



Holger Reibold

# Code or die

Warum wir mehr Hacker brauchen

BRAIN-MEDIA.DE

Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Verlags ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form durch Fotokopien oder ein anderes Verfahren zu vervielfältigen oder zu verbreiten. Dasselbe gilt auch für das Recht der öffentlichen Wiedergabe. Der Verlag macht darauf aufmerksam, dass die genannten Firmen- und Markennamen sowie Produktbezeichnungen in der Regel marken-, patent- oder warenrechtlichem Schutz unterliegen.

Verlag und Autor übernehmen keine Gewähr für die Funktionsfähigkeit beschriebener Verfahren und Standards.

© 2026 Brain-Media.de

ISBN: 978-3-95444-316-1

Cover: Freepik

Brain-Media.de

Dr. Holger Reibold – Hubert-Müller-Str. 52c – 66113 Saarbrücken

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

# Inhaltsverzeichnis

Inhaltsverzeichnis .....	I
Vorwort .....	1
Einleitung – Hacker, Helden oder Feinde? .....	7
1 Die Hackerethik .....	13
1.1 Der Ursprung der Hackerethik .....	14
1.1.1 Die Prinzipien der Hackerethik am MIT .....	15
1.1.2 Der Chaos Computer Club: Hackerethik in Europa .....	16
1.1.3 Das Hacker-Manifesto .....	18
1.1.4 Hackerethik als Gegenmodell zur Technokratie .....	19
1.1.5 Warum diese Geschichte heute wichtig ist .....	20
1.2 Die Prinzipien der Hackerethik .....	21
1.2.1 Zugang zu Informationen – Wissen muss frei sein .....	21
1.2.2 Technologie als Werkzeug zur Selbstermächtigung .....	23
1.2.3 Misstrauen gegenüber Autorität .....	24
1.2.4 Transparenz über Systeme .....	25
1.2.5 Verantwortung statt Beliebigkeit .....	26
1.2.6 Teilen als kulturelles Prinzip .....	27
1.2.7 Freude am Lernen, Spieltrieb und Kreativität .....	28

1.2.8	Fazit: Eine Ethik für das 21. Jahrhundert .....	29
2	Hack the System – wie Hacker Innovation schaffen .....	31
2.1	Von Linus Torvalds bis Richard Stallman.....	33
2.1.1	Stallman und die Freien Software .....	33
2.1.2	Linus Torvalds und die Kraft der Offenheit .....	35
2.1.3	Freie Software vs. Open Source .....	36
2.1.4	Was wir von beiden lernen können.....	37
2.2	Erfolgsmodelle aus der Hackerkultur .....	37
2.2.1	Open Source – Der Code gehört allen.....	38
2.2.2	Peer Review – die kollektive Intelligenz nutzen .....	39
2.2.3	Agiles Arbeiten – Flexibilität als Prinzip .....	40
2.2.4	Gemeinsame Wurzeln, unterschiedliche Effekte.....	42
2.3	Zweckentfremden als Methode .....	43
2.3.1	Subversion als schöpferischer Akt .....	43
2.3.2	Beispiele aus der Geschichte .....	44
2.3.3	Künstlerisches Hacken: Von Glitch bis Circuit Bending... 44	
2.3.4	Reverse Engineering als kreative Strategie .....	45
2.3.5	Hacken als Lernmethode .....	46
2.3.6	Warum das unbequem ist – und notwendig .....	46
2.3.7	Fazit: Hacken heißt anders denken .....	47
3	Sicherheitslücken sind kein Zufall.....	49

3.1	Warum Schwachstellen entstehen.....	50
3.1.1	Fehler als systemische Realität.....	50
3.1.2	Ökonomien der Unsicherheit.....	51
3.1.3	Komplexität und vernetzte Systeme .....	51
3.1.4	Wie Hacker Schwachstellen finden .....	52
3.1.5	Umgang mit Schwachstellen: Responsible Disclosure ...	54
3.1.6	Warum wir Hacker brauchen .....	54
3.1.7	Fazit .....	55
3.2	Stuxnet, Heartbleed, SolarWinds & Co.....	56
3.2.1	Stuxnet – Der erste digitale Sabotageakt.....	57
3.2.2	Heartbleed – Der Fehler im Herzen des Internets.....	58
3.2.3	SolarWinds – Die unsichtbare Hintertür.....	59
3.2.4	Gemeinsamkeiten und Lehren.....	61
3.2.5	Fazit .....	62
3.3	Responsible Disclosure vs. Industrieinteressen.....	62
3.3.1	Was bedeutet Responsible Disclosure? .....	63
3.3.2	Die Realität: Misstrauen und Repression.....	63
3.3.3	Beispiel: CCC und die elektronische Patientenakte.....	64
3.3.4	Warum Disclosure wichtig ist .....	64
3.3.5	Coordinated Vulnerability Disclosure als Lösung .....	65
3.3.6	Der kulturelle Wandel .....	66

3.3.7	Fazit .....	66
4	Bildung braucht Hackergeist .....	69
4.1	Wie Schulen technische Neugier töten.....	70
4.1.1	Schule als Ort der Technikkonformität.....	70
4.1.2	Digitale Bildung als Produkttraining.....	71
4.1.3	Technisches Interesse wird nicht gefördert.....	72
4.1.4	Digitale Systeme als Blackboxes .....	72
4.1.5	Fehlende Vorbilder und Rollenmodelle .....	74
4.1.6	Prüfungsformate gegen Neugier .....	74
4.1.7	Eine verlorene Generation?.....	75
4.2	Vorschlag: Hack the Curriculum .....	76
4.3	Hackathons, Hackspaces, Makerspaces.....	80
5	Hacker im Alltag.....	85
5.1	Unbequeme Fragen stellen.....	86
5.2	Geschichten von Alltags-Hackern .....	90
6	Gegen das Klischee .....	97
6.1	Klischees, Strafrecht, Mythos des Einzeltäters .....	98
6.2	Warum Sichtbarkeit wichtig ist .....	102
7	Eine Kultur retten – und stärken.....	109
7.1	Warum die Hackerkultur verschwindet.....	110
7.2	Wie man sie schützt, fördert, sichtbar macht.....	115

7.3	Plädoyer für digitale Aufklärung .....	120
7.3.1	Hackerclubs, Orte der Neugier .....	120
7.3.2	Förderprogramme: Impulse mit Wirkung .....	121
7.3.3	Digitale Aufklärung: Bildung für das 21. Jahrhundert ...	122
7.3.4	Sichtbarkeit und Anerkennung .....	123
7.3.5	Fazit: Der Wert einer kritischen Kultur.....	124
8	Was jetzt zu tun ist.....	125
8.1	Recht auf Reparatur und Modifikation.....	127
8.2	Hackergeist als Bildungsprimat.....	129
8.3	Public Money? Public Code! .....	132
8.4	Schutz für Sicherheitsforschung .....	135
8.5	Interoperabilität als Bürgerrecht .....	138
8.6	Gemeinwohlorientierte Infrastruktur fördern.....	141
8.7	Transparenzpflicht für Algorithmen .....	144
	Zum Schluss .....	149
	Quellenverzeichnis.....	VII
	Das Glossar der Dinosaurier .....	IX
	Stichwortverzeichnis .....	XIII
	Mehr von Brain-Media.de .....	XIX
	IT-Texter.one .....	XXIII



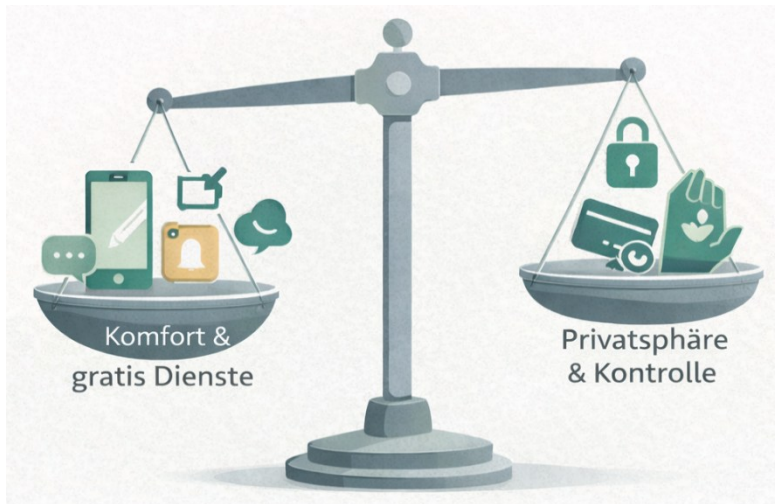
# Vorwort

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.

# 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 Super-group Might Just Save the World. New York: PublicAffairs.
- Open Knowledge Foundation (2022). Transparenzindex 2022: Offene Daten in Deutschland. Berlin: Open Knowledge Foundation.

- Perloth, 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 Universum)**

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 (Update)**

Ein digitaler Flicker. 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

## A

Agiles Arbeiten.....	40
Algorithmus .....	7, 144
Amazon .....	59
Angriffsszenario.....	8
Auditierbarkeit.....	25
Authentifizierung .....	7

## B

Backdoor .....	60
Berners-Lee, Tim .....	44
Bildung.....	69
Bildungsansatz .....	77
Bildungsprimat .....	129
Bildungsraum .....	81
Bildungssystem .....	69, 74, 111
Blackbox .....	20
Blankenship, Llyod .....	18
BTX-Hack.....	16
Bug.....	49
Bugcrowd .....	65

## C

CERN .....	44
Chaos Communication Congress ..	104
Chaos Computer Club.....	9, 13, 16
Circuit Bending .....	44
Code.....	37
Codezeile.....	85
Cyberkriminalität .....	8
Cyberwarfare .....	53

## D

Daten.....	7
Datendiebstahl .....	8
Daten-Kreislauf .....	26
Datenschutz .....	13
Denkweise .....	13
Deutsche Post.....	16
Dezentrale Infrastruktur .....	13
Dezentralisierung.....	20
Digital Markets Act .....	140
Digitale Aufklärung.....	122
Digitale Bildung .....	69
Digitale Souveränität .....	89

Digitale Waage.....	2
Digitalisierung.....	1
DRM .....	20

## E

EFF.....	119
Elektronische Patientenakte .....	54
Entscheidungssystem.....	9
ePA.....	64
EU AI Act.....	73
Extreme Programming .....	41

## F

Flickr .....	53
Forderungen .....	125
Framework .....	51
Free Software Foundation Europe ...	22
Freie Software .....	36
Fuzzing .....	52

## G

Gestalter .....	86
GitHub.....	28
Glitch .....	44
GNU .....	34
Google.....	39, 59

## H

Hack the Curriculum .....	76
Hackathon .....	81
Hacker .....	8
Hackerbibel .....	17
Hackerethik .....	9, 13
Hackerfond .....	121
Hackerhaltung .....	125
Hackerkultur .....	109, 113
Hacker-Manifesto .....	18
HackerOne.....	65
Hackerparagraf .....	54
Hackerparagrafen .....	27
Hackers .....	99
Hackspace.....	28, 80
Heartbleed.....	53, 58
Holland, Wau .....	16
HTTPS .....	58

## I

IBM .....	39
Informatik .....	116
Informatiker .....	85
Innovation.....	31
Innovationsdruck .....	51
Innovationsmotor.....	38
Interoperabilität .....	4, 138
INTIGriti .....	65
Intransparenz.....	13

## K

Kanban.....	41
Kapuzenpullover.....	97
KI 25	
Kommerzialisierung.....	111
Kompetenz.....	2
Kompetenzsprung.....	86
Kompetenzzentrum.....	122
Künstliche Intelligenz.....	9

## L

Lernen.....	70
Levy, Steven.....	8
Linux.....	35
Lizenzmodell.....	38
Log4j.....	53
Log4Shell.....	53

## M

Macht.....	3
Mailserver.....	59
Makerspace.....	81
Massachusetts Institute of Technology.....	15
Meta.....	59
Microsoft.....	39
Minicomputer.....	15
Misstrauen.....	24

MIT.....	13
Monopol.....	13
Mozilla.....	119

## N

Nerd.....	97, 112
Netzpolitik.....	13
Netzprotokoll.....	7
Netzwerk.....	8
Neugier.....	74
NGO.....	66
NSA.....	57

## O

Ökosystem.....	1
Open Hardware.....	4
Open Source.....	36, 38, 78
Open-Source-Projekt.....	13
OpenSSL.....	53, 58

## P

Paywall.....	20
PDP-1.....	15
Peer Review.....	39
Penetration Testing.....	52
Phrack.....	18
Plattform.....	13
Plattformmonopol.....	32

Postman, Neil .....	9
Produkttraining .....	71
Proprietäre Systeme .....	3
Public Code .....	133
Public Money .....	132

## Q

Quellcode .....	25
-----------------	----

## R

Raspberry Pi .....	93
Recht auf Reparatur .....	127
Responsible Disclosure .....	40, 54, 62
Reverse Engineering .....	45, 52

## S

SAP .....	39
SCADA .....	57
Schnittstelle .....	51
Schwachstelle .....	10
Scriptkiddie .....	113
Scrum .....	41
Selbstbestimmung .....	4
Selbstermächtigung .....	23
Sicherheitsforschung .....	135
Sicherheitslücke .....	49, 90
Sicherheitsstatus .....	51
Smart Home .....	44

Smart-Home .....	85
Smartphone .....	1
SMS .....	44
Sneakers .....	99
Software .....	8
SolarWinds .....	59
Souveränität .....	87
Sparkasse .....	17
Spracherkennung .....	44
Stallman, Richard .....	9, 33
Static Code Analysis .....	52
Stereotypisierung .....	117
Strafgesetzbuch .....	135
Stuxnet .....	53, 57
Subversion .....	43
Supply-Chain .....	52
Systemdenker .....	97
Systemkompetenz .....	37
Systemverständnis .....	3

## T

Tech Model Railroad Club .....	15
Technikkonformität .....	70
The Matrix .....	99
Torvalds, Linus .....	9, 35
Transparenz .....	24
Transparenzpflicht .....	144

## V

Vandalismus .....	8
Verantwortung .....	26
Verletzbarkeit .....	61
Verschlüsselung .....	7
VPN .....	59

## W

WarGames .....	99
Website .....	59

Who Am I .....	99
WinCC .....	57
Wissen .....	22, 77
Wurm .....	53

## Y

Yahoo .....	53
-------------	----

## Z

Zero-Day .....	57
Zero-Day-Exploit .....	51



# 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

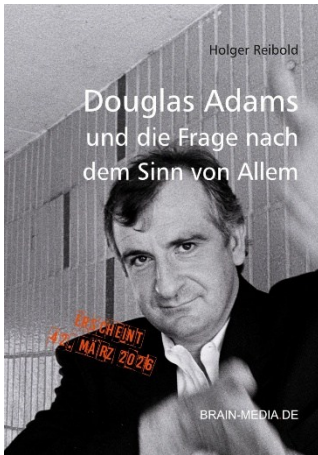


## **KI Incident Response – Wie man Sicherheitsvorfälle in KI-Systemen erkennt, eindämmt und verantwortet**

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, nachhaltige 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 FACH-TEXTE, 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](mailto:info@it-texter.one)). Oder besser noch: Rufen Sie mich an (+49 681 91005698).