Holger Reibold

Code or die

Warum wir mehr Hacker brauchen

BRAIN-MEDIA.DE

Holger Reibold

Code or die

Warum wir mehr Hacker brauchen

BRAIN-MEDIA.DE

ISBN: 978-3-95444-316-1

Cover: Freepik

Druck: Libri Plueros GmbH, Friedensallee 273, 22763 Hamburg

Brain-Media.de – St. Johanner Str. 41-43 – 66111 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

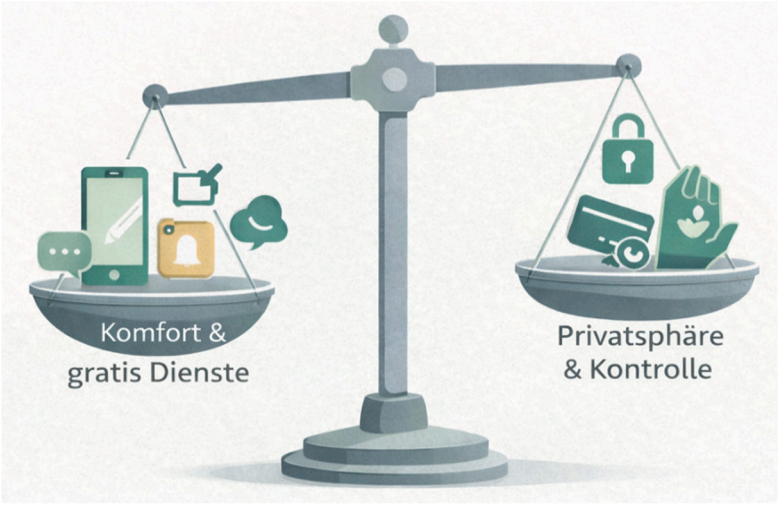
Prolog

Die Digitalisierung hat unseren Alltag tiefgreifend verändert. Viele Menschen in meinem Umfeld sind rund um die Uhr vernetzt, steuern ihren Tagesablauf per App und verlassen sich selbstverständlich auf digitale Helfer. Wer, wie ich, nicht jede Funktion des Smartphones nutzt, gilt schnell als eigenwillig oder gar rückständig. Es ist zur Ausnahme geworden, einmal nicht erreichbar zu sein. Ein Beispiel: Ich hatte kürzlich keinen Zutrittscode zur Sportanlage zur Hand – das Handy lag zuhause. Die Folge: Ich musste einen Menschen suchen, um Zugang zu bekommen. Auch der Getränkeautomat ließ sich ohne digitales Endgerät nicht bedienen. Solche Alltagssituationen zeigen: Wer offline ist, ist zunehmend außen vor. Die Teilhabe an ganz banalen Prozessen des Lebens wird zunehmend an technische Verfügbarkeit gekoppelt.

Dabei ist gegen Digitalisierung grundsätzlich nichts einzuwenden – im Gegenteil: Technik kann den Alltag enorm erleichtern. Ich bin ein Freund des Fortschritts und nutze digitale Dienste seit den frühen 1990er-Jahren. Was mir jedoch Sorge bereitet, ist die zunehmende Abhängigkeit: von Plattformen, von Geräten, von digitalen Ökosystemen, die wir kaum noch durchdringen.

Wir geben im Tausch gegen Bequemlichkeit unsere Souveränität auf – oft, ohne es zu merken. Bezahlt wird nicht mehr nur mit Geld, sondern mit Daten. Mit Bewegungsprofilen, Vorlieben, sozialen Beziehungen und biometrischen Merkmalen. Wir liefern diese Daten bereitwillig ab –

in der Annahme, dass es „praktisch“ sei. Nur wenige wissen, was mit diesen Informationen geschieht. Noch weniger können es beurteilen. Digitale Dienste versprechen Bequemlichkeit – und sie halten dieses Versprechen. Doch selten fragen wir, womit wir tatsächlich bezahlen. Die folgende Abbildung zeigt dieses Ungleichgewicht.



Die digitale Waage – Bequemlichkeit versus Freiheit: Die Abbildung visualisiert den zentralen Zielkonflikt der digitalen Gegenwart. Auf der einen Seite stehen Komfort und scheinbar kostenlose Dienste, auf der anderen Privatsphäre, Kontrolle und Selbstbestimmung. Jede Gratis-App verschiebt das Gleichgewicht – oft unbemerkt, aber mit langfristigen Folgen.

Die meisten Nutzer verwechseln digitale Routine mit technischer Kompetenz. Sie bedienen Systeme, ohne sie zu verstehen. Das ist vergleichbar mit jemandem, der ein Auto fährt, aber keine Vorstellung davon hat,

was sich unter der Motorhaube abspielt. Das mag im analogen Bereich noch akzeptabel sein – im digitalen Raum ist es gefährlich.

Denn digitale Systeme sind nicht neutral. Sie sind Ausdruck von Macht. Wer die Architektur eines Systems nicht kennt, kann weder seine Grenzen einschätzen noch sich vor seinen Risiken schützen. Noch dramatischer: Wer keine Kontrolle über seine digitale Umwelt hat, wird selbst zum Produkt. Das gilt für Einzelpersonen ebenso wie für staatliche Institutionen.

Ein besonders eindrucksvolles Beispiel ist der Fall, bei dem der Zugang zu einem internationalen Gerichtshof auf Anweisung eines Politikers über einen US-Digitalkonzern unterbunden wurde. Es zeigt, wie verwundbar öffentliche Institutionen sein können, wenn sie sich vollständig in die Hände proprietärer Systeme begeben. Dass über 90 % deutscher Behörden mit Software eines einzigen Anbieters arbeiten, ist unter Sicherheitsaspekten schwer nachvollziehbar – und unter demokratischen Gesichtspunkten hoch problematisch.

Digitale Resilienz – also die Fähigkeit, digitale Systeme zu verstehen, zu gestalten und zu hinterfragen – muss deshalb zu einer gesamtgesellschaftlichen Kompetenz werden. Wir brauchen ein Bildungssystem, das nicht nur Anwendung, sondern Systemverständnis vermittelt. Wir brauchen Hardware, die nicht abgeschottet, sondern reparier- und modifizierbar ist. Wir brauchen digitale Infrastrukturen, die dem Gemeinwohl dienen, nicht den Interessen einzelner Konzerne.

Kurz gesagt: Wir brauchen mehr digitale Mündigkeit. Und dafür brauchen wir mehr Menschen, die denken wie Hacker – im besten Sinne:

neugierig, verantwortungsvoll und gestaltend. Dieses Buch ist ein Plädoyer für genau diesen Weg. Es geht um digitale Selbstbestimmung – und um die sieben konkreten Forderungen, die dafür den Rahmen setzen:

- Recht auf Reparatur und Modifikation (Open Hardware)
- Hackergeist als Bildungsprinzip – statt Bedienkompetenz
- Public Money? Public Code! – Transparente öffentliche Software
- Schutz für Sicherheitsforschung – Hacker dürfen keine Kriminellen sein
- Interoperabilität als Bürgerrecht – keine Plattform-Monopole mehr
- Gemeinwohlorientierte Infrastruktur statt reinem Marktdenken
- Transparenzpflicht für Algorithmen – keine Blackbox-Entscheidungen

Diese Forderungen sind keine Idealvorstellungen, sondern notwendige Voraussetzungen für eine resiliente, demokratische digitale Gesellschaft.

In diesem Sinne wünsche ich mir, dass mehr Menschen Sinn und Zweck der Digitalisierung hinterfragen – gerade auch die Interessen der verschiedenen Akteure.

Holger Reibold

PS: Mein „Zutrittsproblem“ im Sportcenter hat sich leicht lösen lassen. Der Anbieter verschickt seit Jahren denselben Zahlencode. Als zahlenaffiner Mensch konnte ich ihn mir einfach merken. Auch den Getränkeautomaten habe ich seither nicht mehr gebraucht – ich bin vorbereitet.

PPS: Sollten Sie beim Lesen dieses Buchs über Begriffe stolpern, die nach Science-Fiction klingen: Werfen Sie einen Blick in das „Glossar der Dinosaurier“ am Ende des Buches. Dort übersetze ich Nerd-Sprech in gesundem Menschenverstand.

Einleitung – Hacker, Helden oder Feinde?

Die Digitalisierung ist weit in unsere Lebenswelten vorgedrungen. Vom Einkauf über die Kommunikation bis zur Bildung und zum Gesundheitswesen – digitale Systeme sind heute in vielen Fällen nicht mehr nur Ergänzung, sondern Voraussetzung für gesellschaftliche Teilhabe. Doch während die technischen Möglichkeiten enorm gewachsen sind, ist das Wissen über die dahinterliegenden Strukturen oft erschreckend gering.

Im alltäglichen Umgang mit digitalen Technologien beobachten wir eine paradoxe Entwicklung: Die Nutzung wird immer intuitiver, die Abhängigkeit immer größer – und das Verständnis immer kleiner. Viele Menschen empfinden sich als technikkompetent, weil sie mit Apps umgehen oder Passwörter verwalten können. Doch wie Daten gespeichert, verarbeitet oder übertragen werden, bleibt den meisten verborgen. Fragen nach Verschlüsselung, Authentifizierung, Netzprotokollen oder Algorithmen spielen im Alltag kaum eine Rolle – obwohl sie unseren Alltag längst strukturieren.

Das zuvor skizzierte Zutrittsproblem zeigt: Was wie eine banale Alltagsepisode erscheint, steht exemplarisch für eine Gesellschaft, in der technische Infrastruktur zur stillschweigenden Zugangsvoraussetzung geworden ist. Wer die Systeme nicht bedienen oder verstehen kann – sei es aus Alter, Armut, Vorsicht oder bewusster Entscheidung – läuft Gefahr, ausgeschlossen zu werden.

Diese Entwicklung stellt grundlegende Fragen: Wie souverän sind wir im digitalen Raum? Wer kontrolliert die Technologien, die wir täglich nutzen? Und wer gestaltet ihre Regeln?

In diesem Buch geht es um genau diese Fragen. Und es geht um eine gesellschaftliche Figur, die allzu oft missverstanden wird: den Hacker.

Der Begriff Hacker ist in der öffentlichen Wahrnehmung häufig negativ konnotiert. In den Medien ist er meist mit Cyberkriminalität, Datendiebstahl oder Angriffszenarien verknüpft. Wer sich mit Sicherheitslücken beschäftigt, wird schnell unter Generalverdacht gestellt – als potenzielle Bedrohung statt als potenzieller Problemlöser. Dabei ist der Ursprung des Hackertums ein anderer: Neugier, Kreativität und ein tiefes Interesse an der Funktionsweise technischer Systeme.

Ein Hacker im ursprünglichen Sinne ist kein Krimineller, sondern ein Mensch, der Systeme hinterfragt, ihre Strukturen verstehen will und daran interessiert ist, sie zu verbessern. Er oder sie arbeitet mit Leidenschaft daran, Technik nicht nur zu nutzen, sondern zu durchdringen. Diese Haltung hat nichts mit Vandalismus zu tun, sondern mit einem Bildungs- und Erkenntnisideal, das in vielen gesellschaftlichen Bereichen verloren gegangen ist.

Schon in den 1980er Jahren beschrieb Steven Levy in seinem Buch „Hackers: Heroes of the Computer Revolution“ eine Generation von Menschen, die aus reiner Begeisterung für Technologie neue Wege entwickelten, Software schufen, Netzwerke aufbauten und den Grundstein für das legten, was heute als digitale Infrastruktur gilt. Diese Pioniere handelten nicht im Auftrag großer Unternehmen oder Behörden,

sondern aus intrinsischer Motivation – und mit einem Ethos, das auf Offenheit, Teilen und Lernen beruhte.

Die sogenannte Hackerethik, wie sie in der Tradition des MIT, des Chaos Computer Clubs oder von Persönlichkeiten wie Linus Torvalds und Richard Stallman geprägt wurde, steht für Prinzipien wie freien Zugang zu Information, kritisches Hinterfragen von Autorität, Vertrauen in dezentrale Strukturen und eine hohe Wertschätzung von Wissensweitergabe. Es geht um eine Kultur der Selbstermächtigung – und um den Glauben daran, dass Technologie dem Menschen dienen soll, nicht umgekehrt.

Heute, im Zeitalter algorithmischer Entscheidungssysteme, proprietärer Plattformen und intransparenter künstlicher Intelligenz, ist diese Haltung aktueller denn je. Denn viele digitale Systeme entziehen sich demokratischer Kontrolle. Software entscheidet über Kredite, Bewerbungen, Versicherungen oder soziale Leistungen – oft, ohne dass nachvollzogen werden kann, wie diese Entscheidungen zustande kommen. Daten werden massenhaft gesammelt, verarbeitet und verkauft, ohne dass Betroffene wissen, was genau über sie gespeichert ist oder welche Schlüsse daraus gezogen werden.

Die Folge ist ein Zustand, den der Medienkritiker Neil Postman bereits 1985 in seinem Buch „Wir amüsieren uns zu Tode“ beschrieben hat – wenn auch noch bezogen auf das Fernsehen. Seine These: Eine Gesellschaft, die Information nur noch konsumiert, statt sie kritisch zu hinterfragen, verliert ihre Fähigkeit zur Selbstbestimmung. Unterhaltung ersetzt Erkenntnis, Reaktion ersetzt Reflexion. Übertragen auf die digitale

Gegenwart bedeutet das: Wer sich auf Systeme verlässt, die man nicht versteht, gibt seine Freiheit auf – und merkt es womöglich nicht einmal.

In einer solchen Welt ist technisches Verständnis keine Spielerei mehr, sondern eine Frage der Mündigkeit. Wer nicht versteht, wie digitale Systeme funktionieren, ist ihnen ausgeliefert. Wer nicht hinterfragt, welche Interessen in Software eingeschrieben sind, läuft Gefahr, manipuliert zu werden. Und wer die Technik nicht hinterfragen kann, weil sie als Blackbox präsentiert wird, gibt seine Gestaltungsfreiheit auf.

An diesem Punkt wird deutlich, warum Hacker – im ursprünglichen, positiven Sinn – so wichtig sind. Sie verkörpern das Gegenteil von technischer Passivität. Sie sind weder Konsumenten noch blinde Nutzer, sondern aktive Gestalter. Sie decken Schwachstellen auf, entwickeln Alternativen zu kommerziellen Systemen, bauen dezentrale Netzwerke und zeigen, wie Machtstrukturen in der digitalen Welt funktionieren. Sie machen sichtbar, was verborgen ist – und damit oft erst verhandelbar.

Gleichzeitig wird ihr Beitrag zur Gesellschaft zu selten anerkannt. Statt Schutz und Förderung erwartet viele ethische Hacker Unsicherheit und Kriminalisierung. Das Strafrecht hält bis heute Paragraphen bereit, die zwischen verantwortungsbewusster Sicherheitsforschung und tatsächlicher Sabotage kaum unterscheiden. Viele Hacker berichten von Einschüchterung, Missverständnissen oder sogar rechtlichen Konsequenzen – obwohl sie im Interesse der Öffentlichkeit handeln.

Dieses Buch ist ein Plädoyer, den Begriff des Hackers neu zu denken – und ihn dort zurückzuholen, wo er ursprünglich herkam: Aus der Mitte einer technikinteressierten, neugierigen, verantwortungsvollen

Community, die ihre Fähigkeiten nutzt, um digitale Systeme besser, sicherer und gerechter zu machen. Es ist ein Aufruf, Technik wieder als gestaltbares Feld zu begreifen – und nicht als alternativlose Dienstleistung. Es ist eine Einladung, sich selbst als Teil dieser Entwicklung zu verstehen – egal, ob man Programmierkenntnisse hat oder nicht. Denn die Haltung des Hackers ist nicht auf den IT-Bereich beschränkt. Sie kann auch in Bildung, Verwaltung, Gesundheit, Kultur oder Politik ihren Ausdruck finden.

Im weiteren Verlauf dieses Buches geht es daher nicht nur um technische Fragen, sondern um gesellschaftliche. Es geht um Bildung, um Ethik, um Infrastruktur, um Transparenz und um Gemeinwohl. Es geht um die Frage, wie wir mit Technik leben wollen – und wer dabei das Sagen hat. Die Hackerethik liefert dafür wichtige Impulse. Doch damit sie wirksam werden kann, braucht es mehr als nur einzelne Experten.

Was wir brauchen, ist eine Gesellschaft, die sich nicht auf die Rolle der Anwenderin oder des Nutzers beschränkt. Wir brauchen mehr digitale Selbstverteidigung, mehr Eigenverantwortung – und mehr Menschen, die den Mut haben, den Code zu lesen, der ihre Zukunft bestimmt.

1 Die Hackerethik

Wenn in der öffentlichen Debatte über Hacker gesprochen wird, fällt das Wort Ethik selten – und wenn doch, dann meist im Zusammenhang mit Sicherheitslücken, Datenschutzverletzungen oder Cyberangriffen. Doch wer sich ernsthaft mit der Geschichte und Kultur des Hackens beschäftigt, stößt schnell auf einen völlig anderen Zugang: Hacker als Menschen mit Haltung. Mit einem eigenen Wertekanon, der tief in der digitalen Aufklärung verwurzelt ist. Einer Ethik, die sich nicht in Paragrafen pressen lässt, sondern aus einem Weltbild heraus entsteht: Technologie gehört allen – und Wissen muss frei sein.

Die Hackerethik ist kein Gesetzeskatalog, sondern eine Denkweise. Sie ist nicht dogmatisch, sondern offen – und sie ist nicht destruktiv, sondern schöpferisch. Sie entstand in den 1960er-Jahren am MIT, wuchs mit der frühen Netzbewegung, wurde durch Gruppen wie den Chaos Computer Club geprägt und lebt heute in vielfältiger Form weiter: in Open-Source-Projekten, in der Netzpolitik, in Bildung, Forschung, Datenschutz und dezentralen Infrastrukturen. Sie ist kein Relikt, sondern aktueller denn je.

Denn in einer Welt, die von Intransparenz, Monopolen und geschlossenen Plattformen geprägt ist, stellt die Hackerethik einen Gegenpol dar: Sie fordert Offenheit statt Kontrolle, Neugier statt Gehorsam, Teilhabe statt Konsum. Sie verteidigt die Idee, dass Menschen nicht passiv

bleiben müssen im Umgang mit Technik, sondern sie aktiv gestalten können – und sollen.

Dabei ist ein Hacker im Sinne dieser Ethik nicht zwingend ein Programmierer. Hacken ist keine Frage des Berufs, sondern der Haltung. Wer komplexe Systeme verstehen, hinterfragen, auseinandernehmen und neu zusammensetzen will – sei es Software, eine Behörde oder ein Lehrplan – handelt im Geiste der Hackerethik.

In diesem Kapitel geht es darum, was diese Ethik ausmacht. Woher sie kommt. Wie sie sich entwickelt hat. Warum sie falsch verstanden wird – und warum wir sie gerade heute dringend brauchen. Es geht um Neugier, Verantwortung, Kreativität – und um die Frage, warum ausgerechnet eine als subversiv verschriene Subkultur Antworten auf einige der drängendsten Fragen der digitalen Gesellschaft liefert.

1.1 Der Ursprung der Hackerethik

Die Wurzeln der Hackerethik reichen zurück in eine Zeit, in der Computer noch raumfüllende Maschinen waren, die nur wenigen zugänglich waren – Universitäten, Forschungseinrichtungen und Militärs. Inmitten dieser technokratisch organisierten Welt entstand in den 1960er-Jahren eine Subkultur, die Technik nicht als Mittel zur Kontrolle verstand, sondern als Spielfeld, als Möglichkeitsraum. Ihre Vertreter nannte man Hacker. Sie wollten nicht bloß bedienen, sondern verstehen. Und was sie verstanden hatten, wollten sie teilen.

Der erste kulturelle Nährboden für diese Bewegung war das Massachusetts Institute of Technology (MIT) in Cambridge. Im legendären „Tech Model Railroad Club“, einem Verein für elektrische Modelleisenbahnen, fanden sich junge Technikbegeisterte zusammen, die zunehmend weniger an Zügen und mehr an den dahinterliegenden Schaltungen interessiert waren. Bald entdeckten einige von ihnen den Zugang zu einem damals neuen Gerät: dem PDP-1, einem interaktiven Minicomputer. Was folgte, war eine kleine Revolution – nicht auf der Straße, sondern in Bits und Bytes. Die frühen MIT-Hacker arbeiteten in der Nacht, um Rechnerzeit zu bekommen. Sie lernten durch Ausprobieren, durch Zerlegen, durch Umdeuten. Für sie war der Computer kein Arbeitsgerät, sondern ein offenes System – und Programmieren kein Handwerk, sondern Ausdruck von Kreativität.

1.1.1 Die Prinzipien der Hackerethik am MIT

Was in dieser Umgebung entstand, war mehr als bloß ein Hobby: Es war eine neue Haltung gegenüber Technologie. Die wichtigsten Grundprinzipien dieser Hackerethik lassen sich bereits im Verhalten der MIT-Studenten erkennen – auch wenn sie damals noch nicht schriftlich fixiert waren:

- Zugang zu Computern – und allem, was einem helfen könnte, die Welt zu verstehen – sollte unbegrenzt und vollständig sein.
- Alle Informationen müssen frei sein.
- Misstraue Autoritäten – fördere Dezentralisierung.

- Beurteile Hacker nach ihren Taten, nicht nach ihrer Herkunft, ihren Abschlüssen oder Titeln.
- Man kann mit einem Computer Kunst und Schönheit schaffen.
- Computer können das Leben verbessern.

Diese Regeln stammen nicht aus einem Manifest, sondern aus gelebter Praxis. Erst viele Jahre später, in den 1980er-Jahren, wurden sie durch den US-Journalisten Steven Levy in seinem Buch „Hackers: Heroes of the Computer Revolution" zusammengetragen und als Hackerethik formuliert. Damit wurden sie erstmals in die Öffentlichkeit getragen – als ethisches Fundament einer wachsenden digitalen Bewegung.

1.1.2 Der Chaos Computer Club: Hackerethik in Europa

Während die Hackerbewegung in den USA durch das MIT und kalifornische Tech-Kreise geprägt war, entwickelte sich in Deutschland eine eigenständige Kultur: der Chaos Computer Club. Gegründet 1981 von Wau Holland und Gleichgesinnten, verstand sich der CCC von Beginn an nicht nur als Technikkollektiv, sondern als politisch denkender Akteur. Sein Ziel war es, Technik zu verstehen – und öffentlich zu hinterfragen.

Bereits in den ersten Jahren machte der CCC mit spektakulären Aktionen auf sich aufmerksam. 1984 sorgte der sogenannte BTX-Hack für bundesweite Aufmerksamkeit: CCC-Mitglieder hatten über eine Sicherheitslücke im Bildschirmtext-System der Deutschen Post 135.000 D-

Mark von der Hamburger Sparkasse auf ein CCC-Konto transferiert – um die Schwachstelle öffentlich zu demonstrieren. Das Geld wurde sofort zurückgegeben. Doch die Aktion zeigte: Hacker decken auf, was Behörden und Konzerne gerne verschweigen.

Die Ethik des CCC war klar formuliert – und deutlich unterscheidbar von kriminellen Motiven. Hacker wollten keine Systeme zerstören, sondern verbessern. Sie verstanden sich als digitale Aufklärer, nicht als Saboteure. Der CCC veröffentlichte Artikel, Programme, sogar eine eigene Hackerbibel. Man traf sich auf Kongressen, diskutierte offen über Technik und Gesellschaft und warnte früh vor Überwachung, unsicheren Systemen und der Macht großer Technologiekonzerne.

Der CCC war – und ist – keine Organisation im klassischen Sinne, sondern eine Bewegung mit Haltung. Zu seinen zentralen Überzeugungen gehören:

- Transparenz statt Geheimhaltung
- Technische Kompetenz als demokratische Pflicht
- Verantwortungsvoller Umgang mit Wissen
- Kritik an staatlicher und privater Macht im Digitalen

In diesem Sinne war der CCC eine der ersten Organisationen, die Technik- und Gesellschaftskritik auf neue Weise verband – mit dem Hacker als zentraler Figur einer digitalen Zivilgesellschaft.

1.1.3 Das Hacker-Manifesto

Im Jahr 1986 erschien ein Text, der in Hacker-Kreisen Kultstatus erlangte: The Hacker Manifesto, verfasst von Lloyd Blankenship, besser bekannt unter dem Pseudonym „The Mentor“. Der Text wurde unmittelbar nach seiner Verhaftung geschrieben und erschien in der Hackerzeitschrift Phrack.

Trotz seines US-amerikanischen Ursprungs wurde das Manifest weltweit rezipiert – nicht als Aufruf zur Rebellion, sondern als Ausdruck eines tiefen Missverständnisses zwischen Hackern und der Gesellschaft. Ein zentraler Auszug:

„We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat and lie to us and try to make us believe it's for our own good, yet we're the criminals”.

Dieses Manifest war ein emotionales, aber reflektiertes Plädoyer. Es formulierte den Anspruch, dass Hacker nicht in erster Linie zerstören, sondern verstehen wollen. Dass sie sich nicht durch Konventionen, sondern durch Neugier definieren. Und dass sie sich einer Welt verpflichtet fühlen, die auf Wissen, nicht auf Macht basiert.

Das Hacker-Manifesto war keine Rechtfertigung für illegale Aktivitäten. Es war ein Versuch, eine Kultur zu erklären, die in der Öffentlichkeit kaum verstanden wurde – und bis heute oft pauschal verurteilt wird.

Zwei Welten, zwei Logiken: Während die Hackerethik auf Dezentralität, Wissensaustausch und den freien Zugang zu Informationen setzt, folgen die Tech-Giganten dem Prinzip der Gewinnmaximierung durch geschlossene Systeme (Walled Gardens) und künstliche Verknappung.

1.1.4 Hackerethik als Gegenmodell zur Technokratie

Was all diese Ursprünge – vom MIT über den CCC bis zum Manifest – verbindet, ist ein gemeinsames Menschenbild: der Mensch als lernfähiges, kreatives, verantwortungsbewusstes Wesen. Die Technik ist dabei weder Bedrohung noch bloßes Werkzeug – sondern ein Spiegel gesellschaftlicher Verhältnisse. Wer sie versteht, kann sie beeinflussen. Wer sie hinterfragt, kann Alternativen entwickeln.

Quellenverzeichnis

Baecker, D. (2007). Studien zur nächsten Gesellschaft. Frankfurt am Main: Suhrkamp.

Bundesamt für Sicherheit in der Informationstechnik (2023). Die Lage der IT-Sicherheit in Deutschland 2023. Bonn: BSI.

Castells, M. (2010). The Rise of the Network Society. Oxford: Wiley-Blackwell.

Free Software Foundation Europe (FSFE) (2021). Public Money? Public Code!. Berlin: FSFE.

Himanen, P. (2001). Die Hacker-Ethik und der Geist des Informationszeitalters. München: Riemann Verlag.

Initiative D21 (2023). D21-Digital-Index 2023/2024. Berlin: Initiative D21 e. V.

Levy, S. (1984). Hackers: Heroes of the Computer Revolution. New York: Anchor Press/Doubleday.

Menn, J. (2019). Cult of the Dead Cow: How the Original Hacking Supergroup Might Just Save the World. New York: PublicAffairs.

Open Knowledge Foundation (2022). Transparenzindex 2022: Offene Daten in Deutschland. Berlin: Open Knowledge Foundation.

Perlroth, N. (2021). This Is How They Tell Me the World Ends: The Cyberweapons Arms Race. New York: Bloomsbury Publishing.

Postman, N. (1985). Amusing Ourselves to Death: Public Discourse in the Age of Show Business. New York: Viking Penguin.

Raymond, E. S. (2001). The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary. Sebastopol, CA: O'Reilly Media.

Stephens-Davidowitz, S., & Oracle (2023). The Decision Dilemma. Redwood Shores, CA: Oracle Corporation.

Turkle, S. (2011). Alone Together: Why We Expect More from Technology and Less from Each Other. New York: Basic Books.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs.

Das Glossar der Dinosaurier

Technik-Jargon für Menschen, die digitale Souveränität zurückgewinnen wollen.

Algorithmus

Stellen Sie sich ein Kochrezept vor. Aber statt Mehl und Eiern verarbeitet dieses Rezept Ihre persönlichen Daten. Das Problem: Die Köche (Plattformen wie TikTok oder Amazon) halten die Zutaten geheim. Das Ergebnis ist oft so gewürzt, dass Sie immer weiter konsumieren, auch wenn es Ihnen nicht guttut.

API (Application Programming Interface)

Die digitale Entsprechung einer Speisekarte. Sie müssen nicht wissen, wie es in der Küche (dem Server) aussieht. Sie müssen nur wissen, was auf der Karte steht, um eine Bestellung aufzugeben. Eine API regelt genau diesen Austausch zwischen zwei Programmen.

Backdoor (Hintertür)

Ein geheimer Zugang zu einer Software, den Entwickler oder Geheimdienste absichtlich eingebaut haben. Es ist so, als hätte Ihr Vermieter einen Zweitschlüssel zu Ihrer Wohnung, von dem Sie nichts wissen – und jeder, der diesen Schlüssel findet, kann ungebeten in Ihr Wohnzimmer treten.

Blackbox

Ein System, bei dem Sie vorne Daten eingeben und hinten ein Ergebnis erhalten, ohne zu wissen, was dazwischen passiert. Hacker lehnen Blackboxes ab – sie wollen verstehen, wie die Zahnräder im Inneren ineinandergreifen, um nicht manipuliert zu werden.

Cloud (Die Wolke)

Ein poetischer Name für eine profane Sache: „Der Computer von jemand anderem". Wenn Sie Daten in der Cloud speichern, liegen sie in einem Rechenzentrum, das meist einem US-Großkonzern gehört. Sie geben damit die physische Kontrolle über Ihre Daten ab.

Exploit

Ein Werkzeug oder eine Methode, um eine Sicherheitslücke auszunutzen. Wenn jemand bemerkt, dass sich Ihr Türschloss mit einer Büroklammer öffnen lässt, ist die Büroklammer der Exploit. Hacker nutzen dieses Wissen, um auf Fehler aufmerksam zu machen, bevor Kriminelle sie finden.

Fediverse (Föderiertes □ niversum)

Die Hacker-Alternative zu den „eingezäunten Gärten" (Walled Gardens) von Facebook oder X. Es funktioniert wie das E-Mail-System: Sie können bei einem Anbieter Ihrer Wahl sein (z. B. Mastodon) und trotzdem mit Menschen bei anderen Anbietern kommunizieren. Niemand besitzt das Ganze.

Open Source

Ein gläsernes Rezept. Jeder darf den Code lesen, kopieren und verbessern. Es ist die digitale Form von Nachbarschaftshilfe: Jemand baut ein nützliches Werkzeug und teilt den Bauplan mit der Welt, damit alle davon profitieren können.

Patch (□pdate)

Ein digitaler Flicken. Wenn eine Sicherheitslücke gefunden wird, schickt der Hersteller einen Patch, um das Loch zu stopfen. Hacker raten: Installieren Sie Ihre Patches zügig – sonst bleibt das Fenster für Angreifer offen.

Reverse Engineering

Ein fertiges Gerät wird so lange untersucht und zerlegt, bis man verstanden hat, wie es konstruiert wurde. Es ist der Versuch, ein fertiges Gericht so lange zu verkosten, bis man das Rezept selbst aufschreiben kann, um es nachzukochen oder zu verbessern.

Stichwortverzeichnis

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

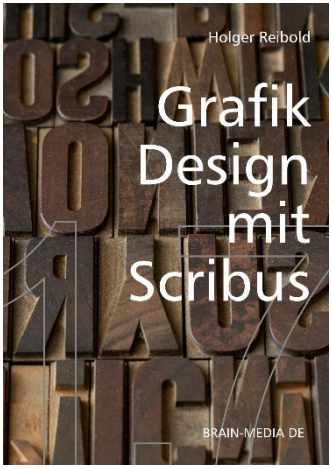
V

W

Y

Z

Mehr von Brain-Media.de



Grafikdesign mit Scribus

In diesem Handbuch erfahren Sie alles, um mit Scribus ein professionelles Projekt umzusetzen – angefangen bei der Entwicklung kreativer Ideen bis zur konkreten Gestaltung.

Preis: 24,99 EUR

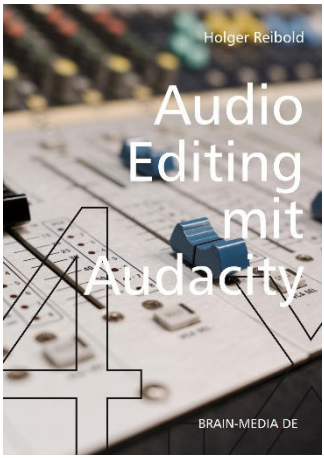
Umfang: 420 Seiten

Virtuelle Maschinen mit VirtualBox 7.x

So verwandeln Sie einen Rechner in ein ganzes Netzwerk oder bauen ein Testumgebung auf. Dieses Handbuch führt Sie in alle wichtigen Funktionen bis hin zur Cloud-Nutzung ein.

Preis: 16,99 EUR

Umfang: 150 Seiten



Audio Editing mit Audacity 4.x

Alles Wichtige, was Sie für den erfolgreichen Einsatz des freien Audioeditors wissen müssen.

Umfang: 220 Seiten

Preis: 19,99 EUR

Erscheint: Frühjahr 2026

BGP als kritische Infrastruktur

Das Buch zeigt BGP als kritische, vertrauensbasierte Internetinfrastruktur und erklärt, warum Routingfehler trotz Redundanz globale Ausfälle verursachen und verantwortungsvollen Betrieb erfordern.

Umfang: 170 Seiten

Preis: 19,99 EUR

Private KI – KI-Systeme lokal betreiben, kontrollieren und verantworten

Alles Wichtige für den sicheren Einsatz von lokalen KI-Systemen.

Umfang: 200 Seiten

Preis: 19,99 EUR

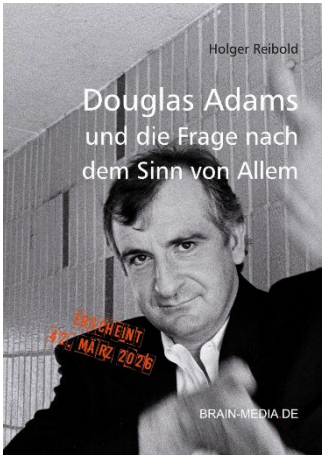
Erscheint: Frühjahr 2026

KI Incident Response – Wie man Sicherheitsvorfälle in KI-Systemen erkennt, eindämmt und verantwortet

Das Buch etabliert KI Incident Response als eigene Disziplin und zeigt, wie KI-Vorfälle erkannt, bewertet und beherrscht werden, damit Organisationen reagieren.

Umfang: 220 Seiten

Preis: 16,99 EUR



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11 Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

Preis: 14,99 EUR

Erscheint: 42. März 2026

Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor. 100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR. Plus+-Abonnenten zahlen nur 24 EUR.

IT-Texter.one

100+ IT-Fachbücher

1500+ Fachartikel

30+ Erfahrung

KOMPLEXE INHALTE PUNKTGENAU AUFZUBEREITEN, IST EINE KUNST. ICH BEHERRSCHE SIE. BEI MIR ERHALTEN SIE FACHTEXTE, DIE KOMPLEXES VERSTÄNDLICH MACHEN.

Seit über 30 Jahren unterstütze ich Unternehmen aus der IT-, Software- und Digitalbranche dabei, ihre technischen Inhalte klar, präzise und zielgruppenorientiert zu kommunizieren. Als promovierter Informatiker und erfahrener IT-Journalist verbinde ich fundiertes Fachwissen mit journalistischem Storytelling. Als Key Account Manager eines IT-Dienstleisters verfüge ich obendrein über konkrete Erfahrungen mit allen gängigen Technologien.

WARUM SIE MIT MIR ARBEITEN SOLLTEN

35 Jahre Erfahrung mit Internet-, Netzwerk- und Webtechnologien

Kooperation mit führenden Akteuren der IT- und Medienbranche

Strategisches Denken: Texte, die nicht nur informieren, sondern auch verkaufen

THEMENSCHWERPUNKTE	WIE KANN ICH SIE UNTERSTÜTZEN
Open-Source	Content Creation
Enterprise IT	Dokumentationen
IT-Consulting	Case Studies
SaaS	Suchmaschinenoptimierung
Künstliche Intelligenz	Tech-Marketing

MEIN VERSPRECHEN

Ich übernehme die inhaltliche und sprachliche Brücke zwischen Technologie und Anwendung. Selbst komplexe Sachverhalte kommen beim Publikum an – fachlich korrekt, prägnant und SEO-wirksam.

PREISMODELLE

Professionelle Leistungen, die ihresgleichen suchen, gibt es nicht umsonst. Sprechen Sie mich an. Gerne vereinbaren wir einen Fixpreis; das vereinfacht Ihre Kalkulation.

KONTAKT AUFNEHMEN

Sprechen wir über Ihr Projekt. Schreibe Sie mir eine Mail (info@it-texter.one). Oder besser noch: Rufen Sie mich an (+49 681 91005698).