

Holger Reibold

# Zero Trust Roadmap

Wie Sie implizites Vertrauen  
eliminieren und jeden  
Zugriff verifizieren

[BRAIN-MEDIA.DE](https://www.brain-media.de)

Holger Reibold

# Zero Trust Roadmap

Wie Sie implizites Vertrauen  
eliminieren und jeden Zugriff  
verifizieren

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: 978-3-95444-343-7

Cover: Freepik / vwalakte

Brain-Media.de

Dr. Holger Reibold – Huber-Müller-Str. 52 – 66113 Saarbrücken

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

# Inhaltsverzeichnis

Inhaltsverzeichnis .....	I
Vorwort .....	1
1 Warum Zero Trust unvermeidbar ist.....	5
1.1 Auflösung klassischer Sicherheitsperimeter .....	6
1.2 Die Beschleuniger .....	9
1.3 Die moderne Bedrohungslandschaft .....	11
1.4 Grenzen klassischer Sicherheitsmodelle .....	13
1.5 Der Business Case für Zero Trust.....	15
1.6 Management Summary .....	18
2 Grundlagen von Zero Trust.....	19
2.1 Definition und Prinzipien von Zero Trust.....	20
2.2 „Never trust, always verify“ in der Praxis .....	22
2.3 Identität als zentraler Sicherheitsanker.....	25
2.4 Mikrosegmentierung und Zugriffskontrolle .....	27
2.5 Abgrenzung zu traditionellen Konzepten .....	30
2.6 Management Summary .....	32
3 Architektur eines Zero-Trust-Modells.....	33
3.1 Referenzarchitekturen im Überblick.....	34

3.2	Identity & Access Management.....	37
3.3	Device Trust und Endpoint Security .....	39
3.4	ZTNA statt VPN .....	41
3.5	Datenzentrierte Sicherheitsarchitektur .....	44
3.6	Management Summary .....	47
4	Die Zero-Trust-Roadmap .....	49
4.1	Reifegradanalyse und Ausgangsbewertung .....	50
4.2	Zielbild und Zielarchitektur definieren.....	53
4.3	Priorisierung von Anwendungsfällen .....	55
4.4	Investitionslogik und ROI-Betrachtung.....	57
4.5	Roadmap-Phasenmodell.....	60
4.6	Management Summary .....	63
5	Technologische Bausteine.....	65
5.1	Identity Provider und Multi-Faktor .....	66
5.2	Zero Trust Network Access.....	69
5.3	Endpoint Detection & Response.....	71
5.4	SIEM, Telemetrie und Policy Enforcement.....	73
5.5	Datenklassifizierung und Verschlüsselung.....	76
5.6	Management Summary .....	79
6	Organisation, Governance und Betriebsmodell.....	81
6.1	Rollen und Verantwortlichkeiten .....	82

6.2	Security als Business Enabler.....	84
6.3	Richtlinien, Compliance und Regulierung.....	87
6.4	Change Management und Transformation.....	90
6.5	Schulung, Awareness und Kulturwandel.....	92
6.6	Management Summary.....	95
7	Umsetzung in der Praxis.....	97
7.1	Pilotprojekte und initiale Use Cases.....	98
7.2	Migration bestehender Systeme.....	100
7.3	Integration in IT- und OT-Landschaften.....	103
7.4	Der Legacy-Faktor.....	105
7.5	Schlüssel: Isolation und Wrapper-Prinzip.....	107
7.6	Management Summary.....	110
8	Die Zukunft von Zero Trust.....	111
8.1	AI-driven Anomaly Detection.....	112
8.2	Signal-Intelligenz als Kern von Zero Trust.....	114
8.3	Echtzeitentscheidungen in Millisekunden.....	117
8.4	Continuous Authentication.....	119
8.5	Zero Trust für OT, IoT und vernetzte Systeme.....	121
8.6	Management Summary.....	123
	Zum Schluss.....	125
	Anhang.....	V

Zero-Trust-Reifegradmodell .....	V
Beispiel: 12-Monats-Roadmap .....	XII
Weitere Downloads .....	XVI
Glossar .....	XVII
Abkürzungsverzeichnis.....	XXI
Literatur- und Quellenverzeichnis .....	XXIII
Stichwortverzeichnis .....	XXV
Mehr von Brain-Media.de .....	XXIX

# Vorwort

*Warum Vertrauen in der IT endgültig ausgedient hat.*

Die IT-Sicherheit hat sich in den letzten drei Jahrzehnten grundlegend gewandelt. In den frühen Tagen der Unternehmens-IT war Sicherheit vor allem ein Randthema – relevant, aber selten geschäftskritisch. Netzwerke waren klar abgegrenzt, Systeme standen physisch in Rechenzentren, und der Zugriff erfolgte nahezu ausschließlich aus dem internen Unternehmensnetz. Sicherheit bedeutete in diesem Kontext vor allem den Schutz der Infrastruktur vor äußeren Angriffen.

Mit der zunehmenden Vernetzung, der Verbreitung des Internets und später der Digitalisierung von Geschäftsprozessen änderte sich dieses Bild drastisch. Anwendungen wurden webbasiert, Partner wurden angebunden, und Mitarbeiter arbeiteten zunehmend mobil. Sicherheit entwickelte sich von einer rein technischen Disziplin zu einer strategischen Funktion.

Dennoch blieb ein Paradigma über viele Jahre nahezu unverändert: das Modell des vertrauenswürdigen internen Netzwerks. Alles innerhalb des Perimeters galt als sicher, alles außerhalb als potenziell gefährlich. Firewalls, VPNs und Netzwerksegmentierung bildeten die

tragenden Säulen dieses Ansatzes. Dieses Modell war lange Zeit erfolgreich, basiert jedoch auf Annahmen, die heute nicht mehr gelten.

Die Vorstellung eines klar definierten, schützenden Perimeters ist in modernen IT-Landschaften nicht mehr haltbar. Unternehmen betreiben hybride Infrastrukturen, nutzen Cloud-Dienste, integrieren SaaS-Anwendungen und ermöglichen ihren Mitarbeitern ortsunabhängiges Arbeiten. Daten und Anwendungen befinden sich längst nicht mehr ausschließlich im eigenen Rechenzentrum. Gleichzeitig haben sich auch die Angriffsmodelle verändert. Angreifer nutzen gezielt Identitäten, kompromittieren Zugangsdaten oder bewegen sich lateral innerhalb von Netzwerken, ohne klassische Sicherheitsgrenzen zu überwinden. Der Angriff beginnt nicht mehr zwingend von außen, sondern erfolgt häufig über legitime Zugriffe.

Damit wird eine zentrale Schwäche des klassischen Sicherheitsmodells sichtbar: Es basiert auf implizitem Vertrauen. Wer sich einmal im Netzwerk befindet, erhält oft weitreichende Zugriffsmöglichkeiten, unabhängig davon, ob dieser Zugriff tatsächlich gerechtfertigt ist. In einer Welt, in der Identitäten, Geräte und Anwendungen dynamisch und verteilt sind, wird Vertrauen selbst zum Risiko. Die logische Konsequenz ist ein Paradigmenwechsel: Vertrauen darf nicht vorausgesetzt, sondern muss kontinuierlich überprüft werden.

Dieses Buch ist aus der Beobachtung entstanden, dass viele Organisationen die Notwendigkeit von Zero Trust zwar erkannt haben, aber an der praktischen Umsetzung scheitern. Zu oft bleibt Zero Trust ein abstraktes Konzept, ein Buzzword oder ein reines

Technologieprojekt. Die Realität ist geprägt von gewachsenen IT-Landschaften mit Legacy-Systemen, komplexen organisatorischen Strukturen, Abhängigkeiten von bestehenden Prozessen und Tools sowie einer fehlenden Verbindung zwischen strategischem Anspruch und operativer Umsetzung.

Gleichzeitig steigt der Druck auf Unternehmen kontinuierlich. Sicherheitsvorfälle haben längst direkte geschäftliche Auswirkungen – finanziell, regulatorisch und reputativ. Entscheider stehen vor der Herausforderung, Sicherheit nicht nur zu erhöhen, sondern gleichzeitig Komplexität und Kosten zu beherrschen. Genau hier setzt dieses Buch an.

Ziel dieses Buches ist es, einen pragmatischen, umsetzbaren Leitfaden zu liefern, der Zero Trust nicht als theoretisches Ideal beschreibt, sondern als realistische Transformationsstrategie. Es geht darum, die grundlegenden Prinzipien von Zero Trust verständlich einzuordnen, eine strukturierte Roadmap für die schrittweise Einführung zu entwickeln und die Herausforderungen der Praxis offen anzusprechen – insbesondere im Umgang mit bestehenden Systemen, organisatorischen Hürden und technologischen Abhängigkeiten.

Ein besonderer Fokus liegt dabei auf der Frage, wie implizites Vertrauen systematisch eliminiert werden kann, ohne den Geschäftsbetrieb zu gefährden. Zero Trust bedeutet nicht, alles Bestehende zu ersetzen, sondern Vertrauen gezielt durch überprüfbare, kontextbasierte Entscheidungen zu ersetzen.

Dieses Buch richtet sich an Entscheider, Architekten und Praktiker gleichermaßen. Es verbindet strategische Perspektiven mit konkreten Umsetzungsansätzen und folgt dabei einem klaren Leitprinzip: Sicherheit muss nicht nur wirksam, sondern auch umsetzbar sein. Zero Trust ist kein Zielzustand, der einmal erreicht wird, sondern ein kontinuierlicher Prozess – und vor allem eine neue Denkweise im Umgang mit Vertrauen, Zugriff und Kontrolle in digitalen Systemen.

Dieses Buch soll Ihnen helfen, diesen Weg strukturiert zu gehen.

Dabei wünsche ich Ihnen viel Erfolg!

Herzlichst

Holger Reibold

# 1 Warum Zero Trust unvermeidbar ist

*Die Illusion Sicherheit: Warum der Perimeter fällt.*

Die Einführung von Zero Trust ist keine optionale Weiterentwicklung bestehender Sicherheitskonzepte, sondern eine direkte Reaktion auf fundamentale Veränderungen in der IT-Landschaft. Unternehmen operieren heute in hochgradig vernetzten, dynamischen Umgebungen, in denen klassische Annahmen über Vertrauen, Netzwerkgrenzen und Zugriffskontrolle nicht mehr greifen. Identitäten sind mobil, Anwendungen verteilt und Daten allgegenwärtig.

Gleichzeitig verschiebt sich die Bedrohungslage von klar erkennbaren externen Angriffen hin zu komplexen, oft schwer detektierbaren Szenarien, bei denen legitime Zugriffe missbraucht werden. Der Schutz eines definierten Netzwerkperimeters reicht unter diesen Bedingungen nicht mehr aus. Stattdessen muss jede einzelne Zugriffsanfrage kontextbasiert bewertet und kontinuierlich überprüft werden.

Zero Trust adressiert genau diese Herausforderung. Es ersetzt implizites Vertrauen durch überprüfbare Sicherheit und zwingt Organisationen, ihre Architektur, Prozesse und Entscheidungslogiken neu zu denken. Dabei geht es nicht nur um Technologie, sondern um eine grundlegende Neuausrichtung von Sicherheitsstrategien.

Dieses Kapitel zeigt, warum dieser Wandel unvermeidbar ist, welche Treiber ihn beschleunigen und warum Zero Trust nicht nur ein Sicherheitskonzept, sondern eine betriebswirtschaftlich sinnvolle Entscheidung ist.

## 1.1 Auflösung klassischer Sicherheitsperimeter

Über viele Jahre hinweg bildete der Sicherheitsperimeter das zentrale Organisationsprinzip der IT-Sicherheit. Die zugrunde liegende Logik war einfach und scheinbar belastbar: Innerhalb des Unternehmensnetzwerks befanden sich vertrauenswürdige Systeme und Benutzer, außerhalb potenzielle Angreifer. Firewalls, Intrusion-Detection-Systeme und VPN-Zugänge dienten dazu, diese Grenze zu kontrollieren und zu schützen.

Dieses Modell war in einer Zeit sinnvoll, in der IT-Infrastrukturen weitgehend statisch waren. Anwendungen liefen im eigenen Rechenzentrum, Endgeräte waren klar zugeordnet und der Zugriff erfolgte überwiegend aus dem internen Netzwerk. Vertrauen war an den Standort gebunden – wer „drinnen“ war, galt als legitim.

Diese Annahmen sind heute nicht mehr tragfähig. Moderne IT-Landschaften sind geprägt von hybriden Architekturen, Cloud-Plattformen und einer Vielzahl externer Dienste. Anwendungen werden nicht mehr ausschließlich im eigenen Netzwerk betrieben, sondern verteilen sich über verschiedene Umgebungen. Gleichzeitig greifen

Benutzer von unterschiedlichsten Orten und Geräten auf Unternehmensressourcen zu.

Damit verliert der Netzwerkstandort seine Aussagekraft als Sicherheitsmerkmal. Ein Zugriff aus dem internen Netz ist nicht automatisch vertrauenswürdig, und ein Zugriff von außen ist nicht zwangsläufig verdächtig. Identität, Gerätezustand und Kontext werden zu den entscheidenden Faktoren.

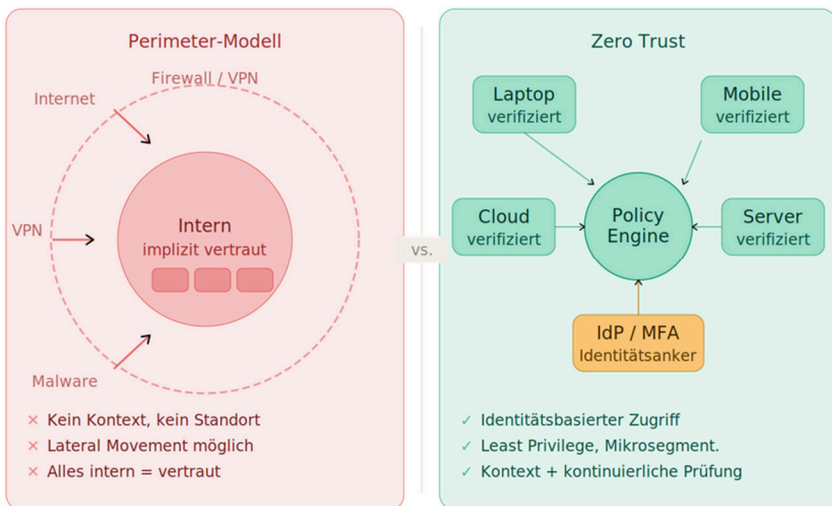
Hinzu kommt, dass Angreifer ihre Strategien angepasst haben. Statt primär zu versuchen, Sicherheitsgrenzen von außen zu durchbrechen, nutzen sie gezielt gestohlene Zugangsdaten, kompromittierte Geräte oder Schwachstellen in Anwendungen. Sobald sie Zugriff auf ein System haben, bewegen sie sich häufig lateral innerhalb des Netzwerks – genau dort, wo klassische Sicherheitsmechanismen weniger wirksam sind.

Der Perimeter existiert damit nicht mehr als klar definierte Grenze, sondern allenfalls als fragmentiertes Konstrukt aus Teilgrenzen, die sich über verschiedene Infrastrukturen erstrecken. In der Praxis bedeutet dies: Das Vertrauen, das früher an den Netzwerkzugang geknüpft war, ist nicht mehr gerechtfertigt.

Die Konsequenz ist ein grundlegender Paradigmenwechsel. Sicherheit darf nicht länger auf der Annahme basieren, dass sich vertrauenswürdige und nicht vertrauenswürdige Bereiche klar trennen lassen. Stattdessen muss jeder Zugriff unabhängig von seinem Ursprung bewertet werden. Vertrauen wird nicht mehr durch

Zugehörigkeit zum Netzwerk impliziert, sondern durch überprüfbare Kriterien hergestellt.

Die Auflösung des klassischen Perimeters ist damit nicht nur eine technische Entwicklung, sondern der zentrale Auslöser für die Entstehung von Zero Trust. Ohne diese Verschiebung wäre das Konzept nicht notwendig – mit ihr ist es unausweichlich.



**Die klassische Perimeter-Sicherheit basiert auf implizitem Vertrauen innerhalb eines Netzwerks. Zero Trust ersetzt dieses Modell durch identitätsbasierte Zugriffskontrollen, bei denen jeder Zugriff unabhängig vom Standort geprüft und kontextabhängig bewertet wird.**

## 1.2 Die Beschleuniger

Die Auflösung des Perimeters ist kein isoliertes Phänomen, sondern das Ergebnis mehrerer technologischer und organisatorischer Entwicklungen, die sich gegenseitig verstärken. Insbesondere Cloud Computing, die breite Nutzung von SaaS-Anwendungen und die Etablierung von Remote Work haben die Rahmenbedingungen für IT-Sicherheit grundlegend verändert.

Mit der Verlagerung von Anwendungen in die Cloud verlieren Unternehmen die vollständige Kontrolle über ihre Infrastruktur. Systeme werden nicht mehr ausschließlich im eigenen Rechenzentrum betrieben, sondern in verteilten Plattformen, die über das Internet erreichbar sind. Gleichzeitig entstehen hybride Architekturen, in denen On-Premises-Systeme, Public-Cloud-Dienste und SaaS-Lösungen parallel existieren. Klassische Netzwerkgrenzen werden dadurch zunehmend irrelevant.

SaaS-Anwendungen verstärken diesen Effekt zusätzlich. Geschäftskritische Prozesse – von Collaboration über CRM bis hin zu Finanzsystemen – werden heute häufig über externe Plattformen abgewickelt. Der Zugriff erfolgt direkt über das Internet, oft unabhängig vom Unternehmensnetzwerk. Sicherheit kann in diesem Modell nicht mehr über Netzwerkzugang gesteuert werden, sondern muss sich auf Identität, Zugriffskontext und Richtlinien stützen.

Parallel dazu hat sich die Arbeitsweise grundlegend verändert. Remote Work ist nicht mehr Ausnahme, sondern Normalität.

# Stichwortverzeichnis

## 1

12-Monats-Roadmap.....XII

## A

Abgrenzung .....30

AI-driven Anomaly Detection ..... 112

Authentifizierung .....23

Authentifizierungsmechanismen ..11

Autorisierung .....26

Awareness .....92

## B

Bedrohungslandschaft .....11

Business Case.....15

Business Enabler.....84

## C

Change Management .....90

Cloud .....6, 9

Collaboration .....9

Compliance .....88

Continuous Authentication.....119

CRM .....9

## D

Datenabfluss ..... 16

Datenkontrolle .....65

Definition .....20

Device Trust .....39

Digitalisierung ..... 1

## E

Echtzeit..... 118

EDR..... 50, 71

Endpoint Detection & Response ...71

Endpoint Security .....39

Endpoint-Security ..... 23, 31

Enforcement .....35

Entkopplung..... 107

Entscheidungslogik .....34

## F

Firewall ..... 1

Fundament .....20

## G

Geschäftskritische Prozesse.....	9
Geschäftsprozess .....	1

## H

Hybride Architektur .....	6
---------------------------	---

## I

IAM.....	37
Identität .....	2, 25
Identitätsmanagement .....	23, 31
Identity & Access Management .....	37
Identity Provider .....	66
IdP .....	66
Implizites Vertrauen .....	2
Infrastruktur .....	9
Integration.....	103
Intrusion-Detection-System.....	6
Investitionslogik .....	57
Isolation .....	21
Isolation-&-Wrapper-Prinzip .....	109
IT-Sicherheit .....	6

## J

Just-in-Time-Access .....	26
---------------------------	----

## K

Klassifizierung.....	44, 77
Kompromittierung .....	11
Konsolidierung .....	58
Kontextsteuerung.....	77
Kulturwandel.....	93

## L

Legacy-System.....	51, 106
Leitidee .....	20
Logging .....	38

## M

Mainframe.....	105
MFA .....	50, 66
Migration.....	100
Mikrosegmentierung.....	28, 108
Multi-Faktor-Authentifizierung	37, 66

## N

Nachvollziehbarkeit .....	88
Netzwerksegmentierung.....	1
Netzwerkzugang.....	23
Never trust, always verify.....	22

## O

OAuth.....	66
On-Premise .....	9, 70
OpenID Connect.....	66
OT.....	103

## P

Paradigmenwechsel .....	7
Patch-Level .....	39
Phasenmodell .....	60
Phishing .....	11
Pilotprojekt.....	98
Policy Enforcement .....	35, 73
Priorisierung.....	55
Privilegierte Zugriffe.....	11

## R

Reaktionsfähigkeit.....	118
Rechtevergabe .....	21
Reifegradanalyse.....	50
Remote Work .....	10
Richtlinie .....	88
Risikoreduktion .....	99
Roadmap .....	60
ROI.....	58
Rolle.....	82

## S

SaaS .....	10
SAML .....	66
Schulung.....	92
Schutzmechanismen .....	78
Security Information and Event Management.....	74
Segmentierung.....	28
Sicherheitsarchitektur.....	44
Sicherheitsgrenze.....	2
Sicherheitskonzept .....	17
Sicherheitsmodell.....	13
Sicherheitsperimeter.....	6
Sicherheitsrisiko .....	16
Sichtbarkeit.....	21
SIEM .....	73
Signal-Intelligenz.....	114
Steuerbarkeit .....	29

## T

Telemetrie.....	35, 73
Token.....	67
Transformation.....	91
Transparenz .....	21

## U

Use Case .....	99
----------------	----

## V

Verantwortlichkeit .....	83
Verschlüsselung .....	77
Vertrauen .....	19
VPN .....	1, 41
VPN-Infrastruktur .....	10

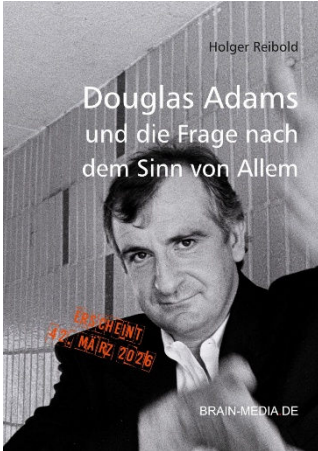
## W

Wildwuchs .....	79
-----------------	----

## Z

Zero Trust .....	2, 20
Zero Trust Network Access .....	41, 69
Zero-Trust-Architektur .....	34
Zero-Trust-Referenzarchitektur .....	35
Zero-Trust-Reifegradmodell .....	V
Zero-Trust-Roadmap .....	50
Zielbild .....	53
ZTNA .....	16, 35
Zugangsdaten .....	2
Zugriffskontrolle .....	16
Zugriffsmodell .....	14

# Mehr von Brain-Media.de



## **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

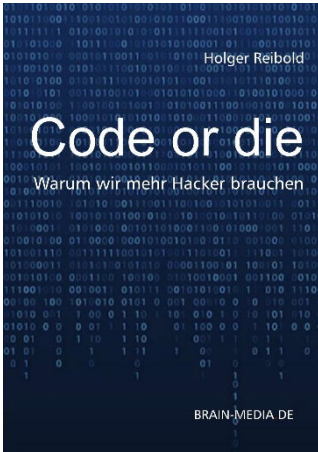
Erscheint: 42. März 2026



## **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.



## Code or die – Warum wir mehr Hacker brauchen

Ein Manifest für mehr digitale Selbstbestimmung, Neugierde und Eigenverantwortung. Medienkompetenzen alleine genügen nicht; die Gesellschaft von morgen braucht Digitalkompetenzen.

Umfang: 120 Seiten

Preis: 19,99 EUR

Erscheint Frühjahr 2026



## Lokale KI – Sichere Architektur, Betrieb und Governance von GenAI- und RAG-Systemen

RAG- und LLM-Plattformen mit klarer Architektur, Guardrails, Monitoring und Governance kontrolliert und resilient betreiben.

Umfang: 270 Seiten

Preis: 29,99 EUR



## Knowledge as a Service

**Personal**  
**Business**  
**Enterprise**

IT-Security, Compliance und KI entwickeln sich schneller als jedes gedruckte Buch. Um dieser Dynamik Rechnung zu tragen, hat Brain-Media.de **KaaS – Knowledge as a Service** entwickelt.

Mit KaaS erhalten Sie ein lebendes **Wissenssystem**: Alle Titel als PDF/E-Book, **regelmäßig aktualisierte Living Documents** sowie **exklusive Downloads** – Checklisten, Vorlagen und sofort einsetzbare Templates.

Speziell für **Regulierung und Audits**: Inhalte zu NIS-2, DORA, CRA & AI Act werden laufend gepflegt und helfen Ihnen, Anforderungen strukturiert umzusetzen und auditfähig zu bleiben. Für fortgeschrittene Nutzung stehen Inhalte zusätzlich als **Markdown- und JSON-Rohdaten** bereit – ideal für die Automatisierung und Integration in Ihre Umgebungen.

KaaS ist die wachsende **Bibliothek für**  
**Praxis, Compliance und Resilienz.**