Alexander Schreiner

DIE DIGITALE ENTMÜNDIGUNG

Daten, Vermögen, Selbstbestimmung.
Wie digitale ID, Big Tech und Banken sie dir nehmen –
und **47 Hacks**, sie zurückzuholen.

MIT VIDEO-ANLEITUNG



zeitfragen EDITION

Alexander Schreiner

DIE DIGITALE ENTMÜNDIGUNG

Daten, Vermögen, Selbstbestimmung.
Wie digitale ID, Big Tech und Banken sie dir nehmen –
und **47 Hacks**, sie zurückzuholen.

MIT VIDEO-ANLEITUNG



zeitfragen EDITION

Alexander Schreiner
DIE DIGITALE ENTMÜNDIGUNG
Daten, Vermögen, Selbstbestimmung. Wie digitale ID, Big Tech und Banken sie dir nehmen – und 47 Hacks, sie zurückzuholen.

Dieses Buch wurde auf FSC®-zertifiziertem Papier gedruckt. FSC® (Forest Stewardship Council®) ist eine nicht staatliche, gemeinnützige Organisation, die sich für eine ökologische und sozial verantwortliche Nutzung der Wälder unserer Erde einsetzt.

Die automatisierte Analyse des Werkes, um daraus Informationen insbesondere über Muster, Trends und Korrelationen gemäß §44b UrhG (Text und Data Mining) zu gewinnen, ist untersagt.

Die Verwendung des Werkes oder Teilen davon zum Training künstlicher Intelligenz-Technologie oder -Systeme ist untersagt.

Copyright dieser Ausgabe
© 2026 Edition Zeitfragen
Alle Rechte vorbehalten.

Dieses Werk einschließlich seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne schriftliche Zustimmung der Edition Zeitfragen unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen in andere Sprachen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronische Systeme.

Covergestaltung: Rouven Kroth
Lektorat: Anke Schenker
Satz und Herstellung: Robert B. Osten
Printed in Germany

1. Auflage 2026
ISBN 978-3-98584-422-7

Mehr Infos finden Sie im Internet unter
www.zeitfragen.de

Edition Zeitfragen · Neumann-Reichardt-Str. 27 · 22041 Hamburg · Germany
info@zeitfragen.de

Inhalt

Vorwort **9**

1| Die bessere Seite der Medaille 15

Die Logik verstehen und nutzen 18

2| Transparent, überwacht & kontrolliert: Das digitale Zeitalter **21**

3| Basis der Neuzeit: Die »digitale ID« in der EU 25

Der (vermeintliche) Nutzen 26

Funktionen: Was kann die digitale ID? 27

Die Ausweisfunktion 28

Speicherung von Bankdaten und digitaler Euro 28

Ausreisen via Identifizierungsverfahren 29

Zugangsvoraussetzung für den Jobmarkt 30

Zentrale Verifizierung für Plattformen und Co. 31

Für wen gilt die digitale ID – und für wen nicht? 32

Wie werden die Daten ausgewertet und kombiniert? 33

Ist die digitale ID ein globales Phänomen? 34

Gibt es rechtliche Konsequenzen, wenn du die digitale ID ablehnst? 35

4| Digitale Sicherheit: Schütze dich, deine Daten und deine Geräte 37

Einstieg: Diese Gefahren solltest du beseitigen 38

Grundlage: Deine Verbindungen schützen 39

Hack #1: Virtual Private Networks (VPNs) nutzen 39

Hack #2: Passwörter ändern 41

Hack #3: WPA2 oder (besser) WPA3 aktivieren 44

Mobile Geräte vor externen Zugriffen schützen 45
Hack #4: Remote Lock aktivieren 46
Hack #5: »Private Space« für Android-Geräte und alternative Cloudspeicher nutzen 48
Hack #6: Fremdzugriff per Kabel erschweren 49
Hack #7: Im Härtefall – Blockierungsmodus im iPhone 51
Dein wichtigster Schutz in sozialen Netzen 51
Hack #8: Die richtigen Messenger nutzen – inklusive optimaler Einstellungen 52
Hack #9: Eine komplett getrennte Online-Identität aufbauen 54
Hack #10: Die Kontoregistrierung besonders gut schützen 56
Hack #11: Niemals Standort- und Metadaten im Rohformat posten 57
Hack #12: Plattformen keinen Zugriff auf dein Adressbuch geben . 59
Private Daten optimal geschützt speichern 60
Hack #13: Richtige Back-ups, richtige Clouds 61
Hack #14: Diversifizierung – nicht alles an einem Ort speichern ... 63
Hack #15: Lockscreen-Vorschauen abschalten 64
Hack #16: Passwörter vom Rest des Telefons trennen 66
Hack #17: Die richtigen Messenger-Einstellungen wählen 68
Digitale Daten verschlüsseln und verschleiern 70
Hack #18: Daten im Ruhezustand verschlüsseln 71
Hack #19: Ende-zu-Ende-Verschlüsselung nutzen 72
Hack #20: Metadaten bedenken – und entsprechend handeln. 73
Hack #21: Weniger speichern, mehr erinnern. Auf allen Ebenen!... 74
Deine Gesundheitsdaten kontrollieren und sichern 75
Hack #22: Nicht alles tracken, nur weil es geht 76
Hack #23: »Medizinisch nötig« von »Wellness-Spielzeug« trennen 77
Hack #24: Die ePA nicht als »Alles-rein-Ablage« nutzen 78
Hack #25: Widerspruch ist ein Datenschutzwerkzeug, kein Tabu... 79
Hack #26: Regelmäßig exportieren und entrümpeln 80
Biometrische Daten vor Zugriffen schützen 81
Hack #27: Biometrische Daten zum Login nicht nutzen 82

Hack #28: App-Zugriffe auf Biometrie klein halten 83
Hack #29: Gesichtsscan nur dort, wo unumgänglich 84
Hack #30: Biometrische Daten nicht mit Identitätszwang verknüpfen lassen 84

Bisher geteilte Daten nachträglich löschen 85
Hack #31: Alte Konten wirklich schließen..... 86
Hack #32: Erst an der Quelle löschen..... 87
Hack #33: Lecks und Wiederauftauchen überwachen 88
Hack #34: Für Härtefälle: Eine formelle Löschanfrage nach DSGVO stellen..... 89
Hack #35: Dienste nutzen, die die Datenlöschung bernehmen 89

5| Digitale Souveränität meistern: Banken, Vermögen & Datenkontrolle 93

Die drei Hebel für digitale Souveränität 94

Internationale Banken kennen und nutzen 95
Hack #36: Den Common-Reporting-Standard verstehen & nutzen 96
Hack #37: Der richtige Mix aus Fintechs und Vollbanken 98
Hack #38: Unter dem Radar fliegen 99
Hack #39: Schatten-Scoring vermeiden..... 100

Dein Vermögen digital dezentralisieren: Bitcoin als einzige digitale Option 102
Hack #40: Bitcoin ohne KYC kaufen 103
Hack #41: Bitcoin außerhalb der EU kaufen 104

Edelmetalle und mehr: Warum du harte Wertspeicher bevorzugen solltest 105
Hack #42: Die richtigen Zollfreilager wählen..... 106
Hack #43: Edelmetalle anonym kaufen 107

Sichere Kommunikation und Datensicherheit herstellen 109
Hack #44: Die perfekten und privatesten E-Mail-Provider nutzen 110
Hack #45: Der richtige Umgang mit Newslettern & Co. 110

6| Digitale Freiheit: Dezentrale und digitale Lebensentwürfe entwickeln 113
Warum die »digitale ID« nicht so funktioniert, wie du denkst ... 113
Ist Auswandern die Lösung? 114
Hack #46 (Premium-Hack): Ortsungebunden leben 115
Digitale Wege nutzen, um ortsunabhängig Geld zu verdienen ... 119
Hack #47: Ortsunabhängig Geld verdienen 120
Wie du stets auf der »besseren« Seite der Medaille lebst 122

Schlusswort und Zukunftsaussichten 125

Vorwort

Alle Tiere sind gleich, doch manche Tiere sind gleicher. Ein Blick in unsere heutige Welt erinnert stark an George Orwells *Farm der Tiere*: Während sich der Großteil der Bevölkerung mit den Folgen der Pandemiejahre, mit Debatten über innere Sicherheit, der Einführung digitaler Verwaltung und einer eskalierenden geopolitischen Lage auseinandersetzt, bleiben die politisch Verantwortlichen selbst weitgehend unberührt. An den Schulen ihrer Kinder, in ihren Wohnvierteln, an ihren Lebensgewohnheiten ist von alldem wenig zu spüren.

Inzwischen jedoch scheinen wir an einem Kipppunkt angekommen zu sein: Die Bevölkerung spielt nicht mehr mit. Sie wählt nicht im Sinne des Systems, geht zuweilen sogar auf die Straße. Sie mutiert in Teilen zu einer Masse, die sich dem System nicht mehr fügt, was wiederum zu noch drastischeren Maßnahmen zu führen scheint.

Und so stellen sich jedem, der das aufmerksam beobachtet, früher oder später dieselben Fragen: Wie schützt man sich in Zeiten überbordender staatlicher Kontrolle? Was ist *wahre Freiheit*? Und wie wird sie uns allen genommen, ohne dass wir etwas davon merken?

Fragen, auf die kaum jemand eine ernst zu nehmende Antwort weiß. Zwar werden Schlagworte wie »digitale ID« und »Social Scoring« gern in den Raum geworfen und als grobe Konzepte umrissen, doch was genau auf uns – die *Bevölkerung* – zukommt, das kann wohl niemand exakt sagen.

Wie sollte man auch, wurden die Konzepte doch weitestgehend über die Köpfe derer hinweg ausgearbeitet, die sie fortan mit Leben – mit *ihrem* Leben – füllen sollen. Es scheint, als würden wir in einer Welt der totalen Hilflosigkeit und des endgültigen Ausgeliefertseins leben.

Oder etwa nicht?

Während diese Zeilen ihren Weg aufs Papier finden, beschließt die CDU auf ihrem Parteitag just die Altersverifizierung für die sozialen Medien. Ein Paradebeispiel für unser politisches Zeitalter. Das Narrativ klingt hervorragend. Jugendliche wolle man schützen: vor Fake News, vor sozialen Medien allgemein und ohnehin vor all dem »Bösen« da draußen, das es nicht gut mit »unserer Jugend« meint. »Unsere Jugend« ist dabei zu einer Art Argumentationsschablone geworden – ähnlich wirkungsvoll wie das Schlagwort vom Schutz der Demokratie.

Eins dürfte uns, dem *Volk*, in der Vergangenheit aufgefallen sein: Es beginnt immer im Kleinen. Auffällig ist ein wiederkehrendes Muster. Eine als besonders schutzbedürftig markierte Gruppe rückt ins Zentrum der politischen Kommunikation und wird zum Anlass genommen für Maßnahmen, die im Ergebnis die ganze Bevölkerung betreffen. So ließen sich in den letzten Jahren in verschiedenen Politikfeldern – von der Migrations- über die Gesundheits- bis hin zur Jugend- und Medienpolitik – ähnlich gebaute Argumentationen beobachten.

Den Preis für diese vermeintliche Wohltat zahlt dann die Bevölkerung als Ganzes. Lediglich die Argumentationskette bleibt bei jedem Szenario dieselbe: *Eine* sensible Gruppe bedarf nun unser *aller* Aufmerksamkeit und unseres Zusammenhalts. Deshalb sollten wir alle bereit sein, etwas zu tun, das uns zwar schadet, aber besagter *kleiner Gruppe* vermeintlich hilft.

Ob diese »Maßnahmen« wirklich Wirkung zeigen, darf natürlich stark bezweifelt werden. Doch der Preis wurde bis heute stets gezahlt: mit innerer Sicherheit, der eigenen Gesundheit und nun der eigenen Freiheit.

Denkt man das aktuellste Konstrukt des »Jugendschutzes« einmal zu Ende, so wird dem aufmerksamen Bürger schnell klar: Es handelt sich um ein simples Totschlagargument. Wer würde schon den *Kindern*, den Jüngsten der Gesellschaft, den von *Experten* als notwendig definierten Schutz absprechen? Natürlich nur jene, die sich *nicht* um sie sorgen. Die nicht – Achtung, Schlagwort – *solidarisch* sind.

Und schon ist sie geöffnet, die Büchse der Pandora. Auf Verifizierung via digitaler ID in sozialen Medien folgt die Chatkontrolle. Auf die Chatkontrolle folgt die digitale ID in den Schulen. Und wenn Zeugnisse und Sozialverhalten schon mal in einer digitalen Ablage liegen, kann man Letztere auch gleich verpflichtend für den Jobmarkt einführen. Immerhin ist es *bequemer.* Und natürlich sicherer. Für alle Beteiligten. Keine Betrügereien, keine Unwahrheiten mehr. Nichts dergleichen. Denn in unseren unsicheren Zeiten ist jeder Strohhalm, an den wir uns klammern können, ein Segen.

Und so wurde in wenigen Schritten eine gesamte Generation, inklusive jener, die folgen werden, an eine neue Ebene absoluter Kontrolle gewöhnt. Das *neue Normal* ist geboren. Oder um ein anderes Bild George Orwells zu bemühen: *Big Brother is watching you.* Aber paradoxerweise nicht gegen den Willen des Individuums, sondern auf expliziten Wunsch desselben. Und das, verehrter Leser, ist der Unterschied zu allen Dystopien der letzten Jahrzehnte:

Die Bevölkerung wird dem »System« nicht unterworfen, sie unterwirft sich ganz freiwillig. Denn es ist bequem, sicher und fordert vor allem nicht zum eigenen Denken auf. Kollektivismus

ersetzt Individualismus. Der *Big Brother* heißt nun ChatGPT, Religion wurde ersetzt durch »die Wissenschaft« und die stetige Überwachung wird (natürlich) nur zum Schutze von Minderheiten eingesetzt. Was früher als Pauschalverdacht oder kollektive Vorverurteilung kritisiert worden wäre, gilt heute zunehmend als legitimes Mittel der Plattformregulierung. Aber diese Widerstände schwinden zunehmend. Denn von Tag zu Tag gilt immer mehr: *Vorwärts immer, rückwärts nimmer.*[1]

Zugegeben, all das ist eine ziemlich düstere Analyse des Ist-Zustandes des »besten Deutschlands aller Zeiten«. Und dennoch: Sie trifft. Selten stand es in den letzten Jahrzehnten so bedrückend um die Freiheit der westlichen Zivilisation. Aber davon sollten wir uns nicht entmutigen lassen. Schließlich gibt es sie – *noch* –, die kritischen Stimmen. Jene, die sich nicht unterkriegen lassen. Die den Entzug der Freiheit nicht einfach so hinnehmen. Und mit nicht allzu geringer Wahrscheinlichkeit bist du, lieber Leser, einer davon. Darum möchte ich dich ermutigen, daran festzuhalten, dem, was wir als *Matrix*, *das System* oder anderswie bezeichnen, zu entkommen und den Kampf gegen Windmühlen weiterzuführen.

Denn am Ende ist vieles von dem, was gerade geschieht, nicht mehr als ein windiger Papiertiger. Nicht mehr als Maßnahmen eines Staates, einer Organisation, die aus den letzten Löchern pfeift und innerlich vor dem Kollaps steht. Die lediglich *probiert*, was eine Bevölkerung mitzumachen bereit ist, und so weit geht, wie es ihr möglich ist.

Repressionen dieser Art haben sich in der Historie der Menschheit selten langfristig durchgesetzt. Und dass es ausgerechnet *jetzt* so weit sein sollte, ist vor diesem Hintergrund doch eher unwahr-

1 Das war eine beliebte Losung Erich Honeckers, zuletzt verwendet in seiner Rede zum 40. Jahrestag der DDR 1989 – wenige Wochen vor dem Mauerfall.

scheinlich. Halten wir es schlicht mit Ernest Hemingway, der einst sagte: »Die Welt ist ein schöner Ort und wert, dass man für sie kämpft.« Und beginnen wir mit dem ersten Schritt in diesem Kampf: der Rückgewinnung unserer Freiheit.

Kapitel 1

Die bessere Seite der Medaille

Steigt man intensiver in das Thema »staatliche Kontrolle« und »digitaler Zwang« ein, wird dem geschulten Auge sehr schnell klar: All unsere heutigen »Waffen« können für und gegen beide Seiten verwendet werden. Doch beschränken sich jene *Waffen* längst nicht mehr nur auf den militärischen Bereich, sondern sie sind auch auf zahlreichen anderen Ebenen zu finden. Es stellt sich also die berechtigte Frage: Von welchen Waffen sprechen wir hier überhaupt? Und von welchen Seiten?

Ist das grundlegende Geheimnis erst einmal gelüftet, gestaltet es sich eigentlich erstaunlich simpel: Der Großteil der *Technologien*, die wir heutzutage nutzen, findet seinen Ursprung im amerikanischen (oder einem anderen staatlichen) Militärprogramm. Die Ableitung des Waffenbegriffs trifft hier also durchaus zu. Das Internet etwa entstand in den 1960er-Jahren als militärisches Forschungsprojekt der USA – bevor es für die breite Bevölkerung zugänglich gemacht wurde. Stets mit freundlichen »Pioniergesichtern« wie Mark Zuckerberg (Meta), Larry Page (Google) und Co. Niemand würde ein Militärprogramm in seinem Zuhause installieren, nicht wahr? Das tolle Tool eines sympathischen und pickligen Studienabbrechers der Harvard-Universität? Immer her damit. Das ist *Innovation*!

Ähnlich verhält es sich mit dem inzwischen auf allen Geräten nutzbaren GPS: Was wäre eine Welt, in der man nicht den eige-

nen Standort per WhatsApp an Freunde schicken könnte, weil sich Straßenschilder ja so schwer merken lassen und es einfach *bequemer* ist? Tatsächlich ist unser täglicher Begleiter, das GPS *(Global Positioning System)*, nicht mehr und nicht weniger als – genau! – eine Erfindung des amerikanischen Militärs. Die Idee dahinter: die militärischen Waffen per Satelliten präziser zu lenken, Schiffe und Flugzeuge ausfindig machen zu können und vieles mehr. Das klingt schon gar nicht mehr so freundlich, oder? Ein Schelm, wer da noch denkt, es wurde aus reiner Nächstenliebe und purem Innovationsgeist der Bevölkerung zugänglich gemacht.

Die Beispiele sind zahlreich und würden dieses Kapitel deutlich länger gestalten als nötig. Doch eine entscheidende Entwicklung »unserer Zeit« sollten wir noch beleuchten: die künstliche Intelligenz.

Während seit 2022 nichts mehr so zu sein scheint, wie es einst war – ChatGPT feierte zu dieser Zeit seinen endgültigen Durchbruch –, erlebte die künstliche Intelligenz schon Jahrzehnte früher ihre eigentliche Sternstunde. Bereits in den 1990er-Jahren, zu Zeiten des Golfkrieges, wurde vom US-amerikanischen Militär die künstliche Intelligenz »DART« *(Dynamic Analysis and Replanning Tool)* eingesetzt, mit einem praktischen Zweck: Binnen kürzester Zeit konnten nicht nur Ressourcen für eine effizientere Kriegsführung neu geplant und verteilt werden, sondern das gesamte Kriegsgeschehen konnte mithilfe der KI neu bewertet und somit komplett umstrukturiert werden. Man war der Gegenseite stets einen Schritt voraus. Das einzige Problem: Die dazu notwendigen Daten mussten händisch eingepflegt werden. In unserer heutigen schnelllebigen Welt eine absolut unlösbare Aufgabe. Halten wir also fest, dass es ein System war, das eine neuerliche Kriegslage geschickt planen

und organisieren konnte, sofern die *Dateneingabe* korrekt und optimal gepflegt wurde.

Und so springen wir ins Jahr 2022, in dem Sam Altman, ein absolut in seine Zeit passender und keineswegs bedrohlich wirkender Mann, aus einer vermeintlichen Non-Profit-Organisation das mächtigste Tool seiner Zeit schaffte, das genau dieses Problem zu lösen scheint: Anders als bei Suchmaschinen wie Google werden Daten nicht mehr zur Selbstorganisation aufbereitet, sondern auf Nachfrage auf dem Silbertablett serviert – dazu anregend, wiederum mehr persönliche Daten, Fragen und Co. einzutragen. Was im Anschluss mit deinen Daten passiert, kannst du dir selbst ausrechnen. OpenAIs größter wirtschaftlicher Anteilseigner ist inzwischen übrigens niemand Geringerer als Microsoft. Amazon, Nvidia und Co. sind inzwischen auch mit eingestiegen. Damit dürfte das Datenproblem weitestgehend gelöst sein, oder?

Wir bedienen also auch im Bereich der wohl größten Umwälzung unserer Zeit das übliche Klischee: Militärische Technologien finden den Weg in unseren Alltag, saugen sämtliche persönlichen Daten förmlich auf – und das wie gewohnt hinter freundlichen Gesichtern, die überhaupt nichts mit militärischen Komplexen zu tun zu haben scheinen. Wo wird uns das hinführen? Unser so »bequemer« digitaler Alltag ist nichts weiter als eine durch und durch militärisch geprägte Kontrollaktion einiger Weniger, die schlicht und ergreifend mit mehr Daten mehr Macht und somit mehr Kontrolle aufbauen können. So weit, so einfach – und so dystopisch.

Wo aber hat diese Situation etwas Positives? Wo ist die »bessere« Seite der Medaille?

Die Logik verstehen und nutzen

Vieles von dem, was wir heute nutzen, ist sogenannte »Open Source«-Technologie. Das bedeutet, dass theoretisch jeder den Code einsehen, ihn für eigene Zwecke adaptieren und davon profitieren kann. So entwickelten findige Köpfe Smartphones, Software und vieles mehr, die »sicherer« sind als die gängigen Standardversionen – obwohl die Basis derselbe Code bildet. Daraus lernen wir: Sobald du als Nutzer vom reinen Konsumenten zu einer Art »Produzent« wirst, veränderst du das Spiel. Sobald du beispielsweise in der Lage bist, deine Daten vollumfänglich zu schützen (und ja, das geht), steht dir der wahre *Nutzen* digitaler Technologien offen. Das gelingt aber nur, wenn du den Blick abwendest von den 08/15-Lösungen der heutigen Zeit hin zu hervorragenden Alternativen, die dich in eine besser geschützte Position bringen.

Und auch das sehen wir an Personen wie Zuckerberg und Co. Nutzen die ihre eigenen Technologien? Ja, natürlich. Aber in oftmals allzu offensichtlicher Abwandlung: Kameras und Mikrofone sind stets abgeklebt, privat geschützte WLAN-Netzwerke werden den öffentlichen vorgezogen. Sie nutzen nicht die Standard-Browser, und Passwörter werden nicht in billigen Passwort-Managern gespeichert. Das Telefon ist nicht zwingend das Neueste, sondern das Sicherste. Und die Kommunikation läuft über dezentrale Alternativen zu den vermeintlich tollen Messengern des Marktes.

Was übrig bleibt: Software und digitale Tools, die das Leben *wirklich* leichter machen, ohne die privatesten Daten gleich zu verschenken. Und genau das ist der Weg, den jeder von uns gehen sollte, um in einer digitalen Welt von Innovationen profitieren zu können, sich dabei aber nicht völlig offenbaren zu müssen. Das ist die *bessere* Seite der Medaille: Du nutzt das, was dir nützt. Du lässt

weg, was dich kontrollierbar macht. So gelingt es. Du musst lediglich wissen, *wie*. Entscheidend dabei ist, die Bequemlichkeit abzulegen.

Viele Schritte, die wir in den nächsten Kapiteln gemeinsam gehen, werden dir vielleicht komplex oder umständlich erscheinen. Dabei geht es lediglich darum, dein Gehirn wieder einzuschalten und aus dem Gewohnheitstrott auszusteigen. Schließlich ist das der Trick hinter all dem Datensammeln dieser Welt: Es ist bequemer, die *Rechte* an den eigenen Daten abzutreten, statt nach anderen Lösungen zu suchen.

Vielleicht wirst du auch deinem persönlichen Umfeld davon berichten und versuchen, es zu überzeugen, bei diesem großen Schritt mitzumachen. Nur zu! Je mehr Menschen *Nein* sagen und eigene Wege gehen, desto besser. Denn genau das ist es, was uns Tag für Tag abtrainiert wird – seinen Verstand zu benutzen und zu 100 Prozent darauf zu vertrauen. Gelingt dir dies jedoch, stehen die Chancen so gut wie nie zuvor.

Kapitel 2

Transparent, überwacht und kontrolliert: Das digitale Zeitalter

Beginnen wir ganz vorn, quasi beim digitalen »Adam und Eva«. Warum üben Staaten zunehmend Kontrolle aus? Wie funktioniert diese und welche Risikofaktoren (Smartphones, Smartwatches und Co.) gibt es? Und warum ist es überhaupt wichtig, deine Daten zu schützen?

Kontrolle scheint inzwischen zum Selbstzweck verkommen zu sein. Wer sie ausübt, ist in der Lage, seine Macht samt eigener Position zu sichern und davon zu profitieren. Jenes Muster also, das wir in der westlichen Welt zunehmend wahrnehmen. Und dennoch gibt es heute – wie auch in tiefster Vergangenheit – noch weitere Gründe, die eigene Bevölkerung aus Perspektive des Staates weitgehend zu kontrollieren: Religion, das Bewahren kultureller Traditionen und gewisser Werte, der Schutz des Reichtums, des Territoriums und so weiter und so fort. Es geht also darum, das Bestehende zu schützen. Zumindest im ursprünglichen Kern.

Viel spannender wird es, wenn wir uns ansehen, wozu Kontrolle bereits heutzutage intensiv eingesetzt wird: um *Meinung zu machen* und Meinungen zu verändern hinsichtlich vermeintlich erstrebenswerter Lebenswelten, Werte und Co., die auf natürlichem Wege niemals auf den gesellschaftlichen Plan geraten wären. Die aber vorhandene Strukturen und Lebensideale derart umwälzen kön-

nen, dass am Ende nichts mehr bleibt, wie es war – in etwa vergleichbar mit Christopher Nolans Film *Inception*, wo einer Zielperson ein Gedanke so tief eingepflanzt werden soll, dass sie ihn als den eigenen anerkennt, verteidigt und heranwachsen lässt, bis ein neues Ideal entstanden ist.

Mit dieser Form der *Kontrolle* haben wir es inzwischen überall zu tun. Durch gezieltes Tracking, Targeting und andere Technologien in deinem Smartphone, auf deiner Smartwatch und in anderen Geräten wirst du rund um die Uhr mit (auch auf dich abgestimmten) Inhalten bombardiert, die dich in eine bestimmte Gedankenwelt bringen sollen. Nicht nur durch die vermeintlich freie Privatwirtschaft, sondern zunehmend durch staatliche Organisationen und das dahinterliegende Reglement, das hier und da bestimmte Inhalte nicht zulässt und damit den Meinungskorridor künstlich verengt, ergo *Kontrolle* ausübt.

Wir halten fest: Staaten üben Kontrolle aus, um eigene Ziele zu erreichen. Dabei geht es nicht immer um den Staat, der dir deinen Reisepass ausgestellt hat. Auch andere Staaten oder elitäre Klassen nutzen ihre Einflusssphären, um dir im *Inception*-Stil neue Gedanken einzupflanzen – ohne dass du es merkst. Und um das noch besser zu beherrschen, benötigen sie genau eins: mehr Daten von dir, mehr Informationen. Denn Informationen sind der primäre Rohstoff für die Kontrolle der Zukunft.

Insbesondere *mobile* Geräte sind zunehmend ins Zentrum des Lebens gerückt. Und das natürlich nicht ohne Grund. Denn über diesen Weg ist nicht nur reine Informationskontrolle möglich, man erfährt außerdem noch, wo du dich gerade befindest; wie du dich dabei fühlst, wenn du in dein Gerät schreibst – auch wenn du etwas wieder löschst (ja, auch das geht) –, und ob du dabei eher nervös

oder gelassen bist. Und das sind nur ein paar Beispiele. Kurz: Die Nutznießer deiner Daten wissen mehr über dich als du selbst.

Die gute Nachricht ist, dass es bisher eher unwahrscheinlich ist, dass Staaten all diese Informationen kombiniert mit deinen offiziellen Ausweisdokumenten und Co. zentral auf einem Server gespeichert haben, den sie bei Bedarf anzapfen können, um dich in die Bredouille zu bringen. Wenn wir ehrlich sind, nutzt bislang vor allem die Privatwirtschaft, die diesen Namen kaum noch verdient[2], das Gros der Daten, um damit noch mehr Umsatz zu generieren und dich abhängig von ihren Produkten zu machen.

Die schlechte Nachricht ist jedoch: Zahlreiche Staaten sind auf dem Weg in genau das oben geschilderte Worst-Case-Szenario. Hin zum Sammeln, Auswerten und Katalogisieren deiner Daten. Man weiß ja nie. Gebündelt würde das dann, samt all deiner offiziellen Dokumente, in der *digitalen ID*. Und sobald dieser Mechanismus einmal in Gang gesetzt ist, lässt er sich kaum mehr aufhalten. Denn *sicher* sind diese digitalen ID-Ablagen keineswegs. Wie groß dieses Risiko ist, zeigt bereits heute der Blick nach Indien – dazu aber mehr im nächsten Kapitel. Ist dein Fingerabdruck erst einmal in der Welt, dann ist er in der Welt. Ändern wirst du das kaum mehr.

Spätestens an dieser Stelle merkst du sicherlich, dass es Zeit ist, dich zu schützen. Vor digitalen IDs, aber auch vor privatwirtschaftlicher Ausspähung durch verschiedenste Dienste, die du als »normaler« Verbraucher tagtäglich nutzt. Aber keine Sorge, genau damit befassen wir uns jetzt. Im nächsten Kapitel widmen wir uns der allem zugrunde liegenden digitalen ID und all den Features,

2 Durch die Marktmacht weniger Tech-Konzerne und deren wachsende Verflechtung mit staatlichen Projekten (z. B. Sam Altmans Iris-Scan-basiertes »World«-Projekt in Malaysia) kann von einer freien Privatwirtschaft kaum noch die Rede sein.

die dazugehören. Damit du erkennst, was genau geplant ist, welche Daten, Geräte und Co. schützenswert sind und wie du diesen Schutz Schritt für Schritt in die Tat umsetzt.

Begeben wir uns also mit einem kurzen Deep Dive in das Herzstück der digitalen Kontrolle und sorgen dafür, dass es dein Leben (vorerst) nicht weiter beeinflusst.

LESEPROBE

Sprung ins Buch

Kapitel 3 über die digitale ID in der EU lassen wir in dieser Leseprobe aus. Weiter geht es mit Kapitel 4 und den ersten drei der 47 Hacks: so schützt du dein WLAN und deine Verbindungen. Zu Hack 2 und 3 gibt es im Buch eine Videoanleitung per QR-Code.

Kapitel 4

Digitale Sicherheit: Schütze dich, deine Daten und deine Geräte

Es wirkt im ersten Moment schwer materialistisch, neben sich selbst und seinen Daten auch seine Geräte zu schützen. Immerhin sollten uns Letztere doch verhältnismäßig egal sein, wenn es um nicht weniger als um uns selbst und unsere Privatsphäre geht. Oder? Theoretisch korrekt. Allerdings sind all unsere Geräte nicht weniger als das größte Einfallstor zu uns selbst. Ein mobiles Gerät ohne ausreichenden Schutz wäre in etwa so, als hätte man im Mittelalter den Bergfried schützen wollen, ohne die Torhäuser bewachen zu lassen. Nicht sonderlich zielführend. Und genau deshalb fokussieren wir uns auf diese drei Ebenen:

- Zuerst definieren wir, *welche* Daten eigentlich schützenswert sind.
- Dann erörtern wir, wie wir sie schützen können und welche Medien, Geräte und Co. dabei eine Rolle spielen.
- Im Anschluss gehen wir auf den finalen Schutz deiner selbst und deinen realen Alltag ein.

Ein kurzer Hinweis, bevor wir einsteigen: Insgesamt werden wir uns durch 47 Strategien arbeiten, um der digitalen Matrix zu ent-

gehen – beginnend bei der digitalen Sicherheit, in diesem Kapitel und endend bei deiner digitalen Freiheit im letzten Kapitel.

Einstieg: Diese Gefahren solltest du beseitigen

Um die herannahende digitale Kontrolle optimal zu vermeiden, gilt es, nicht bloß der digitalen ID auf lokaler Ebene zu »entkommen« oder diese zu verweigern. Dieses Ziel erreichen wir insbesondere durch die Maßnahmen zur digitalen Souveränität und zur Freiheit. Es gilt vielmehr, dich samt deiner Daten und jener, die du *täglich* erzeugst, von vornherein zu schützen, damit in herannahenden Worst-Case-Szenarien so wenig wie möglich von deinen Daten extrahiert und missbraucht werden kann. Egal ob von Staaten oder »böswilligen« Dritten.

Damit dies gelingt, arbeiten wir im Folgenden an mehreren Ebenen, die ohne Schutzmaßnahmen die größte Angriffsfläche für Diebstahl und Missbrauch deiner Daten bieten. Dazu widmen wir uns dem Schutz deiner genutzten Netzwerke, mobilen Endgeräte, sozialen Medien, Privatsphäre-Einstellungen sowie deiner Gesundheitsdaten und bemühen uns um die geringstmögliche Streuung neuer digitaler Daten. Außerdem sehen wir uns an, wie du bereits geteilte Daten »zurückholen« und löschen kannst, und finden heraus, welche biometrischen Daten von dir bereits geteilt wurden und wie diese verwendet werden.

Was insgesamt unfassbar technisch versiert klingen mag, ist in Wahrheit kein Hexenwerk: All das gelingt uns auf anfängerfreundliche Weise, sodass du Schritt für Schritt mitarbeiten und dich umfangreich vorbereiten kannst.

Grundlage: Deine Verbindungen schützen

Ohne eine stetige Internetverbindung geht dieser Tage nichts mehr. Kein Essen würde geliefert werden, ohne dass man sich vom Sofa erheben müsste, kein Geldtransfer in Windeseile bereitgestellt. Fakt ist: Ohne ein Netzwerk, das uns die Verbindung zu den Geräten anderer Menschen oder Unternehmen ermöglicht, sind wir fast schon aufgeschmissen. Zumindest wenn die gesellschaftliche Teilhabe halbwegs erstrebenswert erscheint.

Dummerweise beginnt hier auch der größte Teil des Problems: Internet ist nicht gleich Internet – und jede Form der Verbindung birgt ganz eigene Tücken. Es macht eben doch einen Unterschied, ob du im klassischen WLAN bei dir zu Hause, im Hotel oder im persönlichen Hotspot deines Handys eingeloggt bist. Ohnehin wäre dann wieder zu unterscheiden zwischen mobiler Datenverbindung am Smartphone und öffentlichen Netzwerken, in die du dich beispielsweise innerhalb von Großstädten einloggst. Du merkst schon – es wird nicht weniger komplex. Doch keine Sorge, auch das lässt sich lösen. Immerhin haben wir ein simples Ziel: Wir möchten deine Verbindungen maximal effektiv schützen und Zugriffe von außen *jederzeit* – egal in welchem Netzwerk – vermeiden. Ob du nun deinen persönlichen Hotspot, mobile Datennetzwerke oder klassische WLAN-Netzwerke nutzt – im Folgenden findest du Hilfestellungen, um so sicher wie möglich im Netz zu surfen.

✓ Hack #1: Virtual Private Networks (VPNs) nutzen

Zur Vermeidung des Zugriffs durch Dritte auf deine Daten während des Surfens empfiehlt es sich grundsätzlich, ein sogenann-

tes *Virtual Private Network* einzusetzen. Dabei handelt es sich (in der Praxis) oftmals nur um eine simple App, die du auf deinem Smartphone, WLAN-Router oder Laptop installierst. Diese aktiviert eine »überbrückende« Netzwerkverbindung, die deine Datenübertragung dem eigentlichen Netzwerk gegenüber verschlüsselt. Das macht insbesondere in öffentlichen WLAN-Netzwerken Sinn, damit andere Nutzer desselben Netzwerks deinen Datenverkehr nicht einfach auslesen können.

Außerdem hat ein VPN auch noch einen anderen praktischen Vorteil: Befindest du dich etwa im Ausland und kannst aufgrund von digitalen Länderblockaden etwa deine Lieblingsserie nicht ansehen, kann ein VPN deinen Standort aus einem anderen Land simulieren, sodass der Bereitsteller der Inhalte annimmt, du befändest dich in einer Region, in der die gewünschten Inhalte verfügbar sind.

Ein VPN ist eine große Hilfe, wenn es um die direkte Datenverschlüsselung während des Surfens geht. Es ersetzt aber kein starkes Passwort bei einem WLAN-Netzwerk, gute Einstellungen deines WLAN-Routers oder teils notwendige Sicherheits-Updates. Zudem ist ein VPN natürlich auch nur so gut, wie sein Anbieter es aufbereitet. Ähnlich wie bei einem Auto: Fahren kann es in der Regel – doch sind einige schneller, effizienter, leiser oder besser gewartet als andere.

Welcher VPN-Anbieter ist empfehlenswert? Die Zahl an VPN-Anbietern steigt inzwischen ins Unermessliche. Um auf Nummer sicher zu gehen, solltest du als Einsteiger auf jene Anbieter zurückgreifen, die praxiserprobt *und* einfach genug zu bedienen sind. Besonders hervorzuheben sind hier *Surfshark* und *NordVPN*.

Letzteres ist die bekannteste Bastion im VPN-Markt, dominiert hier aber nicht umsonst.

Es ist völlig egal, für welche Option du dich entscheidest – die Aktivierung des virtuellen Netzwerks ist grundlegend dieselbe: Als Basis solltest du eine Form der Netzwerkverbindung (WLAN, mobile Daten) bereits aktiviert und somit Internetzugang haben. Anschließend lädst du dir die App aus dem App-Store o. Ä. herunter. Alternativ auch direkt von der Anbieter-Website, wenn du lieber am Laptop agierst. Im Anschluss daran erstellst du einen Account beim Anbieter. Hier kannst du oftmals auch per Kryptowährung oder ohne Angabe von Namen zahlen, was deine Account-Details angeht. Stelle sicher, dass du dazu eine Mail-Adresse nutzt, die nicht mit deinen privaten E-Mails verknüpft ist. Zu diesem Thema kommen wir später noch ausführlicher.

Einmal registriert und angemeldet, wählst du einen Serverstandort aus, den du simulieren möchtest. Wählst du zum Beispiel »Frankfurt« aus, simuliert das VPN der besuchten Website, dass du dich in Frankfurt aufhältst, und privatisiert zeitgleich deine Datenströme. Volle Privatsphäre also – egal, ob du im Browser surfst oder Apps nutzt.

✓ Hack #2: Passwörter ändern – inklusive jener, von denen du nichts weißt

Wenn du eigene Netzwerke wie WLANs oder persönliche Hotspots nutzt oder gar anbietest, solltest du auch diese vor äußeren Zugriffen schützen. Dazu sind zwei Dinge relevant:

1) Grundlegend sollte dir daran gelegen sein, das Netzwerkpasswort sicher zu gestalten. *Sicher* meint hier: mindestens zehn Zeichen, darunter Buchstaben in Groß- wie Kleinschreibung sowie Ziffern und Zeichen. Und idealerweise so aufgebaut, dass es nicht von dir nahestehenden Personen erraten werden kann. Heißt dein Sohn zum Beispiel Peter und ist am 01.06.2000 geboren, ist das Passwort *Peter2000* nicht sonderlich schwer zu erraten. Dir ist sicher klar, worauf das hinausläuft: Je komplexer das Passwort, desto besser. Zur Sicherung dessen kannst du entweder einen Passwortmanager nutzen, wobei auch hier etwas Vorsicht geboten ist (dazu kommen wir noch in aller Ausführlichkeit). Alternativ *merkst* du dir das Passwort einfach oder bewahrst es *offline* an einem sicheren Ort auf.

2) Dein WLAN-Router hat nicht nur ein, sondern zwei Passwörter. Das tatsächliche WLAN-Passwort, das du an deinem Endgerät einträgst, und ein Admin-Passwort, das dir Zugang zu den Router-Einstellungen gewährt. Letzteres vergisst die Mehrheit aller Router-Besitzer nur allzu gern, womit die womöglich größte Schwachstelle des Systems entsteht: Wer in den Besitz dieses Passworts kommt, kontrolliert im Handumdrehen das gesamte Netzwerk. Es wird mit dem Gerät oftmals als »admin« oder »0000« mitgeliefert – daher gilt: unbedingt ändern. Setze hier ein möglichst komplexes Passwort ein, das nicht jeder einfach so erraten kann. Sonderzeichen, Groß- und Kleinschreibung sowie Zahlen inklusive.

Ist dir das einmal gelungen, kannst du noch einen Schritt weiter gehen und für Gäste, die bei dir hin und wieder vorbeischauen, ein eigenes Gäste-Netzwerk einrichten. Ein komplett getrenntes

WLAN also: eigener Netzwerkname inklusive eigenem Passwort. Nutzbar nur für Besucher. Warum das sinnvoll ist, liegt auf der Hand: Deine Gäste können das Internet nutzen, aber nicht auf deine privaten Geräte im Netzwerk selbst zugreifen.

Wichtig dabei ist Folgendes: Auch smarte Geräte, wie etwa Alexa-Boxen, smarte Heimkameras etc., sollten ausschließlich über das Gäste-Netzwerk laufen. Immerhin sind gerade diese Gadgets sehr schwach abgesichert und können damit leicht gekapert werden. Verwendest du diese über ein Gästenetzwerk, ist schon viel gewonnen.

Darüber hinaus kann es sinnvoll sein, ein VPN auf WLAN-Routern zu installieren. Das gelingt über einen Download auf der Herstellerseite, ist aber um einiges komplexer als eine simple Aktivierung auf dem Smartphone (die im Falle eines persönlichen Hotspots das gesamte Netzwerk bereits abdeckt). An dieser Stelle gehen wir nicht tiefer auf die WLAN-Installation ein, dennoch sei sie als wichtiger Sicherheitsfaktor genannt.

Entscheidend ist, dass du dein Passwort – egal ob im WLAN oder Hotspot – in (un)regelmäßigen Abständen änderst. So gelangen in der Vergangenheit eingeloggte Geräte nicht ohne Weiteres wieder ins Netzwerk, falls du das nicht wünschst. Als empfehlenswerter Zeitraum sei hier einmal der Rahmen von vier Wochen angegeben. Wenn du also monatlich deine Passwörter änderst, hast du langwierige Netzwerkangriffe um einiges unwahrscheinlicher gemacht.

✓ Hack #3: WPA2 oder (besser) WPA3 aktivieren

Vielleicht fragst du dich beim Lesen dieses Hacks: »Bitte was genau soll ich tun? Das ist viel zu technisch für mich!« Und ja, genau so klingt es im ersten Moment. Dennoch ist es erstens wichtig und zweitens gar nicht so komplex, wie es scheint.

Gehen wir einmal ins Detail: *WPA2* und *WPA3* sind Sicherheitstechnologien, um den Datenverkehr im WLAN zu verschlüsseln. Bei Aktivierung wird es für Fremde schwerer, Daten mit- oder auszulesen oder sich ohne Erlaubnis ins Netzwerk einzuloggen. Bei privaten Netzwerken ist das inzwischen gängiger Standard. Bei öffentlichen Netzwerken werden leider oftmals veraltete Standards wie WEP verwendet, was die Sicherheit rapide herabsetzt.

Wie genau unterscheiden sich aber WPA2 und WPA3? Nicht großartig. Während WPA2 bereits einen hohen Sicherheitsstandard bietet, ist WPA3 mit einem erweiterten Schutz gegen Brute-Force-Angriffe und Co. einen Schritt voraus. Für den alltäglichen Gebrauch ist es aber absolut akzeptabel, solange einer der beiden Standards aktiviert ist.

Für dich ist an dieser Stelle relevant, einmal dein heimisches WLAN zu überprüfen: Rufe dafür dein Router-Menü auf, die URL dazu steht zumeist am Gerät selbst. Im Bereich »WLAN« oder »Wi-Fi« solltest du eine Option mit dem Titel »Sicherheit« oder »Verschlüsselung« finden. Öffne diese und wähle als Sicherheitsstandard dort mindestens WPA2-PSK aus. Sollte eine WPA3-Option vorhanden sein, wähle diese. Speichere die Änderungen und starte den Router neu. Prüfe im Anschluss, ob sich deine alten Geräte noch verbinden, oder verbinde sie falls nötig neu.

Damit solltest du deine Netzwerkeinstellungen optimal aktualisiert haben und kannst mit dem Einsatz von VPNs, neuen Passwörtern und mindestens WPA2 sicherer surfen denn je.

Mobile Geräte vor externen Zugriffen schützen

Ist deine Verbindung einmal gesichert, hast du bereits einen entscheidenden Schritt in Sachen *digitaler Sicherheit* getan. Weit mehr als die meisten Nutzer des World Wide Web. Du kannst dir aber vermutlich denken, dass es damit längst nicht getan ist. Die Verbindung mag zwar sicher sein, aber deine mobilen Geräte bieten noch genug Einfallstore, um deine Daten und vieles mehr zu gefährden. Daher begeben wir uns nun auf die nächste Ebene: deine mobilen Endgeräte, damit verbundene Apps und anderweitige Software.

Grundlegend solltest du verstehen, dass mobile Geräte – unabhängig von geschützter Verbindung – stets geortet werden können. Auch das Abrufen vermeintlich privater Daten auf staatliche Anweisung hin ist im Worst Case möglich. Zwar hat sich Apple als Hersteller hier in der Vergangenheit oftmals erfolgreich geweigert, um die Privatsphäre seiner Kunden zu wahren. Allerdings solltest du dich auf eine Fortsetzung dessen nicht zwingend verlassen.

Link zum Video: https://nomadmaster.de/router-absichern

ENDE DER LESEPROBE

Weiterlesen?

Die digitale Entmündigung · 128 Seiten · handsigniert direkt beim Verlag

Jetzt direkt beim Verlag bestellen