

Datenschutz PRAXIS

rechtssicher • vollständig • dauerhaft

September 2026



Cyberkriminelle nutzen heute agentische KI, um Angriffe zu optimieren und großflächiger durchzuführen. Dies erzwingt eine neue Risikobewertung – auch im Hinblick auf den Datenschutz.

Bild: iStock.com/bymuradeniz

Künstliche Intelligenz als Risikofaktor für die Datensicherheit

Angriffe durch KI-Agenten – so können DSB beraten

Künstliche Intelligenz (KI) verändert Cyberangriffe in der Breite nicht, weil KI plötzlich eigenständige Hacking-Aktionen durchführen will. Die Veränderung ist viel banaler: KI-Agenten machen Angriffsschritte schlicht schneller, billiger und besser skalierbar.

Zugleich setzen Unternehmen selbst KI-Systeme ein, die E-Mails lesen, Dokumente auswerten oder Workflows anstoßen. Diese KI-Systeme bilden selbst eine Angriffsfläche.

Was sind KI-Agenten?

KI-Agenten sind Sprachmodelle, die nicht nur Text erzeugen, sondern selbstständig Werkzeuge nutzen: Sie können Webseiten

abrufen, Dateien lesen, Code ausführen oder Schnittstellen ansprechen und ihre nächsten Schritte am Zwischenergebnis ausrichten. Aus einer einzelnen Anfrage wird so eine Kette von Aktionen, die der Agent weitgehend ohne menschliches Zutun abarbeitet.

Genau diese Handlungsfähigkeit macht agentische KI in zweierlei Hinsicht relevant:

- als Werkzeug für Angreifer, um Angriffsschritte zu automatisieren, und
- als Angriffsfläche im eigenen Haus, wenn der Agent auf produktive Daten und Systeme zugreifen darf.

Warum ist das für Art. 32 DSGVO (auch) bei KI wichtig?

Art. 32 der Datenschutz-Grundverordnung (DSGVO) verlangt keine perfekte Sicherheit, sondern geeignete technische und organisatorische Maßnahmen. Maßstab sind das Risiko der Rechte und Freiheiten, der Stand der Technik, die Kosten sowie die konkrete Verarbeitung.

Diese Prüfung soll zudem nicht nur einmal erfolgen und dann dauerhaft als ausreichend gelten. Wenn sich Angriffe verändern, muss sich auch die Bewertung verändern. Genau dieser Wandel findet derzeit statt. →

Titel

- 01** Angriffe durch KI-Agenten – so können DSB beraten

Schulen & sensibilisieren

- 05** Wie sich generative KI in Browsern abschalten lässt

Best Practice

- 07** NIS 2: zwischen Cybersicherheit und Nutzerüberwachung

News & Tipps

- 11** Cyberbedrohungen durch KI

Beraten & überwachen

- 12** So bekommen Unternehmen KI-Protokolle in den Griff

- 15** Post-Quanten-Kryptografie: Wann damit anfangen?

Beraten & überwachen

- 17** Sanktionslisten-Screening

Daten-Schluss

- 20** Datenschutzverstoß durch die Hecke