschlussreich Metadaten tatsächlich sein können.

Es ist bekannt, dass Paul auf drei verschiedenen Webseiten war, die sich mit Privatsphäre beschäftigen, und dass er danach eine Überweisung an eine VPN-Firma getätigt hat. Was er auf diesen Seiten getan oder gekauft hat, bleibt unbekannt.

Es ist bekannt, dass Roman einen Anruf von der Polizei erhalten hat und unmittelbar danach seinen Anwalt für eine Stunde angerufen hat. Den Inhalt beider Gespräche kennt niemand.

Es ist bekannt, dass Moritz und Luis beide auf einer Peer-to-Peer-Bitcoin-Webseite waren und sich 30 Minuten später an demselben Ort befanden, basierend auf Handystandortdaten. Was genau auf der Webseite oder bei ihrem Treffen passiert ist, bleibt unklar.

Es ist bekannt, dass Dominik von einem Hochhaus aus die Suizid-Hotline angerufen hat und ein 15-minütiges Gespräch führte. Über den Inhalt des Gesprächs gibt es jedoch keine Informationen.

Es ist bekannt, dass Theodor nach dem Erhalt einer E-Mail von einem Arzt auf Webseiten über Tod und Erbschaften recherchiert hat. Der Inhalt der E-Mail sowie Informationen über das, was er genau auf den Webseiten gemacht hat, bleiben unklar.

Linus postet ein Foto seines Essens auf Social Media. Jetzt weiß man, wo das Foto aufgenommen wurde, wann, mit welchem Gerät und mit welchen Einstellungen.

Wie du siehst, können Metadaten genauso aufschlussreich sein, wie die eigentlichen Inhalte selbst – manchmal sind sie sogar noch informativer. Metadaten sollten also genauso geschützt werden wie die Daten, die sie begleiten. Ein ehemaliger NSA-Chef sagte einmal, dass das US-Militär Menschen allein auf Basis von Metadaten tötet. In einem anderen Fall konnte die Polizei einen Mörder nur durch die Metadaten seiner Smartwatch und Nachrichten fassen. Es gibt viele solcher Geschichten, Metadaten sind also nicht zu vernachlässigen.

„Metadaten sind unglaublich aufschlussreich. Als Analyst würde ich immer zuerst auf Metadaten schauen, weil sie schneller und leichter zugänglich sind und nicht lügen."
~ Edward Snowden

Leider erzeugt jeder digitale Klick Metadaten. In den ersten Kapiteln haben wir bereits Programme und Dienste eingerichtet, die entweder gar keine Metadaten sammeln oder sie nur so lange speichern, wie es unbedingt nötig ist, und sie dann löschen. Auch der VPN und DNS, die wir konfiguriert haben, helfen dabei, unsere Metadaten zu schützen. Unsere Messaging-Apps sammeln ebenfalls keine Daten, was uns zusätzliche Sicherheit bietet.

Der wichtigste Schritt ist jedoch, sich der Existenz von Metadaten immer bewusst zu sein und darauf zu achten, diese so gut wie möglich zu minimieren. In diesem Kapitel möchten wir uns besonders mit den Metadaten von Fotos befassen. Wie bereits erwähnt, speichern Fotos zahlreiche Informationen über die Aufnahme. Du kannst dies selbst überprüfen, indem du in deiner Galerie auf das Informationssymbol eines Fotos klickst.

Es ist wichtig zu beachten, dass nicht nur die Kameraeinstellungen und das verwendete Gerät in den Metadaten eines Fotos gespeichert werden, sondern auch die genaue Uhrzeit, der Standort und viele weitere Informationen zum Zeitpunkt der Aufnahme. Wenn du Fotos ohne vorherige Überprüfung dieser Metadaten versendest oder hochlädst, kannst du damit deine Sicherheit und Privatsphäre erheblich gefährden. Daher ist es ratsam, diese Metadaten zu entfernen, bevor du ein Bild teilst. Einige Dienste, wie Twitter, entfernen diese Metadaten automatisch beim Hochladen. Dennoch empfehle ich dir, diesen Schritt selbst zu übernehmen, um sicherzustellen, dass du niemandem blind vertraust.

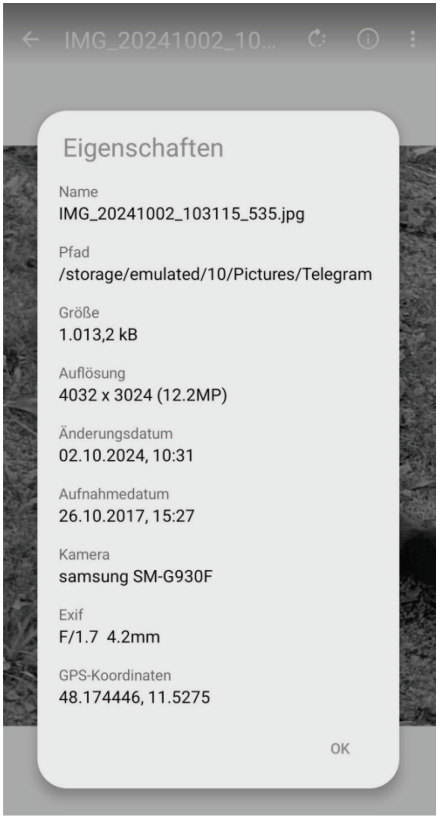

Abbildung 19: Metadaten bei Fotos

- Lade das Bildbearbeitungsprogramm GIMP herunter (verfügbar für Linux, MacOS und Windows).
- Öffne das Bild, dessen Metadaten du entfernen möchtest, in GIMP.
- Klicke auf „Datei“ und anschließend auf „Exportieren als …“. Wähle einen Speicherort aus und gib einen Dateinamen ein. Achte darauf, dass der Dateiname keine sensiblen Informationen enthält – standardmäßig könnten hier das Datum und die Uhrzeit der Aufnahme angezeigt werden.
- Klicke auf „Exportieren“.
- Es öffnet sich ein Fenster mit Exportoptionen.

- Entferne die Häkchen bei „EXIF-Daten speichern“, „XMP-Daten speichern“ und „Erstellungszeit speichern“.
- Klicke erneut auf „Exportieren“. Die Metadaten wurden nun aus dem Bild entfernt.
- Du kannst dies überprüfen, indem du in deiner Galerie erneut auf das Infosymbol des Bildes klickst.

„Plant your flag“

Obwohl wir unsere Online-Präsenz so weit wie möglich reduzieren möchten, kann es dennoch sinnvoll sein, bei bestimmten Institutionen einen Account unter dem echten Namen zu erstellen. Im Englischen spricht man dabei von „Plant your flag“ – also „Setze deine Flagge“. Das Ziel ist nicht, diese Konten regelmäßig zu nutzen, sondern sich vor Identitätsdiebstahl zu schützen. Wenn Betrüger in unserem Namen Konten erstellen, kann das erhebliche Probleme verursachen. Besonders bei finanziellen oder staatlichen Angelegenheiten kann es schnell kompliziert werden. Daher ist es ratsam, einen Account in unserem Namen zu erstellen, um zu verhindern, dass ein Angreifer dies später tun kann. Hier sind einige Beispiele, bei denen es sinnvoll ist, sich abzusichern:

Elster Mit einem persönlichen Konto kannst du sicherstellen, dass niemand auf deine Steuerinformationen zugreifen oder in deinem Namen Anträge einreichen kann.
Besuche die Webseite: www.elster.de

BundID Das digitale Identitätskonto BundID ist ein zentraler Identitätsnachweis für zahlreiche Online-Dienste. Es schützt vor Identitätsmissbrauch und gewährleistet eine sichere und einfache Nutzung digitaler Angebote. Weitere Informationen findest du auf der Webseite: www.bundid.de

Online-Funktion des Personalausweises (nPa): Diese Funktion ermöglicht die Identifizierung für zahlreiche Dienste und schützt dein Konto vor Identitätsmissbrauch. www.personalausweisportal.de
BAföG-Dienste und Sozialleistungen: Bei Plattformen für Sozialleistungen wie Arbeitslosengeld oder BAföG ist es sinnvoll, ein

Konto unter dem eigenen Namen zu führen, um betrügerische Anträge zu verhindern. Weitere Informationen findest du auf den folgenden Webseiten: www.bafög.de und www.arbeitsagentur.de

Deutsche Rentenversicherung: Hier kannst du Rentenauskünfte einsehen und Anträge stellen. Ein offizielles Konto schützt deine gesetzlichen Renteninformationen.
Besuche die Webseite: www.deutsche-rentenversicherung.de

Gesundheitswesen (elektronische Patientenakte und E-Rezepte): Um deine elektronische Patientenakte und Gesundheitsdaten effektiv zu schützen, ist die Erstellung eines Accounts auf folgender Webseite empfehlenswert: www.gematik.de

Meldewesen und Online-Anmeldung bei Behörden: Viele Städte bieten Online-Services zur Ummeldung und zur Terminbuchung bei Behörden an. Um sich vor unberechtigten Anfragen mit dem eigenen Namen zu schützen, ist es sinnvoll, ein Konto anzulegen.

Portale für Führerschein und Fahrzeugzulassung: Diese sind länderabhängig, aber wenn Online-Zulassungen für Führerschein und Fahrzeug möglich sind, sollte man ein Konto erstellen, um rechtliche Probleme zu vermeiden.

Software und Apps von Autoherstellern: Viele moderne Fahrzeuge sind mit Apps oder Online-Portalen verbunden, die Funktionen wie das Ab- und Abschließen des Autos, die Fernsteuerung der Klimaanlage sowie die Anzeige des aktuellen Standorts und des Fahrzeugstatus bieten. Es ist ratsam, einen Account zu erstellen, um sicherzustellen, dass niemand unbefugt auf diese Daten zugreifen kann.

Du musst diese Konten nicht nutzen; es ist oft sogar besser für deine Privatsphäre, wenn du auf analoge Wege setzt. Indem du ein Konto unter deinem Namen erstellst, stellst du sicher, dass niemand anderes in deinem Namen handelt und Probleme verursacht.

Private Informationen schützen

Es kommt häufig vor, dass Unternehmen – sowohl online als auch in der realen Welt – nach deinen persönlichen Informationen fragen. Einfach zu sagen, dass du aus Gründen der Privatsphäre keine Angaben machen möchtest, wird oft nicht gut aufgenommen und kann dazu führen, dass du abgewiesen wirst. In den meisten Fällen sprichst du jedoch mit Mitarbeitern, und mit ein wenig Geschick lässt sich vieles erreichen, ohne persönliche Daten preiszugeben.

Stalker: Wenn du von einem Stalker oder einem gewalttätigen Ex-Partner berichtest, kann das oft auf Verständnis stoßen. Es ist jedoch wichtig, so wenig Informationen wie möglich preiszugeben, um nicht erneut in eine gefährliche Situation zu geraten. Die Mitarbeiter möchten vermeiden, dass durch ihr Handeln etwas Schlimmes passiert.

Rache: Man kann auch eine ähnliche Geschichte nutzen, indem man von einer rachsüchtigen Person berichtet, die bereits Gewalt angedroht oder versucht hat, einem zu schaden. Die Angst vor erneuten Bedrohungen kann denselben Effekt haben – niemand möchte für eine Eskalation verantwortlich gemacht werden.

Es gibt viele kreative Methoden, deine Privatsphäre zu schützen. Manche mögen das übertrieben finden, aber für Menschen, denen ihre Privatsphäre wirklich am Herzen liegt, sind solche Maßnahmen oft notwendig. Immer wieder werden persönliche Daten abgefragt, doch mit kleinen Tricks kannst du deine Sicherheit und Privatsphäre wahren.

Wenn nach deiner Telefonnummer oder einer Bestätigung per E-Mail über dein Handy gefragt wird, reicht meist nicht, zu sagen, dass du dein Handy vergessen hast. Ein nützlicher Trick ist, ein kaputtes Handy vorzuzeigen und zu behaupten, es sei gerade heruntergefallen und nicht mehr funktionsfähig. Bisher hat niemand weiter nachgehakt, und die Forderung nach der Handynummer wurde schnell fallengelassen. Solche defekten Handys bekommst du günstig auf eBay und kannst sie bei Bedarf einfach vorzeigen.

Wenn nach deiner Adresse gefragt wird, kannst du, ohne komplett zu lügen, nur einen Teil der Adresse angeben, z. B. nur die Straße ohne Hausnummer. Auch beim Namen kannst du nur den ersten Buchstaben des Vor- oder Nachnamens verwenden. Sei besonders vorsichtig, bei staatlichen Institutionen niemals falsche Angaben zu machen – das ist illegal. Aber braucht Facebook wirklich deine genaue Adresse? Wohl eher nicht.

Wenn nach deinem Ausweis gefragt wird, ist der Reisepass oft die bessere Wahl, da er weniger persönliche Informationen enthält. Vermeide es außerdem, deinen Ausweis scannen zu lassen. Nach einer kurzen Nachfrage lassen viele Unternehmen davon ab und akzeptieren es, wenn du den Ausweis nur zeigst. Wenn du Kopien anfertigen musst, solltest du diese selbst erstellen, anstatt sie vom Unternehmen machen zu lassen. So kannst du auf die Kopie ein Wasserzeichen setzen, auf dem steht: „Kopie für [Name des Unternehmens]. Nicht zur Identifikation geeignet." Das schützt dich im Falle eines Datenlecks, und das Unternehmen wird sorgsamer mit der Kopie umgehen. Zusätzlich kannst du dein Foto auf der Kopie abdecken, um noch mehr Privatsphäre zu wahren. Dies erfordert allerdings, dass du im Voraus weißt, wo du die Kopie benötigst, und sie entsprechend vorbereitest. Besonders für Hotels macht das Sinn.

Daten nach dem Tod?

Hast du dir schon einmal Gedanken darüber gemacht, was mit deinen Daten nach deinem Tod passiert? Wenn du alle Schritte dieses Buches befolgst, sind deine Daten sicher und geschützt. Das bedeutet jedoch auch, dass nach deinem Tod weder Familienmitglieder noch Unternehmen oder Dienstleister Zugriff darauf haben werden.

Einige Menschen wünschen sich genau das: Ihre Daten sollen auch nach dem Tod sicher bleiben. Andere hingegen möchten, dass ihre Familie auf bestimmte oder sogar alle Daten zugreifen kann. Wenn du zu dieser Gruppe gehörst, solltest du jetzt Vorkehrungen treffen. Eine Möglichkeit besteht darin, wichtige Backups auf einem USB-Stick zu speichern und einer vertrauenswürdigen Person sowohl den Speicherort als auch das Passwort für die verschlüsselte Datei (z. B.

mit VeraCrypt) mitzuteilen. Wenn du nur einen Teil deiner Daten freigeben möchtest, kannst du dafür einen speziellen verschlüsselten Container erstellen. Es gibt viele Wege, wie du mit deinen Daten umgehen kannst. Wichtig ist, dass du einen Plan für den Umgang mit deinen Daten nach deinem Tod hast.

Adresse schützen

Die meisten von uns erhalten regelmäßig Werbung, die oft ungeöffnet im Papierkorb landet. Wenn du dir jedoch bewusst machst, welche Werbung du bekommst und in welchem Umfang, wird schnell klar, wie viele Unternehmen tatsächlich deine Privatadresse und den damit verbundenen Namen kennen. Hotelketten, die nicht nur für ihre eigenen Hotels werben, sondern auch Daten an Dritte weitergeben, Modekataloge, Technikangebote, Lieferdienste und vieles mehr – all diese Unternehmen haben Zugriff auf deine Adresse. Deine Wohnadresse ist also ein wichtiges Thema, wenn dir deine Privatsphäre am Herzen liegt und du ungewollte Post vermeiden möchtest. In diesem Kapitel möchte ich dir einige Ideen vorstellen, wie du deine Privatadresse besser schützen kannst.

Postfach

Der effektivste Weg, deine Adresse zu schützen, besteht darin, sie nicht überall preiszugeben. Eine weit verbreitete Möglichkeit hierfür ist das Postfach der DHL. Damit kannst du zumindest in bestimmten Fällen deine private Wohnadresse schützen. Das Postfach ist besonders nützlich für Onlinebestellungen oder bei Onlinekonten, bei denen du Post erhalten möchtest. Die Anmeldung ist unkompliziert und schnell, jedoch ist eine Identifikation erforderlich. Außer dem Namen für die Post, die dir persönlich zugestellt wird, kannst du auch ein Pseudonym angeben, um unter diesem Namen Post zu empfangen. Ein Nachteil des Postfachs ist jedoch, dass es nicht überall akzeptiert wird. Bei Arbeitgebern, Banken, Finanzdienstleistern oder Vereinsmitgliedschaften wird häufig eine physische Adresse verlangt, die ein Postfach nicht ersetzen kann.

- Ein Postfach kannst du dir einrichten unter: www.dhl.de

Anstatt deinen vollständigen Namen anzugeben, kannst du hier auch lediglich deinen Nachnamen sowie den Anfangsbuchstaben deines Vornamens verwenden. Das wird funktionieren.

Um deine Adresse zusätzlich zu schützen, benötigst du jedoch eine Alternative, die auch als physische Adresse anerkannt wird. In Deutschland ist das leider nicht ganz so einfach. Es gibt keinen einheitlichen Weg, sondern viele Optionen, die sich ständig ändern können. Eine eigene Recherche ist daher unerlässlich. Hier möchte ich dir einige Ideen vorstellen.

Hinweis
Die Informationen in diesem Buch dienen nur allgemeinen Zwecken und stellen keine rechtliche Beratung dar. Bei rechtlichen Fragen solltest du dich an einen qualifizierten Anwalt oder Berater wenden.

Postadresse bei Unternehmen

Betrachten wir zunächst die Geschäftswelt. Aufgrund der Impressumspflicht sind Unternehmen verpflichtet, eine Adresse auf ihren Webseiten anzugeben. Um ihre Privatsphäre zu schützen, nutzen viele Geschäftsleute spezielle Dienstleister, die eine Geschäftsadresse bereitstellen. Diese Option kann auch für Privatpersonen von Interesse sein, die ihre private Adresse schützen möchten.

Ein **Virtual Office** (virtuelles Büro) bietet eine Geschäftsadresse sowie administrative Dienstleistungen an, ohne dass eine physische Präsenz erforderlich ist. Besonders attraktiv ist der Postannahme- und Weiterleitungsservice. Die Kosten hierfür liegen zwischen 30 und 100 € pro Monat.

Ein **Coworking Space** bietet in erster Linie Arbeitsplätze an, doch viele dieser Einrichtungen ermöglichen es, ihre Adresse als Geschäftsadresse zu nutzen. Dadurch kannst du Post und Pakete dort empfangen und deine private Adresse schützen. Die Kosten liegen zwischen 80 und 300 Euro pro Monat.

Es empfiehlt sich, die Anbieter direkt zu kontaktieren und nach den Möglichkeiten zu fragen, eine solche Adresse zu nutzen. Wenn du den Schutz deiner Privatsphäre als Grund angibst, könnte dies jedoch zu Ablehnungen führen. Stattdessen könntest du dich als Autor ausgeben, der seine Privatadresse schützen möchte. Wenn dein Buch unter einem Pseudonym veröffentlicht wurde (was häufig der Fall ist), kannst du das Pseudonym ebenfalls verwenden, um Post zu empfangen. In der Regel wird dies nicht überprüft, solange du nicht auffällst.

Postadresse für Reisen

Schauen wir uns eine weitere Gruppe an, die eine Adresse benötigt, aber aufgrund längerer Reisen keine eigene Adresse mehr hat. Sich als Reisender auszugeben kann neue Möglichkeiten eröffnen. Auch Wohnungssuchende fallen in diese Kategorie. Wenn du auf der Suche nach einer neuen Wohnung bist und derzeit nur in Hotels übernachtest, benötigst du ebenfalls eine Möglichkeit, Post zu empfangen. Eine gängige Lösung besteht darin, sich bei einem Freund oder jemandem aus der Familie anzumelden, der bereit ist, deine Post für dich zu empfangen. Diese Adresse wird dann als deine offizielle Anschrift anerkannt und von Banken sowie staatlichen Institutionen akzeptiert. Für langfristige Reisen ist dies ideal. Jedoch stellt sich die Frage, ob es eine nachhaltige Lösung ist, um dauerhaft deine Privatadresse zu schützen. In diesem Fall müsstest du möglicherweise einen Haupt- und Nebenwohnsitz anmelden, was rechtlich problematisch sein kann, da die Gefahr besteht, eine „Scheinadresse“ anzugeben. Zudem muss die Person, bei der du dich anmeldest, bereit sein, dich bei diesem Schutz deiner Privatsphäre zu unterstützen. Rechtlich ist dies also eine heikle Angelegenheit. Eine weitere Möglichkeit ist die Nutzung einer c/o-Adresse, bei der die Post an eine Vertrauensperson gesendet wird. Diese Adresse könnte dann beispielsweise so aussehen:

Max Mustermann
c/o Martina Maier
Martinastraße 10
53174 Bonn

In diesem Fall wird die Post für Max Mustermann an Martina Maier zugestellt. Du kannst bei Banken oder anderen Institutionen nachfragen, ob sie c/o-Adressen akzeptieren. Dabei solltest du den Grund „Privatsphäre“ nicht direkt erwähnen, da dies zu Ablehnungen führen könnte. Stattdessen könntest du erklären, dass du eine längere Reise planst und deinen Mietvertrag gekündigt hast, aber dennoch eine Adresse benötigst, um wichtige Post zu empfangen.

Postadresse bei privaten Kontakten

Die einfachste und kostengünstigste Lösung besteht darin, jemanden aus deinem Bekanntenkreis zu finden, der bereit ist, als Empfangsstelle für dich zu fungieren. Wenn du beispielsweise jemanden kennst, der ein eigenes Geschäft betreibt, könntest du ihn fragen, ob du seine Geschäftsadresse für den Empfang deiner Post nutzen darfst. So hast du die Möglichkeit, auch unter einem Pseudonym Post zu empfangen, was zusätzlich zu deiner Adresse auch deinen Namen schützt – besonders bei Online-Bestellungen. Solltest du diese Option nicht nutzen können, kannst du dich bei kleineren lokalen Postdienstleistern erkundigen. Frage nach den angebotenen Optionen und den entsprechenden Konditionen, denn oft sind diese Shops flexibler als große Unternehmen, die sich strikt an interne Vorgaben halten müssen.

Zusammenfassend ist festzuhalten, dass es in Deutschland nicht einfach ist, die eigene Adresse vollständig zu schützen. Besonders bei staatlichen Angelegenheiten, Steuern, Arbeit oder Finanzen ist es erforderlich, eine physische Adresse anzugeben. Idealerweise gelingt es dir jedoch, deine Adresse bei Online-Bestellungen und gegenüber Unternehmen, die gerne deine Daten sammeln, zu schützen.

Autos

Unser Auto weiß oft mehr über uns, als wir uns vorstellen können. Es registriert unsere täglichen Fahrten, weiß, wo wir arbeiten und kennt sogar unseren Musikgeschmack. Das Erschreckendste daran? Wir geben diese Informationen freiwillig preis – häufig, ohne es überhaupt zu bemerken.

Welche Daten sammelt unser Auto?

Ähnlich wie bei großen Tech-Konzernen ist es oft unklar, welche Daten genau gesammelt und wie sie verwendet werden. Zwar gibt es Datenschutzerklärungen mit hunderten Seiten an Kleingedrucktem, aber kaum jemand liest sie. Stattdessen sehen wir häufig nur eine kleine Meldung auf dem Bildschirm des Autos, begleitet von einem großen „OK"-Button. Um weiterfahren zu können, drücken die meisten einfach darauf, ohne lange darüber nachzudenken. Und genau das genügt den Herstellern, um unsere Daten zu sammeln und sie nach eigenem Ermessen zu verwenden.

Mozilla hat in einem Bericht 25 Automarken untersucht und festgestellt: Autos sind ein Albtraum für die Privatsphäre. [13] Tatsächlich gehen sie so weit, zu behaupten, dass Autos das schlechteste Produkt in Bezug auf den Datenschutz sind. Es gibt kaum Möglichkeiten, die Funktionen eines modernen Autos zu nutzen, ohne gleichzeitig eine Fülle an persönlichen Daten preiszugeben. Einige Autohersteller drohen sogar damit, dass das Fahrzeug bei Ablehnung der Datennutzung nicht mehr richtig funktioniert. Ein Beispiel ist Tesla: Wer sich aus der umfassenden Datensammlung zurückziehen möchte, erhält die Mitteilung, dass wichtige Funktionen des Fahrzeugs dann nicht mehr verfügbar sind und die Weiterfahrt nicht empfohlen wird. Leider gibt es derzeit nur wenige Optionen, die eigenen Daten im Auto effektiv zu schützen.

Wenn wir unser Handy mit dem Auto verbinden – sei es über USB oder Bluetooth – werden nicht nur die gewünschten Daten wie Musik oder Navigationsinformationen übertragen. Das Auto erhält oft auch Zugriff auf Kontakte, genutzte Apps, Telefonnummern, E-Mail-Adressen und sogar Gesundheitsdaten. Sowohl Apple als auch Android übermitteln diese Daten automatisch. Und es bleibt nicht dabei: Auch das Auto selbst sammelt fleißig Informationen. Sprachsteuerungen, die in den meisten modernen Autos integriert sind, erfassen Gespräche und andere Daten von uns und unseren Mitfahrenden.

Je mehr „smarte" Technik in einem Auto steckt, die uns das Leben erleichtern soll, desto mehr Daten werden über uns gesammelt. Wir

stehen also ständig vor der Entscheidung: Bequemlichkeit oder Privatsphäre?

Falls du denkst, das sei übertrieben, betrachten wir das Beispiel Nissan. Bis zu einem Update im Dezember 2023 sammelte Nissan Daten zu Gesundheit, Fahrverhalten, Standort und Müdigkeit des Fahrers. Das klingt nicht nur beunruhigend, sondern wirft auch die Frage auf, was mit diesen Daten geschieht. Oft werden sie intern genutzt, um gezielte Werbung zu schalten oder beim nächsten Autokauf passende Angebote zu machen. Manchmal landen die Daten auch bei Tochterfirmen – wie bei Toyota, wo sie an „Toyota Financial Services" weitergegeben werden, die sich um Autofinanzierung und Leasingverträge kümmern. [14] In vielen Fällen werden die Daten sogar an externe Dritte verkauft, etwa an Datenhändler, Versicherungen oder staatliche Behörden. Was kann man also tun?

Automodell

Wenn du über den Kauf eines neuen Autos nachdenkst, ist es der perfekte Zeitpunkt, um deine Privatsphäre von Anfang an zu schützen. Die Wahl des Automodells und des Herstellers ist entscheidend dafür, welche und wie viele Daten über dich gesammelt und weitergegeben werden.

In Deutschland ist es gesetzlich vorgeschrieben, dass alle Autos mit einer eingebauten SIM-Karte ausgestattet sind. Offiziell dient diese etwaigen Notfallsituationen, ermöglicht jedoch auch die Übermittlung von Informationen über die Fahrzeugsoftware und alle verbundenen Geräte an den Autohersteller. Hat dein Auto beispielsweise einen Geschwindigkeitsassistenten? Praktisch, aber er könnte auch alle Geschwindigkeitsüberschreitungen aufzeichnen. Oder einen Spurhalteassistenten? Auch hier besteht die Möglichkeit, dass Fahrmuster wie unaufmerksames oder möglicherweise betrunkenes Fahren erfasst und zukünftig geteilt werden könnten. Obwohl dies derzeit nicht der Fall ist, könnte eine kleine Gesetzesänderung die Tür zu einer umfassenden Überwachung weit öffnen.

Moderne Fahrzeuge – von teuren BMWs bis hin zu günstigeren Toyotas – verfügen fast alle über große Infotainmentsysteme. Was

früher ein einfaches Autoradio war, ist heute ein Touchscreen, der nicht nur Musik abspielt, sondern auch eine Vielzahl an Daten über uns sammelt.

Diese modernen Fahrassistenz- und Infotainmentsysteme machen das Fahren zwar komfortabler, stellen jedoch auch einen tiefgreifenden Eingriff in unsere Privatsphäre dar. Auch wenn es aktuell nicht wie eine dystopische Überwachungszukunft aussieht, könnte sich dies schnell ändern. Wenn dir Privatsphäre wichtig ist, solltest du in Betracht ziehen, ein älteres Modell zu wählen – eines mit so wenigen Assistenzsystemen wie möglich, am besten nur mit einem einfachen Radio anstelle eines Bildschirms.

Das mag extrem klingen, aber ein möglichst mechanisches Auto mit minimaler Software ist der beste Schutz für deine Privatsphäre. Natürlich verstehe ich, dass dies nicht für jeden der ideale Weg ist. In Deutschland hat das Auto einen hohen Stellenwert, und viele möchten sich ungern von modernen Funktionen verabschieden. Wenn das bei dir der Fall ist, kannst du zum nächsten Abschnitt über die Autosoftware springen, um zu erfahren, wie du dein aktuelles Fahrzeug so privat wie möglich halten kannst.

Werfen wir auch einen Blick auf den Kauf gebrauchter Autos. Es gibt zahlreiche Geschichten, in denen der ursprüngliche Besitzer eines Fahrzeugs Jahre nach dem Verkauf noch Zugriff auf das Auto hatte. Diese Personen erhielten E-Mails mit Anmeldedaten für die neue Auto-App des Herstellers und konnten nach dem Einloggen den aktuellen Standort des Autos einsehen. In manchen Fällen konnten sie sogar Funktionen wie das Öffnen und Schließen der Türen oder die Klimaanlage aus der Ferne steuern. Noch beunruhigender ist, dass sie den gesamten Standortverlauf des Fahrzeugs einsehen konnten, einschließlich der Wohn- und Arbeitsadresse des neuen Besitzers.

Beim Kauf eines gebrauchten Autos musst du daher unbedingt sicherstellen, dass das Fahrzeug vollständig zurückgesetzt ist und keine Daten des Vorbesitzers mehr vorhanden sind. Am besten beauftragst du jemanden, der sich professionell damit auskennt, um sicherzugehen, dass wirklich alles gelöscht ist. Andernfalls könnte es

passieren, dass der Vorbesitzer dich weiterhin überwachen kann – ein Szenario, das sicher niemand erleben möchte.

Ältere Automodelle bieten mehr Privatsphäre, und bei Gebrauchtwagen solltest du darauf achten, dass der Vorbesitzer keinen Zugriff mehr hat. Bei der Wahl eines Modells sind unauffällige, häufig genutzte Farben wie Weiß, Grau oder Schwarz empfehlenswert, ebenso wie verbreitete Fahrzeugmodelle, die weniger Aufmerksamkeit erregen. Ein Lamborghini oder ein auffälliger blauer Tesla zieht weitaus mehr Blicke auf sich als ein weißer Toyota. Auch Chromfelgen oder Spoiler sorgen für mehr Aufmerksamkeit – und genau das wollen wir vermeiden, wenn uns Privatsphäre wichtig ist.

Bevor du den Kaufvertrag unterschreibst, informiere dich darüber, welche Daten dein potenzielles Auto sammelt und ob du einige Funktionen deaktivieren kannst. Gibt es die Möglichkeit, das gesamte Infotainmentsystem abzuschalten? Perfekt. Kannst du zumindest einen Teil der Datensammlung über ein „Privacy Center“ im Auto minimieren? Auch gut. Falls das Auto dich zwingt, allen Datensammlungen und -weitergaben zuzustimmen, solltest du überlegen, ob du nicht ein anderes Modell wählst. Für viele ist das vielleicht kein Grund, die Lieblingsautomarke zu wechseln, aber wer maximale Privatsphäre erreichen will, sollte diesen Schritt in Erwägung ziehen.

Kurz vor der Vertragsunterzeichnung ist auch der richtige Zeitpunkt, zusätzliche Forderungen zu stellen. Es ist der Moment, in dem der Verkäufer alles tun wird, um den Deal abzuschließen. Viele Händler bringen kleine Werbeanzeigen am Auto an, oft unauffällig unter dem Kennzeichen oder auffälliger in Form von Aufklebern.

Fordere, dass diese entfernt werden – sonst fährst du kostenlos als Werbeträger herum. Jetzt ist auch die beste Gelegenheit, alle datensammelnden Funktionen deaktivieren zu lassen. Die meisten Verkäufer könnten zwar erstaunt schauen, aber du wirst wahrscheinlich nur auf wenig Widerstand stoßen, da sie alles tun werden, um das Auto zu verkaufen.

Abbildung 20 Werbung unter dem Kennzeichen

Autosoftware

Einige Automarken, wie Toyota oder Lexus, bieten benutzerfreundliche Datenschutzeinstellungen, mit denen du schnell viele invasive Funktionen deaktivieren kannst. Bei anderen Herstellern gestaltet sich dies hingegen deutlich komplizierter. Da jedes Fahrzeug unterschiedlich ist, kann ich dir keine spezifische Anleitung für jede Marke geben. Stattdessen möchte ich dir grundlegende Tipps an die Hand geben, die du in deinem Auto anwenden kannst, um deine Privatsphäre bestmöglich zu schützen.

Datenschutzeinstellungen anpassen: Dies ist der offensichtlichste und einfachste Schritt, der jedoch häufig von vielen, selbst in der Privatsphäre-Community, übersehen wird. Fast alle Autohersteller bieten die Möglichkeit, die Menge an geteilten Daten zu begrenzen. Einige bieten mehr Optionen als andere, aber du solltest in jedem Fall nach den Einstellungen für „Datenschutz“ oder „Privatsphäre“ suchen. Dort kannst du Funktionen wie die Übertragung von Telemetriedaten oder die Verbindung zu Cloud-Diensten deaktivieren. Gehe alle Optionen sorgfältig durch und deaktiviere alles, was nicht unbedingt erforderlich ist.

App-Datenschutz: Viele Hersteller haben inzwischen begleitende Apps für ihre Fahrzeuge entwickelt, die in manchen Fällen sogar notwendig sind, um bestimmte Funktionen nutzen zu können. Auch

hier ist es ratsam, wie beim Infotainmentsystem im Auto, alle unnötigen Funktionen zu deaktivieren.

Verbindungen kontrollieren: Die meisten modernen Autos verfügen über Bluetooth- und WLAN-Verbindungen, die ständig aktiv sind, um sich mit Geräten zu koppeln und Daten zu sammeln. Dies kann ein erhebliches Risiko für deine Privatsphäre darstellen. Um dieses Risiko zu minimieren, solltest du vermeiden, dein Handy dauerhaft mit dem Auto zu koppeln. Schalte Bluetooth und WLAN im Auto vollständig ab, wenn du sie nicht aktiv benötigst – genauso wie bei deinem Handy auch.

Sprachassistenten deaktivieren: Sprachassistenten im Auto sind ebenso problematisch wie diese, die zu Hause benutzt werden. Sie hören ständig zu, was ein erhebliches Risiko für deine Privatsphäre darstellt. Wenn möglich, deaktiviere den Sprachassistenten vollständig oder entferne ihn sogar.

Navigation: Die Navigationssysteme in Autos sind zwar praktisch, jedoch erfassen sie häufig mehr Daten über dich als Google Maps. Daher ist es ratsam, diese Funktionen zu meiden und stattdessen die sicher eingerichtete Handy-Navigation zu nutzen. Eine Handyhalterung, die an der Windschutzscheibe oder vor dem Radio angebracht wird, kostet nur etwa 10 € und bietet dir den gleichen Komfort, ohne deine Privatsphäre zu gefährden. Alternativ kannst du auch ein externes GPS-Gerät verwenden, achte jedoch darauf, dass es deine Privatsphäre respektiert.

Auto-Apps: Einige der neuesten Fahrzeugmodelle ermöglichen es dir sogar, Apps direkt im Auto zu installieren. Das solltest du jedoch möglichst vermeiden. Entferne vorinstallierte Apps, wenn das möglich ist, oder deaktiviere sie zumindest, um deine Daten zu schützen. Da das Auto oft als das „schlimmste“ Gerät für unsere Privatsphäre bezeichnet wird, bleibt uns leider nicht viel Spielraum. Das Beste, was wir tun können, ist, uns anzugewöhnen, das Auto hin und wieder einfach stehen zu lassen – so wie wir es auch mit dem Handy machen sollten. Für viele von uns ist das jedoch keine realistische Option, daher ist es umso wichtiger, die Datensammlung im Auto zu minimieren.

Viele Fahrzeuge sind mit einer SIM-Karte ausgestattet und verfügen somit über eine Mobilfunkverbindung. Die Telekom nutzte diese Daten früher, um den Standort der Fahrzeuge zu analysieren und Rückschlüsse auf den Verkehrsfluss zu ziehen. Wenn beispielsweise nur ein Auto mit 30 km/h durch eine 60er-Zone fuhr, war das uninteressant. Fuhren jedoch viele Autos zur gleichen Zeit nur 30 km/h, konnte man auf einen Stau schließen. Seitdem hat sich die Technologie in Autos erheblich weiterentwickelt, und die Menge an Daten, die heute erfasst wird, ist unvorstellbar. Es ist wichtig zu beachten, dass alles was du mit deinem Auto machst, potenziell überwacht wird. Dein Auto ist also kein „sicherer Ort" in Bezug auf deine Privatsphäre.

Physische Sicherheit und Privatsphäre

Zum Abschluss dieses Kapitels möchte ich den Fokus auf die physische Sicherheit und die Privatsphäre legen. Wir haben bereits viel unternommen, um unsere Privatsphäre und Sicherheit in der digitalen Welt zu schützen, doch auch im realen Leben gibt es Risiken, die nicht unterschätzt werden sollten. Es geht darum, auch hier unnötige Gefahren zu vermeiden und sorgsam mit unseren persönlichen Informationen umzugehen.

An einem Nachmittag suchte ich auf Reddit nach den neuesten Entwicklungen im Bereich der Privatsphäre und stieß auf einen Artikel, der um eine „Privatsphäre-Bewertung" bat. Im Wesentlichen bat eine Person um ein ehrliches Feedback zu ihrem Lebensstil in Bezug auf den Schutz der Privatsphäre und die von ihr verwendeten Werkzeuge. Ich scrollte nach unten und stellte fest, dass es sicherlich einige Lücken in ihrer Strategie gab, aber insgesamt schien sie solide genug zu sein. Doch dann brachte der erste Kommentar die Dinge in die richtige Perspektive: „Wie sicher sind dein physischer Computer und deine Dokumente zu Hause? Wenn jemand einbricht, was wird er finden?"

Diese Frage liegt wirklich im Kern der Privatsphäre. Ich bin erstaunt, dass so viele Ratschläge da draußen wenig bis gar nichts über physische Privatsphäre zu sagen haben. Sicher, dein Leben kann rein

durch digitale Mittel zerstört werden, aber dein echtes Leben und deine physischen Besitztümer weisen andere, in dem Fall physische Angriffspunkte.

Müll entsorgen

Während wir online großen Wert auf den Schutz unserer Daten legen, gehen viele im realen Leben oft nachlässig mit sensiblen Informationen um. Diverse Finanzdokumente, Steuerunterlagen und offizielle Schreiben landen häufig ungeschützt im Papiermüll, wo sie von unbefugten Personen gefunden und missbraucht werden können. Dies stellt nicht nur eine Verletzung der Privatsphäre dar, sondern birgt auch ein erhebliches Sicherheitsrisiko. Es ist daher ratsam, alle Dokumente, die persönliche Informationen enthalten, vor der Entsorgung unkenntlich zu machen. Ein Schredder ist eine einfache und effektive Lösung dafür. Die wenigen Sekunden, die es dauert, sind gut investiert, wenn man bedenkt, welche sensiblen Daten geschützt werden müssen – seien es Bestellungen oder noch heiklere Träger von Informationen wie Finanz- oder Staatsdokumente.

Alte Geräte

Ähnlich dem Müll können auch alte Handys, Computer oder Festplatten weiterhin viele persönliche Informationen enthalten – selbst, wenn du diese vollständig zurückgesetzt hast. Der Verkauf solcher Geräte an andere Personen birgt daher immer ein gewisses Risiko. Ich verstehe, dass nicht jeder die Mittel hat, regelmäßig neue Hardware zu kaufen und auf den Verkauf alter Geräte angewiesen ist. Dennoch solltest du dir der Risiken bewusst sein, dass Käufer möglicherweise mit den verbliebenen Daten Missbrauch treiben könnten. Überlege daher gut, ob der Verkauf wirklich notwendig ist.

Verstecke vermeiden

Wenn du Wertgegenstände, Hardware-Wallets oder Schlüssel verstecken möchtest, solltest du gängige Verstecke wie Bücherattrappen oder gefälschte Steine im Garten vermeiden, da diese von Einbrechern häufig sofort erkannt werden. Stattdessen ist es ratsam,

die Gegenstände in alltäglichen, unscheinbaren Objekten zu verstecken – z. B. in einem alten Pokal, einem Lego-Modell oder veralteter Technik, die für Einbrecher uninteressant ist. Diese vermeintlich wertlosen Gegenstände bieten oft die besten Verstecke, da sie selten durchwühlt werden, weil der Einbrecher darin keinen Wert vermutet.

Aufmerksamkeit vermeiden

Es ist ratsam, nicht unnötig aufzufallen. Teure Markenkleidung, Uhren oder auffällige Villen ziehen schnell Aufmerksamkeit auf sich und wecken das Interesse anderer, mehr über dich zu erfahren. Auch auf Reisen solltest du vermeiden, wie ein typischer Tourist auszusehen – z. B. durch T-Shirts mit touristischen Aufdrucken oder Kameras um den Hals. Am besten ist es, in der Menge zu verschwinden und unauffällig zu bleiben.

Reisen

Seit den Anschlägen vom 11. September 2001 sind die Sicherheitskontrollen an Flughäfen weltweit erheblich strenger geworden. Früher oder später wirst du in die Situation kommen, in der ein Beamter von dir verlangt, dein Handy oder deinen Laptop zu entsperren, um Einsicht zu erhalten. An diesem Punkt zu diskutieren, bringt wenig. Daher ist es wichtig, sich im Vorfeld Gedanken darüber zu machen, wie du in solchen Situationen reagieren möchtest. Es gibt verschiedene Ansätze, je nachdem, wie stark du deine Daten schützen möchtest. Oft hört man das Argument, man habe nichts zu verbergen, und deshalb sei es kein Problem, wenn ein Beamter kurz auf das Gerät schaut. Das mag in den meisten Fällen zutreffen, aber wenn diese Daten unsicher bei den Grenzbeamten gespeichert werden, können Hacker später darauf zugreifen. Daher solltest du dich auch auf diese Möglichkeit vorbereiten.

Inlandsflüge

In Deutschland sind Inlandsflüge in Bezug auf den Datenschutz in der Regel unproblematisch. Die Sicherheitskontrollen sind minimal, und Geräte werden selten überprüft. In den meisten Fällen musst du

weder Passwörter noch Zugangsdaten angeben. Oft wird vor dem Flug nicht einmal eine Identifikation verlangt. Daher stellen Inlandsflüge kein großes Risiko für deine Daten dar.

Flüge innerhalb der Schengen-Zone

Ähnlich wie bei Inlandsflügen sind auch Flüge innerhalb der Schengen-Zone (EU-Flüge) relativ unproblematisch. Die Kontrollen sind selten und beschränken sich meist auf die Überprüfung physischer Gegenstände, während digitale Daten in der Regel nicht überprüft werden. Daher gibt es wenig Anlass zur Sorge, und besondere Maßnahmen sind oft nicht erforderlich. Bei internationalen Reisen hingegen gestaltet sich die Situation anders.

Internationale Reisen

Egal, ob mit dem Auto oder dem Flugzeug – sobald du außerhalb der EU reist, steigt das Risiko, dass ein Grenzbeamter Zugang zu deinen Geräten verlangt, erheblich. Leider hast du in solchen Fällen kaum Rechte. Wenn du den Zugriff verweigerst, wirst du zwar nicht festgenommen, aber die Beamten zeigen dir einfach den Weg zurück. Du musst also allen Forderungen nachkommen. Deshalb ist es wichtig, sich im Vorfeld gut vorzubereiten. Es gibt zwei Optionen.

Laptop: Wenn du den Schritten in diesem Buch gefolgt bist, ist dein Laptop bereits gut gegen Angriffe geschützt. Sollte jedoch ein Beamter Zugang zu deinem Gerät erhalten, kann all diese Sicherheit gefährdet werden. Eine Möglichkeit, dies zu verhindern, besteht darin, alle sensiblen Daten manuell zu löschen: Programme, Dateien, Bilder, Logins und Browserdaten. Eine gründlichere Methode ist, das Betriebssystem vollständig neu aufzusetzen, sodass keine persönlichen Daten mehr auf dem Gerät vorhanden sind. Anschließend kannst du die für die Reise benötigten Apps installieren, solltest dich jedoch nicht anmelden.

In beiden Fällen ist es ratsam, ein Backup aller wichtigen Daten zu erstellen. Hierfür kannst du einen verschlüsselten VeraCrypt-Container nutzen (siehe Kapitel 4), den du in einer sicheren, verschlüsselten Cloud wie ProtonMail Drive ablegst. Selbst wenn jemand

Zugriff auf die Cloud erhält, sieht er nur den verschlüsselten Container. Sollte der Grenzbeamte also deinen Laptop durchsuchen, findet er entweder ein frisch installiertes System oder einen Laptop ohne persönliche Daten. Nach der Grenzkontrolle kannst du den Container herunterladen und auf deine Daten zugreifen.

Handy: Ähnlich wie bei einem Laptop kannst du auch von den Daten deines Handys ein Backup erstellen und die Daten in der Cloud speichern. Ein komplettes Zurücksetzen des Geräts könnte jedoch verdächtig wirken. Daher empfehle ich einen anderen Ansatz: Erstelle ein Backup aller wichtigen Dateien und speichere es in der Cloud. Lösche anschließend alle Benutzerprofile bis auf eines. Melde dich von allen Apps ab und lasse die SIM-Karte zu Hause, da sie im Ausland ohnehin nicht funktioniert und potenziell zur Überwachung genutzt werden könnte. Sollte ein Grenzbeamter dein Handy kontrollieren, sieht er nur ein leeres Profil ohne gespeicherte Daten. Nach der Grenzüberquerung kannst du die Profile wiederherstellen und, falls nötig, eine anonyme SIM-Karte erwerben.

USA: Die USA zählen zu den Ländern mit den umfassendsten Grenzkontrollen. Dort werden nicht nur elektronische Geräte überprüft, sondern es kann auch verlangt werden, Zugangsdaten zu E-Mail-Konten oder sozialen Netzwerken preiszugeben. Zudem werden häufig persönliche Fragen gestellt, beispielsweise zu deinem Arbeitgeber oder deinem sozialen Umfeld. Sei dir dessen bewusst und überlege im Voraus, wie du damit umgehen möchtest.

• • •

Während die vorherigen Kapitel den Aufbau unserer digitalen Sicherheit und Privatsphäre im Detail behandelt haben, liegt der Fokus in diesem Kapitel auf der praktischen Umsetzung im Alltag. Mit diesen Tipps meistern wir die täglichen Herausforderungen hinsichtlich des Schutzes unserer Privatsphäre und bewahren uns vor äußeren Eingriffen. Das erworbene Wissen unterstützt uns in allen Bereichen – von wiederkehrenden Aufgaben an den zuvor eingerichteten Betriebssystemen über private Zahlungsoptionen bis hin zu physischer Sicherheit und Privatsphäre.

Das Ziel des vorliegenden Buches, umfassende digitale Sicherheit und Privatsphäre zu erreichen, haben wir nun in den wesentlichen und entscheidenden Bereichen verwirklicht. Wir verfügen über sichere Handys und Computer, nutzen sichere Programme sowie Verschlüsselungen, und schützen unsere Verbindungen und Finanzen. Doch damit endet unser Vorhaben nicht.

Deine Reise zur Wahrung der Privatsphäre ist ein fortlaufender Prozess. Neue Technologien und Methoden zur Verbesserung von Sicherheit und Privatsphäre werden ständig entwickelt – aber genauso erzielen auch die Angreifer Fortschritte. Indem du dich regelmäßig informierst und die neuesten Tools und Techniken anwendest, kannst du dein digitales Leben privater und sicherer gestalten. Ein guter Startpunkt ist privatopia.de; weitere Links und Literatur findest du in der Tool-Sektion.

Ein kleiner Gefallen?

Hat dir dieser Ratgeber gefallen und konntest du deine Privatsphäre zurückgewinnen? Dann würde es mich freuen, wenn du eine kurze Bewertung schreibst. Eine positive Bewertung hilft mir sowie anderen Lesern die ihre Privatsphäre schützen möchten.

Fazit

„Privatsphäre ist wertvoll. Ich denke, dass Privatsphäre der letzte wahre Luxus ist, den wir haben. Dein Leben so leben zu können, wie du es willst, ohne dass jeder darüber kommentiert oder davon weiß."
~ Valerie Plame

Wir haben gemeinsam einen weiten Weg zurückgelegt, doch das Thema „Privatsphäre und Sicherheit" ist so umfassend, dass es nicht in einem einzigen Buch vollständig behandelt werden kann. Mein Ziel bei der Erstellung dieses Leitfadens war es, ein solides Fundament zu schaffen, das dich gegen die größten Bedrohungen schützt und dir hilft, die Kontrolle über deine digitale Freiheit zurückzugewinnen.

Wenn du den Strategien in diesem Buch gefolgt bist – herzlichen Glückwunsch! Zu Beginn haben wir einen sicheren, privaten Computer eingerichtet, indem wir Ubuntu als Hauptbetriebssystem installiert haben – eine Plattform, die sicherstellt, dass keine unnötigen Daten über dich gesammelt oder weitergegeben werden.

Dieses sichere Fundament konnten wir dann auf dein Smartphone übertragen, das wohl am stärksten verfolgte Gerät in unserem Alltag. Mithilfe von GrapheneOS haben wir es so konfiguriert, dass die Kontrolle über deine Daten fest in deinen Händen liegt.

Anschließend installierten wir auf beiden Geräten die optimalen Anwendungen, um maximale Sicherheit und Privatsphäre zu gewährleisten. Wir haben überall für den bestmöglichen Schutz gesorgt – von einem zuverlässigen Passwortmanager über sichere Browser bis hin zu alltäglichen Apps wie Karten- und Unterhaltungsdiensten. Auch die digitalen Spuren unserer Vergangenheit konnten wir beseitigen und nutzen stattdessen Aliase, um im Internet anonym zu bleiben. Das Gleiche gilt hinsichtlich der zahlreichen Eingriffe in unsere Privatsphäre, gegen die wir im täglichen Leben nun gewappnet sind, um online wie offline sicherer und privater zu sein.

Wir haben großen Unternehmen und staatlichen Institutionen die Macht entzogen, unsere Daten zur Überwachung und Einschränkung unserer Freiheit zu nutzen. Es war ein anstrengender Prozess, aber wir können uns nun beruhigt zurücklehnen, in dem Wissen, dass unsere digitale Welt ein wenig sicherer und privater geworden ist.

Mit der Zeit werden neue Technologien und wissenschaftliche Fortschritte unsere Welt weiterhin verändern – oft auf eine Weise, die wir uns heute noch gar nicht vorstellen können. Das bedeutet, dass Institutionen neue Werkzeuge zur Überwachung und Kontrolle erhalten, aber auch wir Zugang zu neuen Tools bekommen, die uns helfen, uns gegen diese Einflüsse zu schützen.

Mit dem Wissen aus diesem Buch kannst du deine digitale Privatsphäre stärken und neue Tools nutzen, um dein Leben sicherer und einfacher zu gestalten. Es gibt leider keinen perfekten, allgemeingültigen Plan für Privatsphäre, da jeder individuelle Bedürfnisse und Anforderungen hat, die oft von Arbeit, Familie oder anderen Umständen beeinflusst werden. Sollten dir auf deinem Weg zur Privatsphäre größere Hürden begegnen, die du nicht leicht eigenständig lösen kannst, kontaktiere uns.

Wir unterstützen unsere Klienten dabei, individuelle Herausforderungen in den Bereichen Privatsphäre, Sicherheit und Bitcoin zu meistern. Mehr zu unseren Dienstleistungen findest du auf:
privatopia.de/beratung

Falls du an den neuesten Entwicklungen zu Privatsphäre, Sicherheit und Bitcoin interessiert bist und erfahren möchtest, welche neuen Tools und Strategien es gibt, besuche unsere Website unter privatopia.de. Dort erwarten dich kostenlose Blogbeiträge, Ressourcen und ein Newsletter, der dich stets auf dem neuesten Stand hält.

Das Schreiben dieses Buches war ein wunderbares Erlebnis. Ich bin dankbar, meine Erfahrungen und Gedanken mit dir teilen zu können, und hoffe, dass ich dich ein Stück näher zur vollumfänglichen Privatsphäre gebracht habe

Danke für deine Zeit und Aufmerksamkeit. Ich wünsche dir das Beste auf deinem Weg zur digitalen Freiheit.

Wichtige Begriffe zur Privatsphäre – einfach erklärt

Hier findest du eine kompakte Übersicht der wichtigsten Begriffe zu Privatsphäre, Sicherheit und Bitcoin – ideal zum schnellen Nachschlagen bei Fragen. Für mehr Details und ausführlichere Anleitungen steht unter privatopia.de/wörterbuch eine erweiterte Sammlung bereit.

2FA: Zwei-Faktor-Authentifizierung, bei der ein zusätzlicher Sicherheitsschritt zur Anmeldung erforderlich ist.
Algorithmus: Berechnungsvorschrift zur Lösung einer Aufgabe durch eine festgelegte Abfolge von Schritten.
Alias: Ein alternativer Name oder Benutzername, oft zur Wahrung der Anonymität verwendet. Ein Pseudonym.
Anonymität: Zustand, in dem die Identität einer Person nicht bekannt oder erkennbar ist.
Anwendungen/Apps: Softwareprogramme oder Apps, für Computer und Handys.
App-Store: Plattform zum Herunterladen von Apps für mobile Geräte sowie Computer.
Backdoor: Versteckter Zugang zu einem System, der meist für unberechtigte Zugriffe genutzt wird.
Backup: Sicherheitskopie von Daten, um Datenverlust vorzubeugen.
Benutzerkonto: Persönliches Profil in einem System oder einer App, das Zugriff und Einstellungen verwaltet.
Betriebssystem: Grundlegende Software eines Computers oder Geräts, die alle Programme und Hardware steuert.
Biometrische Daten: Körperbezogene Merkmale wie Fingerabdruck oder Gesichtserkennung, die zur Identifikation verwendet werden.
BIOS: Grundsoftware eines Computers, die beim Start die Hardware lädt und steuert.
Bitcoin: Digitales Geld, das auf einem dezentralen Netzwerk basiert.
Blockchain: Datenstruktur zur sicheren und transparenten Speicherung von Transaktionen in Blöcken (z.B. bei Bitcoin).

Blockexplorer: Online-Tool, mit dem Informationen über alle Blockchain-Transaktionen abgerufen werden können.
Booten: Startvorgang eines Computers oder mobilen Geräts nachdem es ausgeschaltet wurde.
Börse: Plattform zum Kauf und Verkauf von Kryptowährungen.
Browser: Programm zum Surfen im Internet, z. B. Chrome oder Firefox.
Brute Force: Methode, bei der alle möglichen Passwörter ausprobiert werden, um Zugriff zu erhalten.
Cache: Zwischenspeicher, der häufig genutzte Daten speichert, um den Zugriff zu beschleunigen.
Captcha: Test, um zu unterscheiden, ob ein Nutzer Mensch oder Bot ist.
CBDC: Zentralbank-Digitalwährung, eine digitale Version staatlicher Währungen.
Cloud-Speicher: Online-Speicherplatz für Daten, auf den von überall zugegriffen werden kann.
Commands: Befehle, die zur Steuerung von Programmen oder Systemen verwendet werden.
Cookies: Kleine Dateien, die vom Browser gespeichert werden, um Informationen über den Nutzer zu speichern.
Datenleck: Unbeabsichtigte Veröffentlichung oder Verlust von vertraulichen Daten.
Datenschutz: Maßnahmen zum Schutz persönlicher Daten vor unberechtigtem Zugriff.
Datenverschlüsselung: Schutzmethode, bei der Daten durch Umwandlung unlesbar gemacht werden ohne dem richtigen Passwort.
Deep Web: Bereich des Internets, der nicht über normale Suchmaschinen zugänglich ist, sondern über den Tor-Browser.
Dezentralisierung: Verteilung von Kontrolle und Verantwortung auf mehrere, unabhängige Stellen.
DNS: System zur Umwandlung von Domainnamen (z. B. www.example.com) in IP-Adressen (124.283.293.2).
Download: Herunterladen von Daten oder Programmen aus dem Internet.
Doxen: Veröffentlichen von privaten Informationen einer Person ohne deren Zustimmung.
Drive: Laufwerk oder Speicherort für Daten auf einem Computer oder in der Cloud.

Ende-zu-Ende-Verschlüsselung: Verschlüsselung, bei der nur Absender und Empfänger die Nachricht lesen können.
Ent-googelt: Entfernung oder Reduzierung von Google-Diensten zur Verbesserung der Privatsphäre.
Exploit: Sicherheitslücke, die zur Manipulation von Systemen ausgenutzt werden kann.
Fake-Account: Falscher oder gefälschter Benutzeraccount, meist zur Irreführung erstellt.
Festplatte: Speichergerät eines Computers, auf dem Daten dauerhaft gespeichert werden.
Fiat-Geld: Staatlich ausgegebene Währung wie Euro oder Dollar.
Fingerprinting: Techniken, um Nutzer anhand ihrer digitalen Spuren zu identifizieren, wie dem Betriebsystem oder Browser.
Fintech-Banken: Finanztechnologie-Banken, die hauptsächlich digitale Bankdienste anbieten.
Firewall: Schutzsystem, das unautorisierten Zugriff auf ein Netzwerk verhindert.
Flashen: Neuinstallation oder Aktualisierung einer Firmware auf einem Gerät.
For-You-Page: Personalisierte Seite in Social-Media-Apps mit empfohlenen Inhalten.
Fork: Abspaltung oder Anpassung eines bestehenden Softwareprojekts oder einer Blockchain.
Formatieren: Löschen und Neuanordnen eines Speichermediums zur Vorbereitung auf die Datenspeicherung.
gehostet: Auf einem Server gespeichert und bereitgestellt.
Gemountet: Mit einem Computer verbunden und als nutzbares Laufwerk erkannt.
GrapheneOS: Datenschutzorientiertes Betriebssystem für Android-Geräte.
Hacker: Person, die in Systeme eindringt, oft um Sicherheitslücken zu nutzen.
Hardware: Physische Komponenten eines Computers, wie Festplatten oder Prozessoren.
Hardwarewallet: Physisches Gerät zur sicheren Aufbewahrung von Kryptowährungen.
Herunterladen: Speichern von Dateien oder Daten aus dem Internet auf einem Gerät.

Identitätsdiebstahl: Missbrauch von persönlichen Daten, um sich als jemand anderes auszugeben.
Installieren: Einrichten und Speichern einer Software auf einem Gerät.
Internetprotokoll (IP): Regelwerk zur Übertragung von Daten über das Internet.
IP-Adresse: Eindeutige Nummer, die ein Gerät im Internet identifiziert.
ISP: Internetdienstanbieter, der den Zugang zum Internet ermöglicht.
Keylogger: Programm, das Tastatureingaben aufzeichnet, oft zur Spionage genutzt.
Knotenpunkte: Verbindungsstellen in einem Netzwerk, die Daten weiterleiten.
Kryptografie: Wissenschaft der Verschlüsselung zum Schutz von Daten.
KYC: Know Your Customer; Identitätsprüfung bei der Nutzung bestimmter Dienste.
Linux: Open-Source-Betriebssystem, oft als sicherere Alternative zu Windows genutzt.
Login: Anmeldung mit Benutzernamen und Kennwort bei einem System.
LTS: Long-Term Support; längere Supportdauer für Softwareversionen.
Malware: Schadsoftware, die Systeme infiziert und Schaden verursacht.
Man-in-the-Middle-Angriff: Abfangen und Manipulieren von Daten zwischen zwei Kommunikationspartnern.
Metadaten: Zusatzinformationen zu Daten, wie Datum und Ort einer Aufnahme.
No-KYC: Dienst oder Plattform ohne Identitätsprüfung.
Open-Source: Software, deren Quellcode öffentlich zugänglich und veränderbar ist.
Passwort-Manager: Software zur sicheren Verwaltung von Passwörtern.
Peer-to-Peer: Direktverbindung zwischen Geräten oder Personen ohne zentrale Vermittlungsstelle.
PGP: Pretty Good Privacy; Verschlüsselungsmethode zum Schutz von Nachrichten und Dateien.

Pop-up: Fenster oder Anzeige, die auf dem Bildschirm erscheint.
Privacy: Schutz persönlicher Informationen und Privatsphäre.
Privacy-Community: Gemeinschaft, die sich für den Schutz der Privatsphäre einsetzt.
Private key: Geheimer Teil eines Schlüsselpaares, zur Entschlüsselung genutzt.
Privates Fenster: Browser-Modus ohne Speicherung von Verlauf und Cookies.
Public key (Öffentlicher Schlüssel): Öffentlich zugänglicher Schlüssel für Verschlüsselung.
RAM: Arbeitsspeicher eines Computers zur kurzfristigen Datenspeicherung.
Schadsoftware: Software, die Schaden an Systemen verursacht (z. B. Malware).
Server: Computer, der Daten oder Dienste in einem Netzwerk bereitstellt.
Software: Programme und Anwendungen, die auf Computern oder Geräten ausgeführt werden.
Softwarewallet: Digitale Geldbörse für Kryptowährungen auf einem Gerät.
Spam: Unerwünschte Nachrichten, meist per E-Mail.
Telemetrie: Automatisierte Übertragung von Nutzungs- und Diagnosedaten an Anbieter.
Terminal: Textbasiertes Eingabefenster zur Steuerung von Computerfunktionen.
Tor-Netzwerk: Netzwerk zur Anonymisierung der Internetverbindung.
Tracker: Software, die das Online-Verhalten von Nutzern aufzeichnet.
Tracking: Verfolgung und Analyse von Aktivitäten im Internet.
Überspielen: Übertragen von Dateien von einem Medium oder Gerät auf ein anderes.
Ubuntu: Kostenloses, auf Linux basierendes Betriebssystem.
VPN: Virtuelles Privates Netzwerk, das eine verschlüsselte Verbindung herstellt, um die Internetaktivitäten zu schützen.
Zero-Knowledge-Prinzip: Methode, bei der keine vertraulichen Daten vom Dienstleister gespeichert werden.

Tool Sektion,
Links und weiterführende Artikel

Kapitel 1 Sicherer und privater Computer

System 76 (sichere und private Linux-Computer):
https://system76.com
FrameWork (sichere und private Linux-Computer):
https://frame.work
Ubuntu herunterladen: https://ubuntu.com/download/desktop
Ubuntu Download verifizieren:
https://ubuntu.com/tutorials/how-to-verify-ubuntu#1-overview
Balena Etcher (Ubuntu auf USB-Stick flashen)
https://etcher.balena.io/
Artikel zu Dual Boot (Windows und Ubuntu gleichzeitig benutzen) https://thefilibusterblog.com/de/stepbystep-guide-to-dual-booting-linux-alongside-windows-11/
VirtualBox (Virtuelle Maschinen auf Linux Ubuntu):
https://www.virtualbox.org/
Artikel – VirtualBox für Ubuntu: https://ubuntu-user.de/tech/ubuntu-fuer-virtualbox-leitfaden-zur-einrichtung/
Tails (Linux auf einem USB-Stick)
https://tails.net/install/download/

Kapitel 2 Sicheres und privates Handy

GrapheneOS unterstützte Geräte und Updates:
https://grapheneos.org/faq#device-lifetime.
Anleitung – GrapheneOS über das Terminal installieren:
https://grapheneos.org/install/cli
Anleitung – GrapheneOS über den Browser installieren:
https://grapheneos.org/install/web
Artikel – Was ist VOIP? https://privatopia.de/voip
F-Droid (Open-Source App-Store) https://f-droid.org/
Links – spenden an Open-Source Projekte:
privatopia.de/open-source-spenden

Kapitel 3 – Anonym surfen

LibreWolf installieren: https://librewolf.net/installation/
Tor-Browser Download: https://www.torproject.org/download/
Mullvad VPN: https://mullvad.net/de/vpn
Proton VPN: https://protonvpn.com/
NextDNS: https://my.nextdns.io/signup

Kapitel 4 Passwörter und Verschlüsselung

Bitwarden herunterladen (Passwortmanger):
https://bitwarden.com/download/
KeyPassXC herunterladen (Offline-Passwortmanager):
https://keepassxc.org/download/
Bitwarden Add-on für LibreWolf (Firefox):
https://addons.mozilla.org/de-de/firefox/addon/bitwarden-password-manager/
YubiKey (Hardware 2FA): https://www.yubico.com/?lang=de
YubiKey unterstütze Dienste und einrichten:
https://www.yubico.com/works-with-yubikey/catalog/?sort=a-z
EnteAuth App (App für 2FA): https://ente.io/auth/
VeraCrypt (Verschlüsselung für Dateien und USB-Sticks):
https://veracrypt.eu/en/Downloads.html
FreeFileSync (Synchronisation zwischen Geräten/USB-Sticks):
https://freefilesync.org/

Kapitel 5 Private Kommunikation

Protonmail (sicherer und privater E-Mail-Anbieter):
https://mail.proton.me
Protonmail Import-Export-App (E-Mails sichern):
https://proton.me/support/export-emails-import-export-app
TutaMail (alternativer, sicherer und privater E-Mail-Anbieter):
https://tuta.com
SimpleLogin (E-Mail-Aliase): https://simplelogin.io/
TempMail (Temporäre E-Mail-Adressen): https://tempmail.email/
Throwawaymail (Temporäre E-Mail-Adressen):
https://www.throwawaymail.com/
Anonyme eSIM Karten: https://silent.link/

SMS4Sats (Temporäre Telefonnummern für SMS-Bestätigungen): https://sms4sats.com/
Signal Messenger Download: https://signal.org/download/
Molly Messenger Download: https://molly.im/
SimpleX Messenger Download: https://simplex.chat/
Wire Messenger: https://wire.com/de/
Matrix Messenger: https://matrix.org/
Jitsy Meet Videokonferenz: https://meet.jit.si
FFMeet (Private Videokonferenz)**:** https://meet.ffmuc.net/

Kapitel 6 Digitale Werkzeuge und Alternativen

Proton-Kalender (privater und sicherer Kalender): https://calendar.proton.me/
Fossify-Kalender (Kalender für GrapheneOS): https://github.com/FossifyOrg/Calendar
Etesync (E2EE, Synchronisation von Kalendern und Kontakten): https://www.etesync.com/
Evolution (Kontakte und Kalender beuntzen und speichern auf Linux): https://help.gnome.org/users/evolution/stable/
Storage Scopes für GrapheneOS: https://grapheneos.org/usage#storage-scopes
Standart Notes (private Notiz-App mit Synchronisation): https://standardnotes.com/
Obsidian (private Notiz-App mit vielen Funktionen): https://obsidian.md/
OnlyOffice (Alternative zu Microsoft Office): https://www.onlyoffice.com/de/
Odysee (Alternative zu YouTube): https://odysee.com/
NewPipe (Private Oberfläche für YouTube – Android): https://newpipe.net/
Invidious (private Oberfläche für YouTube – Webseite): https://invidious.io/
Ri Music (Android-App für privates Musikstreamen): https://rimusic.xyz/
AntennaPod (private Podcast-App für Android): https://antennapod.org/de/
Nostr App (dezentrale Social-Media): https://primal.net/
JanAI (private und lokale KI): https://jan.ai/

DuckAI (private KI von DuckDuckGo): https://duck.ai/
VeniceAI (private, online KI; Alternative zu ChatGPT):
https://venice.ai/
PGP (Verschlüsselung und Verifizierung von Dateien/Texten):
https://www.gpg4win.org/ (Windows);
https://apps.kde.org/kleopatra/ (Linux);
https://gpgtools.org/ (MacOS)
MoneyManagerEx (privater Ausgabentracker):
https://moneymanagerex.org/
OpenStreetMaps (private Karten; Alternative zu Google Maps):
https://www.openstreetmap.org
OSM And~ (private Karten; Alternative zu Google Maps):
https://osmand.net/
Organic Maps (private Karten; Alternative zu Google Maps):
https://organicmaps.app/de/
Magic Earth (private Karten; Alternative zu Google Maps):
https://www.magicearth.com/

Kapitel 7 Unsichtbar werden

Anleitungen zum Account Löschen bei vielen Unternehmern:
https://backgroundchecks.org/justdeleteme/
OSINT (Suche von persönlichen Informationen):
https://osintframework.com/
Google-Account-Einstellungen: https://myaccount.google.com
Google-Daten exportieren und herunterladen:
https://takeout.google.com/
Google-Fotos exportieren und herunterladen:
https://photos.google.com/
Google-Drive-Daten exportieren und herunterladen:
https://drive.google.com/
Weitere Google-Daten exportieren und herunterladen:
https://about.google/products/#all-products
Google-Suchergebnisse entfernen:
https://search.google.com/search-console/remove-outdated-content
Bing Suchergebnisse entfernen:
https://www.microsoft.com/de-de/concern/bing
Databroker: https://privacyrights.org/data-brokers
Namensgenerator: https://randomwordgenerator.com/name.php

Bildgenerator: https://www.thispersondoesnotexist.com/
LinkdIn: https://www.linkedin.com/login
Carrd (Webseiten einfach erstellen): https://carrd.co/
Schufa Holding AG: www.schufa.de; datenschutz@schufa.de
Creditreform: www.creditreform.de; datenschutz@creditreform.de
Bürgel Wirtschaftsinformationen: www.buergel.de; datenschutz@buergel.de
Acxiom Deutschland GmbH: www.acxiom.de; datenschutz@acxiom.com

Kapitel 8 Zahlungen, Finanzen und Bitcoin

Komplette und ausführliche Bitcoin-Privacy-Anleitung: https://privatopia.de/bitcoin-privacy-guide
Bitcoin Einsteigerinformationen: https://bitcoinlighthouse.de/rabbithole/schritt-fuer-schritt-anleitung-zu-bitcoin/
Einsteigerartikel Bitcoin: https://bitcoinlighthouse.de/bitcoin-ganzheitlich-verstehen/
BlueWallet (Software Bitcoin Wallet): https://bluewallet.io/
BitBox02 Bitcoin Only (Hardware Bitcoin Hardware Wallet): https://bitbox.swiss/de/
Specter DIY (Fortgeschrittene Bitcoin Hardware Wallet): https://clavastack.com/specter-diy/
SeedSigner (Fortgeschrittene günstige Bitcoin Hardware Wallet): https://seedsigner.com/
Sparrow Wallet (Fortgeschrittene Wallet App): https://sparrowwallet.com
Peach-Bitcoin (Bitcoin privat kaufen – App): https://peachbitcoin.com/de/
RoboSats (Bitcoin privat kaufen über den Tor-Browser): https://robosats.org/docs/quick-start/
Bisq (Dezentrale Bitcoin Peer-to-Peer Börse): https://bisq.network/
HodlHodl (Bitcoin Peer-to-Peer Börse): https://hodlhodl.com/
Artikel – Bitcoin Node Raspberry Pi 5: https://privatopia.de/node
UmbrelOS (Anfänger-Betriebssystem für Bitcoin Node): https://github.com/getumbrel/umbrel
Start9OS (Fortgeschrittenes Betriebssystem für Bitcoin Node): https://docs.start9.com/latest/diy/

RaspiBlitz (Fortgeschrittenes Betriebssystem für Bitcoin Node): https://github.com/raspiblitz/raspiblitz
Mempool.space (Blockexplorer zum Nachverfolgen von Transaktionen): https://mempool.space/de/
Bitcoin CoinJoin:
https://www.whatisbitcoin.com/learn/what-is-coinjoin
Artikel – Der Kampf gegen Coinjoin und Privacy:
https://privatopia.de/samourai-wallet/
Artikel – Was ist das Liquid Netzwerk: https://liquid.net/
Artikel – Was ist das Lightning Netzwerk:
https://bitcoinlighthouse.de/bitcoin/lightning-network/
Boltz Exchange (Swaps zwischen verschiedenen Netzwerken): https://boltz.exchange/
Fixed Float (Swaps zwischen verschiedenen Netzwerken): https://ff.io/
Aqua Wallet (App für Swaps zwischen verschiedenen Netzwerken): https://aquawallet.io/
Shopinbit (Das „Amazon" mit Bitcoin als Bezahlmethode): https://shopinbit.com/de/
Bitcoin Maps (lokale Geschäfte und Anbieter, die Bitcoin akzeptieren): https://btcmaps.org
Bitrefill (Gutscheine kaufen und mit Bitcoin bezahlen): https://www.bitrefill.com/de/de/

Kapitel 9 Sicher und privat bleiben

Elster (schützt Steuerinformationen vor unbefugtem Zugriff): https://www.elster.de/
BundID (schützt vor Identitätsmissbrauch): https://www.bundid.de/
Onlinefunktion des Personalausweises (schützt vor Identitätsmissbrauch): https://www.personalausweisportal.de/
BAföG-Dienste und Sozialleistungen (verhindert betrügerische Anträge): https://www.bafög.de/; https://www.arbeitsagentur.de/
Deutsche Rentenversicherung (schützt Renteninformationen): https://www.deutsche-rentenversicherung.de/
Gesundheitswesen (schützt Gesundheitsdaten): https://www.gematik.de/
DHL Paketbox: https://www.dhl.de/

Fazit

Angebote für Beratungen: https://privatopia.de/angebote
Newsletter zu Privatsphäre: https://privatopia/newsletter
Lexikon mit Fachbegriffen: https://privatopia/wörterbuch

Quellen

(1) www.theguardian.com/technology/2010/jan/11/Facebook-privacy

(2) abcnews.go.com/Business/mark-zuckerberg-buys-homes-surrounding-palo-alto-calif/story?id=20542803

(3) psycnet.apa.org/record/1956-07332-001;
psycnet.apa.org/record/1963-07030-001;
psycnet.apa.org/record/1974-25314-001

(4) de.wikipedia.org/wiki/Panopticon;
www.ucl.ac.uk/bentham-project/about-jeremy-bentham/panopticon

(5) www.microsoft.com/en-us/privacy/data-collection-windows

(6) www.apple.com/apple-intelligence/;
time.com/6980911/microsoft-copilot-recall-ai-features-privacy-concerns/

(7) www.nzp.ch/studie-2020-das-jahr-der-online-kommunikation/

(8) www.forbes.com/sites/hollieslade/2014/05/19/the-only-email-system-the-nsa-cant-access/

(9) federal-lawyer.com/blocked-transactions-what-financial-institutions-need-to-know-about-ofac-compliance/; ofac.treasury.gov/faqs/topic/1601

(10) www.faz.net/aktuell/finanzen/banken-begrenzen-ausgabe-von-bargeld-wegen-hoher-nachfrage-16688789.html;
https://www.investopedia.com/terms/b/bank-deposits.asp

(11) https://www.investopedia.com/terms/m/mt-gox.asp

(12) https://www.investopedia.com/what-went-wrong-with-ftx-6828447

(13) foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/

(14) https://www.anwalt.de/rechtstipps/toyota-datenleck-was-kunden-jetzt-wissen-muessen-225258.html

Abbildungsverzeichnis

Abbildung 1 Panopticon 12
Abbildung 2 Privatsphäre oder Bequemlichkeit 16
Abbildung 3 Balena Etcher 29
Abbildung 4 Das Terminal 36
Abbildung 5 Terminal-Downloads 38
Abbildung 6 Terminal-Veracrypt-Installation 39
Abbildung 7 Bootemenü GrapheneOS 54
Abbildung 8 Schnelleinstellungen 58
Abbildung 9 GrapheneOS-Nutzer 59
Abbildung 10 Kamera- und Mikrofonblocker 72
Abbildung 11VPN 89
Abbildung 12 NextDNS Anfrage 94
Abbildung 13 FreeFileSync-Synchronisation 112
Abbildung 14 Kleopatra 161
Abbildung 15 Kleopatra Webseite 162
Abbildung 16 Kleopatra Verifikation 163
Abbildung 17 Bitcoin-Passphrasen 218
Abbildung 18 Bitcoin Coinjoin 227
Abbildung 19 Metadaten bei Fotos 242
Abbildung 20 Werbung unter dem Kennzeichen 255