Schulung

KI – Chancen und Risiken für die Sicherheit bewerten

DIE SCHULUNG

Alle wollen sich jetzt von künstlicher Intelligenz bei ihrer Arbeit unterstützen lassen. Aber was bedeutet das aus Sicherheitssicht? Um entscheiden zu können, ob und wie der Einsatz reglementiert werden kann und sollte, muss man die Chancen und Risiken für die Informationssicherheit kennen. In dieser Schulung werden wir uns zuerst die wichtigsten Grundlagen zu aktuellen KI-Verfahren wie maschinelles Lernen (ML) und große Sprachmodelle (LLM) anschauen. Darauf basierend gehen wir dann auf die aktuellen Sicherheitsauswirkungen beim Einsatz dieser Verfahren in der Praxis ein. Die Themenauswahl orientiert sich dabei an den häufigsten Fragestellungen, die Informationssicherheitsbeauftragte (ISB) an uns herantragen.

ZIELGRUPPE

Die Schulung richtet sich an:

- Informationssicherheitsbeauftragte, die sich auf Fragen zum KI-Einsatz im Unternehmen vorbereiten wollen
- IT-Verantwortliche, die KI-Techniken einsetzen wollen und im Sinne des „Security-by-Design"-Ansatzes, die Sicherheitsrisiken direkt mitbetrachten wollen

IHRE ANSPRECHPARTNERIN

Rabea Hildner
academy@hisolutions.com
+49 30 533 289 0

INHALTE

Im ersten Teil der Schulung werden Grundlagen besprochen, um die aktuellen Trends und Fachbegriffe einordnen zu können:

- Hatten wir das nicht alles schon einmal?
  Kurze Historie zur Einordnung
- Wie funktioniert es unter der Haube?
  Die Techniken hinter ML, LLMs und ChatGPT …
- Welche KI-Techniken gehen direkt im Gerät, On-Premise oder nur in der Cloud?

Im zweiten Teil geht es um die praktische Anwendung und die Chancen und Risiken von KI:

- gute und riskante Anwendungsfälle für das Unternehmen
- Anwendungsfälle, die Informationssicherheitsbeauftragten die Arbeit erleichtern
- allgemeine Sicherheitsrisiken und KI/LLM-spezifische Sicherheitsrisiken
- Ermöglichung der sicheren Nutzung in der Praxis

Die Theorie wird durch interaktive Übungen und Praxisbeispiele aufgelockert, bei denen die Teilnehmer beispielsweise Prompt Injektion und iteratives Prompt Engineering selbst ausprobieren können.

Die Schulung ist als Online-Schulung ausgelegt und dauert einen Tag.

KOSTEN PRO TEILNEHMER

599€ zzgl. Mehrwertsteuer.