

Wahlweise als Inhouse-Seminar oder Webinar buchbar

# KI & Sicherheit

## Erkenne neue Bedrohungen, Angriffsvektoren und Schutzmaßnahmen im Zeitalter künstlicher Intelligenz

### Zielgruppe

- ▶ IT-Sicherheitsverantwortliche, Security-Architekten, CISO, SOC-Teams, IT-Leiter sowie alle Fach- und Führungskräfte, die sich mit der sicheren Einführung und dem Betrieb von KI-Systemen im Unternehmensumfeld befassen (Informationssicherheit, IT, Datenschutz, Compliance, Recht, Risikomanagement etc.)

### Dauer

- ▶ Empfohlen als 1-tägiges Vor-Ort-Seminar oder Webinar

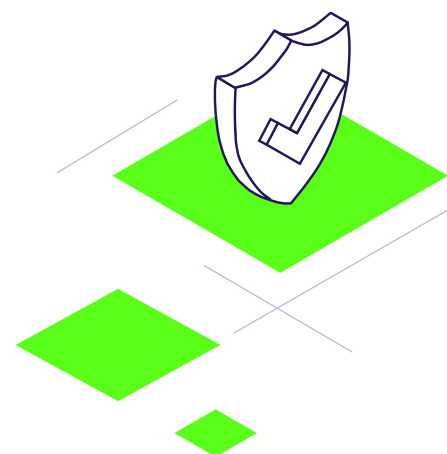
### Preis

- ▶ EUR 800,- p. P. zzgl. MwSt., zzgl. Reisekosten bei Durchführung vor Ort. Mindestteilnehmerzahl 4 Personen. Bei kleineren oder größeren Gruppen Preis auf Anfrage.

Künstliche Intelligenz verändert die Sicherheitslage in Unternehmen grundlegend – auf beiden Seiten. Angreifer nutzen KI, um Phishing-Angriffe zu skalieren, Identitäten zu fälschen und Angriffsketten zu automatisieren. Gleichzeitig bringen KI-Systeme im eigenen Unternehmen neue Risiken mit sich: von unbeabsichtigtem Datenverlust über Prompt Injection bis hin zu vollautonomen Agenten, die unkontrolliert Aktionen ausführen.

Dieses Seminar gibt euch einen kompakten, praxisorientierten **Überblick über die neue Bedrohungslandschaft** – sowohl aus der Perspektive externer Angriffe als auch aus der internen Sicht beim Betrieb eigener KI-Lösungen. Ihr lernt, wie verschiedene **KI-Architekturen** unterschiedliche Risikoprofile erzeugen, wo etablierte **Sicherheitskontrollen** an ihre Grenzen stoßen und welche spezialisierten Werkzeuge und **Frameworks für KI-Sicherheit** heute verfügbar sind.

Das Seminar verbindet technisches Verständnis mit strategischer Perspektive – und liefert euch ein belastbares Fundament, um KI sicher einzuführen, zu betreiben und zu überwachen. Denn nur wer die Risiken kennt und wirksam beherrscht, kann KI-Systeme vertrauenswürdig gestalten – nach innen wie nach außen. So wird Informationssicherheit zur **Grundlage für Digital Trust** – und KI zum vertrauenswürdigen Bestandteil eurer digitalen Infrastruktur.



**Besprech euren individuellen Bedarf in einem persönlichen Gespräch mit uns**

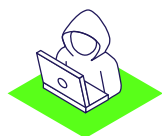


**Stephanie Knappe-Stauder**

T +49 6172 / 177 630

E [anfrage@microfin.de](mailto:anfrage@microfin.de)

# Inhalte



## Neue Bedrohungen durch KI: Die veränderte Angriffsfläche

u.a. KI-gestütztes Phishing und Social Engineering, Deepfakes (Video- & Sprachmanipulation), Prompt Injection (direkt & indirekt), Model Drift in Agenten Workflows, Data Leakage & Shadow, AI, Model Poisoning, Model Extraction, Jailbreaking sowie Halluzinationen als Angriffsvektor



## KI-Sicherheits-Frameworks und Grenzen bestehender Kontrollen

Überblick über relevante Standards und Frameworks (OWASP Top 10 for LLMs, NIST AI RMF, ISO/IEC 42001, MITRE ATLAS) sowie Analyse, wo klassische Controls wie DLP, RBAC, SIEM und Supply-Chain-Sicherheit bei KI-Systemen an ihre Grenzen stoßen



## KI-Architekturen und ihre Sicherheitsprofile

Überblick und Risikobewertung der relevanten Einsatzformen: Web-Chats (SaaS), persönliche Assistenzen (z. B. MS 365 Copilot), persönliche KI-Agenten (z. B. Claude Code, GitHub Copilot CLI), Pipeline-Agenten, orchestrierte Multi-Agenten-Systeme, vollautonome Agenten-Workflows sowie eigene KI-basierte Produkte und Services im Kundeneinsatz (Customer-Facing AI)



## KI-Sicherheits-Tooling: Der neue Werkzeugkasten

Überblick über spezialisierte Werkzeuge für KI-Sicherheit: AI Gateways & Guardrails, Prompt Scanning, KI-System- und Modell-Evaluation, AI Red Teaming, Sicherheitstools für KI-generierten Code sowie MCP-Sicherheit (Absicherung, Vetting und Monitoring von Model Context Protocol-Servern als Integrationsschicht für KI-Agenten)



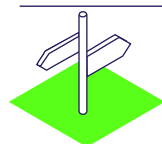
## Regulatorische Anforderungen für KI Nutzung

Überblick über die relevanten gesetzlichen und regulatorischen Pflichten beim Einsatz von KI im Unternehmen - von Datenschutz und Transparenzpflichten (DSGVO, KI-VQ) bis hin zu Anforderungen an IKT-Risikomanagement und Meldepflichten (DORA, NIS-2)



## Governance, Awareness und Handlungsempfehlungen

Integration von KI-Sicherheit in bestehende ISMS-Strukturen durch z. B. Leitplanken, KI-Observability (Tracing, Telemetrie, Laufzeitüberwachung, Logging, Audit-Dokumentation), Shadow-AI-Steuerung, Klassifizierungsschema für Daten und Modelle sowie Aufbau einer priorisierten KI-Security-Roadmap



## LLM, SLM, Cloud oder lokal - Abwägungen und Einsatzempfehlungen

Vor- und Nachteile cloudbasierter LLMs, privat gehosteter Modelle und lokaler SLMs aus Sicherheits- und Compliance-Perspektive

## Eure Trainer



**Dr. Julia Pergande**

Enabler |  
Managing Principal



**Andreas Hedderich**

Enabler |  
Senior Consultant