



Neues Fachbuch zeigt, wie Unternehmen lokale KI-Systeme sicher betreiben

Mit dem rasanten Einsatz generativer KI in Unternehmen wächst auch der Bedarf nach kontrollierbaren, sicheren KI-Plattformen. Viele Organisationen nutzen bereits Large Language Models und Retrieval-Augmented Generation (RAG), betreiben diese jedoch häufig noch in experimentellen oder nur unzureichend abgesicherten Umgebungen. Gleichzeitig steigen Anforderungen an Datenschutz, Compliance und Betriebssicherheit deutlich.

Das neue Fachbuch „**Lokale KI unter Kontrolle – Sichere Architektur, Betrieb und Governance von GenAI- und RAG-Systemen**“ zeigt, wie Unternehmen generative KI-Plattformen sicher und nachhaltig im eigenen Verantwortungsbereich betreiben können. Der Leitfaden richtet sich an Organisationen, die KI nicht ausschließlich über externe Cloud-Dienste nutzen wollen, sondern Kontrolle über Daten, Infrastruktur und Modellbetrieb behalten möchten.

Im Mittelpunkt steht eine praxisorientierte Sicherheitsarchitektur für lokale GenAI-Systeme. Der Autor beschreibt typische Angriffsszenarien wie Prompt-Injection, Datenvergiftung oder Model Extraction und zeigt, wie sich diese Risiken durch strukturierte Architekturentscheidungen, klare Trust Boundaries und abgestimmte Sicherheitsmaßnahmen reduzieren lassen. Darüber hinaus erläutert das Buch, wie sich moderne KI-Stacks mit RAG-Pipelines, Vektordatenbanken und Modellservern sicher betreiben und überwachen lassen.

Neben technischen Aspekten behandelt der Leitfaden auch organisatorische Fragen rund um Governance, Compliance und wirtschaftlichen Betrieb lokaler KI-

Infrastrukturen. Checklisten, Referenzarchitekturen und konkrete Handlungsempfehlungen helfen Unternehmen dabei, experimentelle KI-Projekte in stabile, produktionsreife Plattformen zu überführen.

Ergänzende Materialien, Checklisten und Downloads zum Buch stehen über die Website des Verlags bereit. Dort können Interessierte auch den Newsletter abonnieren, der regelmäßig über neue Fachpublikationen und aktuelle Entwicklungen rund um IT-Security, Cloud, KI und digitale Infrastruktur informiert. Zusätzlich bietet der Verlag mit KaaS (Knowledge as a Service) eine E-Book-Flatrate mit ergänzenden Downloads (editierbare Checklisten, Templates, Code-Beispiele) zu aktuellen Büchern an.

Bibliografische Angaben

Titel: Lokale KI unter Kontrolle

Untertitel: Sichere Architektur, Betrieb und Governance von GenAI- und RAG-Systemen

Autor: Holger Reibold

Verlag: Brain-Media.de

ISBN: 978-3-95444-314-7

Umfang: 270 Seiten

Preis: 24,99 EUR

Über den Autor

Dr. Holger Reibold ist Informatiker und publiziert seit über 30 Jahren zu Internet-, Netzwerk- und Open-Source-Themen. Er gehört zu den prägenden Stimmen der deutschen IT-Fachszene und hat sich durch zahlreiche erfolgreiche Fachbücher und Publikationen einen Namen in der Branche gemacht. In seiner Rolle als Key Account Manager bei einem Internet Service Provider ist er unmittelbar mit praktischen Herausforderungen konfrontiert. Diese Verbindung aus langjähriger theoretischer Auseinandersetzung und operativer Praxis prägt die Perspektive seiner Publikationen.