Newsletter 04/2026

FOX Group

Ethische Voreingenommenheit durch KI

In der Welt der Künstlichen Intelligenz ist die Verwendung von kleinen und großen Sprachmodellen (LLM) weit mehr als eine technische Routine. Ein zentrales Problem ist die systematische Voreingenommenheit (Bias) durch die Gewichtung von Zielwerten. Ein prägnantes Beispiel für diese ethische Verzerrung findet sich in der Logistik-Optimierung: Wird eine KI ausschließlich darauf trainiert, die Liefergeschwindigkeit zu maximieren, vernachlässigt sie automatisch die Sicherheit oder angemessene Pausenzeiten in der Logistik. Die ethische Fehlentscheidung liegt hier in der Priorisierung von Profit über das menschliche Wohlbefinden.

Um dies praktisch zu verhindern, integrieren Betreuende heute die Optimierungen mehrere Ziele. Dabei werden dem Algorithmus feste ethische Grenzwerte als mathematische Bedingungen auferlegt, die nicht unterschritten werden dürfen. Eine verantwortungsvolle Wartung erfordert kontinuierliche Audits, die neben der Effizienz auch diese sozialen Leitplanken prüfen. Nur durch die bewusste Verknüpfung von Werten und Code wird Technologie gesellschaftlichen Standards gerecht. Letztlich entscheidet die Qualität der menschlichen Aufsicht über die moralische Integrität digitaler Entscheidungen.

Vorgabe
Art. 9–10/14–15
KI-VO

Thema 1

Ethische Voreingenommen-heit durch KI

Thema 2

Multi-Faktor-Authentifizierung ist nicht mehr sicher

Thema 3

Erhalten Mitarbeitende eine Schulung zur KI-Nutzung?

Multi-Faktor-Authentifizierung ist nicht mehr sicher

Die Mehrfaktor-Authentifizierung (MFA) gilt als eine zentrale Sicherheitsmaßnahme zum Schutz digitaler Identitäten. Neben dem Passwort wird ein zusätzlicher Faktor verlangt, etwa eine Bestätigung über eine Authenticator-App oder einen einmaligen Sicherheitscode. Dadurch sollen unbefugte Zugriffe auf Benutzerkonten verhindert werden.
Im Vortrag „Turning Microsoft's Login Page into our Phishing Infrastructure" von Keanu Nys auf der DEF CON 33 (2025), der weltweit größten Veranstaltungen für Hacker, wurde jedoch aufgezeigt, dass MFA unter bestimmten Umständen durch Angreifer umgangen oder missbraucht werden kann. Dabei werden nicht klassische Softwarelücken ausgenutzt, sondern legitime Funktionen moderner Authentifizierungssysteme.

Ein zentraler Ansatz besteht darin, die offizielle Login-Infrastruktur von Microsoft zu nutzen. Da Login-Seiten über vertrauenswürdige Domains bereitgestellt werden, werden entsprechende Links häufig von E-Mail-Sicherheitslösungen oder Webfiltern als legitim eingestuft. Angreifer können diesen Vertrauensvorschuss ausnutzen, um Benutzer zunächst auf eine echte Microsoft-Login-Seite zu führen.

Im nächsten Schritt wird der Benutzer zur Eingabe seiner Zugangsdaten aufgefordert. Nach erfolgreicher Anmeldung wird die echte MFA-Abfrage ausgelöst. Bestätigt der Benutzer diese Anfrage über seine Authenticator-App, gilt die Anmeldung als legitim.

Angreifer zielen dabei auf das Sitzungs-Token, das nach erfolgreicher Anmeldung erstellt wird, ab. Dieses Token erlaubt es, eine bestehende Sitzung zu übernehmen, ohne dass erneut eine Authentifizierung erforderlich ist.
Bei den sogenannten MFA-Fatigue-Angriffen werden wiederholt Authentifizierungsanfragen ausgelöst, bis ein Benutzer eine der Anfragen aus Versehen oder aus Frustration bestätigt.

Um sich vor solchen Angreifern zu schützen, sind Verfahren wie FIDO2/Passkeys/Security Keys einzusetzen. Diese kryptografischen Verfahren prüfen die Echtheit der Domain und den physischen Schlüssel des Nutzers**.** Wenn die Domain falsch ist, funktioniert der Login automatisch nicht.

DEF CON Vortrag von Heanu Nys: https://www.youtube.com/watch?v=z6GJqrkL0S0

Erhalten Mitarbeitende eine Schulung zur KI-Nutzung?

Obwohl Künstliche Intelligenz (KI) die Arbeitswelt rasant verändert, hinkt die berufliche Weiterbildung in Sachen KI-Nutzung in Deutschland hinterher. Laut einer aktuellen Umfrage des Digitalverbandes Bitkom haben etwa 70 Prozent der Mitarbeitenden keinerlei Angebote für KI-Schulungen von ihren Arbeitgebern erhalten. Lediglich 20 Prozent der Beschäftigten erhielten eine Unterweisung im Umgang mit der neuen bahnbrechenden Technologie. Weitere sechs Prozent ließen bestehende Angebote ungenutzt. Diese Zurückhaltung der Unternehmen ist nicht nur strategisch riskant, sondern könnte womöglich rechtliche Konsequenzen nach sich ziehen.

Seit Februar 2025 ist die KI-Verordnung der EU (AI-Act) in Kraft. Diese schreibt vor, dass Unternehmen, welche KI-Systeme einsetzen, ein „ausreichendes Maß an KI-Kompetenz“ bei allen beteiligten Personen sicherstellen müssen. Dies betrifft nicht nur festangestellte Mitarbeiter, sondern ausdrücklich auch externe Kräfte, wie freie Mitarbeitende oder Personen in Zeitarbeit. Die praktische Umsetzung dieser gesetzlichen Vorgabe stellt viele Betriebe weiterhin vor große Herausforderungen.

Es ist offensichtlich, dass die Nutzung von Künstliche Intelligenz Arbeitsprozesse effizienter machen, eine korrekte Bedienung somit essenziell ist. Beschäftigte müssen nicht nur die Funktionsweise verstehen, sondern auch über Datenschutz, Datensicherheit und die ethischen Grenzen der Technologie aufgeklärt werden. Selbst Unternehmen ohne offizielle KI-Strategie sollten Schulungen anbieten, da Angestellte bereits private Tools eigenmächtig im Berufsalltag nutzen („Shadow AI“).

Die Umfrage zeigt zudem eine tiefe Verunsicherung in der Belegschaft: 14 Prozent der Befragten fürchten, durch KI komplett ersetzt zu werden. Interessanterweise glauben 33 Prozent, dass KI sogar Führungspositionen übernehmen könnte. Ein regelmäßiges, zielgruppenspezifisches Schulungsangebot ist daher entscheidend, um Ängste abzubauen und die Chancen der Transformation rechtssicher und fürs Unternehmen produktiv zu nutzen.

Quelle Bitkom: https://www.bitkom.org/Presse/Presseinformation/Ein-Fuenftel-im-Job-zu-KI-geschult

Impressum

complimant AG, Edt 4, 84558 Kirchweidach

Vorstand: Franz Obermayer, Ann-Karina Wrede

Vorsitzender des Aufsichtsrates: Christian Volkmer

Telefon: +49 8683 99390-40

E-Mail: info@complimant.de / datenschutz@complimant.de

www.complimant.de

Eintragung im Handelsregister: Amtsgericht: Traunstein

Registernummer: HRB 20500 Steuernummer: 141/120/07009

Umsatzsteuer-Identifikationsnummer gemäß §27a

Umsatzsteuergesetz: DE274380239

Verantwortlich für den Inhalt nach §18 Abs. 2 MStV Franz Obermayer