



Warum klassische IT-Sicherheit bei KI versagt: Neues Fachbuch zeigt reale Angriffsflächen moderner KI-Systeme

Saarbrücken, Januar 2026 – Künstliche Intelligenz gilt als Schlüsseltechnologie der digitalen Transformation. Doch während Unternehmen massiv in KI-Anwendungen investieren, bleibt ein zentrales Risiko oft unterschätzt: die Sicherheit dieser Systeme. Mit dem neuen Buch „KI-Sicherheit – Einstieg in die Praxis“ legt der IT-Sicherheitsexperte Holger Reibold eine fundierte und praxisnahe Analyse vor, warum klassische Sicherheitskonzepte bei KI-Systemen nicht mehr ausreichen – und was stattdessen erforderlich ist.

Reibold zeigt, dass Angriffe auf KI-Systeme häufig ohne klassische Exploits auskommen. Statt Software oder Infrastruktur zu kompromittieren, zielen Angreifer auf Daten, Modelle und Entscheidungsprozesse. Manipulierte Trainingsdaten, versteckte Backdoors, adversariale Eingaben oder Prompt-Injection können dazu führen, dass Systeme formal korrekt arbeiten – aber dennoch systematisch falsche oder gefährliche Entscheidungen treffen.

„Ein vollständig gepatchtes und gehärtetes System kann katastrophale Fehlentscheidungen treffen, wenn Wahrnehmung und Kontext der KI manipuliert werden“, so Reibold. „KI-Sicherheit bedeutet nicht mehr, Systeme zu schützen, sondern Entscheidungen.“

Das Buch analysiert den gesamten KI-Lebenszyklus aus Angreiferperspektive: von der Datensammlung über Training und Inferenz bis hin zu Betrieb, Monitoring und Incident Response. Dabei wird deutlich, warum Firewalls, Penetrationstests und Compliance-Frameworks allein keine ausreichende Sicherheit bieten. Stattdessen fordert der Autor ein Umdenken hin zu architekturbasierten Schutzkonzepten, kontinuierlichem Red-Teaming und einer realistischen Bewertung von Restrisiken.

„KI-Sicherheit – Einstieg in die Praxis“ richtet sich an Praktikerinnen und Praktiker aus IT-Sicherheit, Softwareentwicklung, Architektur, Compliance und Management, die KI-Systeme verantworten oder absichern müssen. Das Buch verzichtet bewusst auf theoretische Abhandlungen und ethische Grundsatzdebatten und konzentriert sich auf reale Angriffsformen, technische Zusammenhänge und umsetzbare Maßnahmen.

Bibliografische Angaben

Titel: KI-Sicherheit – Einstieg in die Praxis

Autor: Holger Reibold

Verlag: Brain-Media.de

Erscheinungsjahr: 2026

ISBN: 978-3-95444-302-4

Umfang: 120 Seiten

Preis: 16,99 EUR

Keywords

Künstliche Intelligenz, KI-Sicherheit, IT-Sicherheit, Informationssicherheit, Cybersecurity, KI-Angriffe

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.