microfin
enables
transformation.

Wahlweise als Inhouse-Seminar oder Webinar buchbar

KI & Sicherheit

Lerne, wie du potenziellen Angriffen auf KI-Systeme vorbeugst

Zielgruppe: IT-Sicherheit, Revision, Datenschutz, IT, Geschäftsführung, KI-Experten in Unternehmen aller Branchen. Nach Bedarf Fokus auf die Finanzbranche – auch unter Berücksichtigung von Digital Operational Resilience Act (DORA) - Verordnung (EU) 2022/2554

Dauer: Empfohlen als halbtägiges Vor-Ort-Seminar oder Webinar

Preis: EUR 500 p. P. zzgl. MwSt., zzgl. Reisekosten bei Durchführung vor Ort
Mindestteilnehmerzahl 4 Personen. Bei kleineren oder größeren Gruppen auf Anfrage.

Adversarial Attacks, Data und Privacy Leaks, Data Poisoning oder Model Stealing: Die Vielfalt denkbarer Angriffe und Bedrohungen bei der Nutzung Künstlicher Intelligenz ist während des gesamten Lebenszyklus groß. Mit unserem Kompakteinstieg bekommst du und dein Team erste Lösungsansätze an die Hand, wie ihr die Manipulation von Daten, das Einschleusen von Schadcode oder die Überlastung der Systeme bestmöglich verhindert.

Dabei können KI-Tools selbst einen Beitrag leisten, die Informationssicherheit zu schützen wie beispielsweise in der automatisierten Früherkennung von Cyber Attacken oder in der biometrischen Authentifizierung.

Einen inhaltlichen Schwerpunkt legen wir auf relevante Normen und Standards, die sich im KI-Kontext zur Informationssicherheit etabliert und bewährt haben.

Stimme deinen Bedarf in einem persönlichen Gespräch ab

Irina Shapiro

T +49 6172 / 177 630
E anfrage@microfin.de

Inhalte:

Typische Bedrohungen und Risiken aus der Nutzung von KI im Kontext von Authentizität, Integrität, Vertraulichkeit, Verfügbarkeit und Widerstandsfähigkeit

- Spezifische Risiken und Herausforderungen bei Nutzung von KI im Unternehmensalltag einfach und pragmatisch erklärt

Lösungsansätze zur Risiko(früh-)erkennung und Schadensabwehr – unter Berücksichtigung aktueller Gesetze, Frameworks und Leitlinien EU AI Act, BSI AIC4, NIST AI RMF, ENISA, ISO/IEC, NIS-2-Richtlinie, weitere nach Bedarf

- Bewältigung von Risiken aus der Nutzung von KI
- Vertrauenswürdigkeit in der Künstlichen Intelligenz
- Umgang mit Sicherheitsbedrohungen und Fehlern in KI-Systemen
- Festlegung von Sicherheitsstandards für KI-Cloud-Dienste und Risikoprüfung
- Einblicke in die Leitlinien für die Prüfungspraxis der KI-Systeme (branchenneutral sowie nach Bedarf für Banken und Versicherungen in Deutschland)
- Tipps für die Praxis (Risikomanagement)

Übliche Sicherheitsmaßnahmen der Anbieter von KI-Tools

Maßnahmen zur Überwachung der Informationssicherheit bei KI-Nutzung für euer Unternehmen oder Team

Deine Trainer:

Claudia Dölker
Enabler | Senior Consultant

Sebastian Dosch
Enabler | Principal Consultant

Profitiere von der Projekterfahrung unserer Trainerinnen und Trainer sowie von unserer Unabhängigkeit und Spezialisierung im Outsourcing.

microfin – driven by enabling transformation

microfin Unternehmensberatung GmbH
Rathausplatz12
61348 Bad Homburg
www.microfin.de