



## Neues Fachbuch: KI Incident Response – Sicherheitsvorfälle in KI- Systemen erkennen, eindämmen und beherrschen

Saarbrücken, 2026 – Künstliche Intelligenz ist in den operativen Kern vieler Organisationen vorgedrungen. Gleichzeitig wächst die Zahl und Tragweite von Situationen, in denen KI-Systeme unerwartet, fehlerhaft oder schädlich agieren – nicht als hypothetisches Zukunftsszenario, sondern im produktiven Betrieb. Mit dem neuen Buch „KI Incident Response – Wie man Sicherheitsvorfälle in KI-Systemen erkennt, eindämmt und beherrscht“ legt Holger Reibold eine praxisorientierte Arbeitsgrundlage vor, die KI Incident Response als eigenständige, anschlussfähige Disziplin beschreibt: technisch fundiert, organisatorisch umsetzbar und regulatorisch einbettbar.

Im Zentrum steht die These, dass KI-Incidents erwartbar sind und Incident Response deshalb nicht als Ausnahmezustand, sondern als Normalform verantwortbaren KI-Betriebs verstanden werden muss. Das Buch zeigt, warum klassische Incident-Response-Ansätze oft zu kurz greifen: Sie setzen deterministische Systeme, klare Systemgrenzen und reproduzierbare Fehler voraus – Annahmen, die für moderne KI-Systeme häufig nicht gelten.

### **Von Definition bis Governance: ein durchgängiger Praxisrahmen**

„KI Incident Response“ schafft zunächst begriffliche Klarheit und liefert eine praxistaugliche Arbeitsdefinition: Ein KI-Incident ist ein beobachtbares Ereignis oder eine Ereignisfolge, bei der das Verhalten eines KI-Systems außerhalb vorgesehener,

akzeptierter oder regulatorisch zulässiger Grenzen liegt und eine Reaktion erforderlich macht. Damit verschiebt sich der Fokus von reiner Schadensbetrachtung hin zu einem kontrollorientierten Handlungsbegriff – einschließlich der systematischen Nutzung von Near Misses als Frühindikatoren.

Aufbauend darauf behandelt das Buch die Besonderheiten von KI-Systemen als sozio-technische Systeme (Verantwortung über Lifecycle-Phasen hinweg, Kopplungen zwischen Technik, Organisation und Nutzung) und entwickelt anschlussfähige Modelle für Risiko-, Threat- und Incident-Management.

### **Operative Response: Maßnahmen, Entscheidungen, Kommunikation**

Ein Schwerpunkt liegt auf konkreten Response-Praktiken: von Detection und initialem Assessment über Eskalation, Rollen und Entscheidungsstrukturen bis zu technischen und organisatorischen Gegenmaßnahmen (u. a. Sofortmaßnahmen im Betrieb, Filterung, Zugriffsbeschränkungen, Fallbacks, Systemanpassungen sowie Retraining- und Modellwechselstrategien). Ergänzt wird dies durch Anforderungen an Dokumentation, Nachvollziehbarkeit, Post-Incident-Analysen und systematisches Lernen.

### **Regulatorische Anschlussfähigkeit: auditierbar und berichtspflichtig**

Mit Blick auf wachsende Anforderungen – u. a. durch den EU AI Act – betont das Buch, dass Incident Response zunehmend prüf- und berichtspflichtig wird. Organisationen müssen künftig nachweisen können, dass sie Incidents erkennen, geeignete Reaktionen definieren und aus Vorfällen systematisch lernen. Incident Response wird damit zur Compliance- und Governance-Fähigkeit, die Engineering, Security, Governance und Recht zusammenführt.

### **Zielgruppe**

Das Buch richtet sich an alle, die KI nicht nur entwickeln oder einsetzen, sondern für den Betrieb Verantwortung tragen – insbesondere in Security-, Engineering-, Risk-, Governance- und Compliance-Funktionen. Es setzt kein tiefes mathematisches Vorwissen voraus; entscheidend ist das Verhalten von KI-Systemen im Betrieb.

## **Bibliografische Angaben**

Titel: Titel: KI Incident Response

Untertitel: Wie man Sicherheitsvorfälle in KI-Systemen erkennt, eindämmt und beherrscht

Autor: Holger Reibold

Verlag: Brain-Media.de

Erscheinungsjahr: 2026

ISBN: 978-3-95444-306-2

Umfang: 220 Seiten

Preis: 14,99 EUR

## **Keywords**

KI Incident Response, KI-Sicherheitsvorfälle, AI Incident Management, AI Security, KI-Risikomanagement, Threat Modeling für KI, LLM Security

## **Über den Verlag**

Brain-Media.de ist ein auf IT- und Technologiethemen spezialisierter Fachverlag mit Schwerpunkt auf praxisnaher Wissensvermittlung für professionelle Anwender.

## **Über den Autor**

Autor ist der Informatiker Dr. Holger Reibold, der seit über 30 Jahren zu Internet- und Open-Source-Themen publiziert. Reibold gilt als Urgestein der deutschen IT-Szene. Er hat sich durch unzählige Bestseller in den vergangenen Jahren einen Namen in der Branche erarbeitet. Als Key Account Manager eines IT-Dienstleisters hat er unmittelbare Einblick in die Entwicklung von KI-Systeme und kennt die sicherheitsspezifischen Herausforderungen aus der Praxis.