

Holger Reibold

# Cyber Exposure Management

CTEM-Framework für moderne

Cybersecurity: Angriffsflächen

erkennen, priorisieren und reduzieren

BRAIN-MEDIA.DE

Holger Reibold

# Cyber Exposure Management

CTEM-Framework für moderne  
Cybersecurity: Angriffsflächen  
erkennen, priorisieren und  
reduzieren

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: 978-3-95444-337-6

Cover: ESA

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
1 Paradigmenwechsel.....	5
1.1 Grenzen klassischer Sicherheitsprogramme.....	7
1.2 Warum Schwachstellenlisten keine Sicherheit erzeugen .....	10
1.3 Attack Surface vs. Cyber Exposure .....	13
1.4 Entstehung des CTEM-Konzepts .....	17
1.5 Warum CTEM zum neuen Standard wird.....	20
1.6 Management Summary .....	23
2 Die neue Realität der Angriffsflächen.....	25
2.1 Ausweitung digitaler Angriffsflächen .....	26
2.2 Cloud, SaaS und Schatten-IT als Risiko-Multiplikatoren.....	29
2.3 Remote Work und verteilte Infrastrukturen .....	32
2.4 Identitäten und Fehlkonfigurationen.....	36
2.5 Warum Unternehmen CTEM brauchen .....	39
2.6 Management Summary .....	42
3 Das CTEM-Framework im Detail .....	43
3.1 Die Phasen des CTEM-Zyklus .....	45

3.2	Abgrenzung zu Pentests und Audits .....	48
3.3	Rollen und Verantwortlichkeiten .....	50
3.4	Erfolg messbar machen: KPIs .....	53
3.5	Integration in Sicherheitsprogramme.....	55
3.6	Management Summary .....	60
4	Scoping – Fokus aufs Wesentliche .....	61
4.1	Identifikation geschäftskritischer Assets .....	62
4.2	Einbindung der Business-Impact-Analyse.....	65
4.3	Stakeholder und Risikoentscheidungen .....	67
4.4	Typische Scoping-Fehler vermeiden .....	70
4.5	Mapping der digitalen Angriffsfläche .....	73
4.6	Management Summary .....	76
5	Discovery – Sichtbarkeit schaffen.....	77
5.1	External Attack Surface Management .....	78
5.2	Interne Exposures hybrider Umgebungen .....	81
5.3	Supply-Chain-Risiken .....	84
5.4	Kontinuierliches Monitoring .....	87
5.5	Konsolidierung von Sicherheitsdaten.....	89
5.6	Management Summary .....	93
6	Priorisierung – Risiken richtig bewerten .....	95
6.1	Warum CVSS allein nicht ausreicht .....	96

6.2	Kontextualisierung.....	99
6.3	Bewertung des Business-Schadens .....	102
6.4	Angriffspfade statt Einzelfunde .....	105
6.5	Fokus auf High-Risk-Exposures .....	107
6.6	Management Summary .....	110
7	Validierung – Sicherheitskontrollen überprüfen.....	111
7.1	Continuous Security Validation.....	112
7.2	Breach- and Attack-Simulation.....	114
7.3	Automatisierte Tests vs. Red Teaming .....	118
7.4	False Positives reduzieren.....	121
7.5	Lernzyklen für Security-Operations-Teams .....	124
7.6	Management Summary .....	127
8	Operationalisierung – Vom Risiko zur Maßnahme .....	129
8.1	Effiziente Remediation-Prozesse etablieren .....	130
8.2	Kooperation: Security und IT-Operations.....	134
8.3	Kompensationsmaßnahmen .....	136
8.4	Automatisierung .....	139
8.5	Reporting für Management und Vorstand .....	142
8.6	Management Summary .....	145
9	Technologie und Tool-Auswahl.....	147
9.1	Technologien für Exposure Management.....	148

9.2	Exposure-Management-Plattformen.....	151
9.3	Build vs. Buy – Architekturentscheidungen.....	154
9.4	APIs und Integration in Security-Stacks .....	156
9.5	Auswahlkriterien für Anbieter.....	159
9.6	Management Summary .....	162
10	Implementierungshürden.....	163
10.1	Kulturelle Hürden in IT-Organisationen .....	164
10.2	Datenqualität und Tool-Fragmentierung.....	167
10.3	Budgetierung und Ressourcenplanung.....	170
10.4	Compliance-Anforderungen .....	172
10.5	Vom Pilotprojekt zum Rollout.....	175
10.6	Management Summary .....	177
11	Zukunft des Exposure Managements.....	179
11.1	Predictive Security und Threat Intelligence .....	180
11.2	CTEM als Teil der Zero-Trust-Architektur.....	182
11.3	Autonomes Cyber-Risikomanagement .....	185
11.4	Die Rolle des CISO als Business-Enabler .....	188
11.5	Strategischer Ausblick .....	190
11.6	Management Summary .....	193
	Zum Schluss .....	195
	Anhang.....	VII

CTEM-Reifegradmodell zur Selbsteinschätzung .....	VII
Checklisten für die fünf CTEM-Phasen .....	XI
Weitere Hilfsmittel.....	XV
Glossar .....	XVII
Abkürzungsverzeichnis.....	XXI
Literatur- und Quellenverzeichnis .....	XXIII
Stichwortverzeichnis .....	XXVI
Mehr von Brain-Media.de .....	XXX



# Vorwort

*Das Ende der punktuellen Sicherheit.*

Warum klassische Sicherheitsansätze nicht mehr ausreichen und weshalb kontinuierliches Exposure Management zum neuen Standard moderner Cybersecurity wird.

Über viele Jahre folgte Cybersecurity einem klaren und scheinbar logischen Muster: Systeme wurden regelmäßig überprüft, Schwachstellen identifiziert und anschließend behoben. Vulnerability Scans, Penetrationstests und Audits galten als zentrale Instrumente, um den Sicherheitszustand einer Organisation zu bewerten. Diese Maßnahmen lieferten Momentaufnahmen der IT-Sicherheit – wertvoll, aber letztlich statisch.

Doch die Realität moderner IT-Landschaften hat sich grundlegend verändert.

Digitale Infrastrukturen sind heute dynamisch, verteilt und hochgradig komplex. Cloud-Plattformen, hybride Architekturen, Software-as-a-Service, Container-Umgebungen und eine ständig wachsende Zahl vernetzter Systeme sorgen dafür, dass sich Angriffsflächen kontinuierlich verändern. Neue Assets entstehen, Konfigurationen werden angepasst, Identitäten erhalten zusätzliche Berechtigungen und

externe Schnittstellen werden geschaffen – oft schneller, als klassische Sicherheitsprozesse Schritt halten können.

Hinzu kommt, dass Angreifer längst nicht mehr nur einzelne Schwachstellen ausnutzen. Moderne Angriffe entstehen aus der Kombination vieler Faktoren: Fehlkonfigurationen, überprivilegierte Identitäten, exponierte Dienste, ungepatchte Systeme oder unsichere Integrationen entlang der digitalen Lieferkette. Erst die Zusammenführung dieser Elemente schafft reale Angriffswege.

Die Folge ist ein grundlegendes Problem: Traditionelle Sicherheitsmethoden konzentrieren sich meist auf einzelne Schwachstellen, während Angreifer in Zusammenhängen denken.

Genau hier setzt ein neuer Ansatz an, der in den letzten Jahren zunehmend an Bedeutung gewonnen hat: Cyber Exposure Management.

Statt isolierte Schwachstellen zu betrachten, richtet Exposure Management den Blick auf die tatsächliche Angriffsfläche einer Organisation und bewertet Risiken im Kontext ihrer realen Ausnutzbarkeit und ihres potenziellen geschäftlichen Schadens. Entscheidend ist dabei nicht nur, ob eine Schwachstelle existiert, sondern ob sie in einem realistischen Angriffsszenario tatsächlich ausgenutzt werden kann und welche Auswirkungen dies auf kritische Geschäftsprozesse hätte.

Aus dieser Perspektive ist Sicherheit kein statischer Zustand mehr, sondern ein kontinuierlicher Prozess.

Mit dem Konzept des Continuous Threat Exposure Management (CTEM) hat sich ein strukturiertes Framework etabliert, das genau diesen kontinuierlichen Ansatz verfolgt. CTEM beschreibt einen fortlaufenden Zyklus aus fünf Phasen: Scoping, Discovery, Priorisierung, Validierung und Mobilisierung. Das Ziel ist es, die tatsächlichen Risiken innerhalb der digitalen Angriffsfläche sichtbar zu machen, ihre Bedeutung für das Unternehmen zu bewerten und geeignete Maßnahmen zur Risikoreduktion einzuleiten.

Der entscheidende Unterschied zu klassischen Sicherheitsprogrammen liegt dabei in der Perspektive: CTEM betrachtet die Organisation konsequent aus Sicht eines potenziellen Angreifers. Welche Systeme sind sichtbar? Welche Konfigurationen eröffnen Angriffsmöglichkeiten? Welche Kombination von Schwachstellen könnte zu einem erfolgreichen Angriff führen?

Diese Sichtweise verändert nicht nur die technische Analyse, sondern auch die Art und Weise, wie Organisationen Sicherheit steuern. Anstatt tausende Einzelfunde zu verwalten, rückt die Priorisierung realer Risiken in den Mittelpunkt. Sicherheitsmaßnahmen werden stärker an geschäftlichen Auswirkungen ausgerichtet, und Security-Teams arbeiten enger mit IT-Betrieb, Risiko-Management und Unternehmensführung zusammen.

Dieses Buch soll einen praxisnahen Einstieg in das Konzept des Cyber Exposure Management bieten und zeigen, wie sich das CTEM-Framework in modernen Organisationen anwenden lässt. Es richtet sich an Sicherheitsverantwortliche, IT-Architekten, Risiko-Manager

und Entscheidungsträger, die ihre Sicherheitsstrategie an die veränderten Realitäten digitaler Infrastrukturen anpassen möchten.

Dabei geht es nicht nur um Technologien oder einzelne Tools. Im Mittelpunkt steht vielmehr die Frage, wie Organisationen ihre Angriffsflächen systematisch verstehen, Risiken sinnvoll priorisieren und Sicherheitsmaßnahmen kontinuierlich verbessern können.

Cybersecurity ist heute weniger eine Frage einzelner Sicherheitslösungen als vielmehr eine Frage der richtigen Perspektive.

Wer Sicherheit nur punktuell betrachtet, reagiert zwangsläufig zu spät. Wer hingegen kontinuierlich versteht, wo reale Risiken entstehen, kann Angriffe verhindern, bevor sie stattfinden.

Cyber Exposure Management markiert daher nicht nur eine neue Methodik – sondern einen grundlegenden Wandel im Denken über Sicherheit.

Ich wünsche Ihnen bei diesem Paradigmenwechsel viel Erfolg!

Herzlichst

Holger Reibold

# 1 Paradigmenwechsel

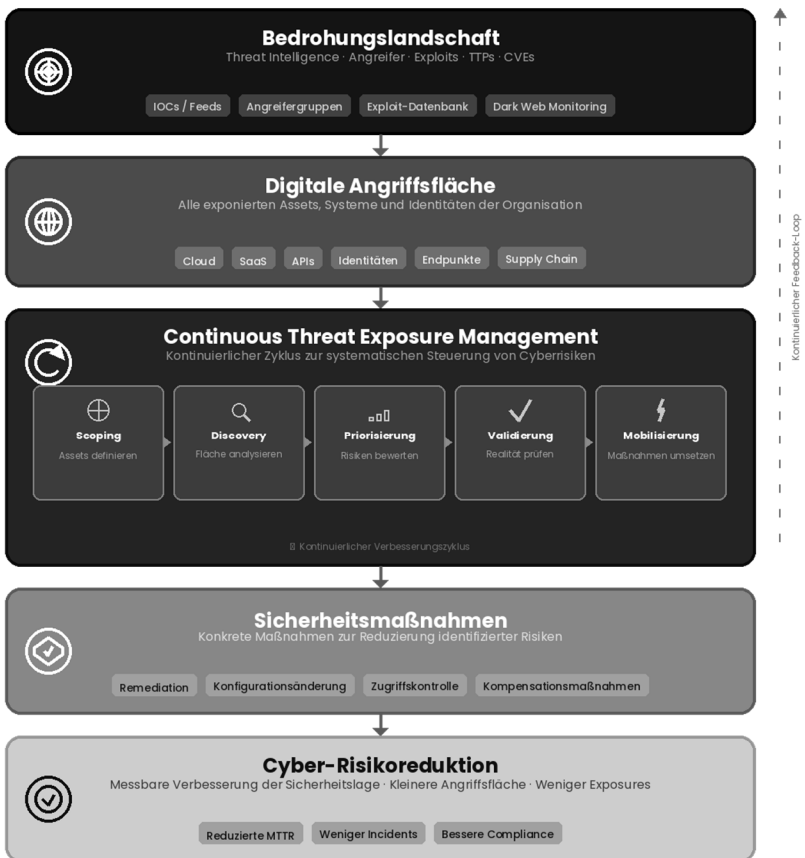
*Schwachstellenlisten stoppen keine Angreifer. Cybersecurity braucht ein neues Denken.*

Die Art und Weise, wie Organisationen ihre IT-Sicherheit bewerten und steuern, befindet sich in einem grundlegenden Wandel. Über viele Jahre stand das klassische Vulnerability Management im Mittelpunkt der Sicherheitsstrategie. Regelmäßige Scans identifizierten Schwachstellen, Sicherheitslücken wurden priorisiert und anschließend behoben. Dieses Vorgehen war lange Zeit ein wichtiger Bestandteil moderner Cyberabwehr.

Doch mit der zunehmenden Digitalisierung von Geschäftsprozessen hat sich die technologische Landschaft massiv verändert. Cloud-Infrastrukturen, hybride Architekturen, SaaS-Plattformen und verteilte Identitätsmodelle sorgen dafür, dass sich Angriffsflächen ständig erweitern und verändern. Sicherheitsrisiken entstehen heute nicht mehr ausschließlich durch einzelne Softwarelücken, sondern häufig durch komplexe Kombinationen aus Fehlkonfigurationen, exponierten Diensten, überprivilegierten Identitäten und miteinander verknüpften Systemen.

Klassische Sicherheitsprogramme stoßen unter diesen Bedingungen zunehmend an ihre Grenzen. Sie liefern umfangreiche Listen von

Schwachstellen, bieten jedoch oft nur begrenzte Aussagekraft darüber, welche dieser Funde tatsächlich ein relevantes Risiko für das Unternehmen darstellen.



**Das Gesamtmodell des Cyber Exposure Management zeigt, wie Organisationen ihre Angriffsfläche analysieren, Risiken priorisieren und Sicherheitsmaßnahmen kontinuierlich steuern.**

Genau hier setzt ein neuer Ansatz an: Exposure Management. Anstatt isolierte Schwachstellen zu betrachten, richtet dieser Ansatz den Fokus auf reale Angriffswege und die tatsächliche Ausnutzbarkeit von Sicherheitslücken. Mit dem Konzept des Continuous Threat Exposure Management (CTEM) entsteht damit ein Framework, das Sicherheit als kontinuierlichen, kontextbasierten Prozess versteht.

## 1.1 Grenzen klassischer Sicherheitsprogramme

Über viele Jahre bildeten klassische Sicherheitsprogramme die Grundlage der IT-Sicherheit in Unternehmen. Vulnerability Management, regelmäßige Schwachstellenscans, Penetrationstests sowie Compliance-Audits galten als zentrale Instrumente, um Sicherheitslücken zu identifizieren und Risiken zu reduzieren. Der grundlegende Ansatz war dabei vergleichsweise klar strukturiert: Schwachstellen werden entdeckt, bewertet und anschließend behoben.

Dieses Modell funktionierte in einer Zeit, in der IT-Infrastrukturen weitgehend stabil, zentralisiert und überschaubar waren. Unternehmensnetzwerke bestanden aus klar definierten Systemlandschaften, Anwendungen liefen überwiegend im eigenen Rechenzentrum, und Veränderungen an der Infrastruktur erfolgten in kontrollierten und relativ langsamen Zyklen. Sicherheitsüberprüfungen in regelmäßigen Intervallen konnten daher ein realistisches Bild der Sicherheitslage liefern.

Mit der fortschreitenden Digitalisierung hat sich diese Situation jedoch grundlegend verändert. Moderne IT-Umgebungen sind dynamisch, verteilt und stark automatisiert. Cloud-Plattformen, Container-Umgebungen, DevOps-Prozesse und Software-as-a-Service-Lösungen führen dazu, dass neue Systeme, Dienste und Konfigurationen in sehr kurzen Zeitabständen entstehen. Gleichzeitig greifen Mitarbeiter, Partner und Kunden über unterschiedlichste Geräte und Netzwerke auf Unternehmensressourcen zu.

In dieser dynamischen Umgebung stoßen klassische Sicherheitsprogramme zunehmend an ihre Grenzen. Viele Sicherheitsprozesse sind noch immer auf punktuelle Prüfungen ausgelegt – beispielsweise durch periodische Schwachstellenscans oder jährliche Penetrationstests. Diese liefern zwar wertvolle Erkenntnisse, stellen jedoch immer nur eine Momentaufnahme der Sicherheitslage dar. Bereits kurze Zeit nach einer solchen Prüfung können neue Systeme online gehen, Konfigurationen geändert oder zusätzliche Schnittstellen geschaffen worden sein.

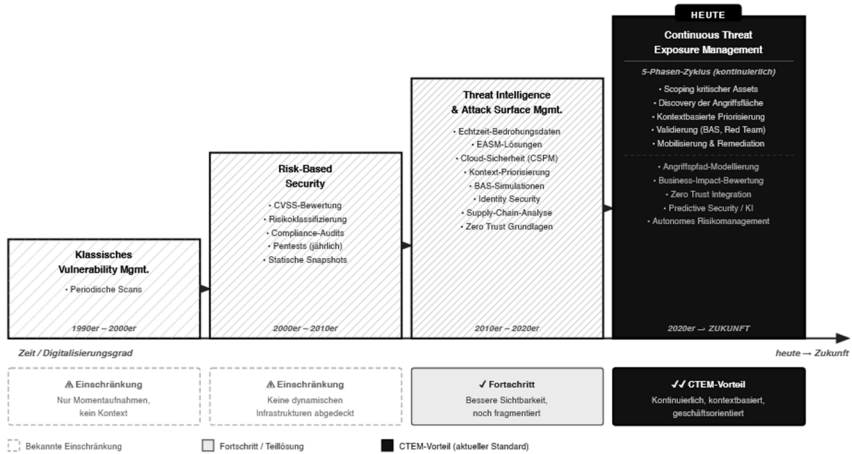
Ein weiteres Problem besteht darin, dass traditionelle Sicherheitsprogramme häufig eine sehr große Anzahl einzelner Schwachstellen identifizieren. In komplexen IT-Umgebungen können Vulnerability-Scanner schnell tausende oder sogar zehntausende Funde generieren. Für Security-Teams entsteht dadurch eine enorme Menge an Arbeit, während gleichzeitig unklar bleibt, welche dieser Schwachstellen tatsächlich ein relevantes Risiko darstellen.

Hinzu kommt, dass viele Sicherheitsprogramme Schwachstellen isoliert betrachten. Eine einzelne Sicherheitslücke mag für sich genommen nur ein moderates Risiko darstellen. In Kombination mit anderen Schwachstellen, Fehlkonfigurationen oder überhöhten Zugriffsrechten kann sie jedoch Teil eines realistischen Angriffspfads werden. Klassische Schwachstellenbewertungen erfassen diese Zusammenhänge häufig nur unzureichend.

Auch organisatorisch stoßen traditionelle Ansätze an Grenzen. Sicherheits-Teams konzentrieren sich oft auf die Verwaltung von Schwachstellenlisten und Patch-Zyklen, während gleichzeitig die Kommunikation mit IT-Betrieb, Entwicklungsteams und dem Management komplexer wird. Ohne eine klare Priorisierung realer Risiken fällt es schwer, Ressourcen gezielt einzusetzen und Sicherheitsmaßnahmen mit geschäftlichen Anforderungen in Einklang zu bringen.

Diese Herausforderungen zeigen deutlich, dass die reine Identifikation von Schwachstellen heute nicht mehr ausreicht, um den Sicherheitszustand einer Organisation realistisch zu bewerten. Moderne Cybersecurity erfordert einen Ansatz, der dynamische Infrastrukturen berücksichtigt, reale Angriffsszenarien einbezieht und Sicherheitsrisiken im Kontext ihrer tatsächlichen Ausnutzbarkeit bewertet.

Genau an diesem Punkt beginnt der Übergang vom klassischen Vulnerability Management hin zum Exposure Management.



**Die Entwicklung der Cybersecurity zeigt den Wandel von punktuellen Schwachstellenanalysen hin zu kontinuierlichem Exposure Management in dynamischen IT-Umgebungen (Quelle: Gartner 2022).**

## 1.2 Warum Schwachstellenlisten keine Sicherheit erzeugen

In vielen Organisationen bildet die Liste identifizierter Schwachstellen noch immer den zentralen Bezugspunkt für Sicherheitsentscheidungen. Vulnerability-Scanner liefern regelmäßig Berichte mit detaillierten Informationen über bekannte Sicherheitslücken in Betriebssystemen, Anwendungen oder Netzwerkdiensten. Diese Ergebnisse werden anschließend priorisiert, in Ticket-Systeme überführt und schrittweise abgearbeitet.

# Stichwortverzeichnis

## A

Angriffsfläche	5
Angriffspfad	105
API	27, 157
Application Programming Interface	157
Arbeitsmodell	32
Attack Surface	13
Automatisierung	139
Autonome Sicherheitsarchitektur	186

## B

BAS	114
Bewertung	103
BIA	65
Breach- and Attack-Simulation	114
Breach-and-Attack-Simulation	47
Business-Impact-Analyse	65

## C

Chief Information Security Officer	51
CISO	51
Cloud	5, 20
Cloud Security	21
Cloud Security Posture Management	149
Cloud Workload Protection Plattform	149
CMDB	63
Common Vulnerability Scoring System	96
Compliance	172
Compliance-Audit	7
Configuration-Management- Datenbank	63
Continuous Security Validation	112
Continuous Threat Exposure Management	17
Crown Jewel	106
CSPM	149
CSV	112

CTEM	17, 18
CTEM-Zyklus	45
CVSS	96
CWPP	149
Cyber Exposure	13
Cyber Exposure Management	13
Cybersecurity	9

## D

Datenkonsolidierung	91
Datenqualität	168
DevOp	27
Discovery	46, 77
DORA	40
Dynamik	27

## E

EASM	74, 78
External Attack Surface	
Management	74, 78

## F

False Positive	122
Firewall	33
Fragmentierung	169
Framework	43

## G

Gartner	18
Governance, Risk and	
Compliance	58
GRC	58

## H

Heimrouter	33
High-Risk-Exposure	108

## I

IaaS	29
Identität	36
Identity-Management	58
Infrastructure-as-a-Service	29
Innovation	25
Intrusion-Detection-System	33
Inventarisierung	28
IT-Infrastruktur	7
IT-Sicherheit	5

## K

Kennzahl	53
Key Performance Indicator	53, 143
Key Risk Indicator	143
Kompensation	136

Konsolidierung	90
Kontextualisierung	101
KPI	53, 143
KRI	143
Kulturelle Hürde	164

## L

Lernzyklus	124
------------	-----

## M

Management	12
Mapping	73
Mean Time to Remediate	54
MITRE ATT&CK	115
Monitoring	87
MTTR	54

## N

NIS-2	40
-------	----

## O

Operationalisierung	129
---------------------	-----

## P

PaaS	29
Patch	9

Penetrationstest	7, 48
Pilotprojekt	175
Platform-as-a-Service	29
Predictive Security	180
Priorisierung	46, 95
Public Cloud	26

## R

Recovery Point Objective	66
Recovery Time Objective	66
Red Teaming	119
Red-Teaming	47
Reifegradmodell	VII
Remediation	47, 130
Remote Work	32
Reporting	142
Risikoreduktion	21
Rollout	175
RPO	66
RTO	66

## S

SaaS	5, 30
Schatten-IT	31
Schwachstelle	9
Schwachstellenscan	7
Scoping	45, 61

Security Information and Event Management ----- 115

Security Operations Center ----- 58

Security-Alert----- 39

Security-Orchestration-, Automation- and Response 140

Security-Team----- 11

Sicherheits-Audit----- 49

Sicherheitsstrategie ----- 32

SIEM----- 17, 115

SOAR----- 140

SOC----- 58

Social-Engineering-Angriff---- 119

Software-as-a-Service ----- 30

Stakeholder ----- 68

Supply-Chain-Risiko----- 84

**T**

Technologie----- 147

Threat Intelligence ----- 21

Transparenz----- 31, 165

**U**

ulnerability Management----- 5

**V**

Validierung ----- 47

VPN ----- 33

Vulnerability-Scanner - 10, 17, 121

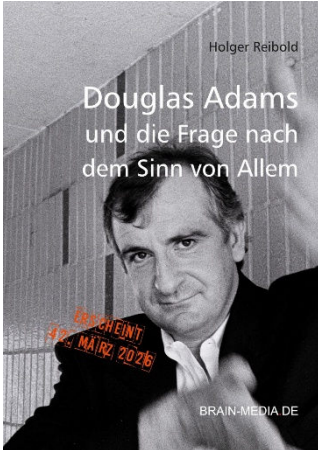
**W**

Webservice ----- 27

WLAN ----- 33

**Z**

Zero-Trust-Architektur ----- 182



## **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

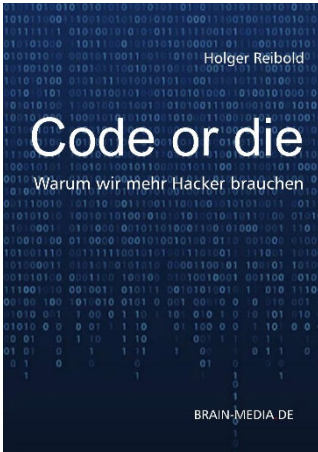
Erscheint: 42. März 2026



## **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: 14,99 EUR

Erscheint Frühjahr 2026

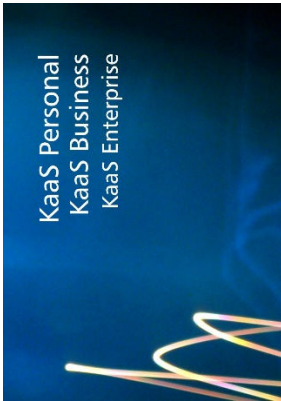


## Lokale KI – Sichere Architektur, Betrieb und Governance von GenAI- und RAG-Systemen

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

Umfang: 270 Seiten

Preis: 24,99 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.**