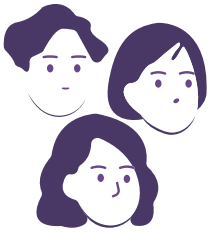
Cybersecurity im Zeitalter von KI

Risiken aus Sicht der deutschen Erwerbstätigen und Organisationen

Die kriminelle Nutzung von KI verschärft die Bedrohungslage. Zudem verwenden auch immer mehr Erwerbstätige KI-Tools und schaffen so ein neues Einfallstor. Doch Unternehmen und Behörden rüsten ebenfalls mit KI auf.

73% der Unternehmen und Behörden sehen eine drastisch verschärfte Bedrohungslage durch die böswillige Nutzung von KI.



71% der Fach- und Führungskräfte sind der Auffassung, dass Cyberkriminelle KI deutlich besser zum Angriff als Unternehmen zur Abwehr nutzen.

65% der Erwerbstätigen probieren KI-Tools bei der Arbeit aus

- **8%** – täglich
- **19%** – mehrmals wöchentlich
- **10%** – wöchentlich

37% mindestens wöch.

Nur **41%** der Arbeitgeber haben Leitlinien zur Nutzung von KI

Größte Schwachstellen:

- **43%** Reaktion auf Phishing-Nachrichten
- **34%** Reaktion auf KI-gestützte Social-Engineering-Angriffe
- **26%** ungeregelte Verwendung von KI-Tools wie ChatGPT, DeepL
- **23%** unzureichende Regelung bei externen Zugriffen von Mitarbeitenden

45% Datendiebstahl und -spionage wird durch den Einsatz von KI in den kommenden 12 Monaten zunehmen

81% wollen in den kommenden zwölf Monaten in die Verbesserung ihrer Cybersecurity investieren

54% der Organisationen sehen ohne den Einsatz von KI künftig keine Chance gegen Cyberangriffe.

33% der Unternehmen und Behörden planen in den kommenden zwölf Monaten eine an KI angepasste Cybersecurity-Strategie.

30% planen den Einsatz von KI in der Cybersecurity.

Quelle: Der Marktforscher F.A.Z. Business Media I research hat im Auftrag von Sopra Steria im April und Mai 1.003 Erwerbstätige ab 15 Jahren in Deutschland repräsentativ befragt. Im April hat das Institut zudem 564 Fach- und Führungskräfte der Branchencluster Finance (Banken und Versicherer) Automotive (inkl. Zulieferer) und öffentliche Verwaltung online befragt.