

**KEEPER®**

Pressemitteilung

EU-Verhaltenskodex für KI lässt Fragen zur Nutzung von KI offen

Ein Kommentar von Jeremy London, Director Engineering,
AI & Threat Analytics bei Keeper Security

Der Schwerpunkt des neuen freiwilligen Verhaltenskodexes der Europäischen Union für künstliche Intelligenz liegt verständlicherweise auf der verantwortungsvollen Entwicklung künstlicher Intelligenz. Doch indirekt wirft er auch die Frage nach einem weiteren wichtigen Pfeiler der gewissenhaften Einführung auf: der Sicherheit bei der Nutzung von KI.

KI-Systeme werden in vielen Unternehmen zunehmend in den täglichen Betrieb integriert. Ein Großteil der bisherigen Diskussionen, Empfehlungen und Gesetzgebungsvorhaben zum Thema Compliance konzentriert sich darauf, wie KI-Modelle aufgebaut sind, um zu funktionieren, und nicht darauf, wie sie von Endnutzern eingesetzt und genutzt werden. Unternehmen trainieren KI heute nicht nur, sondern setzen sie auch ein und nutzen Agentic AI in verschiedenen Abteilungen, um Berichte zu erstellen, Arbeitsabläufe zu automatisieren und auf interne oder externe Systeme zuzugreifen. Damit gewähren sie KI-Modellen Zugriff auf einige der sensibelsten Daten, über die ein Unternehmen verfügt.

Sicherheitsverantwortliche stehen in diesem Szenario vor einer doppelten Herausforderung. Zweifellos lässt sich durch die Integration von KI ein deutlicher Produktivitätsgewinn erzielen. Dieser Gewinn bringt jedoch auch ein wachsendes Risiko mit sich. Jeder KI-Assistent, jedes Skript und jede Modellschnittstelle ist ein potenzieller Angriffspunkt, insbesondere bei der Interaktion mit Anmeldedaten oder privilegierten Systemen.

Die Anwendung von Secure-by-Design-Prinzipien endet nicht mit der Entwicklung der KI, sondern muss sich auch auf die Integration, den Einsatz und die Überwachung von KI erstrecken. Dies ist ein wichtiger Aspekt, den Unternehmen neben dem von der EU empfohlenen Regulierungsrahmen berücksichtigen müssen.

Unternehmen sollten die Einführung eines Model Context Protocol (MCP) für die Integration von Agentic AI ernsthaft in Betracht ziehen. MCP ermöglicht es Unternehmen, KI-Tools von Drittanbietern oder aus dem eigenen Haus mit privilegierten Systemen zu verbinden, ohne Zero-Trust-Grenzen zu verletzen oder Zero-Knowledge-Architekturen zu gefährden.

Wenn ein KI-Agent ohne angemessene Governance Zugangsdaten abrufen oder verwalten kann, könnte dies unbeabsichtigt dazu führen, dass er interne Zugriffskontrollen umgeht oder Compliance-Standards verletzt. Grundsätzlich sollten KI-Agenten wie alle anderen privilegierten Benutzer oder Anwendungen behandelt werden. Das bedeutet Zugriff mit geringsten Privilegien, menschliche Aufsicht, vollständige Prüfpfade und ausdrückliche Freigabe durch Administratoren. Werden solche Sicherheitsvorkehrungen nicht umgesetzt, könnte dies die Rahmenwerke für den Datenschutz, die Unternehmen in den letzten zehn Jahren mühsam aufgebaut haben, erheblich untergraben.

Die Initiative der EU, die KI-Governance durch freiwillige Kodizes zu gestalten, ist ein willkommener Schritt. Aber technische und operative Kontrollen müssen parallel dazu

weiterentwickelt werden, um sicherzustellen, dass die Einführung und Operationalisierung von KI-Systemen wohlüberlegt, beabsichtigt und reguliert erfolgt. Souveräne KI legt die Verantwortung wieder in die Hände der Unternehmen, die ihre eigenen Nutzungsrichtlinien, Zugriffskontrollen und Regeln für die Daten-Governance definieren und durchsetzen müssen.

###

Über Keeper Security:

Keeper Security verändert die Cybersicherheit für Millionen von Einzelpersonen und Tausende von Unternehmen weltweit. Die intuitive Cybersicherheitsplattform von Keeper ist mit einer End-to-End-Verschlüsselung ausgestattet und genießt das Vertrauen von Fortune-100-Unternehmen, um jeden Benutzer auf jedem Gerät und an jedem Standort zu schützen. Unsere patentierte Zero-Trust- und Zero-Knowledge-Lösung für das Privileged Access Management vereint die Verwaltung von Unternehmenspasswörtern, Geheimnissen und Verbindungen mit Zero-Trust-Netzwerkzugriffen und Remote-Browser-Isolation. Durch die Kombination dieser wichtigen Identitäts- und Zugriffsverwaltungskomponenten in einer einzigen cloubasierten Lösung bietet Keeper beispiellose Transparenz, Sicherheit und Kontrolle und gewährleistet gleichzeitig die Einhaltung von Compliance- und Audit-Anforderungen. Erfahren Sie unter [KeeperSecurity.com](https://keepersecurity.com), wie Keeper Ihr Unternehmen vor den heutigen Cyberbedrohungen schützen kann.

Folgen Sie Keeper auf [Facebook](#) [Instagram](#) [LinkedIn](#) [X](#) [YouTube](#) [TikTok](#)

Pressekontakt für Keeper in DACH:

Alexandra Schmidt, +49 170 387 10 64

Thilo Christ, +49 171 622 06 10

keeper@tc-communications.de