Holger Reibold

# Ranomware-Resilienz

## Wie Unternehmen Angriffe überstehen – mit Architektur, Backups und einem 72-Stunden-Plan

BRAIN-MEDIA.DE

Holger Reibold

# Ransomware-Resilienz

## Wie Unternehmen Angriffe überstehen – mit Architektur, Backups und einem 72-Stundenplan

BRAIN-MEDIA.DE

ISBN: 978-3-95444-322-2

Cover: Freepik

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

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

# Inhaltsverzeichnis

# Vorwort – das Scheitern klassischer IT-Security

Ransomware ist kein technisches Problem mehr. Sie ist ein Organisations-, Führungs- und Entscheidungsproblem. Trotzdem reagieren viele Unternehmen noch immer so, als ließe sich diese Bedrohung mit dem nächsten Tool, der nächsten Richtlinie oder dem nächsten Audit „lösen". Firewalls werden erneuert, Endpoint-Produkte ausgetauscht, Awareness-Schulungen durchgeführt – und dennoch stehen selbst gut aufgestellte Organisationen regelmäßig vor verschlüsselten Systemen, gestohlenen Daten und existenziellen Entscheidungen unter massivem Zeitdruck.

Der Grund dafür ist unbequem, aber klar: Die klassische IT-Security basiert auf einer Annahme, die nicht mehr trägt. Sie geht davon aus, dass Angriffe verhindert werden können, wenn nur genug investiert, kontrolliert und reguliert wird. Die Realität zeigt jedoch etwas anderes. Moderne Angriffe umgehen technische Schutzmaßnahmen, nutzen legitime Zugänge, kompromittieren Dienstleister und bewegen sich unauffällig durch Netzwerke, bis der eigentliche Schaden entsteht. In diesem Moment ist Prävention vorbei – und Resilienz entscheidet.

Dieses Buch stellt deshalb bewusst eine andere Frage. Nicht: Wie verhindern wir jeden Angriff?

Sondern: Wie überstehen wir einen Angriff, ohne handlungsunfähig zu werden?

Resilienz bedeutet in diesem Kontext nicht, Sicherheitsmaßnahmen zu vernachlässigen. Sie bedeutet, die eigene Organisation darauf vorzubereiten, dass Schutzmaßnahmen versagen können – und trotzdem kontrolliert zu reagieren. Dazu gehören funktionierende Backups, die tatsächlich wiederherstellbar sind. Eine Architektur, die Angriffe begrenzt, statt sie zu beschleunigen. Früherkennung, die Signale liefert, bevor der Schaden maximal ist. Und vor allem: klare Entscheidungsstrukturen, wenn Zeit, Informationen und Nerven knapp sind.

Viele der schwersten Schäden nach Ransomware-Angriffen entstehen nicht durch die Technik selbst, sondern durch Unsicherheit: Wer darf jetzt entscheiden? Zahlen oder nicht zahlen? Abschalten oder weiterlaufen lassen? Wen informieren wir – und wann? Unternehmen scheitern nicht, weil sie keine Tools haben, sondern weil sie im entscheidenden Moment keinen Plan besitzen, der auch unter Stress funktioniert.

Dieses Buch richtet sich daher nicht nur an IT-Abteilungen, sondern ausdrücklich an Entscheiderinnen und Entscheider. An Geschäftsführungen, Bereichsleitungen, Sicherheitsverantwortliche und alle, die im Ernstfall Verantwortung tragen. Es verbindet

technische Grundlagen mit organisatorischer Realität, rechtlichen Rahmenbedingungen und psychologischen Faktoren, die in Krisen oft unterschätzt werden.

Der Fokus liegt dabei konsequent auf Umsetzbarkeit. Keine theoretischen Idealmodelle, keine herstellergetriebenen Versprechen, keine Checklisten ohne Kontext. Stattdessen eine Architektur des Überlebens: Was muss vorhanden sein, damit ein Unternehmen auch nach einem erfolgreichen Angriff weiterarbeiten kann? Welche Abhängigkeiten sind kritisch? Und was muss in den ersten 72 Stunden passieren, um irreversible Schäden zu vermeiden?

Wenn Sie dieses Buch lesen, werden Sie feststellen: Absolute Sicherheit gibt es nicht. Aber Handlungsfähigkeit ist gestaltbar. Resilienz ist keine Eigenschaft von Software – sie ist eine Eigenschaft von Organisationen.

Dieses Buch soll Ihnen helfen, diese Eigenschaft bewusst aufzubauen.

Herzlichst

Holger Reibold

# Hinweis zur Nutzung dieses Buches

Dieses Buch wurde bewusst nicht als lineares Lehrbuch konzipiert, das von der ersten bis zur letzten Seite in fester Reihenfolge gelesen werden muss. Ransomware betrifft unterschiedliche Rollen in einer Organisation auf unterschiedliche Weise – und nicht jeder Leser benötigt dieselbe Tiefe zu denselben Themen. Um dieser Realität gerecht zu werden, bietet dieses Buch zwei empfohlene Lesepfade.

Der erste Lesepfad richtet sich an Entscheider: Geschäftsführungen, Vorstände, Bereichsleitungen sowie alle Personen, die im Ernstfall Verantwortung tragen, ohne täglich tief in technischen Details zu arbeiten. Dieser Pfad konzentriert sich auf strategische Zusammenhänge, Haftungsfragen, wirtschaftliche Auswirkungen und Entscheidungslogiken unter Zeitdruck. Er vermittelt das notwendige Verständnis, um Risiken realistisch einzuordnen, Prioritäten zu setzen und im Krisenfall handlungsfähig zu bleiben – ohne sich in technischen Einzelheiten zu verlieren.

Empfohlener Lesepfad für Entscheider:

Kapitel 1, 3, 4, 5, 9, 10 und 12 sowie der NIS-2 Quick-Check im Anhang.

Der zweite Lesepfad richtet sich an technisch Verantwortliche: IT-Leitungen, Administratoren, Security-Verantwortliche sowie externe Dienstleister. Dieser Pfad geht deutlich tiefer auf Architekturentscheidungen, Backup-Strategien, Segmentierung, Früherkennung und operative Incident-Response-Maßnahmen ein. Er setzt technisches Grundverständnis voraus und legt den Fokus auf konkrete Umsetzbarkeit, Abhängigkeiten und typische Fehlerquellen in realen Umgebungen.

Empfohlener Lesepfad für technische Vertiefung:

Kapitel 6, 7, 8, 9, 10 und 11 sowie der Anhang mit Checklisten, Vorlagen und Praxisartefakten.

Beide Lesepfade überschneiden sich bewusst in zentralen Kapiteln, insbesondere dort, wo Technik, Organisation und Führung untrennbar zusammenwirken. Ransomware-Resilienz ist keine rein technische Disziplin und keine reine Managementaufgabe – sie entsteht dort, wo beide Perspektiven zusammenfinden. Dieses Buch ist so aufgebaut, dass es genau diese Verbindung unterstützt.

# 1 Der Mythos der 100-%-Sicherheit

Die Vorstellung vollständiger Sicherheit hält sich hartnäckig. Sie prägt Investitionsentscheidungen, Audits, Strategiepapiere und nicht zuletzt das Sicherheitsgefühl vieler Organisationen. Wenn nur genug Firewalls installiert, Richtlinien formuliert und Schulungen durchgeführt werden, so die Annahme, ließen sich Cyberangriffe verhindern. Ransomware zeigt jedoch seit Jahren, dass dieses Sicherheitsversprechen nicht mehr haltbar ist.

Moderne Angriffe scheitern selten an fehlender Technik. Sie scheitern an falschen Annahmen. Angreifer nutzen keine exotischen Zero-Day-Exploits, sondern legitime Zugänge, kompromittierte Identitäten und menschliche Routinen. Sie bewegen sich innerhalb der vorgesehenen Systeme, oft über Wochen oder Monate, ohne Aufmerksamkeit zu erregen. Wenn der Angriff sichtbar wird, ist der eigentliche Schaden bereits entstanden. In diesem Moment spielt es keine Rolle mehr, wie gut die Prävention gedacht war – sondern nur, wie vorbereitet die Organisation ist.

Dieses Kapitel setzt genau an diesem Punkt an. Es stellt die Frage, warum Prävention allein statistisch versagt, obwohl Budgets steigen und Sicherheitsmaßnahmen zunehmen. Es zeigt, weshalb der Mensch nicht „das schwächste Glied", sondern ein struktureller Bestandteil jedes Systems ist – und warum genau darin das

eigentliche Risiko liegt. Vor allem aber führt es in ein Denkmodell ein, das für den Umgang mit Ransomware entscheidend ist: Assume Breach.

Assume Breach bedeutet nicht, Angriffe zu akzeptieren oder Sicherheitsmaßnahmen zu vernachlässigen. Es bedeutet, die Möglichkeit eines erfolgreichen Angriffs realistisch einzuplanen und daraus Konsequenzen abzuleiten. Wer davon ausgeht, dass Schutzmaßnahmen versagen können, plant anders: Backups werden nicht nur erstellt, sondern getestet. Netzwerke werden nicht nur geschützt, sondern so gebaut, dass Schäden begrenzt bleiben. Entscheidungen werden nicht improvisiert, sondern vorbereitet.

Damit verschiebt sich auch die Verantwortung. Resilienz ist keine rein technische Eigenschaft und keine Aufgabe der IT-Abteilung allein. Sie ist eine Führungsaufgabe. Geschäftsführungen und Leitungen entscheiden darüber, ob Handlungsfähigkeit im Krisenfall vorhanden ist – oder ob Organisationen erst dann beginnen, Fragen zu stellen, wenn Zeit und Optionen bereits knapp sind.

Dieses Kapitel legt das Fundament für alles Weitere. Es ersetzt die Illusion absoluter Sicherheit durch ein realistischeres Ziel: kontrollierte Handlungsfähigkeit unter widrigen Bedingungen. Erst auf dieser Grundlage lassen sich Architektur, Prozesse und Krisenpläne sinnvoll gestalten.


**Der Mythos der 100prozentigen Sicherheit: Steigende Präventionsmaßnahmen reduzieren die Angriffsfläche, aber nicht das Gesamtrisiko. Moderne Angriffe durchbrechen technische Schutzmechanismen systematisch. Sicherheit erzeugt Kontrolle – Resilienz erzeugt Handlungsfähigkeit.**

## 1.1 Warum Prävention statistisch versagt

Prävention ist seit Jahrzehnten das dominierende Paradigma der IT-Sicherheit. Firewalls, Virenscanner, Intrusion-Detection-Systeme, Richtlinien, Schulungen und Audits verfolgen ein gemeinsames Ziel: Angriffe sollen verhindert werden, bevor sie Schaden anrichten. Dieses Ziel ist nachvollziehbar – und dennoch zeigt die Realität, dass es zunehmend verfehlt wird. Nicht, weil Prävention

grundsätzlich wirkungslos wäre, sondern weil sie systematisch überschätzt wird.

Statistische Auswertungen der vergangenen Jahre zeigen ein konsistentes Bild: Ein Großteil der Unternehmen, die von Ransomware betroffen sind, verfügte zum Zeitpunkt des Angriffs über aktuelle Sicherheitslösungen, dokumentierte Prozesse und regelmäßige Awareness-Maßnahmen. Trotzdem kam es zur Kompromittierung. Der Grund dafür liegt nicht in individueller Nachlässigkeit, sondern in strukturellen Grenzen präventiver Sicherheitsmodelle.

Moderne Angriffe zielen nicht primär auf technische Schwachstellen, sondern auf Normalbetrieb. Phishing-Mails nutzen legitime Kommunikationswege. Gestohlene Zugangsdaten ermöglichen Anmeldungen über reguläre Authentifizierungsmechanismen. Remote-Zugänge, VPNs oder Cloud-Konten werden nicht „gehackt", sondern missbraucht. Aus Sicht der Systeme verhält sich der Angreifer oft korrekt. Präventive Maßnahmen, die auf bekannte Muster oder Regelverstöße reagieren, greifen hier zu spät oder gar nicht.

Hinzu kommt die zunehmende Komplexität von IT-Landschaften. Hybride Infrastrukturen, Cloud-Dienste, externe Dienstleister und mobile Arbeitsplätze erweitern die Angriffsfläche kontinuierlich. Jede zusätzliche Schnittstelle, jede Identität und jede Abhängigkeit erhöht die Wahrscheinlichkeit, dass ein Angreifer einen Weg

findet, der nicht vollständig abgesichert ist. Prävention skaliert schlecht mit Komplexität: Je mehr geschützt werden muss, desto größer wird die Zahl der Annahmen, die gleichzeitig korrekt sein müssen.

Ein weiterer Faktor ist Zeit. Präventive Sicherheitsmaßnahmen reagieren häufig verzögert. Signaturbasierte Systeme erkennen nur, was bereits bekannt ist. Neue Angriffsmuster, legitime Tools oder leicht angepasste Schadsoftware bewegen sich oft wochenlang unterhalb von Erkennungsschwellen. Währenddessen verschaffen sich Angreifer Persistenz, erweitern ihre Zugriffsrechte und kartieren die Umgebung. Wenn der Angriff schließlich sichtbar wird, hat Prävention ihre Wirkung bereits verloren.

Auch menschliches Verhalten entzieht sich präventiver Kontrolle. Schulungen können sensibilisieren, aber sie eliminieren keine Fehler. Stress, Zeitdruck, Routine und soziale Dynamiken führen dazu, dass selbst gut informierte Mitarbeitende auf manipulierte Inhalte reagieren. Entscheidend ist dabei nicht individuelles Fehlverhalten, sondern die statistische Gewissheit, dass in jeder größeren Organisation früher oder später ein Fehler passiert. Prävention kann Wahrscheinlichkeiten reduzieren, aber sie kann sie nicht auf null senken.

Schließlich verstärkt ein falsches Sicherheitsverständnis das Problem. Wenn Organisationen glauben, ausreichend geschützt zu sein, entsteht ein trügerisches Gefühl von Sicherheit. Backups

werden zwar erstellt, aber nicht regelmäßig getestet. Notfallpläne existieren auf dem Papier, werden jedoch nie geübt. Entscheidungswege sind unklar, weil man davon ausgeht, sie nicht zu benötigen. In diesem Zustand ist ein erfolgreicher Angriff besonders wirkungsvoll – nicht wegen seiner technischen Raffinesse, sondern wegen der organisatorischen Unvorbereitetheit.

Die Statistik ist daher eindeutig, auch wenn sie unbequem ist: Prävention allein verhindert keine Ransomware-Angriffe zuverlässig. Sie reduziert Risiken, verschiebt Zeitpunkte und erhöht den Aufwand für Angreifer – aber sie garantiert keinen Schutz. Wer Sicherheit ausschließlich präventiv denkt, plant implizit für einen Idealfall, der in der Praxis selten eintritt.

Die Konsequenz daraus ist kein Verzicht auf Prävention, sondern ihre Einordnung. Prävention ist notwendig, aber nicht ausreichend. Sie muss ergänzt werden durch Maßnahmen, die davon ausgehen, dass ein Angriff trotz aller Vorkehrungen erfolgreich sein kann. Erst diese Perspektive eröffnet den Raum für Resilienz – und damit für kontrollierte Handlungsfähigkeit, wenn Prävention statistisch versagt.

## 1.2 Der Mensch als primärer Angriffsvektor

In nahezu jeder Analyse von Ransomware-Vorfällen taucht dieselbe Aussage auf: „Der Mensch ist das schwächste Glied." Diese

# Quellenverzeichnis


BAFA – Bundesamt für Wirtschaft und Ausfuhrkontrolle. (2024). Hinweise zu Lösegeldzahlungen im Kontext von Cyber-Angriffen. https://www.bafa.de.

BSI – Bundesamt für Sicherheit in der Informationstechnik. (2022). Notfallmanagement: ISMS nach ISO 27001 (BSI-Standard 200-4). https://www.bsi.bund.de.

BSI – Bundesamt für Sicherheit in der Informationstechnik. (2023). Cybersicherheit für kleine und mittlere Unternehmen (KMU). https://www.bsi.bund.de/kmu.

BSI – Bundesamt für Sicherheit in der Informationstechnik. (2024). NIS-2-Richtlinie: Umsetzungshinweise und Risikomanagementmaßnahmen. https://www.bsi.bund.de/nis2.

Center for Internet Security. (2024). CIS Critical Security Controls Version 8. https://www.cisecurity.org/controls.

CISA – Cybersecurity and Infrastructure Security Agency. (2024). #StopRansomware: Ransomware Guide. https://www.cisa.gov/stopransomware.

CISA – Cybersecurity and Infrastructure Security Agency. (2024). Ransomware impacts to backup systems. https://www.cisa.gov/resources-tools/resources/ransomware-impacts-backups.

Coalition. (2024). Cyber insurance eligibility requirements & security controls. https://www.coalitioninc.com.

CrowdStrike. (2025). Global Threat Report 2025. https://www.crowdstrike.com/global-threat-report.

ENISA – European Union Agency for Cybersecurity. (2023). Ransomware threat landscape 2023. https://www.enisa.europa.eu/publications/ransomware-threat-landscape-2023.

ENISA – European Union Agency for Cybersecurity. (2024). ENISA Threat Landscape 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

International Organization for Standardization. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022). https://www.iso.org/standard/27001.

Mandiant. (2025). M-Trends 2025: Global threat intelligence report. https://www.mandiant.com/resources/m-trends.

MITRE. (2024). MITRE ATT&CK® Framework. https://attack.mitre.org.

National Institute of Standards and Technology. (2012). Contingency planning guide for federal information systems (NIST SP 800-34 Rev. 1). https://csrc.nist.gov/publications/detail/sp/800-34/rev-1/final.

National Institute of Standards and Technology. (2024). Computer security incident handling guide (NIST SP 800-61 Rev. 3). https://csrc.nist.gov/publications/detail/sp/800-61/rev-3/final.

Office of Foreign Assets Control. (2024). Advisory on potential sanctions risks for facilitating ransomware payments. U.S. Department of the Treasury. https://ofac.treasury.gov/recent-actions/20241028.

VdS Schadenverhütung. (2021). VdS 3473: Cybersicherheit für kleine und mittlere Unternehmen (KMU). https://vds.de/publikationen/vds-3473.

Verizon. (2025). Data Breach Investigations Report (DBIR) 2025. https://www.verizon.com/business/resources/reports/dbir.

# Stichwortverzeichnis

## E



## F



## G



## H



## I



## K



## L

## M



## N



## O



## P



## R

## S



## T



## V

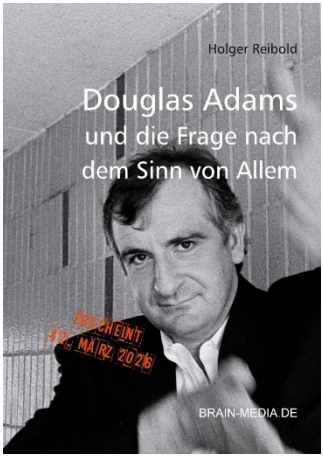


## W



## Z

# 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

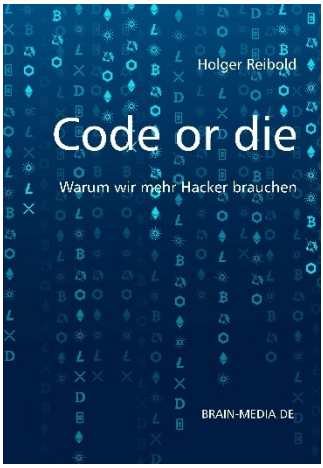
Preis: 14,99 EUR

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: 14,99 EUR

Erscheint Frühjahr 2026


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

Ziel- und punktgenaue Reaktionen für kritischen KI-Vorfälle.

Umfang: 140 Seiten

Preis: 16,99 EUR

Erscheint: Frühjahr 2026


**Knowledge as a Service**

**Individual**

**Business**

KaaS ist der direkte Zugang zum gesamten Brain-Media-Wissensbestand: praxisnahe Fachbücher zu KI, IT-Security, Regulierung und Resilienz. Sie erhalten alle aktuellen Titel, alle Neuerscheinungen während der Laufzeit sowie ausgewählte Vorlagen und Updates.

KaaS richtet sich an Praktiker, die fundierte Entscheidungen treffen müssen – ohne Hype, ohne Marketing, mit Substanz.

**KaaS ist für Privatpersonen und Unternehmen verfügbar.**

# 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 mit an. Gerne vereinbaren wir einen Fixpreis; das vereinfacht Ihre Kalkulation.

## KONTAKT AUFNEHMEN

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