Leitfaden

Sichere KI-Systeme entwickeln

[06.12.2023] Gemeinsam mit den Cyber-Sicherheitsbehörden aus dem Vereinigten Königreich (UK) und den USA hat das BSI einen Leitfaden zur Entwicklung sicherer KI-Systeme erarbeitet.

Künstliche Intelligenz (KI) kann zahlreiche Vorteile bieten. Dazu müssen die Systeme jedoch nicht nur sicher geplant und entwickelt, sondern auch sicher eingeführt und betrieben werden. Die Cyber-Sicherheitsbehörden aus dem Vereinigten Königreich (UK) und den USA haben deshalb jetzt die „Guidelines for Secure AI System Development“ veröffentlicht. An dem Leitfaden zur Entwicklung sicherer KI-Systeme hat auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) mitgewirkt, insgesamt wird der Leitfaden von 23 internationalen Cyber-Sicherheitsbehörden aus 18 Ländern unterstützt.
Wie das BSI berichtet, sollen die Guidelines Betreibern helfen, KI-Systeme zu entwickeln, die wichtige Anforderungen erfüllen: Die Systeme müssen jederzeit bei Bedarf verfügbar sein und dabei erwartungsgemäß und zuverlässig arbeiten. Außerdem dürfen sie keine sensiblen Daten preisgeben. Indem es bei der Entwicklung von KI-Systemen die Cyber-Sicherheit von Anfang an mitgestalte, könne das BSI sicherstellen, dass die Potenziale dieser Schlüsseltechnologie für die Digitalisierung Deutschlands sicher genutzt und Risiken transparent kommuniziert würden, erklärte dazu BSI-Präsidentin Claudia Plattner. Die gemeinsame internationale Veröffentlichung verdeutlicht aus Sicht des BSI, dass Fragen der Sicherheit von KI-Systemen nur im Verbund mit gleichgesinnten internationalen Partnern gelöst werden können. Sie unterstreiche zudem die Bedeutung des Themas und den dringenden Handlungsbedarf.

(bw)

Stichwörter: IT-Sicherheit, BSI, künstliche Intelligenz