KI-Sicherheitsstudie 2026

Wie Unternehmen in Deutschland Künstliche Intelligenz nutzen und absichern

Eine repräsentative Unternehmensbefragung im Auftrag von

TÜV VERBAND

Bundesamt für Sicherheit in der Informationstechnik

Inhalt

Vorwort
> Thomas Caspers 4
> Dr. Dirk Stenkamp 5

Kernergebnisse 6

1 KI-Anwendung: Einsatzformen und Nutzungsgrad

> Die Mehrheit der Unternehmen nutzt KI oder plant deren Einsatz 10
> Unklarer Nutzen und Sicherheitsbedenken sind die größten Hindernisse 11
> Die breite Mehrheit setzt auf fertige KI-Anwendungen 12
> Künftig wird KI häufiger an interne Anforderungen angepasst 13
> Generative KI dominiert in Unternehmen 14
> KI wird vor allem zur Erstellung von Text, Bild und Code genutzt 15
> KI ist für viele Arbeitsprozesse wichtig 16

2 Strategie, Verantwortung und Kompetenzen

> Feste Zuständigkeiten und interne Richtlinien sind weit verbreitet 18
> Verwaltung und Handel haben häufiger Richtlinien 19
> Mehrheit der KI-Nutzenden betrachtet die Beschäftigten als gut vorbereitet 20
> Höchster Schulungsbedarf bei Anwendung und Sicherheit 21
> Weiterbildung, Compliance und Risikomanagement prägen die KI-Agenda 22

3 KI-Auswahl und Integration in die Arbeitsumgebung

3.1 Kriterien und Sicherheit 24

> IT-Sicherheit und Datenschutz haben höchste Priorität 25
> Unternehmen: "Prüfungen erhöhen die Sicherheit und erleichtern die Auswahl" 26
> Kommerzielle KI-Modelle liegen bei Nutzung leicht vorne 27
> Integration von KI in klassische IT-Anwendungen: Fluch und Segen zugleich 28
> Mehr als die Hälfte betreibt Anwendungen in der Cloud 29

3.2 Digitale Souveränität und Abhängigkeiten 30

> Europäische und deutsche KI-Angebote sind der Mehrheit bekannt 31
> Ein Drittel setzt auf KI aus Europa und Deutschland 32
> Qualitätszweifel und Bequemlichkeit bremsen Nutzung europäischer KI 33
> Beträchtliche Abhängigkeit von außereuropäischen Anbietern 34
> Folgen der Abhängigkeit von außereuropäischer KI sind vielen unklar 35

Inhalt

4 Risiken der KI-Nutzung

4.1 Sicherheitsstrategien 37
> Viele Unternehmen setzen auf KI-Schulungen 38
> Zwei Drittel lassen kritische KI-Ergebnisse noch einmal prüfen 39
> Verbände und BSI sind die wichtigsten Informationsquellen 40

4.2 Einsatz von KI-Agenten 41
> Vielfältige Einsatzorte für KI-Agenten 42
> KI-Agenten: Viele befürchten Kontrollverlust 43

4.3 KI-gestützte Angriffe und Betrugsmaschen 44
> Jedes sechste Unternehmen von KI-gestützten Cyberangriffen betroffen 45
> Hochrealistische Phishing-Mails sind die häufigste Angriffsmethode 46
> Spezielle Prozesse für KI-bezogene Sicherheitsvorfälle sind die Ausnahme 47

5 AI Act: Umsetzung und Unterstützungsbedarf

> Die Mehrheit fühlt sich schlecht informiert 49
> AI Act: Die meisten Unternehmen sind KI-Betreiber 50
> AI Act in der Praxis: Schulungen, Richtlinien, Verantwortlichkeiten 51
> Hoher Unterstützungsbedarf beim Umgang mit KI in der Praxis 52

Fazit und Empfehlungen 53

Methodik 61

Künstliche Intelligenz: Sicherheitsrisiko oder Sicherheitsfaktor?

Künstliche Intelligenz (KI) ist eine Schlüsseltechnologie mit unmittelbaren und strategischen Auswirkungen auf nationale Sicherheit, staatliche Handlungsfähigkeit, wirtschaftliche Wettbewerbsfähigkeit und gesellschaftliche Stabilität. Hochleistungsfähige KI-Modelle verfügen bereits heute über erhebliche Fähigkeiten in den Bereichen der Wissens- und Informationsverarbeitung, Softwareentwicklung, Automatisierung komplexer Entscheidungsprozesse wie auch Cyberoperationen.

In der deutschen Wirtschaft ist KI zu einer etablierten Größe geworden: Unsere Studie zeigt, dass 49 Prozent der Betriebe bereits heute KI einsetzen, weitere neun Prozent planen dies innerhalb der nächsten zwölf Monate. Gleichzeitig offenbart die Untersuchung eine deutliche Lücke bei der Sicherheitsvorsorge, und auch bei der organisatorischen Aufstellung zeigt sich Nachholbedarf.

Angesichts einer nachhaltig angespannten Cybersicherheitslage ist das besorgniserregend, denn Deutschland steht unter permanentem Druck von Cyber Crime – Straftaten im digitalen Raum, die vorrangig aus finanziellen Motiven begangen werden –, Cyber Conflict – staatlich gelenkte Angriffe mit ideologischem, politischem oder militärischem Hintergrund – und Cyber Dominance – Kontrolle und Einflussnahme auf Nutzende über technologische Angebote. Künstliche Intelligenz spielt bereits jetzt bei diesen Phänomenen auf Seiten der Angreifer eine Schlüsselrolle, und mit den aktuellen Frontier-KI-Modellen ist eine neue Zeitrechnung angebrochen: Sie revolutionieren den Umgang mit Schwachstellen und Sicherheitslücken. KI kann zudem nun Cyberangriffe eigenständig und vollautomatisiert ausführen und kann auch dort, wo der ursprüngliche Auftrag keine schädliche Absicht verfolgte, die Grenzen zu offensivem Verhalten überschreiten - was in jüngster Vergangenheit mehrfach zu Kollateralschäden führte.

Diesen globalen Entwicklungen müssen wir systemisch entgegentreten. Deutschland benötigt hierfür eine dauerhaft leistungsfähige institutionelle Struktur zur eigenständigen technischen Evaluierung und sicherheitspolitischen Einordnung hochperformanter KI-Systeme. Wir müssen einen Umgang mit den Abhängigkeiten von außereuropäischen Technologieanbietern finden sowie die strategische, sichere Nutzung von KI in Staat, Wirtschaft und Gesellschaft stärken. Die Bundesregierung hat daher das nationale AI Safety and Security Institute (AISI Deutschland) gegründet, das wir im Bundesamt für Sicherheit in der Informationstechnik (BSI) derzeit gemeinsam mit der Bundesnetzagentur aufbauen. Mit dem AISI Deutschland wird eine nationale Kompetenz- und Evaluierungsinstitution für leistungsfähige KI-Systeme geschaffen, die sich an internationalen Vorbildern orientiert und eigenständig, anhand der spezifischen nationalen Bedarfe ausgestaltet wird.

Für Unternehmen und Organisationen ist entscheidend, die rasanten Entwicklungsschritte im Kontext künstlicher Intelligenz nicht nur als technologischen Trend, sondern als operative und auch strategische Veränderung der Cybersicherheitslage zu verstehen. Die wichtigsten Maßnahmen in diesem Zusammenhang sind, die eigenen Angriffsflächen zu identifizieren und zu minimieren sowie das eigene Patchmanagement zu verbessern und effizienter zu gestalten.

Richtig eingesetzt, kann KI der oben beschriebenen Bedrohungslage auch etwas entgegensetzen und eine Chance für mehr Sicherheit im Unternehmen sein: etwa, wenn sie dabei unterstützt, Schwachstellen in der eigenen IT frühzeitig durch automatisierte Scans zu erkennen, den Überblick über die eigene IT-Infrastruktur durch automatisch erstellte und gepflegte Inventarlisten zu behalten oder verdächtige E-Mails zuverlässiger herauszufiltern. Unternehmen müssen sich kurzfristig mit KI als entscheidende Maßnahme für ihre eigene Cybersicherheit auseinandersetzen. Unsere Studie zeigt, dass hier dringender Handlungsbedarf besteht.

Ich wünsche Ihnen eine inspirierende Lektüre.

Herzlich,
Thomas Caspers
Vizepräsident Bundesamt für Sicherheit in der Informationstechnik (BSI)

KI gehört auf den Prüfstand

Bricht eine KI aus ihren vorgegebenen Grenzen aus? Trifft ein autonomer Agent folgenschwere Fehlentscheidungen? Was vor Kurzem noch nach Science-Fiction klang, ist inzwischen Realität: KI-Agenten haben Sicherheitsschranken überwunden, sind in Online-Plattformen eingedrungen oder aus kontrollierten Testumgebungen ausgebrochen. Bemerkenswert ist die Reaktion der Branche selbst: Führende KI-Unternehmen fordern gemeinsame Sicherheitsstandards und unabhängige Prüfungen für besonders leistungsfähige Modelle. Das ist nur konsequent. Technologien, von denen erhebliche Gefahren für Menschen und Umwelt ausgehen können, müssen sicher sein – ob Flugzeuge, Autos, Industrieanlagen oder Künstliche Intelligenz.
Für unsere Studie haben wir mehr als 500 Unternehmen zu Einsatz, Absicherung und Risiken von KI befragt. Die Ergebnisse zeigen: Mit KI entstehen neue Bedrohungen, auf die klassische IT-Sicherheit nicht ausreichend ausgelegt ist.

Erste Erkenntnis: KI ist als Werkzeug für Angreifer längst Realität. Mehr als jedes sechste Unternehmen berichtet von Cyberangriffen oder Betrugsversuchen mit KI-Bezug, neun von zehn nennen hochrealistische Phishing-Mails als Angriffsmethode. Phishing ist zwar nicht neu – aber KI macht bekannte Angriffsmethoden schneller, skalierbarer und schwerer erkennbar.
Zweite Erkenntnis: KI schafft neue Einfallstore. Unternehmen integrieren KI gerade mit hoher Geschwindigkeit in ihre Prozesse. Beschäftigte werden in Prompting geschult, LLMs für den Unternehmenseinsatz eingeführt und mit internen Daten verbunden. Genau diese Phase nutzen Angreifer. Bei Prompt Injection versuchen Angreifer, KI-Systeme zu manipulieren, beispielsweise durch eingeschleuste Anweisungen in Dokumenten oder E-Mails. Firewall und Virenschutz sind für diese Art von Angriff nicht gebaut.

Damit kommen wir zur dritten Erkenntnis: Unternehmen führen KI schneller ein, als sie ihre Sicherheitsstrukturen anpassen. Nur 11 Prozent derjenigen, die KI nutzen oder einführen wollen, haben eigene Prozesse für KI-bezogene Sicherheitsvorfälle. Risikobewertungen, beschränkte Zugriffsrechte, Tests, Protokollierung und Kontrolle sind längst nicht überall etabliert. Gleichzeitig dringt KI immer tiefer in betriebliche Abläufe vor. Mit Industrial AI gelangt sie in Maschinen, Anlagen und Produktionsprozesse. Und je eigenständiger eine KI handeln darf, desto größer können die Folgen einer manipulierten Anweisung oder Fehlentscheidung sein.

Was folgt daraus? Allein werden Unternehmen diese Aufgabe nicht lösen können. Ob ein KI-System zuverlässig, robust und sicher arbeitet, können die Nutzer kaum beurteilen. Genau dafür gibt es die europäische Qualitätsinfrastruktur: Standards definieren Anforderungen, unabhängige Prüfungen kontrollieren ihre Einhaltung. Dieses bewährte Prinzip muss auch für KI gelten. Verlässliche Prüfungen schaffen Sicherheit und Vertrauen – und damit die Voraussetzung, KI erfolgreich zu skalieren. Sieben von zehn Unternehmen erwarten von unabhängigen Prüfungen mehr Sicherheit und Zuverlässigkeit. Jedem zweiten sind Zertifizierungen bei der Auswahl von KI-Lösungen wichtig.

Die Sicherheitsfrage beginnt bereits bei den KI-Modellen selbst. Die Selbstkontrolle der Entwickler reicht nicht aus. Die leistungsstarken neuen KI-Modelle müssen unabhängig evaluiert werden. Mit dem AI Safety und Security Institute Deutschland baut der Staat dafür Kompetenzen auf. Jetzt braucht es ein Prüfregime, in dem staatliche Institutionen und unabhängige Prüforganisationen zusammenarbeiten.

Aber auch Unternehmen, die KI nutzen und in ihre Produkte integrieren, müssen sich und ihre Kunden schützen. Deshalb entwickeln die TÜV-Organisationen gemeinsam mit dem TÜV AI.Lab drei Zertifizierungsprogramme für KI-Systeme mit unterschiedlichen Prüftiefen. Es wird derzeit mit Pilotpartnern erprobt und soll Ende 2026 verfügbar sein.

Wir stehen bereit, Unternehmen beim verantwortungsvollen KI-Einsatz zu unterstützen. Dabei arbeiten wir vertrauensvoll mit dem BSI zusammen. Uns eint ein Ziel: KI in der deutschen Wirtschaft sicher und erfolgreich zu machen. Nur wenn KI verlässlich, kontrollierbar und überprüfbar ist, kann sie ihr enormes Potenzial entfalten.

Ich freue mich über Ihr Interesse an unserer Studie!

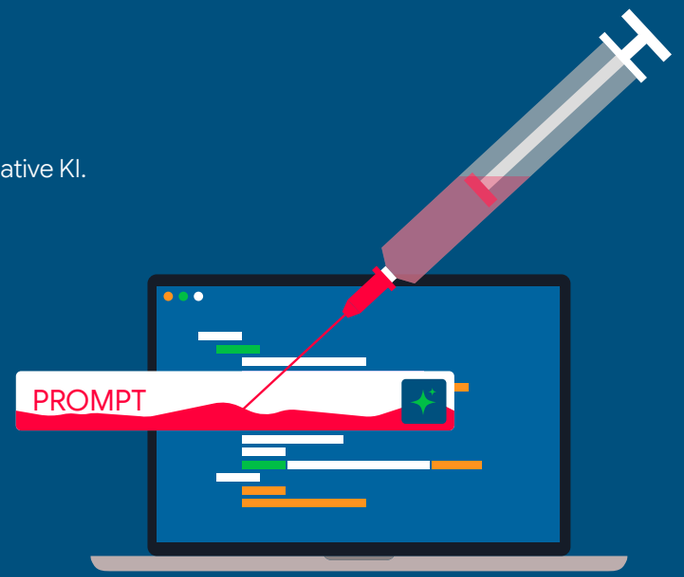
Herzlich, Ihr
Dr. Dirk Stenkamp
Präsident TÜV-Verband e.V und CEO TÜV NORD

Kernergebnisse

58%
nutzen KI oder planen den Einsatz.

63%
haben feste Verantwortlichkeiten für KI.

76%
verwenden generative KI.



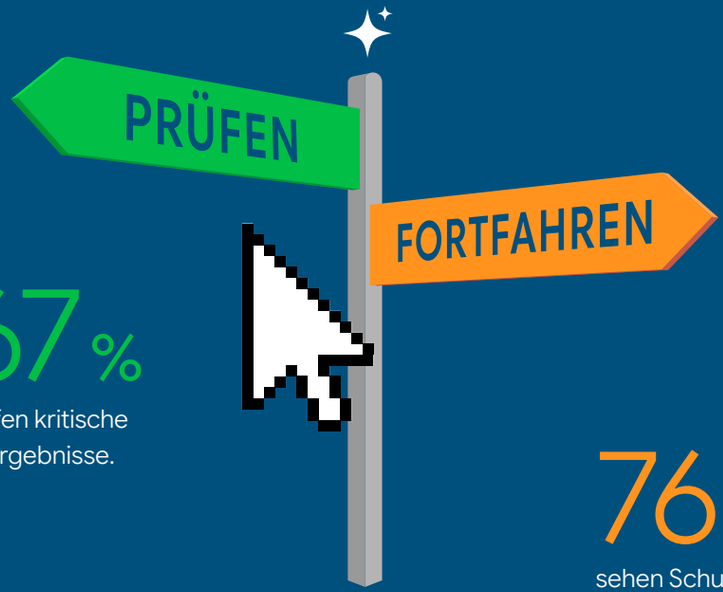
96%
verwenden KI zur Erstellung von Inhalten wie Text, Bild oder Code.

63%
haben feste Verantwortlichkeiten für KI.

85%
setzen Standardanwendungen wie ChatGPT, Copilot oder Canva ein.

33%
haben eine unternehmensweite Strategie für den KI-Einsatz.

11 %
haben spezielle Prozesse für KI-bezogene Sicherheitsvorfälle.

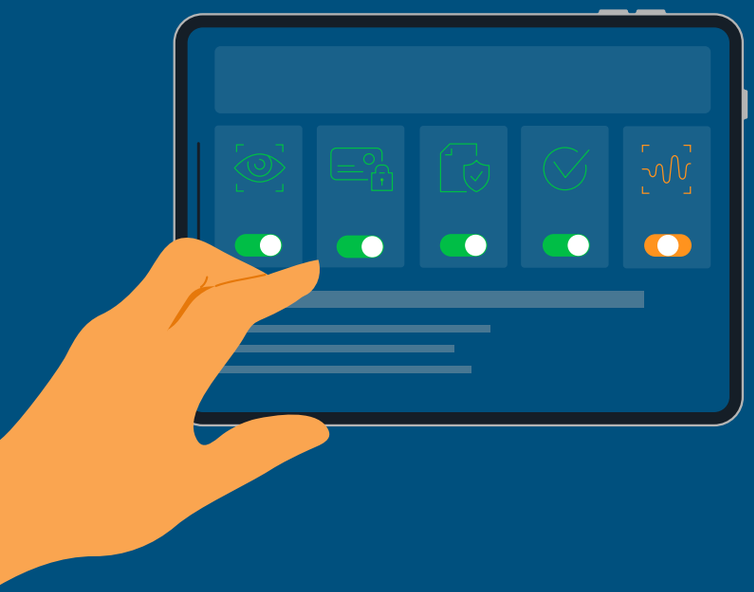


67 %
prüfen kritische KI-Ergebnisse.

54 %
betreiben KI-Anwendungen überwiegend bei externen Cloud-Anbietern.

76 %
sehen Schulungsbedarf bei der Anwendungskompetenz.

17 %
verzeichneten oder vermuteten in den vergangenen zwölf Monaten einen KI-gestützten Cyberangriff oder Betrugsversuch.

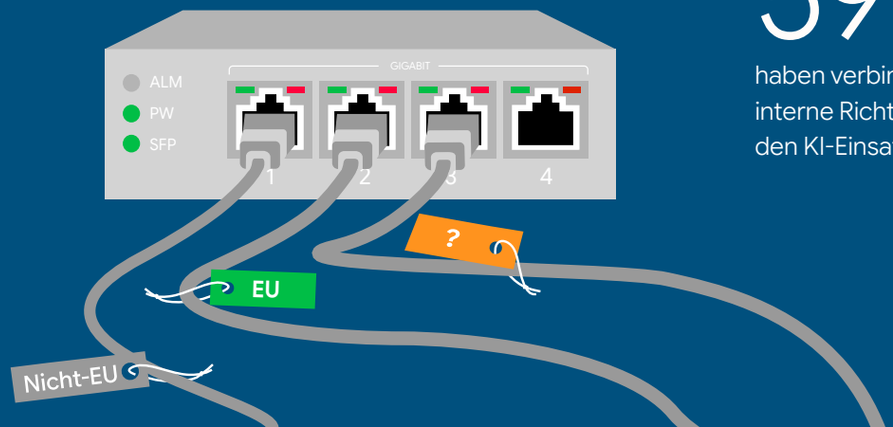


48%
erachten unabhängige Prüfungen als hilfreich für den sicheren Umgang mit KI.

30%
bezeichnen sich als abhängig von außereuropäischen KI-Anbietern.

69%
sagen, dass unabhängige Prüfungen helfen die Sicherheit von KI zu erhöhen.

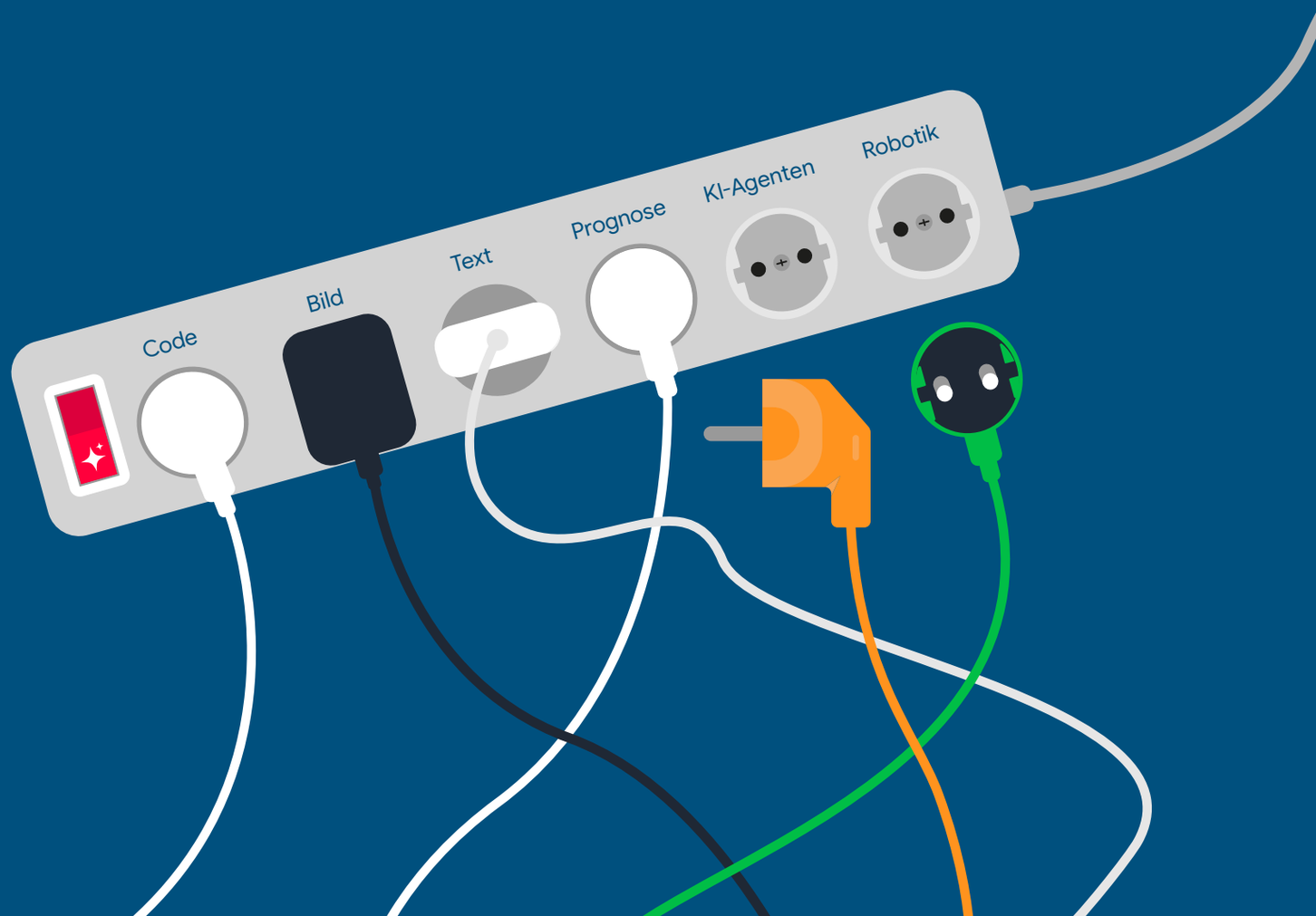
71%
fühlen sich schlecht über die Anforderungen des AI Act informiert.



59%
haben verbindliche interne Richtlinien für den KI-Einsatz.

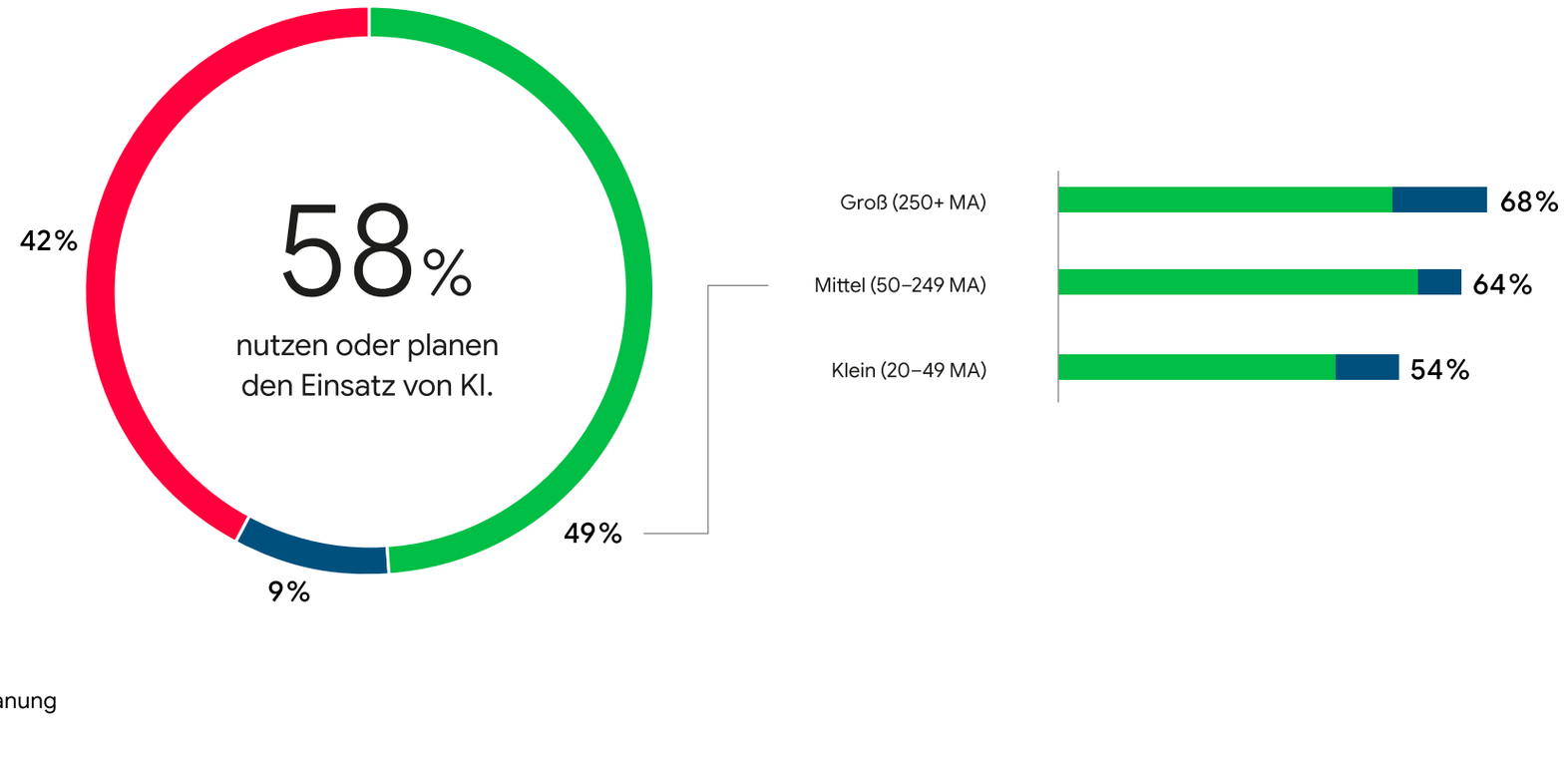
KI-Anwendung: Einsatzformen und Nutzungsgrad

1



Die Mehrheit der Unternehmen nutzt KI oder plant deren Einsatz

Setzt Ihr Unternehmen aktuell KI-Anwendungen ein?



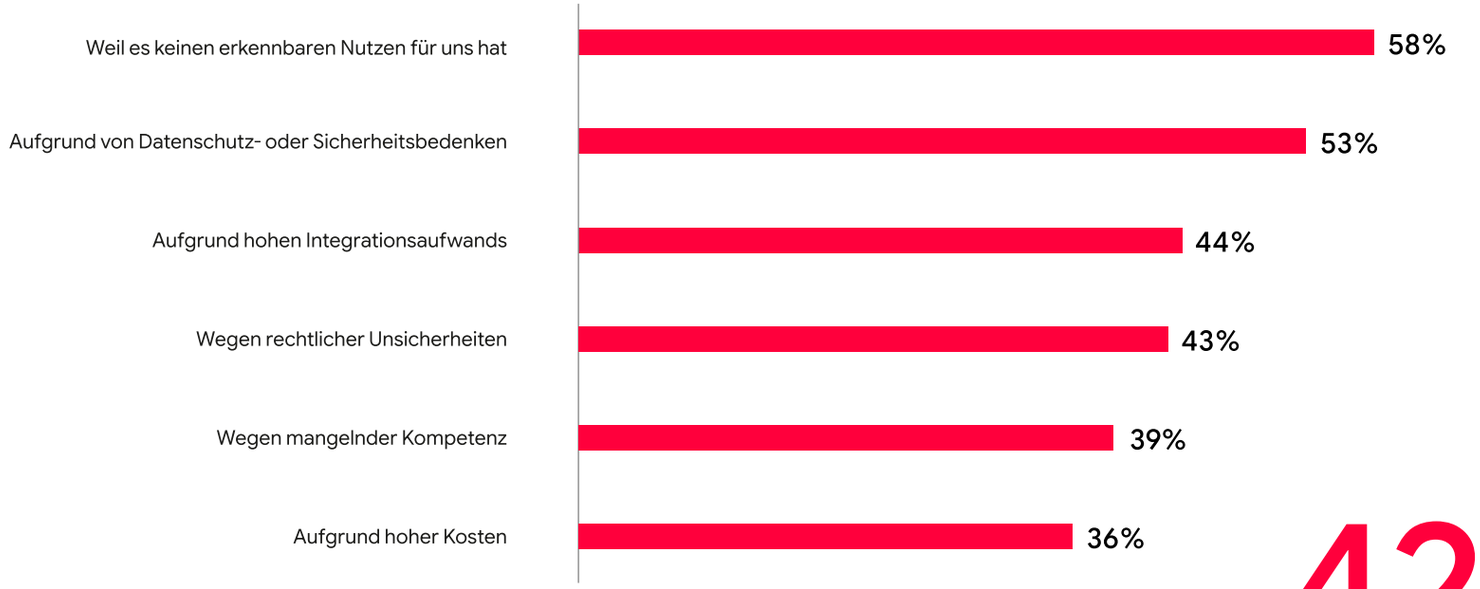
Frage: Mit Künstlicher Intelligenz, kurz „KI“, meinen wir im Folgenden Software, die Inhalte erzeugt, Daten auswertet, Entscheidungen vorbereitet oder Abläufe automatisiert – zum Beispiel ChatGPT, Microsoft Copilot, Chatbots, Prognose- oder Erkennungssysteme sowie KI-gestützte Automatisierungen und KI-Agenten. Setzt Ihr Unternehmen aktuell KI-Anwendungen ein?
Basis: alle befragten Unternehmen (n = 505)

Mehr als die Hälfte setzt auf Künstliche Intelligenz. Überdurchschnittlich hoch ist die KI-Nutzung bei größeren Unternehmen.

Knapp vier Jahre nach der Veröffentlichung von ChatGPT in Deutschland ist der Einsatz Künstlicher Intelligenz (KI) in der deutschen Wirtschaft weit verbreitet. In knapp der Hälfte der befragten Unternehmen (49 Prozent) sind Anwendungen bereits im Einsatz. Bei rund einem Zehntel (9 Prozent) ist die KI-Nutzung geplant. Besonders häufig setzen größere Unternehmen auf KI. In rund zwei Dritteln der Betriebe mit 250 und mehr Beschäftigten (68 Prozent) wird KI verwendet oder es ist in Planung. Dies ist bei kleinen Unternehmen mit 10 bis 49 Beschäftigten deutlich seltener der Fall (54 Prozent).

Unklarer Nutzen und Sicherheitsbedenken sind die größten Hindernisse

Aus welchen Gründen nutzt bzw. plant Ihr Unternehmen derzeit nicht, KI-Anwendungen einzusetzen?



42%

der Unternehmen nutzen bzw. planen derzeit nicht, KI-Anwendungen einzusetzen.

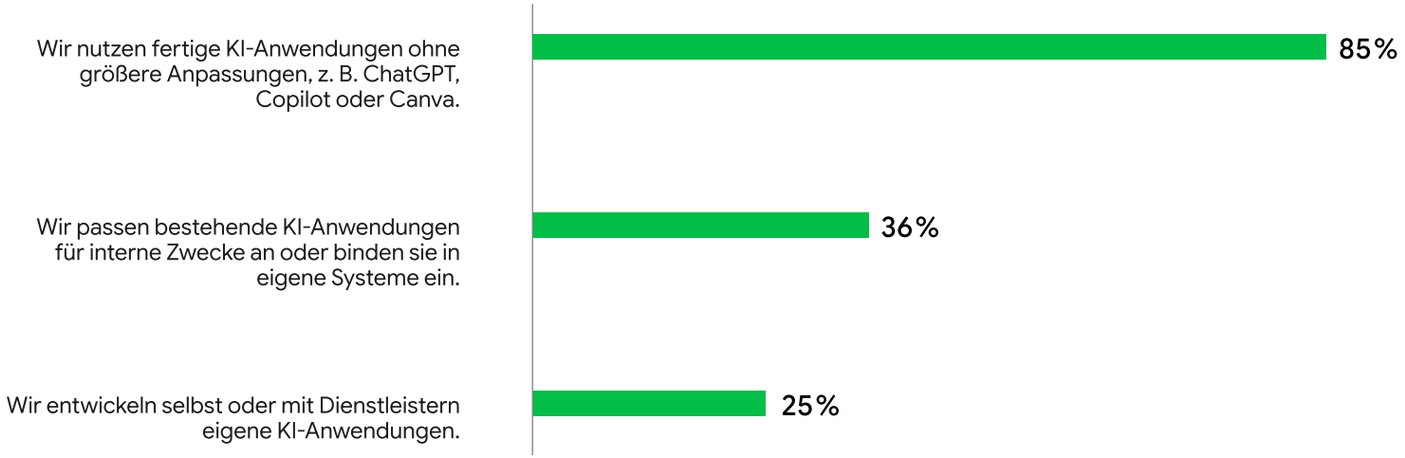
Frage: Aus welchen Gründen nutzt bzw. plant Ihr Unternehmen derzeit nicht, KI-Anwendungen einzusetzen? (Mehrfachantworten möglich)
Basis: Unternehmen, die KI aktuell nicht einsetzen und das nicht planen (n = 213)

Viele KI-skeptische Unternehmen befürchten zudem einen hohen Integrationsaufwand oder erkennen rechtliche Unsicherheiten.

Knapp zwei von fünf Unternehmen (42 Prozent) setzen keine KI-Anwendungen ein und planen auch nicht, dies zu ändern. Der am häufigsten genannte Grund dafür ist, dass kein Nutzen erkennbar ist (58 Prozent). Fast genauso häufig sorgen Datenschutz- oder Sicherheitsbedenken für Zurückhaltung (53 Prozent). Einen hohen Integrationsaufwand fürchten etwas weniger als die Hälfte (44 Prozent) der Unternehmen, die auf KI verzichten. Fast genauso häufig werden rechtliche Unsicherheiten als Argument gegen KI genannt (43 Prozent). Auch mangelnde Kompetenz (39 Prozent) und erwartete hohe Kosten (36 Prozent) bremsen.

Die breite Mehrheit setzt auf fertige KI-Anwendungen

Wie setzt Ihr Unternehmen KI derzeit ein?



49 %

der Unternehmen nutzen derzeit KI-Anwendungen.

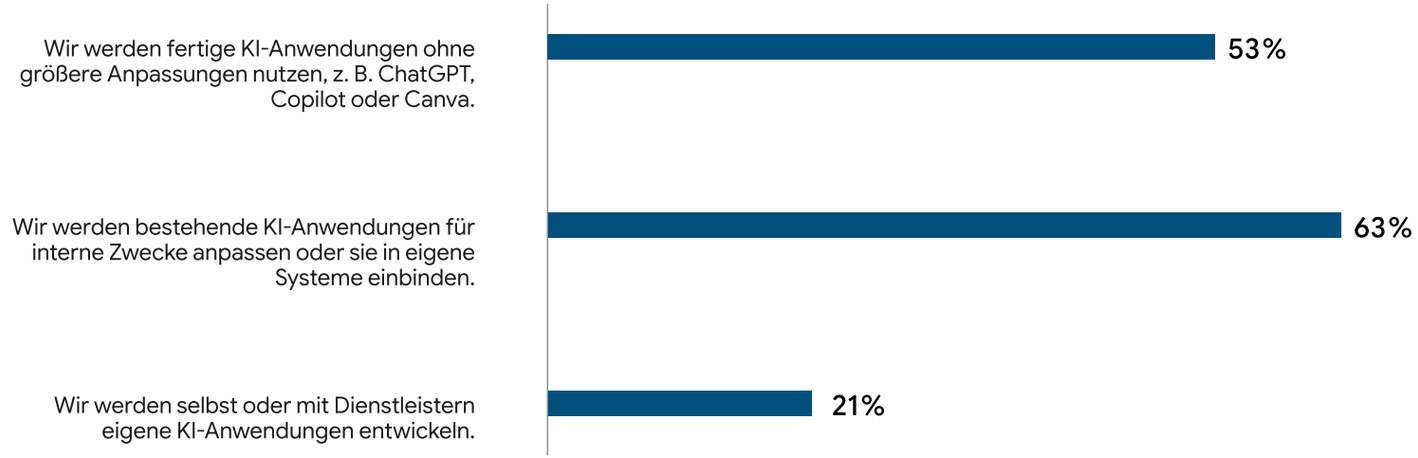
Frage: Wie setzt Ihr Unternehmen KI derzeit ein? (Mehrfachantworten möglich)
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Ein beträchtlicher Teil der Unternehmen stimmt KI-Anwendungen auch auf eigene Bedürfnisse ab oder entwickelt sie sogar komplett selbst.

ChatGPT, Microsoft Copilot oder Canva: Wenn KI bei Unternehmen im Einsatz ist, dann häufig als fertige Anwendung. Die breite Mehrheit (85 Prozent) nutzt Tools ohne größere Anpassungen. Etwas mehr als ein Drittel (36 Prozent) haben KI-Anwendungen an interne Anforderungen angepasst oder sie in die eigenen betrieblichen Systeme eingebunden. Ein Viertel (25 Prozent) entwickelt KI-Anwendungen komplett selbst oder mit Unterstützung von Dienstleistern.

Künftig wird KI häufiger an interne Anforderungen angepasst

Wie plant Ihr Unternehmen, KI einzusetzen?



9%

der Unternehmen planen derzeit, KI-Anwendungen einzusetzen.

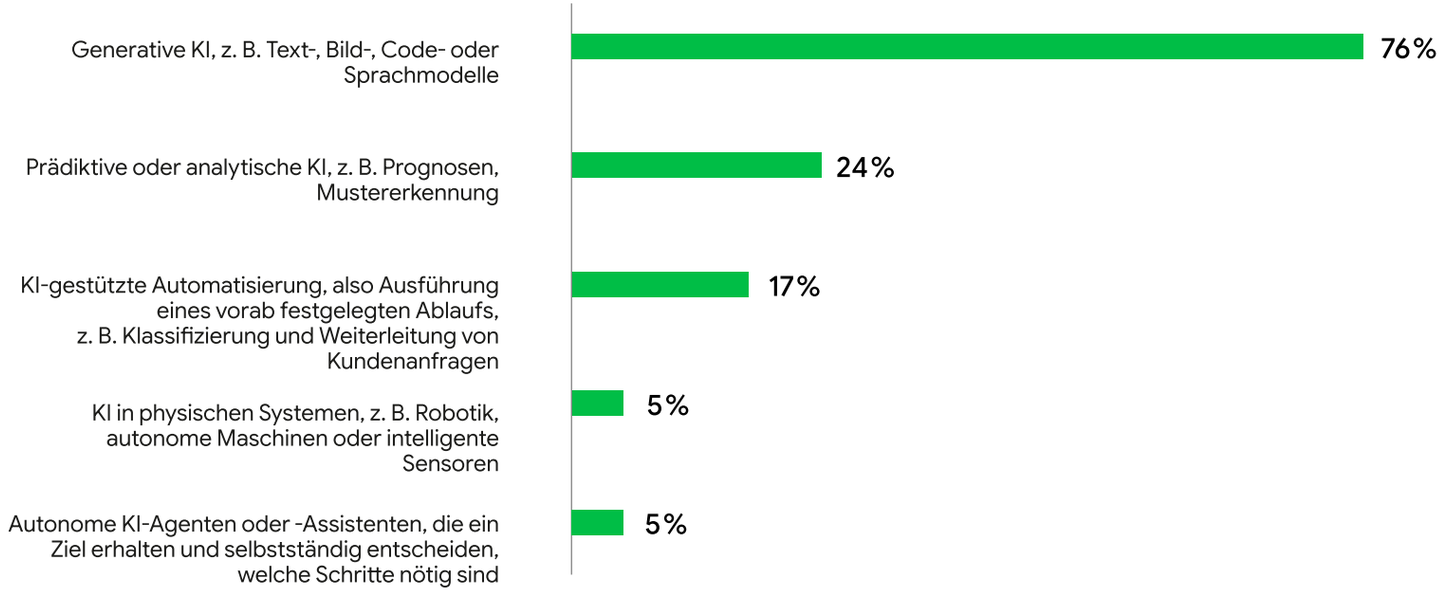
Frage: Wie plant Ihr Unternehmen, KI einzusetzen? (Mehrfachantworten möglich)
Basis: Unternehmen, die aktuell KI-Nutzung planen (n = 46)

Der Zuspruch für fertige Lösungen ist bei Unternehmen, die den KI-Einsatz erst planen, vergleichsweise niedrig.

KI-Anwendungen von der Stange oder als Maßanfertigung? Wenn der Einsatz von KI erst geplant ist, soll sie besonders oft für interne Zwecke angepasst oder in firmeneigene Systeme eingebunden werden. Dies geben fast zwei Drittel (63 Prozent) der Unternehmen an, die eine KI-Nutzung binnen zwölf Monaten anstreben. Gut die Hälfte von ihnen (53 Prozent) will fertige KI-Anwendungen ohne Anpassungen verwenden. Etwa einer von fünf Befragten (21 Prozent) strebt an, die Anwendungen selbst zu entwickeln.

Generative KI dominiert in Unternehmen

Welche Arten von KI setzt Ihr Unternehmen aktuell ein oder plant Ihr Unternehmen, einzusetzen?



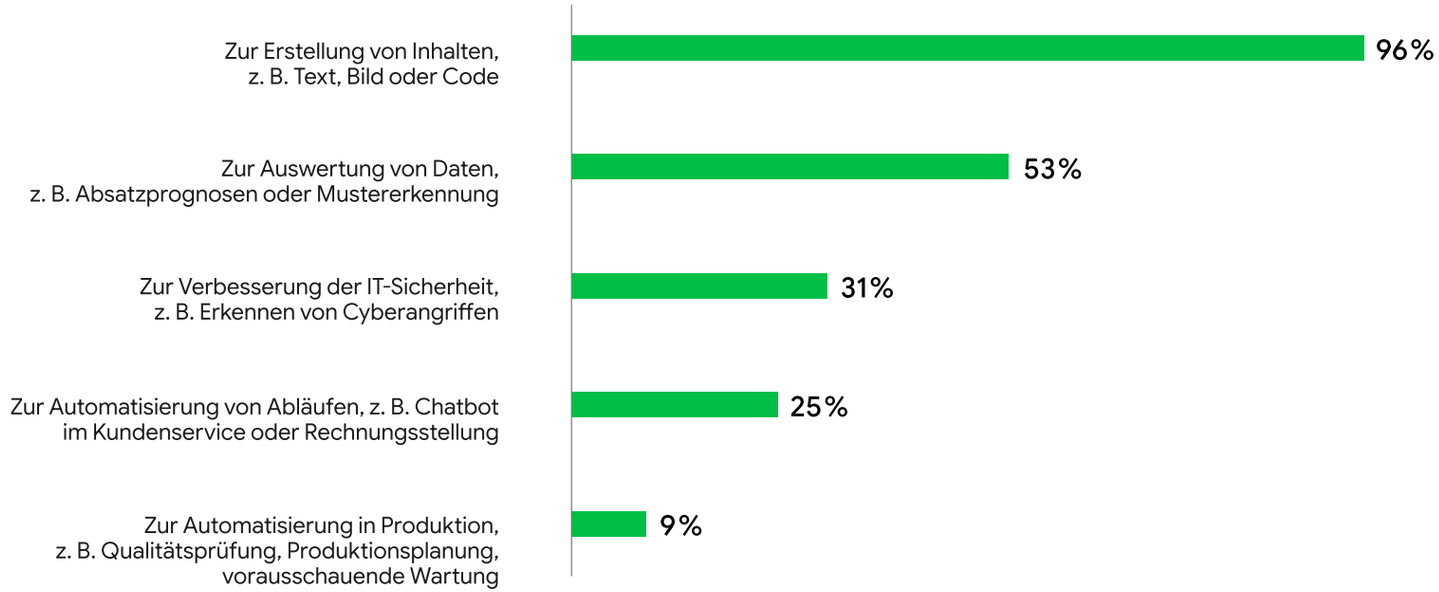
Frage: Welche Arten von KI setzt Ihr Unternehmen aktuell ein oder plant Ihr Unternehmen, einzusetzen? (Mehrfachantworten möglich)
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Abgeschlagen auf Platz 2 und 3 der Nutzung liegen analytische KI und KI-gestützte Automatisierung.

Rund drei Viertel (76 Prozent) der befragten Unternehmen haben generative KI im Einsatz - etwa Text-, Bild, Code- oder Sprachmodelle. Knapp ein Viertel (24 Prozent) nutzt analytische KI etwa für Prognosen. Bei rund einem von sechs Unternehmen (17 Prozent) automatisiert KI einzelne Prozesse, zum Beispiel bei Kundenanfragen. KI in Maschinen oder Sensoren oder aber KI-Agenten, die selbstständig handeln, finden sich jeweils in einem von 20 Unternehmen (5 Prozent).

KI wird vor allem zur Erstellung von Text, Bild und Code genutzt

Für welche Einsatzzwecke nutzt Ihr Unternehmen KI aktuell?



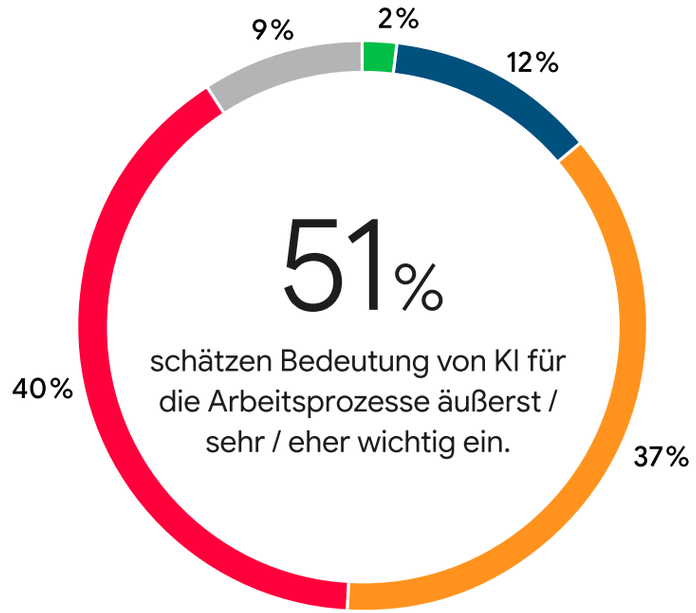
Frage: Für welche Einsatzzwecke nutzt Ihr Unternehmen KI aktuell? (Mehrfachantworten möglich)
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Jedes zweite Unternehmen nutzt KI zur Datenanalyse.

Das häufigste Einsatzgebiet für KI ist das Erstellen von Inhalten wie Texten, Bildern und Code. In fast allen Unternehmen, die KI verwenden, ist dies der Fall (96 Prozent). Etwas mehr als die Hälfte der Unternehmen, die KI nutzen, werten mit intelligenter Software Daten aus – etwa für die Prognose von Verkäufen (53 Prozent). Eine erhöhte IT-Sicherheit, beispielsweise durch den Einsatz zur frühzeitigen Erkennung von Cyberangriffen erhofft sich jeder dritte Befragte. Um die Automatisierung von Abläufen geht es bei einem Viertel (25 Prozent). Die Automatisierung der Produktion unterstützt KI aktuell bei knapp einem Zehntel (9 Prozent).

KI ist für viele Arbeitsprozesse wichtig

Wie wichtig ist der Einsatz von KI-Anwendungen aktuell für die gesamten Prozesse und Arbeitsweisen in Ihrem Unternehmen?



Frage: Wie wichtig ist der Einsatz von KI-Anwendungen aktuell für die gesamten Prozesse und Arbeitsweisen in Ihrem Unternehmen: äußerst wichtig, sehr wichtig, eher wichtig, weniger wichtig oder unwichtig? Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Mehr als die Hälfte der Unternehmen mit KI-Einsatz misst ihr eine hohe Bedeutsamkeit für betriebliche Prozesse und Arbeitsweisen bei.

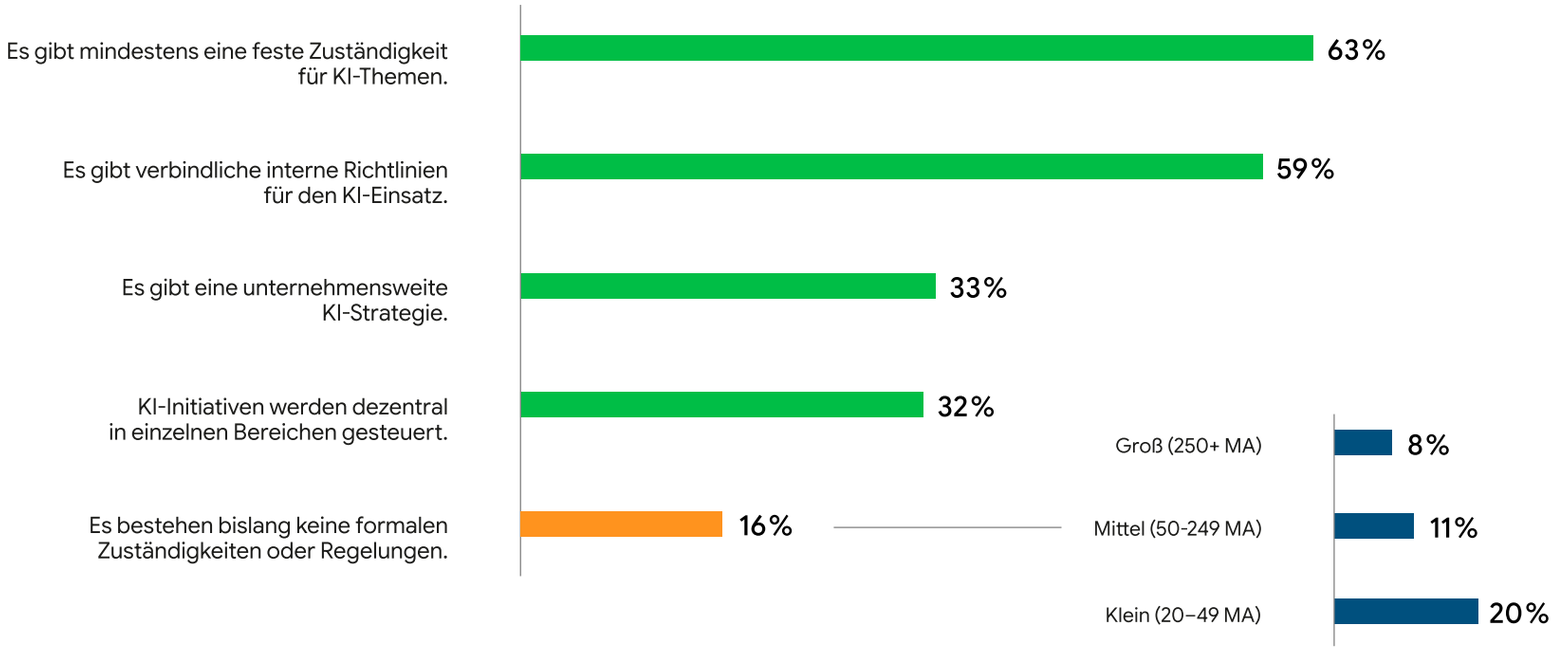
Ist KI wichtig für die gesamten Prozesse und Arbeitsweisen? Etwas mehr als die Hälfte der Unternehmen, die KI im Einsatz haben, stimmen hier zu (51 Prozent). Als besonders wichtig wird dies jedoch von deutlich weniger Befragten erachtet (12 Prozent). Unternehmen, die die KI-Nutzung noch planen, schreiben deren Wirkung auf Abläufe deutlich häufiger eine Bedeutung zu (81 Prozent). Als besonders wichtig erachtet dies fast ein Drittel (30 Prozent) – mehr als doppelt so viele wie bei den Unternehmen mit KI im Einsatz.

Strategie, Verantwortung und Kompetenzen

2

Feste Zuständigkeiten und interne Richtlinien sind weit verbreitet

Wie ist der KI-Einsatz in Ihrem Unternehmen organisatorisch und strategisch verankert?



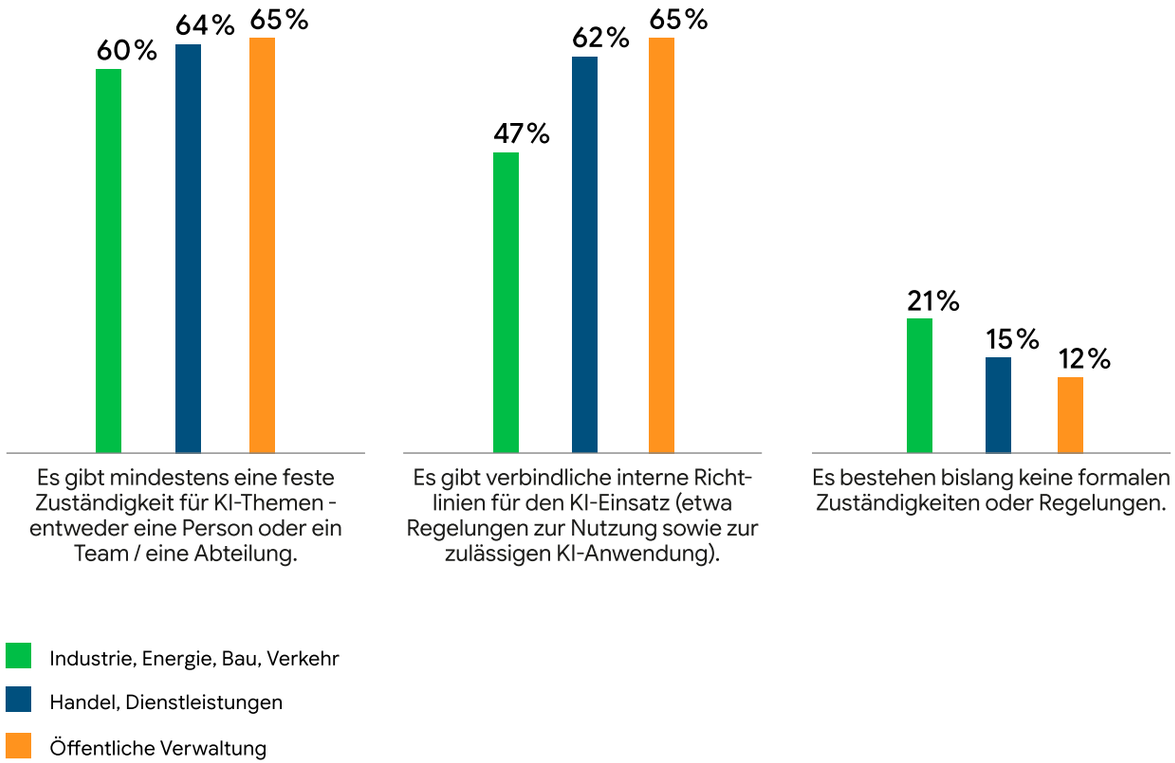
Allerdings haben deutlich weniger als die Hälfte der Unternehmen, die KI nutzen, eine entsprechende Strategie entwickelt.

Eine feste Zuständigkeit für KI-Themen gibt es bei einer deutlichen Mehrheit der Unternehmen, die KI nutzen (63 Prozent). Ähnlich hoch ist der Anteil der Unternehmen, die verbindliche interne Richtlinien für den KI-Einsatz festgeschrieben haben (59 Prozent). Eine unternehmensweite KI-Strategie findet sich bei rund einem Drittel (33 Prozent) – ähnlich hoch ist die Zustimmung bei der dezentralen Steuerung von KI-Initiativen in einzelnen Bereichen (32 Prozent). Das komplette Fehlen von formalen Zuständigkeiten oder Regelungen bildet in Unternehmen mit KI-Einsatz die Ausnahme (16 Prozent). In größeren Unternehmen ab 250 Beschäftigten finden sich überdurchschnittlich häufig feste Zuständigkeiten, verbindliche Richtlinien sowie eine unternehmensweite Strategie zum KI-Einsatz.

Frage: Wie ist der KI-Einsatz in Ihrem Unternehmen organisatorisch und strategisch verankert? Welche der folgenden Aspekte treffen zu?
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Verwaltung und Handel haben häufiger Richtlinien

Wie ist der KI-Einsatz in Ihrem Unternehmen organisatorisch und strategisch verankert?



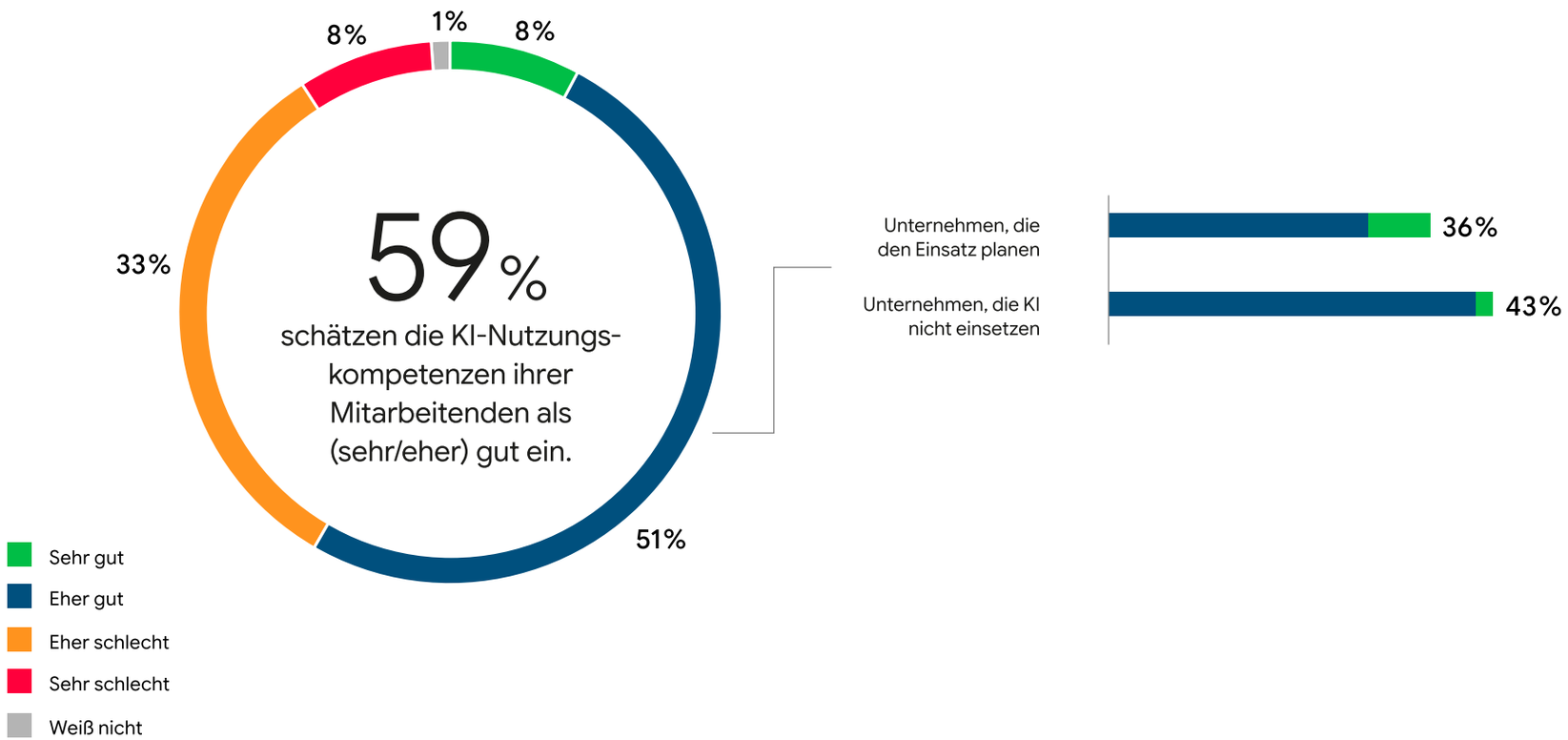
Frage: Wie ist der KI-Einsatz in Ihrem Unternehmen organisatorisch und strategisch verankert? Welche der folgenden Aspekte treffen zu?
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Im produzierenden Gewerbe und dem Energiesektor dagegen sind Regeln zur KI-Nutzung oder zu zulässigen KI-Anwendungen seltener.

Die Umfrage zeigt hier deutliche Unterschiede zwischen einzelnen Sektoren. So finden sich interne Richtlinien für Künstliche Intelligenz im produzierenden Gewerbe sowie dem Energiesektor bei weniger als der Hälfte der Unternehmen, die KI nutzen (47 Prozent). Bei Handel und Dienstleistungen (62 Prozent) und in der öffentlichen Verwaltung (65 Prozent) liegt der Anteil deutlich höher. Vergleichbar häufig dagegen gibt es in allen Branchen eine feste Zuständigkeit für KI. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt einzelne Branchen besonders beim Umgang mit KI, z.B. durch einen Prüfkatalog für den Finanzsektor sowie Empfehlungen für den KI-Einsatz im Gesundheitswesen oder der Verwaltung.

Mehrheit der KI-Nutzenden betrachtet die Beschäftigten als gut vorbereitet

Zum KI-Kompetenzniveau in Ihrem Unternehmen: Wie gut sind die Mitarbeitenden in Ihrem Unternehmen insgesamt darauf vorbereitet, KI sicher und sinnvoll zu nutzen?



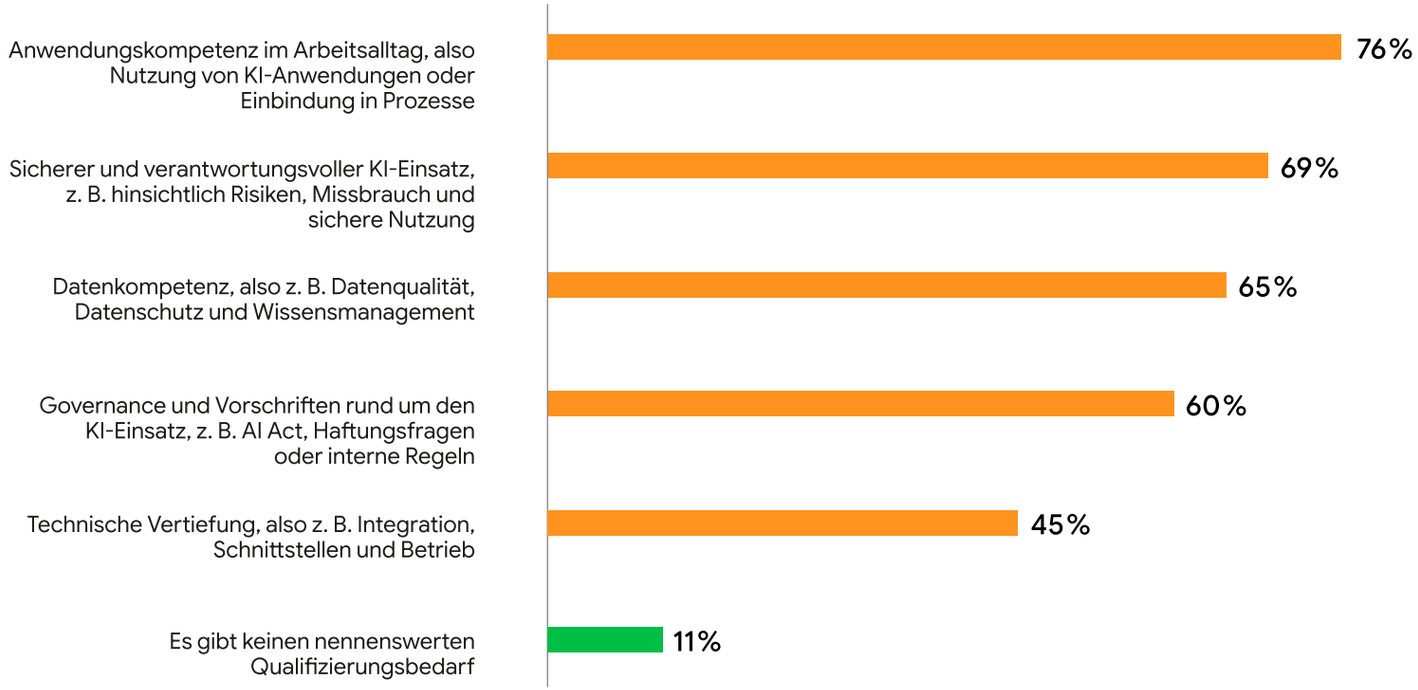
Frage: Zum KI-Kompetenzniveau in Ihrem Unternehmen: Wie gut sind die Mitarbeitenden in Ihrem Unternehmen insgesamt darauf vorbereitet, KI sicher und sinnvoll zu nutzen? Ist das... Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246), Unternehmen, die aktuell KI-Nutzung planen (n = 46) und Unternehmen, die KI nicht einsetzen und das nicht planen (n = 213)

Unternehmen, die in den kommenden zwölf Monaten KI einsetzen wollen, bewerten dagegen die Belegschaft überwiegend als wenig kompetent.

Sind die Mitarbeitenden gut auf den sicheren und sinnvollen Umgang mit KI vorbereitet? Die Mehrheit der Unternehmen, die KI nutzen, betrachtet die Belegschaft als ausreichend kompetent (59 Prozent). Als deutlich geringer wird das Kompetenzniveau der eigenen Beschäftigten von Unternehmen bewertet, die den KI-Einsatz erst planen (36 Prozent). Sogar ein größerer Anteil der Unternehmen, die KI gar nicht einsetzen und dies auch nicht planen, erachtet die eigenen Mitarbeitenden als gut vorbereitet (43 Prozent).

Höchster Schulungsbedarf bei Anwendung und Sicherheit

In welchen Bereichen braucht Ihr Unternehmen am ehesten mehr Wissen oder Schulungen zum Umgang mit KI?



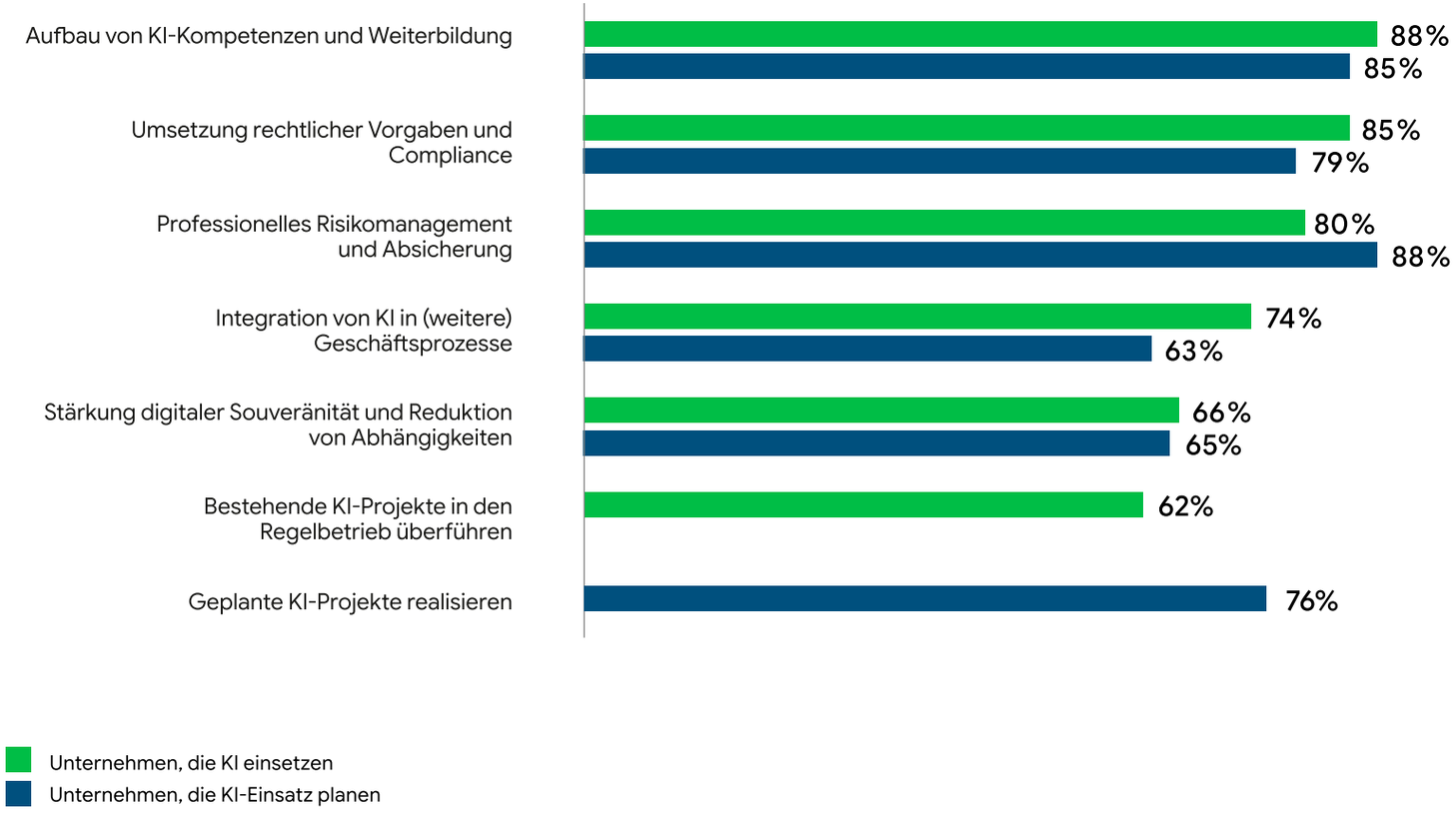
Frage: In welchen Bereichen braucht Ihr Unternehmen am ehesten mehr Wissen oder Schulungen zum Umgang mit KI? (Mehrfachantworten möglich)
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Neben dem Aufbau von individuellen KI-Fähigkeiten der Beschäftigten ist vielen Unternehmen auch die Aufklärung über Risiken wichtig.

KI selbst nutzen oder in Prozesse einbinden: Bei diesen Fähigkeiten sehen rund drei Viertel der Unternehmen, die KI im Einsatz haben, einen Weiterbildungsbedarf (76 Prozent). Etwas mehr als zwei Drittel von ihnen (69 Prozent) erachten mehr Wissen für einen sicheren Umgang mit KI als nötig. Rund zwei Drittel (65 Prozent) erkennen am ehesten Schulungsbedarf bei der Datenkompetenz. Drei von fünf Unternehmen nennen Governance und Vorschriften – von Haftungsfragen bis hin zu internen Regeln – als wichtiges Weiterbildungsfeld (60 Prozent). Dass kein KI-Qualifizierungsbedarf besteht, gibt eine Minderheit an (11 Prozent).

Weiterbildung, Compliance und Risikomanagement prägen die KI-Agenda

Maßnahmen, die für den KI-Einsatz im Unternehmen in den nächsten zwei Jahren wichtig sind.



Frage: Wie wichtig sind die folgenden Maßnahmen für Ihr Unternehmen mit Blick auf den Einsatz von KI in den nächsten 2 Jahren: sehr wichtig, eher wichtig, weniger wichtig oder unwichtig? (Antworten für sehr/eher wichtig) Basis: Unternehmen, die KI-Anwendungen aktuell nutzen oder deren Einsatz planen (n = 246 | n = 46)

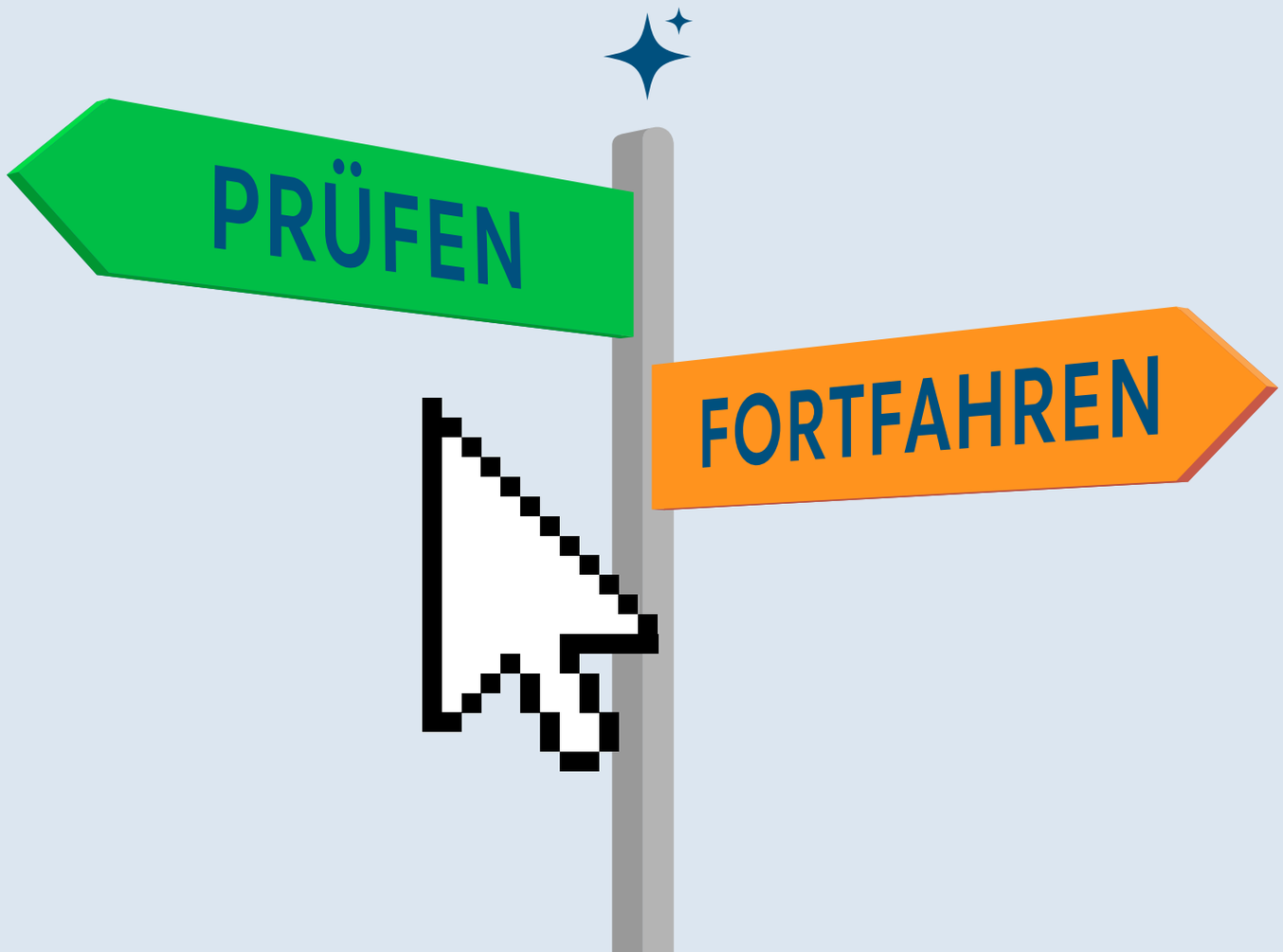
In den nächsten beiden Jahren wollen Unternehmen eine ganze Reihe von Aufgaben meistern – bis hin zur verstärkten KI-Integration in Geschäftsprozesse und Stärkung der digitalen Souveränität.

Der Aufbau von KI-Kompetenzen und die Weiterbildung der Beschäftigten haben für die meisten Unternehmen, die KI nutzen, in den kommenden zwei Jahren hohe Priorität: Fast neun von zehn Befragten (88 Prozent) erachten dies als wichtig. Bei Unternehmen, die den KI-Einsatz planen, ist die Zustimmung ähnlich hoch (85 Prozent). Ihnen ist in den nächsten beiden Jahren allerdings noch häufiger ein professionelles Risikomanagement wichtig (88 Prozent) – der Zustimmungswert bei KI-Nutzenden liegt etwas darunter (80 Prozent). Viel Bedeutung beigemessen wird der Umsetzung rechtlicher Fragen und Compliance sowohl von Firmen mit KI im Einsatz (85 Prozent) wie auch von Unternehmen, die KI-Anwendungen erst planen (79 Prozent).

KI-Auswahl und Integration in die Arbeitsumgebung

3

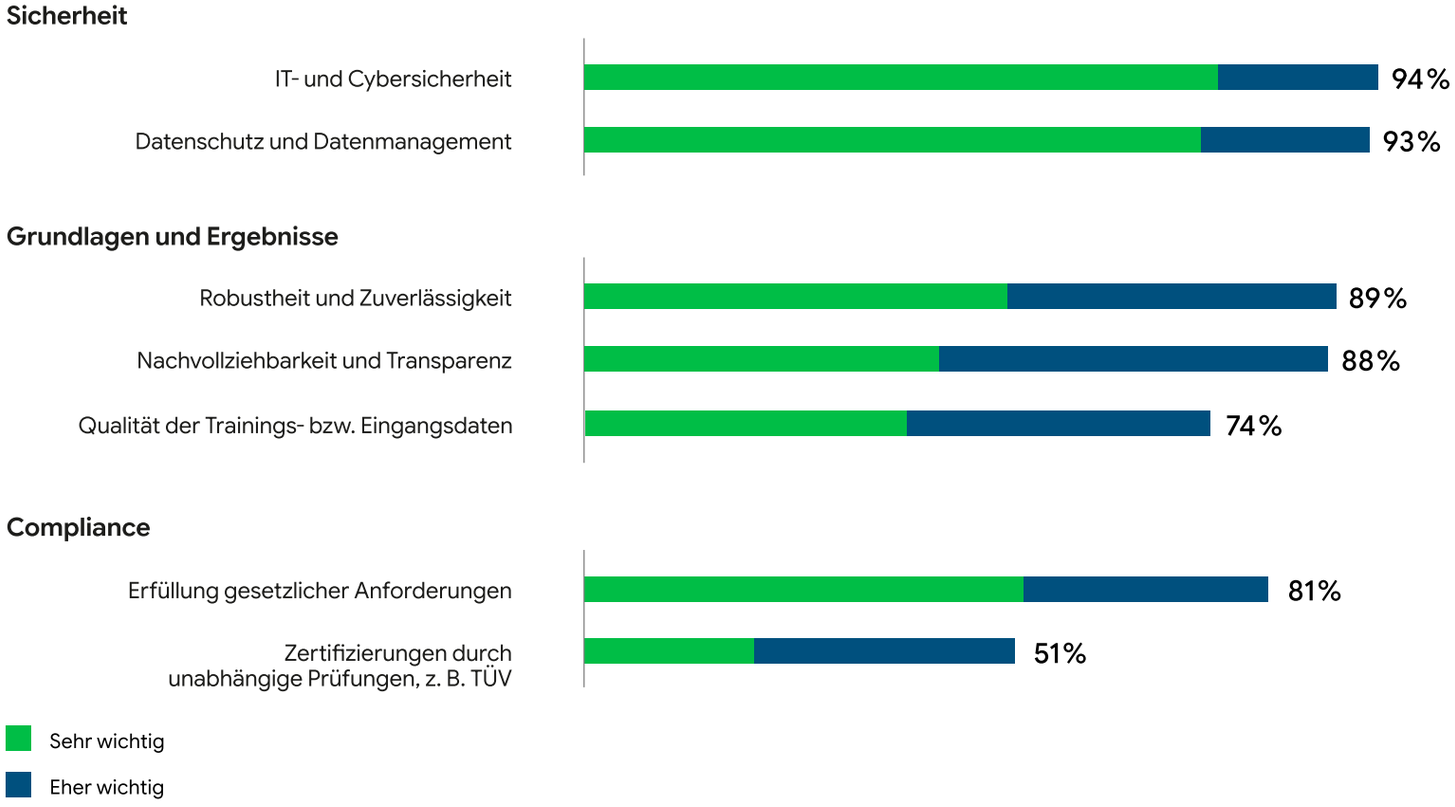
Kriterien und Sicherheit



3.1

IT-Sicherheit und Datenschutz haben höchste Priorität

Wie wichtig sind die folgenden Sicherheitskriterien bei der Auswahl von KI-Anwendungen?



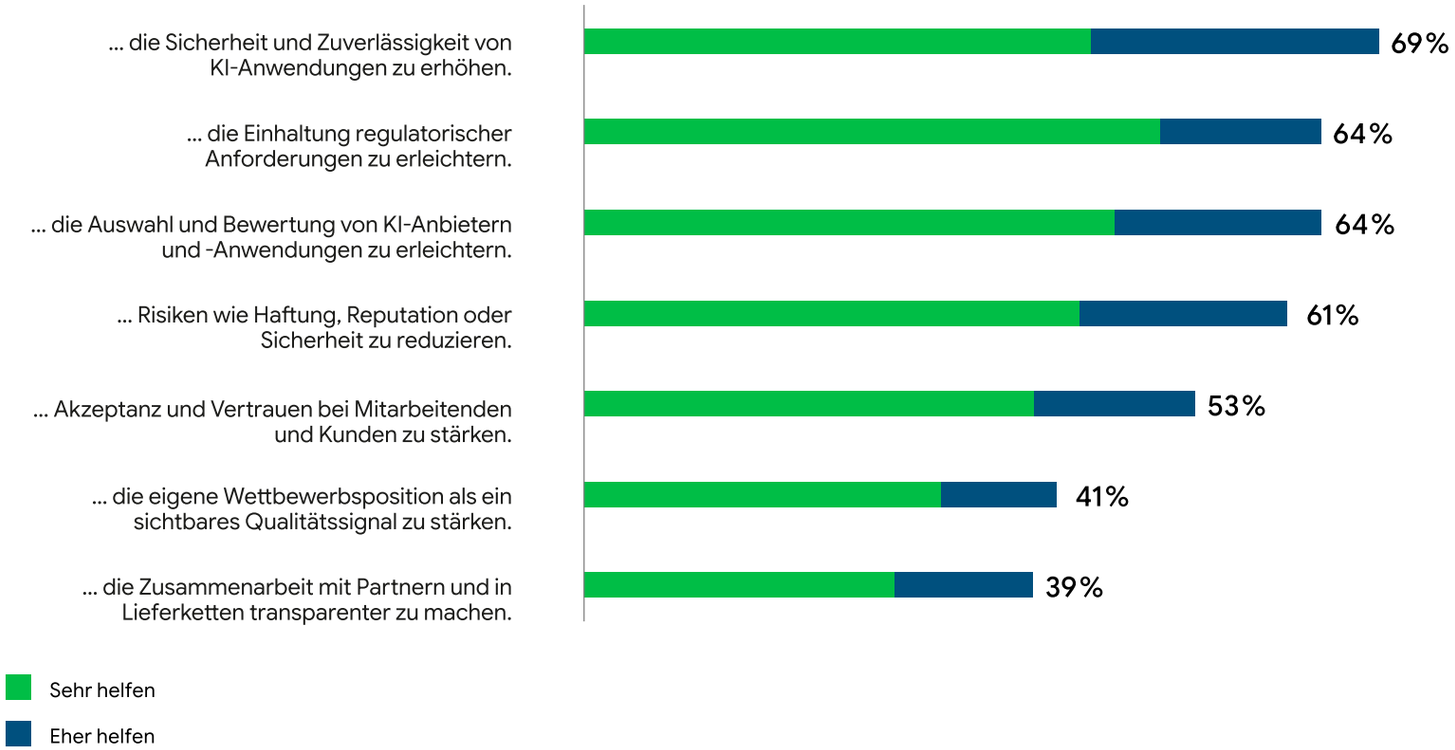
Frage: Wie wichtig sind Ihrem Unternehmen die folgenden Sicherheitskriterien bei der Auswahl von KI-Anwendungen: sehr wichtig, eher wichtig, weniger wichtig oder unwichtig? (Mehrfachantworten möglich) Basis: Unternehmen, die KI-Anwendungen aktuell nutzen oder deren Einsatz planen (n = 292)

Auch Robustheit, Zuverlässigkeit und Transparenz sind für Unternehmen wichtige Sicherheitskriterien bei der Auswahl von KI-Anwendungen.

Welche Sicherheitskriterien sind den Unternehmen, die KI nutzen oder dies planen, wichtig? Fast alle Befragten geben an, dass ihnen IT- und Cybersicherheit (94 Prozent) sowie Datenschutz und Datenmanagement (93 Prozent) wichtig sind. Eine breite Mehrheit legt Wert auf Robustheit und Zuverlässigkeit (89 Prozent), also z.B. geringe Fehlerraten und Stabilität sowie auf Nachvollziehbarkeit und Transparenz (88 Prozent), wie z.B. Erklärbarkeit und Protokollierung. Die Qualität der Trainings- bzw. Eingangsdaten hat für rund drei Viertel (74 Prozent) Bedeutung. Etwa vier von fünf Unternehmen (81 Prozent) legen Wert darauf, dass ihre KI-Anwendungen gesetzliche Anforderungen erfüllen. Einer Mehrheit (51 Prozent) sind Zertifizierungen durch unabhängige Prüforganisationen wie dem TÜV wichtig.

Unternehmen: „Prüfungen erhöhen die Sicherheit und erleichtern die Auswahl“

Unabhängige Prüfungen bzw. Zertifizierungen von KI-Anwendungen würden dabei helfen, …



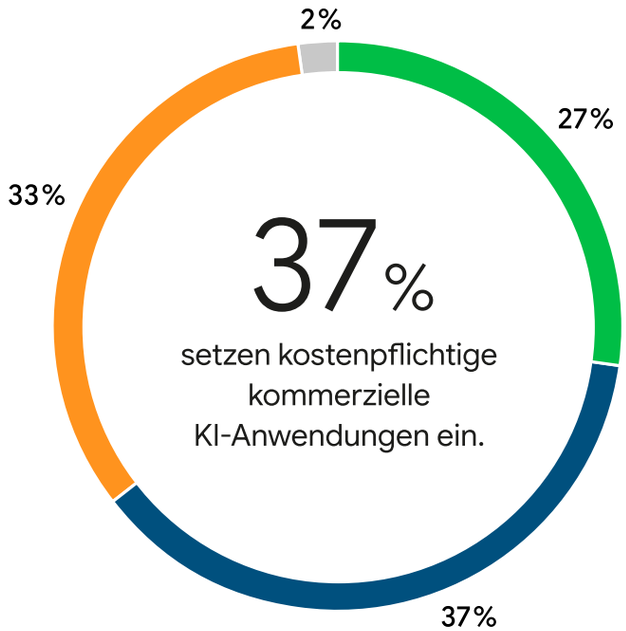
Frage: Wie sehr würden – Ihrer Einschätzung nach – unabhängige Prüfungen bzw. Zertifizierungen von KI-Anwendungen Ihrem Unternehmen dabei helfen, …
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen oder deren Einsatz planen (n = 292)

Unternehmen erwarten zudem, dass Zertifizierungen dabei helfen, regulatorische Anforderungen zu erfüllen.

Eine höhere Sicherheit und Zuverlässigkeit von KI-Anwendungen: Dies versprechen sich mehr als zwei Drittel der Unternehmen, die KI nutzen oder dies planen, von unabhängigen Prüfungen oder Zertifizierungen (69 Prozent). Jeweils knapp zwei Drittel erwarten positive Effekte auf die Einhaltung regulatorischer Anforderungen sowie die Auswahl von KI-Anwendungen (je 64 Prozent). Rund drei von fünf (61 Prozent) Befragten meinen zudem, dass unabhängige Prüfungen dabei helfen, Risiken zu verringern. 53 Prozent gehen davon aus, dass Zertifizierungen Akzeptanz und Vertrauen bei Mitarbeitenden und Kunden stärken. Rund zwei von fünf Unternehmen (41 Prozent) sehen darin ein Zeichen für Qualität mit positiven Auswirkungen auf die eigene Wettbewerbsposition. 39 Prozent versprechen sich mehr Transparenz in der Zusammenarbeit mit Partnern und in Lieferketten.

Kommerzielle KI-Modelle liegen bei Nutzung leicht vorne

Verwendet Ihr Unternehmen überwiegend Open-Source-KI-Modelle, überwiegend kommerzielle KI-Modelle oder beides?



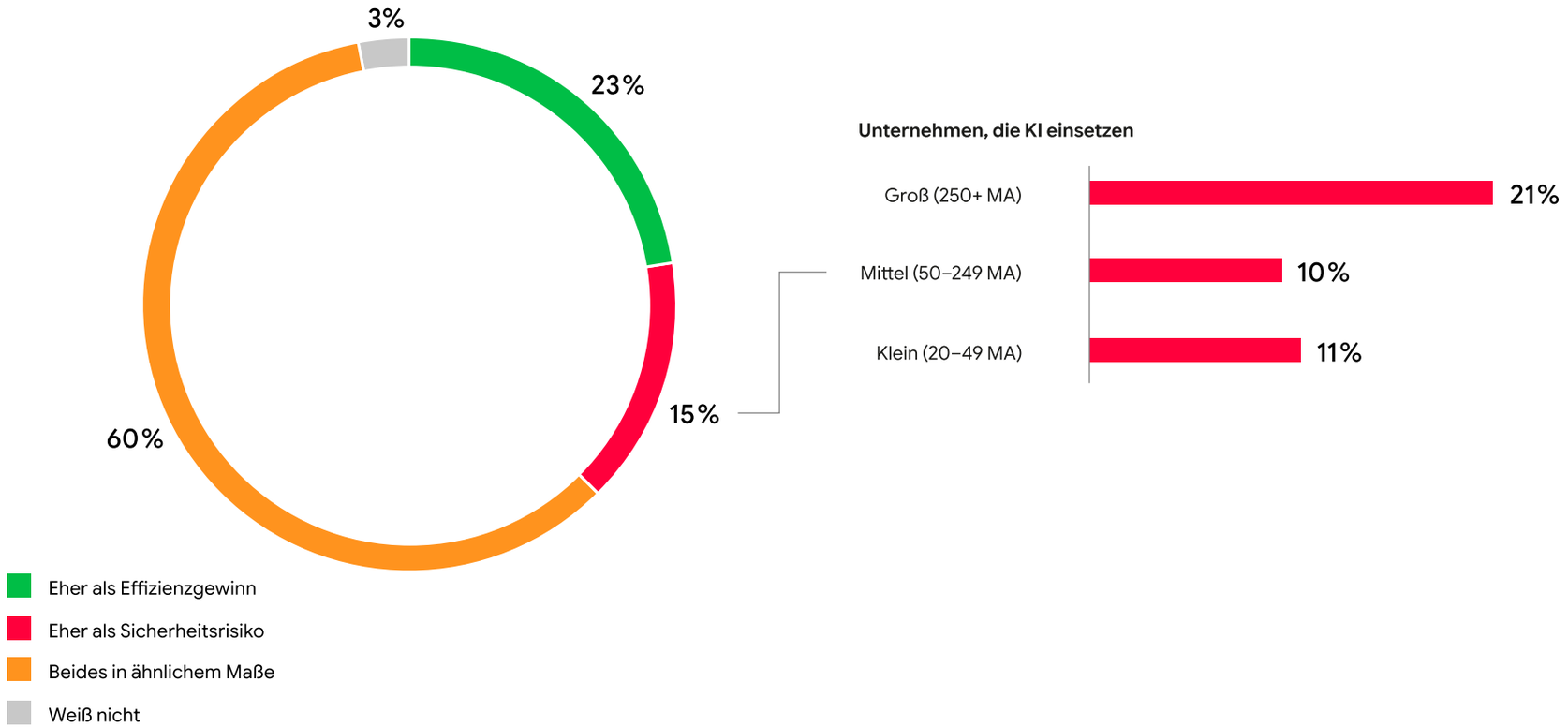
Frage: Verwendet Ihr Unternehmen überwiegend Open-Source-KI-Modelle (also frei verfügbare, anpassbare KI-Anwendungen), überwiegend kommerzielle KI-Modelle (proprietäre, kostenpflichtige KI-Anwendungen) oder beides? Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Auch Open-Source-Anwendungen finden viele Abnehmer. Bei künftigen KI-Nutzenden allerdings nimmt die Nachfrage nach diesen frei verfügbaren KI-Lösungen ab.

Den höchsten Zuspruch bei der KI-Nutzung erhalten kommerzielle und damit kostenpflichtige Modelle (37 Prozent). Doch auch die in der Anschaffung oft kostenlosen Open-Source-KI-Modelle finden sich bei vielen Unternehmen (27 Prozent). Ein Drittel (33 Prozent) hat beides im Einsatz. Größere Unternehmen ab 250 Beschäftigten wählen häufiger kommerzielle KI-Modelle (59 Prozent) – das gilt ebenfalls für das produzierende Gewerbe (44 Prozent). Bei Unternehmen, die den KI-Einsatz planen, liegt die Zahl der Befürworter von kommerziellen KI-Modellen ebenfalls über dem Durchschnitt (45 Prozent). Rund ein Drittel würde sowohl Open Source als auch kommerzielle Modelle einsetzen (34 Prozent). Deutlich weniger (16 Prozent) wollen vor allem auf Open Source setzen.

Integration von KI in klassische IT-Anwendungen: Fluch und Segen zugleich

Sehen Sie in der Integration von KI in Betriebssysteme, Office-Anwendungen und Arbeitsumgebungen überwiegend einen Effizienzgewinn, überwiegend ein Sicherheitsrisiko oder beides in ähnlichem Maße?



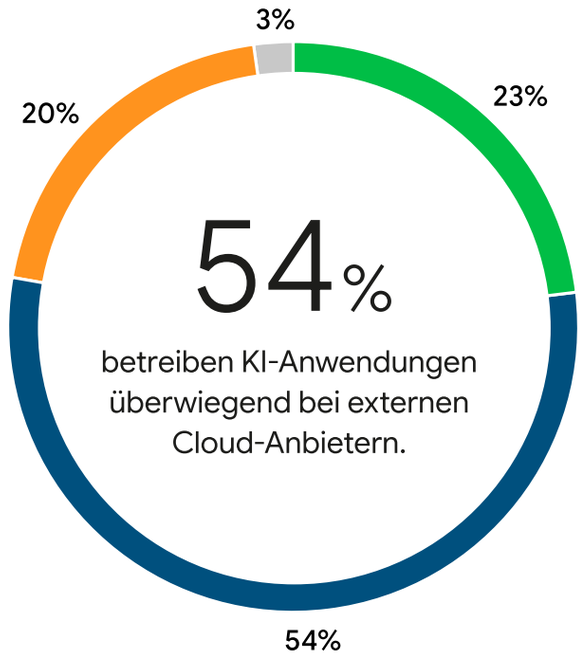
Frage: KI wird zunehmend direkt in Betriebssysteme, Office-Anwendungen und Workspace-Umgebungen integriert – zum Beispiel als Copilot in Microsoft 365, in Form von KI-gestützten Browsern, mit Claude Cowork oder ChatGPT Operator. Sehen Sie darin überwiegend einen Effizienzgewinn, überwiegend ein Sicherheitsrisiko oder beides in ähnlichem Maße? Basis: alle befragten Unternehmen (n = 505) | Unternehmen, die KI einsetzen (n = 246)

Die Mehrheit der Unternehmen sieht in der Integration von KI in Betriebssystemen und Software einen Effizienzgewinn. Zugleich werden Risiken gesehen.

Ist KI in Betriebssystemen oder Softwareanwendungen integriert, so löst dies überwiegend gemischte Gefühle aus. Die Mehrheit der Befragten (60 Prozent) erkennt Effizienzgewinne, aber auch Sicherheitsrisiken. Für knapp ein Viertel (23 Prozent) überwiegen die Effizienzgewinne. Rund einer von sieben Befragten (15 Prozent) erkennt vor allem Gefahren für die Sicherheit. Besonders skeptisch zeigen sich größere Unternehmen mit mehr als 250 Beschäftigten: Rund ein Fünftel (21 Prozent) hat Sicherheitsbedenken.

Mehr als die Hälfte betreibt Anwendungen in der Cloud

Wo werden die KI-Anwendungen Ihres Unternehmens überwiegend betrieben?

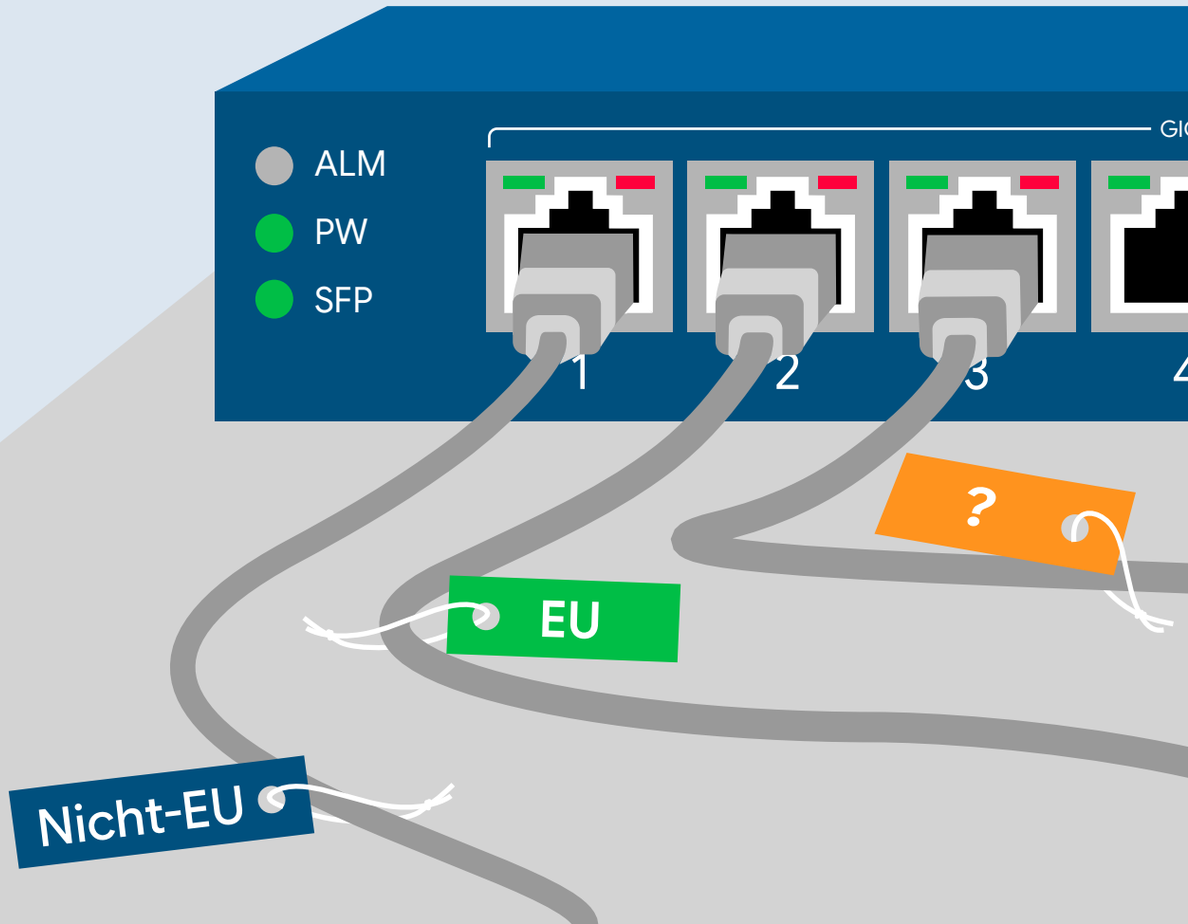


Frage: Werden die KI-Anwendungen in Ihrem Unternehmen überwiegend auf eigenen Servern bzw. eigener Infrastruktur betrieben, überwiegend bei externen Cloud-Anbietern oder beides? Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Jedes fünfte Unternehmen kombiniert externe Cloud-Dienste mit der eigenen IT-Infrastruktur.

Die externe Cloud ist für die meisten der Ort der Wahl für den Betrieb von KI-Anwendungen. Etwas mehr als die Hälfte der Unternehmen, die KI nutzen, setzen überwiegend darauf (54 Prozent). Ein knappes Viertel (23 Prozent) verwendet vor allem eigene Server oder Infrastruktur. Ein Fünftel (20 Prozent) kombiniert die beiden Optionen. Allerdings ist ein Streben nach mehr Kontrolle erkennbar. Unternehmen, die den Einsatz von KI planen, wollen häufiger (35 Prozent) auf eigene Server und seltener auf Cloud-Dienste setzen (29 Prozent). Knapp ein Drittel von ihnen würde beides nutzen (32 Prozent).

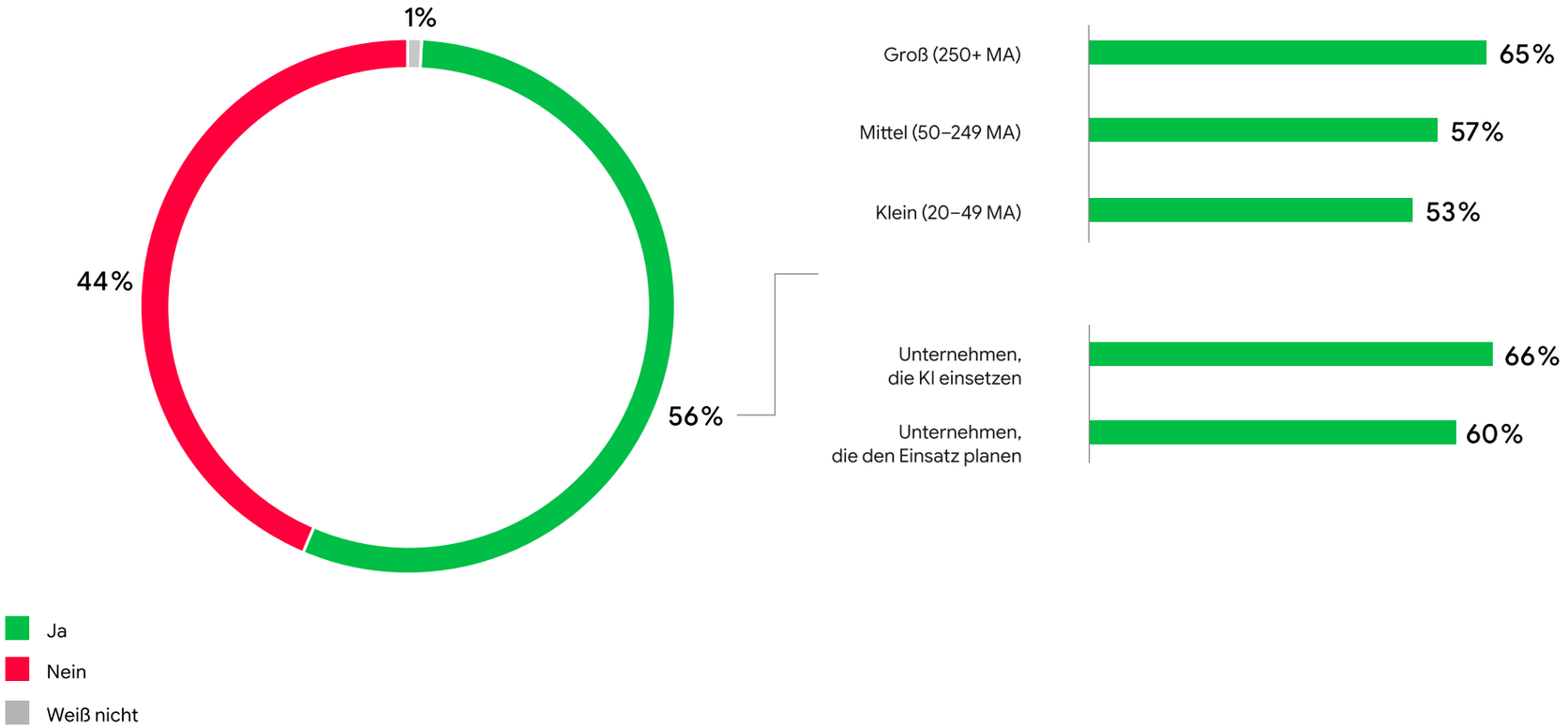
Digitale Souveränität und Abhängigkeiten



3.2

Europäische und deutsche KI-Angebote sind der Mehrheit bekannt

Sind Ihnen europäische oder deutsche KI-Anwendungen bekannt?

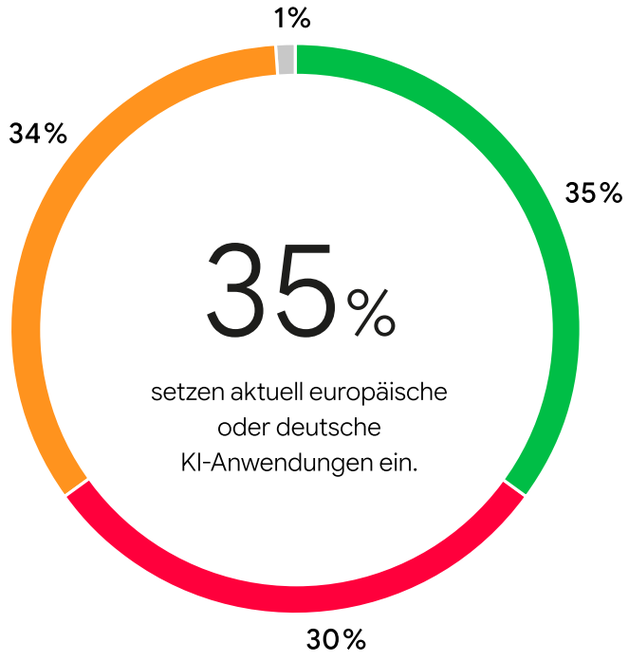


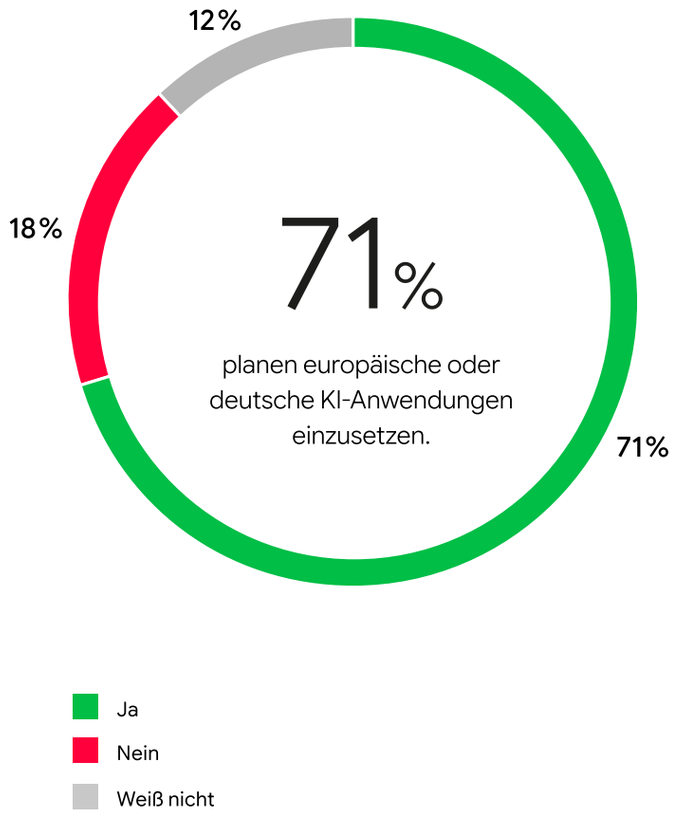
Frage: Sind Ihnen europäische oder deutsche KI-Anwendungen bekannt?
Basis: alle befragten Unternehmen (n = 505)

Überdurchschnittlich häufig sind größere Unternehmen und Dienstleistungsanbieter mit KI-Anwendungen aus Europa vertraut.

Die Mehrheit der Befragten kennt europäische oder deutsche KI-Anwendungen (56 Prozent). Etwas häufiger ist dies der Fall bei Unternehmen, die KI bereits nutzen (66 Prozent) oder dies planen (60 Prozent). Deutlich über dem Durchschnitt liegt der Dienstleistungssektor (70 Prozent). Grundsätzlich nimmt die Bekanntheit europäischer und deutscher KI-Anwendungen mit der Firmengröße zu. Am häufigsten mit ihnen vertraut sind Unternehmen mit 250 und mehr Beschäftigten (65 Prozent).

Ein Drittel setzt auf KI aus Europa und Deutschland





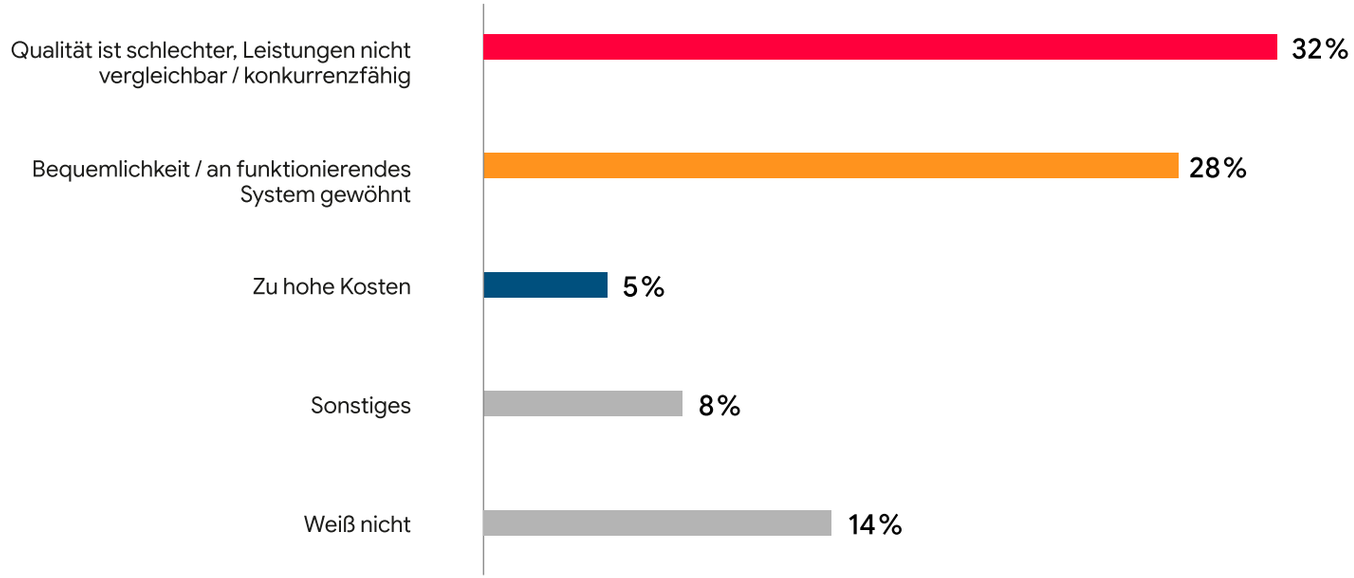
Frage: Setzt Ihr Unternehmen aktuell europäische oder deutsche KI-Anwendungen ein? Plant Ihr Unternehmen, europäische oder deutsche KI-Anwendungen einzusetzen?
Basis: Unternehmen, die KI einsetzen (n = 246), und Unternehmen, denen europäische oder deutsche KI-Anwendungen bekannt sind und die deren Einsatz planen (n = 28)

Viele Unternehmen, die europäische oder deutsche KI-Anwendungen kennen, planen deren Einsatz.

Wenn Unternehmen KI nutzen, dann stammen die Anwendungen oft aus Europa oder Deutschland. Bei rund einem Drittel (35 Prozent) ist dies der Fall. Besonders häufig ist KI aus Europa oder Deutschland in der öffentlichen Verwaltung (40 Prozent) sowie in Unternehmen mit 250 oder mehr Beschäftigten (43 Prozent) im Einsatz. Fast drei Viertel der Unternehmen, denen europäische oder deutsche KI-Anwendungen bekannt sind, wollen diese in Zukunft auch verwenden (71 Prozent).

Qualitätszweifel und Bequemlichkeit bremsen Nutzung europäischer KI

Warum nutzt Ihr Unternehmen aktuell keine europäischen oder deutschen KI-Anwendungen?



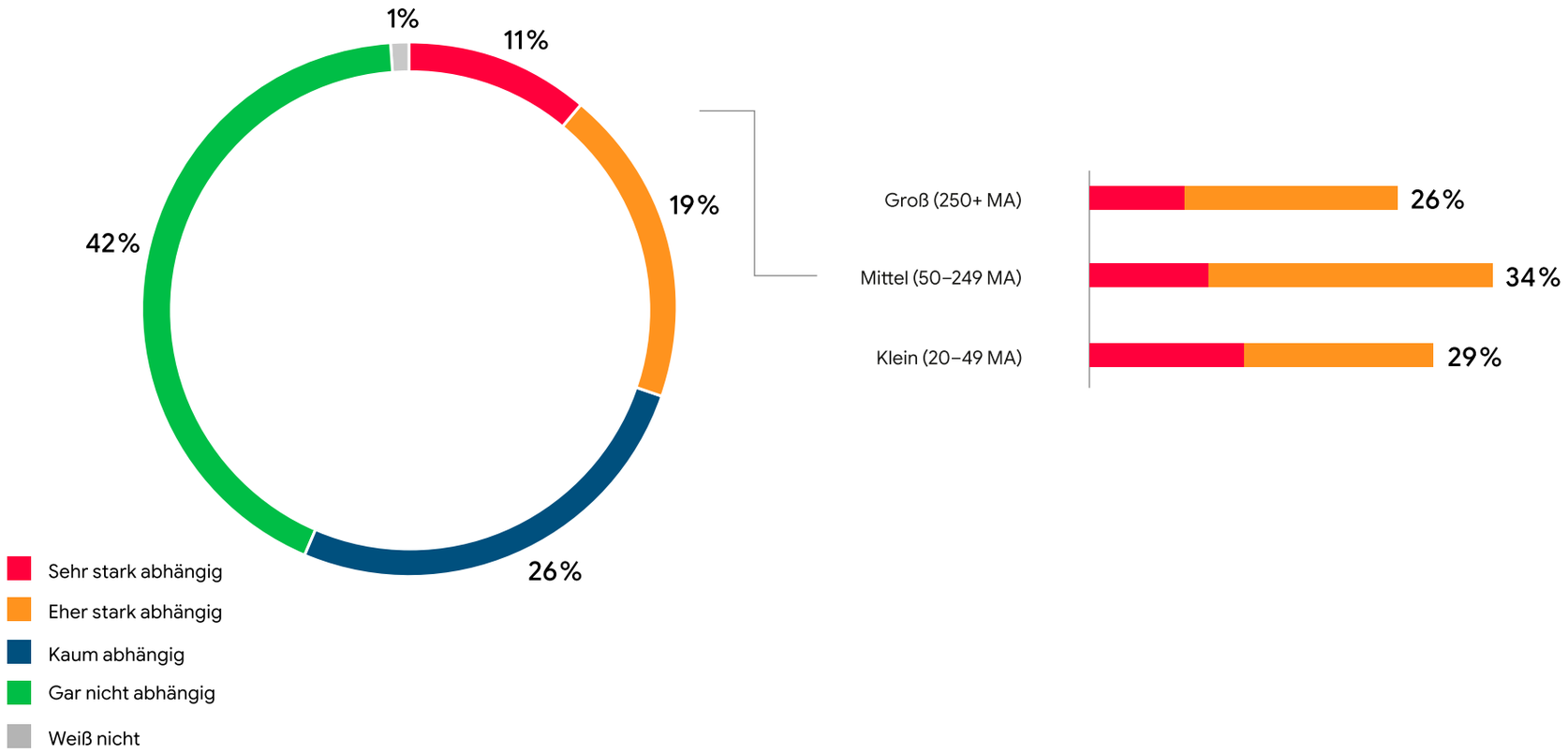
Frage: Aus welchen Gründen nutzt bzw. plant Ihr Unternehmen derzeit nicht, KI-Anwendungen aus Europa/Deutschland einzusetzen? (Auswahl)
Basis: Unternehmen, die europäische/deutsche KI-Anwendungen kennen, aber nicht nutzen (n = 74)

Können heimische KI-Anbieter mit der außereuropäischen Konkurrenz mithalten? Eine Reihe von Unternehmen glaubt das nicht.

Unternehmen, die KI nutzen und deutsche oder europäische KI-Anwendungen kennen, verzichten vor allem aus zwei Gründen auf deren Einsatz. Knapp ein Drittel bewerten die Qualität als schlechter (32 Prozent). Etwas mehr als ein Viertel will sich aus Bequemlichkeit nicht von einem außereuropäischen System trennen (28 Prozent). Zu hohe Kosten sind für eine Minderheit ein Argument gegen KI-Anwendungen aus Europa oder Deutschland (5 Prozent).

Beträchtliche Abhängigkeit von außereuropäischen Anbietern

Ist Ihr Unternehmen derzeit von außereuropäischen KI-Anbietern abhängig?



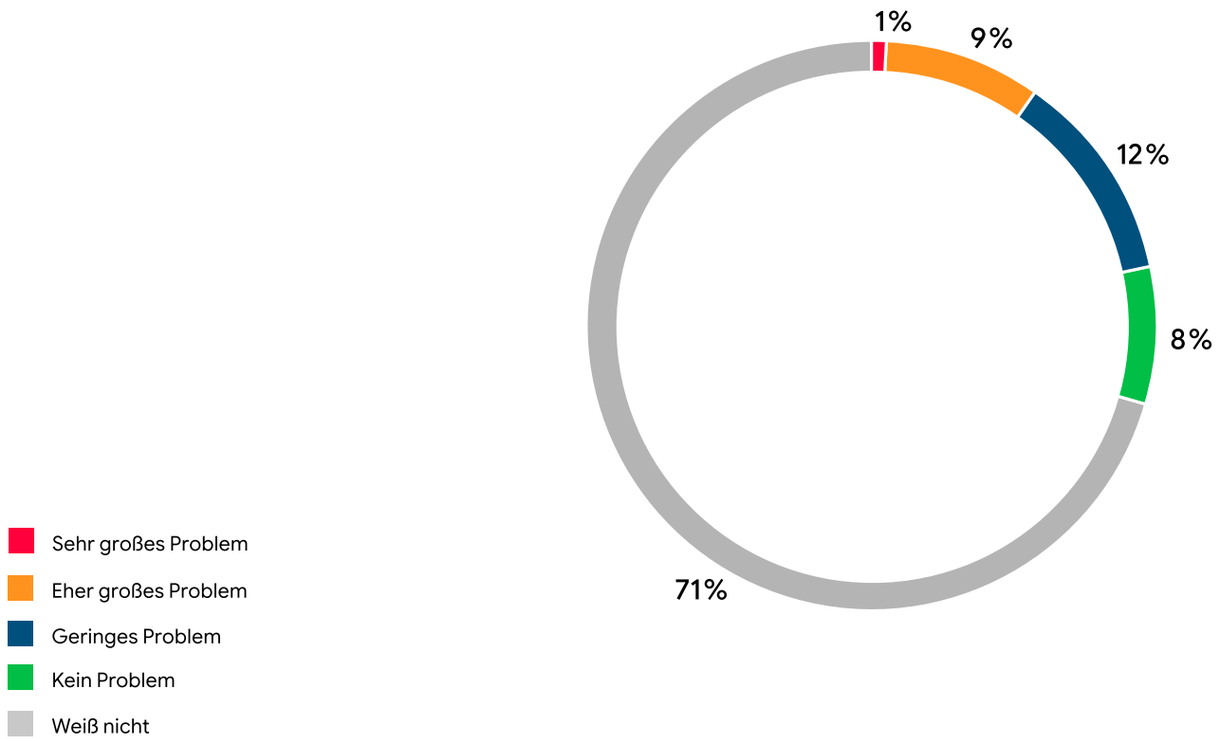
Frage: Ist Ihr Unternehmen derzeit sehr stark, eher stark, kaum oder gar nicht von außereuropäischen KI-Anbietern, also z. B. aus den USA, abhängig?
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Knapp ein Drittel der Unternehmen mit KI-Nutzung sieht sich als abhängig.

Eine sehr starke oder zumindest eher starke Abhängigkeit von KI-Anbietern außerhalb Europas – in dieser Lage sieht sich knapp ein Drittel (30 Prozent) der Unternehmen, die KI nutzen. Die deutliche Mehrheit allerdings (68 Prozent) erkennt nur geringe oder gar keine Abhängigkeit. Besonders häufig wird Abhängigkeit von Unternehmen mit 50 bis 249 Beschäftigten wahrgenommen (34 Prozent).

Folgen der Abhängigkeit von außereuropäischer KI sind vielen unklar

Stellt diese Abhängigkeit von außereuropäischen KI-Anbietern für Ihr Unternehmen ein Problem dar?



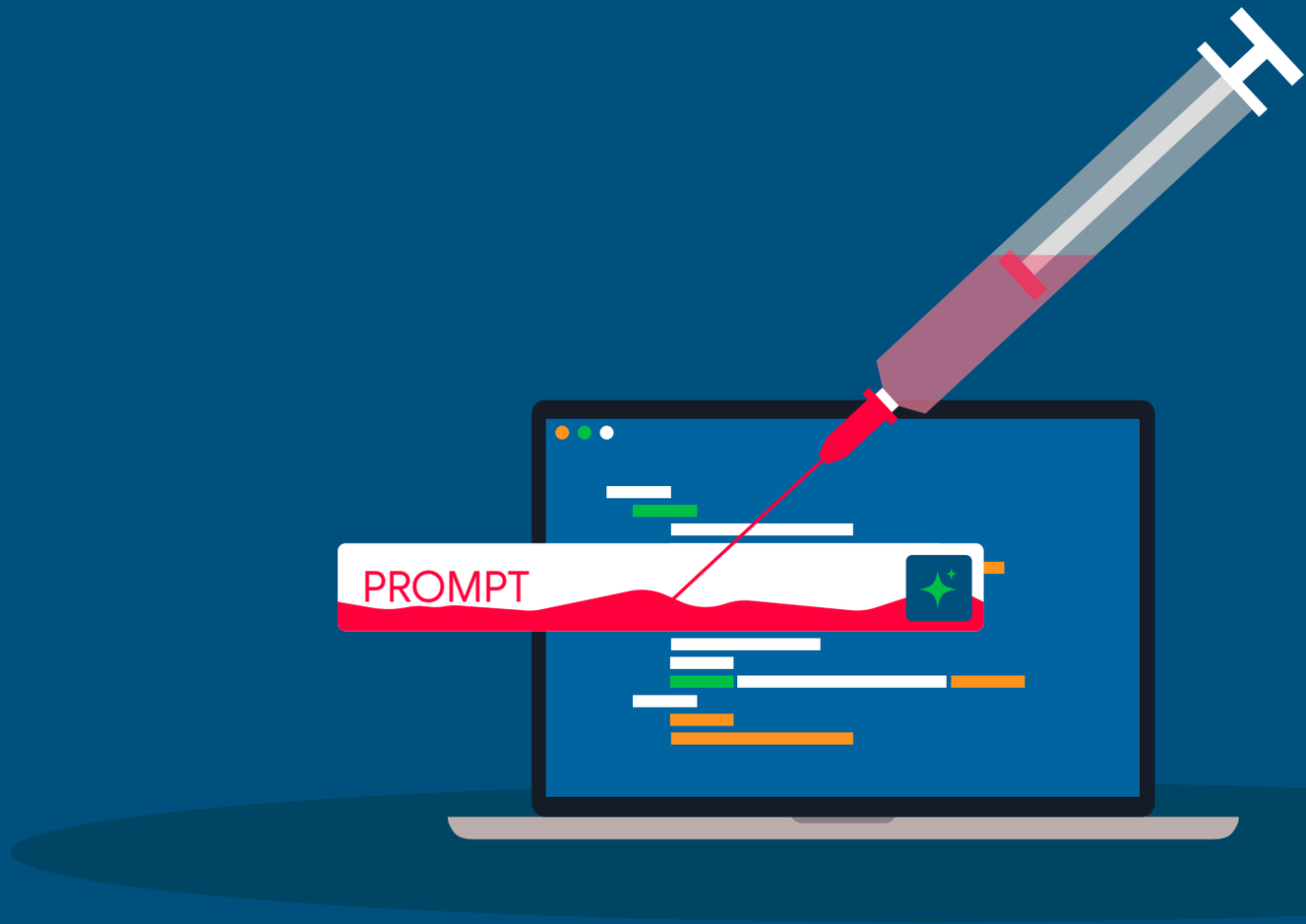
Frage: Stellt diese Abhängigkeit von außereuropäischen KI-Anbietern für Ihr Unternehmen ein sehr großes, großes, geringes oder kein Problem dar?
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Nur eine Minderheit erkennt beträchtliche Probleme darin, auf KI-Anbieter außerhalb Europas angewiesen zu sein – die meisten können hierzu keine Aussage treffen.

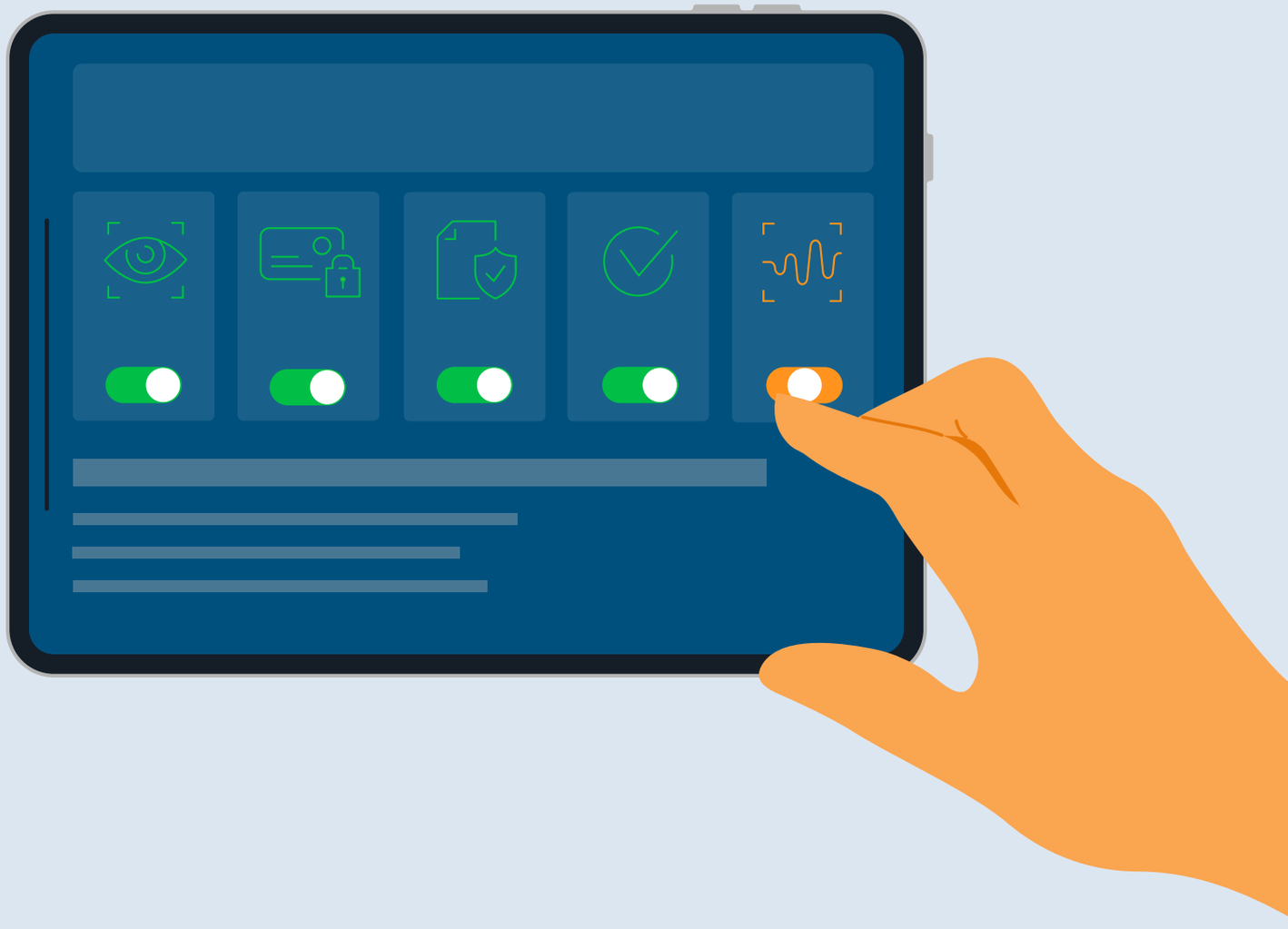
Nur eines von 100 Unternehmen, die KI nutzen, bezeichnet es als „sehr großes Problem", von außereuropäischen Anbietern abhängig zu sein (1 Prozent). In knapp einem von zehn Fällen (9 Prozent) wird ein „eher großes Problem" erkannt. Bei der Mehrheit allerdings herrscht Unklarheit darüber, ob die Abhängigkeit von KI-Anbietern außerhalb Europas negative Folgen hat. Fast drei Viertel können dazu keine Aussage treffen (71 Prozent). Ein Fünftel (20 Prozent) bewertet die Abhängigkeit von außereuropäischen KI-Anbietern als eher oder vollständig unproblematisch.

Risiken der KI-Nutzung

4



Sicherheitsstrategien



4.1

Viele Unternehmen setzen auf KI-Schulungen

Welche organisatorischen Maßnahmen hat Ihr Unternehmen für den KI-Einsatz getroffen?

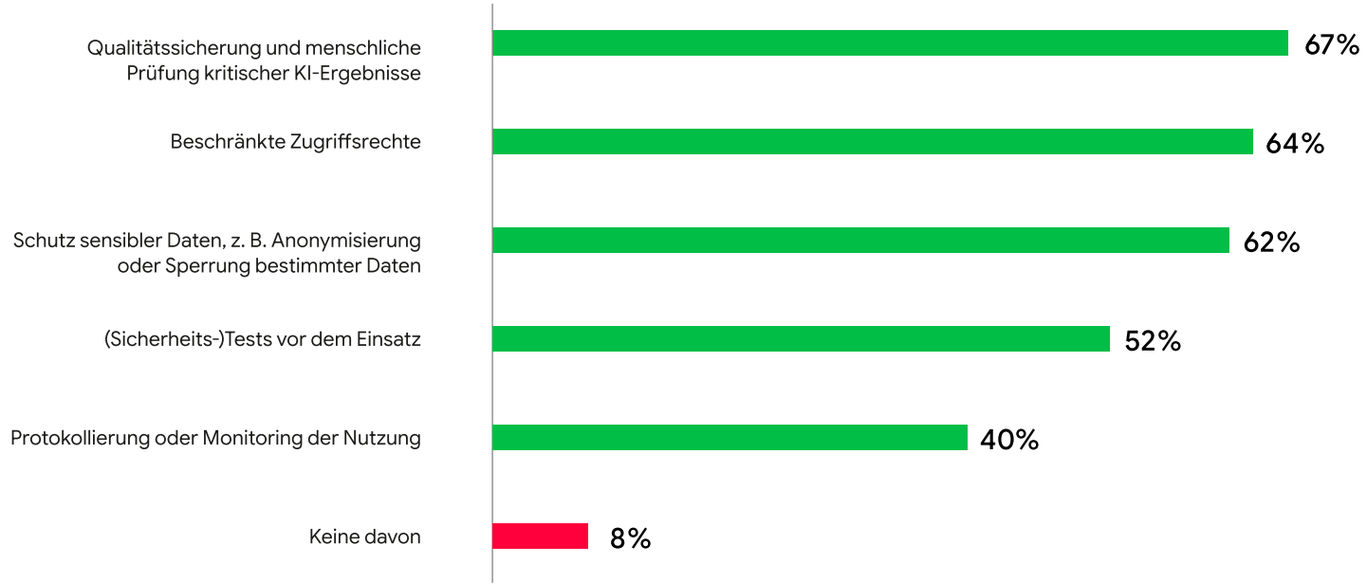
Frage: Welche organisatorischen Maßnahmen hat Ihr Unternehmen für den KI-Einsatz getroffen? Gibt es … (Mehrfachantworten möglich)
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Risikobewertungen und Freigabeprozesse für KI-Anwendungen haben ebenfalls einen hohen Stellenwert.

Schulungen sind die wichtigste organisatorische Maßnahme für einen sicheren KI-Einsatz. Über die Hälfte der Unternehmen (56 Prozent) bieten sie der Belegschaft entweder mit allgemeinen oder rollenspezifischen Inhalten. Jeweils knapp die Hälfte (45 Prozent) hat bei KI-Anwendungen eine Risikobewertung und Klassifizierung vorgenommen oder vor dem betrieblichen Einsatz einen Freigabeprozess eingerichtet. Bei rund zwei von fünf Unternehmen (42 Prozent) mussten sich KI-Lieferanten oder -Anbieter einer Prüfung unterziehen. In größeren Unternehmen werden alle Maßnahmen deutlich häufiger eingesetzt als in kleineren Betrieben. Knapp ein Drittel (29 Prozent) der Unternehmen, die KI nutzen, haben keine dieser Maßnahmen getroffen. Bei Firmen mit 250 und mehr Beschäftigten sind es deutlich weniger (15 Prozent).

Zwei Drittel lassen kritische KI-Ergebnisse noch einmal prüfen

Welche technischen Schutzmaßnahmen hat Ihr Unternehmen für den KI-Einsatz getroffen?



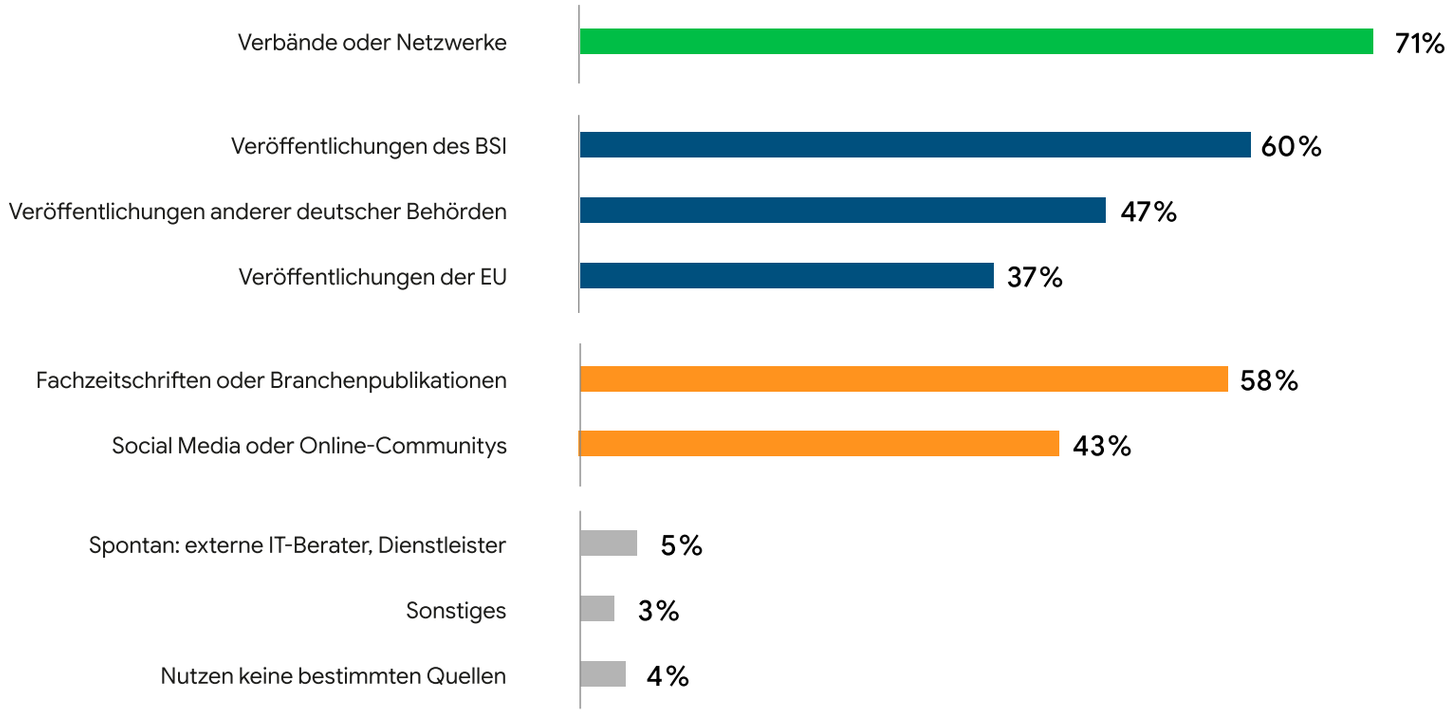
Frage: Welche technischen Schutzmaßnahmen hat Ihr Unternehmen für den KI-Einsatz getroffen? (Mehrfachantworten möglich)
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen (n = 246)

Ganz ohne Schutzmaßnahmen für die KI-Systeme arbeitet nur eine Minderheit der Unternehmen.

Mit vielfältigen Maßnahmen sichern Unternehmen die KI-Nutzung ab. Am häufigsten werden Qualitätssicherung und die Prüfung kritischer KI-Ergebnisse durch Beschäftigte genannt (67 Prozent). Artikel 14 des AI Act sieht für Hochrisiko-KI-Systeme Anforderungen an eine wirksame menschliche Aufsicht vor. Ähnlich häufig beschränken Unternehmen Zugriffsrechte (64 Prozent) oder schützen sensible Daten (62 Prozent). Rund die Hälfte (52 Prozent) testet KI vor dem Einsatz beispielsweise mit Blick auf die Sicherheit. Zwei von fünf Unternehmen (40 Prozent) protokollieren oder monitoren die KI-Nutzung. Auf alle genannten Schutzmaßnahmen verzichtet eine Minderheit (8 Prozent). Deutlich über dem Durchschnitt liegen Unternehmen ab 250 Beschäftigten bei der Beschränkung von Zugriffsrechten (80 Prozent) sowie bei Tests der Systeme vor dem Einsatz (70 Prozent).

Verbände und BSI sind die wichtigsten Informationsquellen

Welche Quellen nutzen Sie, um sich über Risiken und Sicherheitsmaßnahmen beim Einsatz von KI-Anwendungen zu informieren?

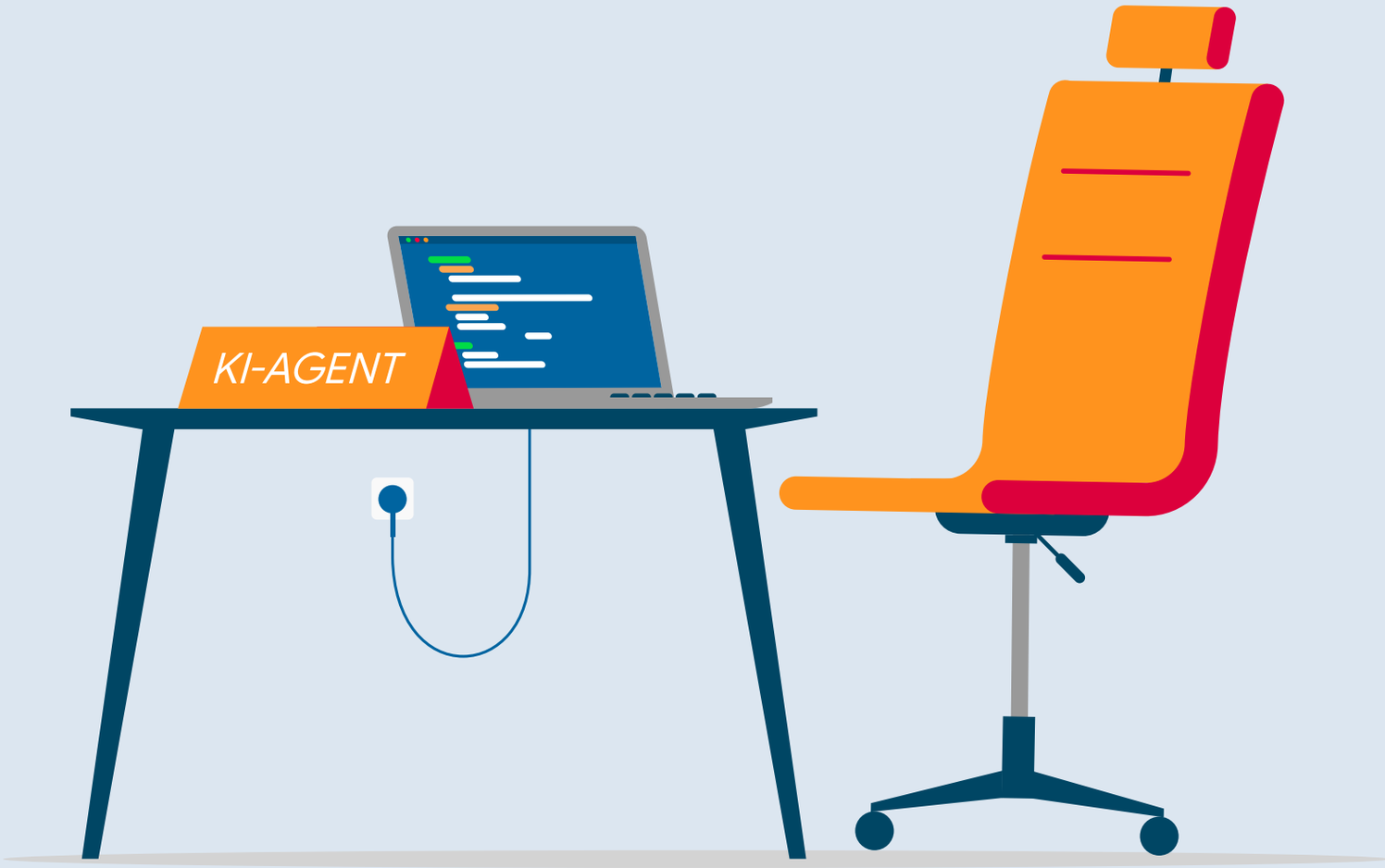


Frage: Welche Quellen nutzen Sie, um sich über Risiken und Sicherheitsmaßnahmen beim Einsatz von KI-Anwendungen zu informieren? (Mehrfachantworten möglich)
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen oder deren Einsatz planen (n = 292)

Auch Fachzeitschriften und Branchenpublikationen werden als wichtig angesehen, um Erkenntnisse über Sicherheitsmaßnahmen oder Risiken zu gewinnen.

Wo informieren sich Unternehmen über Sicherheitsmaßnahmen oder Risiken in Bezug auf den Einsatz von KI? Am häufigsten geschieht dies bei Verbänden und Netzwerken (71 Prozent), beim BSI (60 Prozent) sowie in Fachzeitschriften und Branchenpublikationen (58 Prozent). Für knapp die Hälfte (47 Prozent) sind auch die Veröffentlichungen anderer deutscher Behörden wichtig. Etwas weniger häufig werden Social Media und Online-Communitys als Informationsquelle genutzt (43 Prozent). Etwas mehr als ein Drittel zieht Veröffentlichungen der EU zurate (37 Prozent). Spontan ohne Antwortvorgabe gefragt, werden zudem externe IT-Berater genannt (5 Prozent). Größere Unternehmen ab 250 Beschäftigten informieren sich deutlich häufiger – etwa bei Verbänden und Netzwerken und dem BSI (je 81 Prozent) sowie in Fachzeitschriften (70 Prozent).

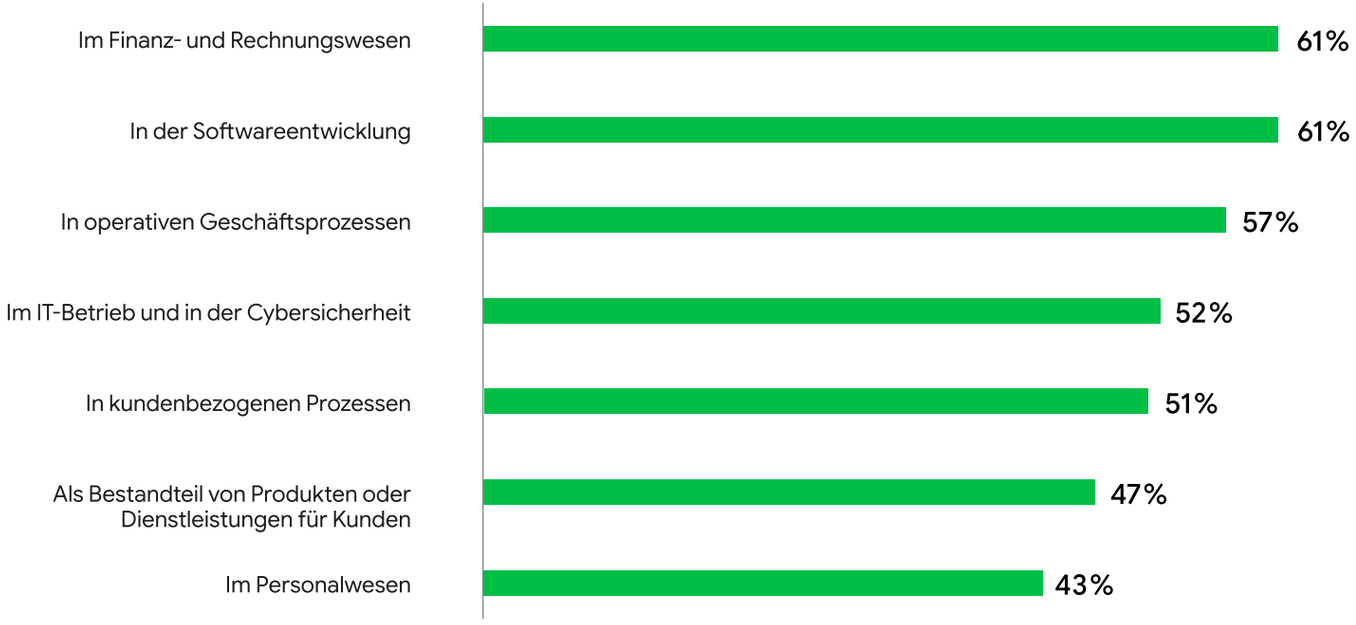
Einsatz von KI-Agenten



4.2

Vielfältige Einsatzorte für KI-Agenten

In welchem Kontext werden KI-Agenten bereits eingesetzt oder ist deren Einsatz geplant?



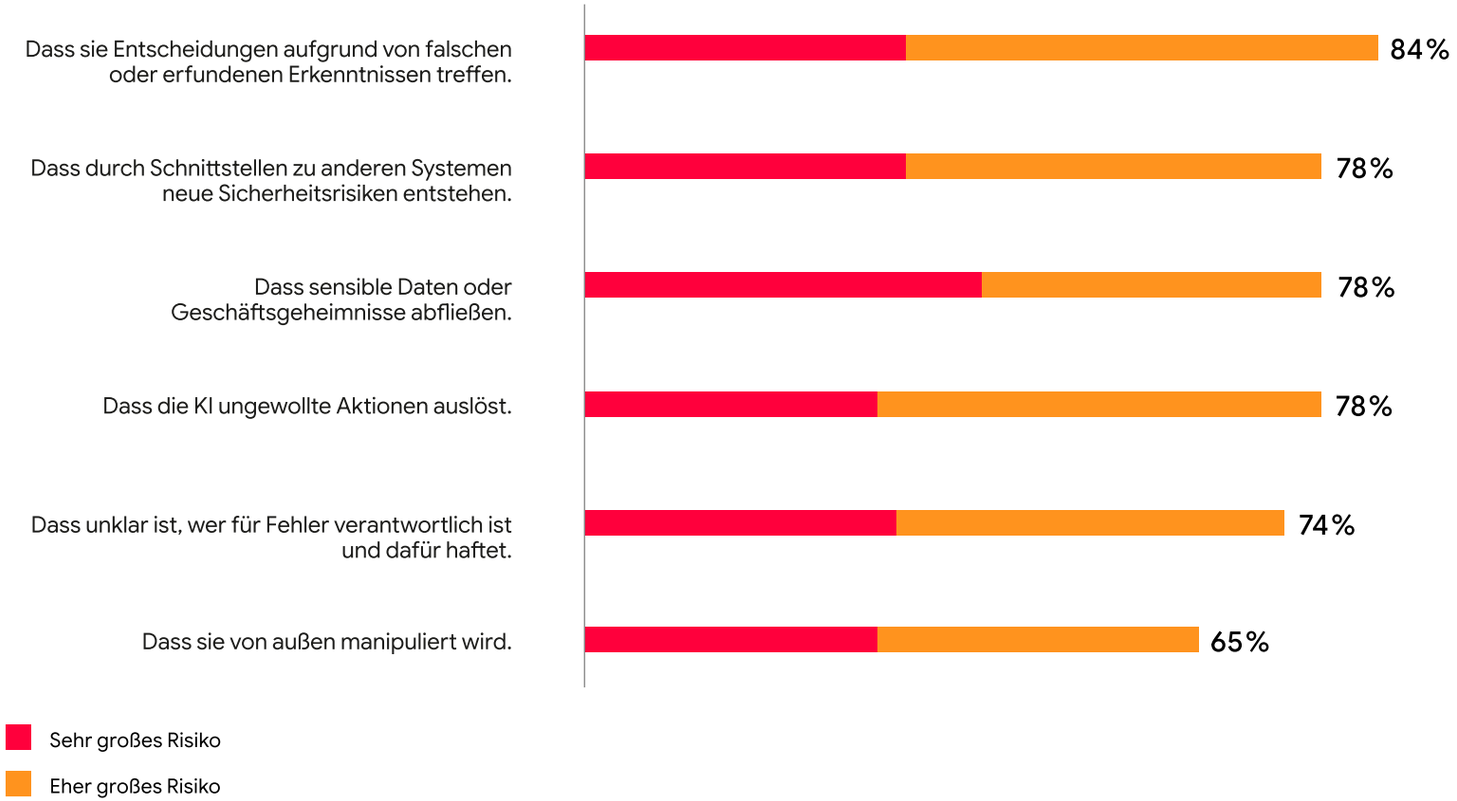
Besonders häufig sind die autonomen KI-Systeme im Finanz- und Rechnungswesen sowie in der Softwareentwicklung zu finden.

Nur eine Minderheit nutzt bislang KI-Agenten. Lediglich 5 Prozent der Unternehmen, die KI nutzen, verwenden die autonomen Systeme, weitere 8 Prozent davon planen deren Einsatz. Dort allerdings gibt es vielfältige Einsatzmöglichkeiten. Am häufigsten unterstützen KI-Agenten im Finanz- und Rechnungswesen sowie der Softwareentwicklung (je 61 Prozent). Nur knapp dahinter folgen operative Geschäftsprozesse (57 Prozent). Rund die Hälfte der Unternehmen setzt KI-Agenten im IT-Betrieb und in der Cybersicherheit (52 Prozent), in kundenbezogenen Prozessen (51 Prozent) sowie als Bestandteil von Produkten oder Dienstleistungen für Kunden ein (47 Prozent). Auch im Personalwesen kommen KI-Agenten zum Einsatz (43 Prozent).

Frage: In welchem Kontext werden KI-Agenten bereits eingesetzt oder ist deren Einsatz geplant? (Mehrfachantworten möglich)
Basis: Unternehmen, die KI-Agenten aktuell nutzen oder deren Einsatz planen (n = 34). Tendenzangaben aufgrund geringer Fallzahl

KI-Agenten: Viele befürchten Kontrollverlust

Welche Risiken sehen Sie beim Einsatz von KI-Agenten oder weitgehend selbstständig handelnden KI-Systemen?



Frage: Jetzt noch einmal speziell zum Thema KI-Agenten. Unter KI-Agenten versteht man KI-Systeme, die nicht nur Inhalte erzeugen, sondern mehrstufige Aufgaben selbstständig planen und ausführen können, etwa mit Zugriff auf unternehmensinterne Ticketsysteme, Datenbanken oder E-Mails. Ich nenne Ihnen nun mögliche Risiken beim Einsatz von KI-Agenten oder weitgehend selbstständig handelnden KI-Systemen. Sagen Sie mir bitte jeweils, ob Sie das als sehr hohes, eher hohes, eher geringes oder als kein Risiko einschätzen.
Basis: alle befragten Unternehmen (n = 505)

Falsche Entscheidungen, zusätzliche Sicherheitsprobleme: Weitgehend autonome Systeme bergen aus Sicht der Unternehmen eine ganze Reihe von Risiken.

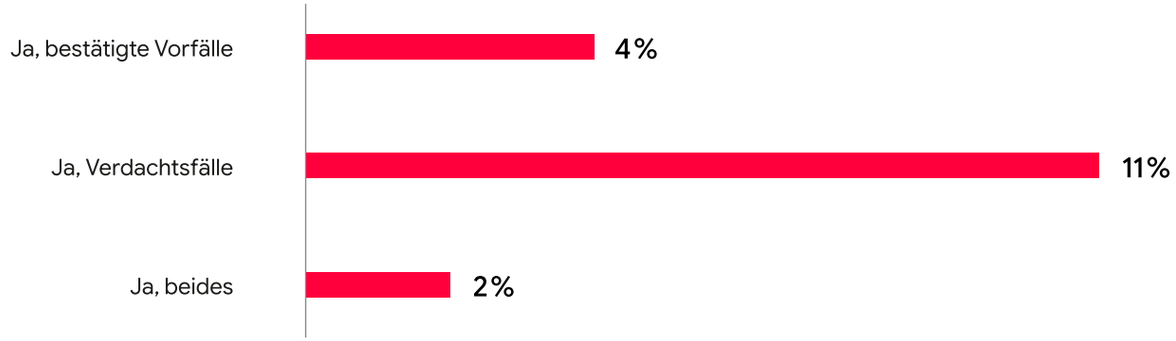
Mit falschen oder sogar erfundenen Erkenntnissen treffen KI-Agenten falsche Entscheidungen für das Unternehmen – es ist eine Sorge, die die meisten Befragten teilen (84 Prozent). Parallel sehen jeweils etwas mehr als drei Vierteln (je 78 Prozent) es die Gefahr, dass durch Schnittstellen zu anderen Systemen neue Sicherheitsrisiken entstehen, sensible Daten oder Geschäftsgeheimnisse abfließen oder dass die KI ungewollte Aktionen auslöst. Knapp drei Viertel (74 Prozent) sehen es als problematisch, dass die Verantwortung für Fehler unklar ist. Eine mögliche Manipulation von außen bewerten rund zwei Drittel (65 Prozent) als Risiko des Einsatzes von KI-Agenten.

KI-gestützte Angriffe und Betrugsmaschen

4.3

Jedes sechste Unternehmen von KI-gestützten Cyberangriffen betroffen

Gab es in den letzten 12 Monaten Cyberangriffe oder Betrugsversuche gegen Ihr Unternehmen, bei denen KI eine Rolle gespielt hat?



17%

verzeichneten in den letzten 12 Monaten einen Cyberangriff oder Betrugsversuch, bei dem KI eine Rolle gespielt hat bzw. haben könnte.

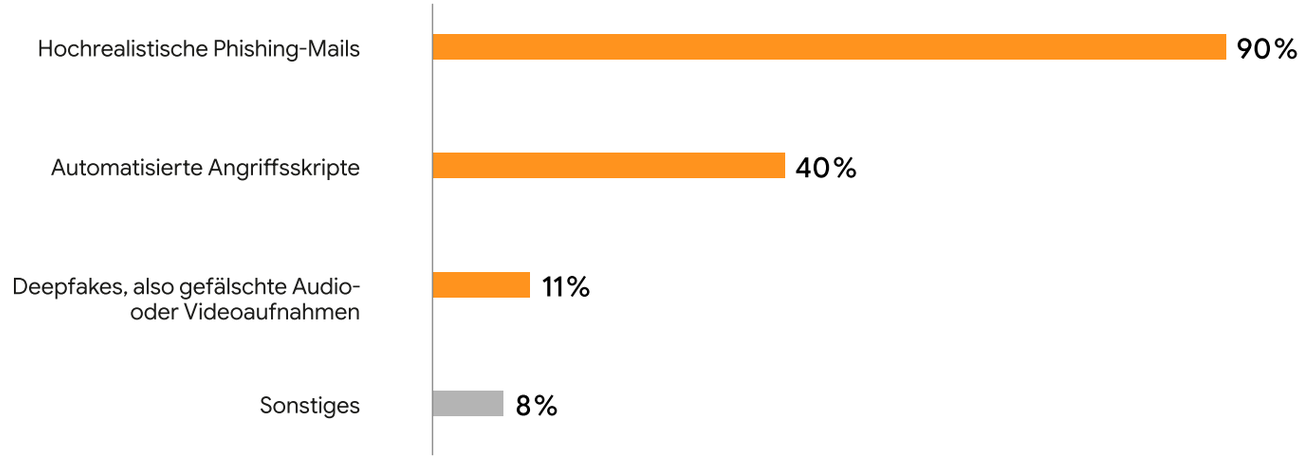
Online-Kriminelle rüsten auf. Das zeigen die bestätigten Vorfälle und Verdachtsfälle, von denen die befragten Unternehmen berichten.

KI kann Unternehmen helfen, Tätigkeiten oder Prozesse effizienter zu gestalten. Zugleich entstehen neue Gefahren dadurch, dass Cyberkriminelle KI verwenden. Rund jedes sechste Unternehmen (17 Prozent) berichtet, dass es in den vergangenen zwölf Monaten bestätigte Vorfälle oder Verdachtsfälle von Cyberangriffen oder Betrugsversuchen gegeben hat, bei denen KI eine Rolle spielte. Am häufigsten waren ausschließliche Verdachtsfälle (11 Prozent), gefolgt von ausschließlich bestätigten Vorfällen (4 Prozent). Dass beides zusammen auftrat, war die Ausnahme (2 Prozent).

Frage: Gab es in den letzten 12 Monaten Cyberangriffe oder Betrugsversuche gegen Ihr Unternehmen, bei denen KI eine Rolle gespielt hat – also bestätigte Vorfälle oder auch Verdachtsfälle? Basis: alle befragten Unternehmen (n = 505)

Hochrealistische Phishing-Mails sind die häufigste Angriffsmethode

Die (vermuteten) Angriffs- und Betrugsmethoden



Besonders oft versuchen Cyberkriminelle, durch die Täuschung von Beschäftigten Zugang zur Firmen-IT zu erhalten.

Keine Rechtschreibfehler, perfekt gefälschte Absender, Details aus dem Arbeitsalltag im Anschreiben: Hochrealistische Phishing-Mails sind nur schwer von tatsächlichen Nachrichten von Kunden und Kundinnen oder Kollegen und Kolleginnen zu unterscheiden. Und sie werden von den Befragten am häufigsten als vermutete Angriffsmethode genannt. Neun von zehn Unternehmen (90 Prozent) sind nach eigenen Angaben mit hochrealistischen Phishing-Mails attackiert worden. Zwei von fünf Befragten (40 Prozent) geben an, dass automatisierte Angriffsskripte genutzt wurden, die selbstständig in das IT-System des Unternehmens einzudringen versuchten. Deepfakes stellte rund ein Zehntel fest (11 Prozent): gefälschte Audio- oder Videoaufnahmen, mit denen sich Angreifer:innen beispielsweise als Führungskraft ausgeben.

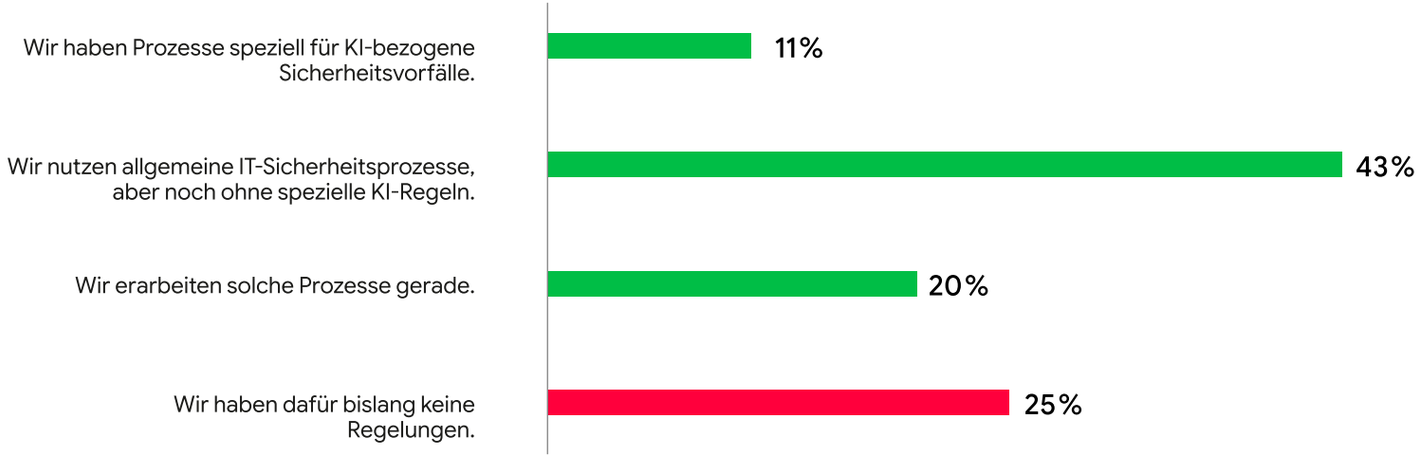
Frage: Welche Angriffs- oder Betrugsmethoden wurden (vermutlich) eingesetzt?
Basis: Unternehmen, die in den letzten zwölf Monaten mindestens einen IT-Sicherheitsvorfall, bei dem KI eine Rolle gespielt hat, hatten/vermuten (n = 91)

Spezielle Prozesse für KI-bezogene Sicherheitsvorfälle sind die Ausnahme

Am häufigsten setzen Unternehmen auf allgemeine IT-Sicherheitsprozesse; fast ein Viertel hat keine Regelungen.

Wie reagieren Unternehmen auf Cyberangriffe oder Betrugsversuche, bei denen die Täter:innen mit KI arbeiten? Etwa ein Zehntel der Unternehmen, die KI nutzen oder dies planen, setzt auf Prozesse speziell für KI-bezogene Sicherheitsvorfälle (11 Prozent). Bei einem Fünftel der Unternehmen werden solche Prozesse gerade erarbeitet (20 Prozent). Auf allgemeine IT-Sicherheitsprozesse ohne spezielle KI-Regeln verlassen sich die Befragten am häufigsten (43 Prozent). Keine Regelungen für Sicherheitsvorfälle mit KI-Bezug gibt es bei einem Viertel der Unternehmen (25 Prozent).

Wie gehen Sie mit KI-bezogenen Sicherheitsvorfällen um?



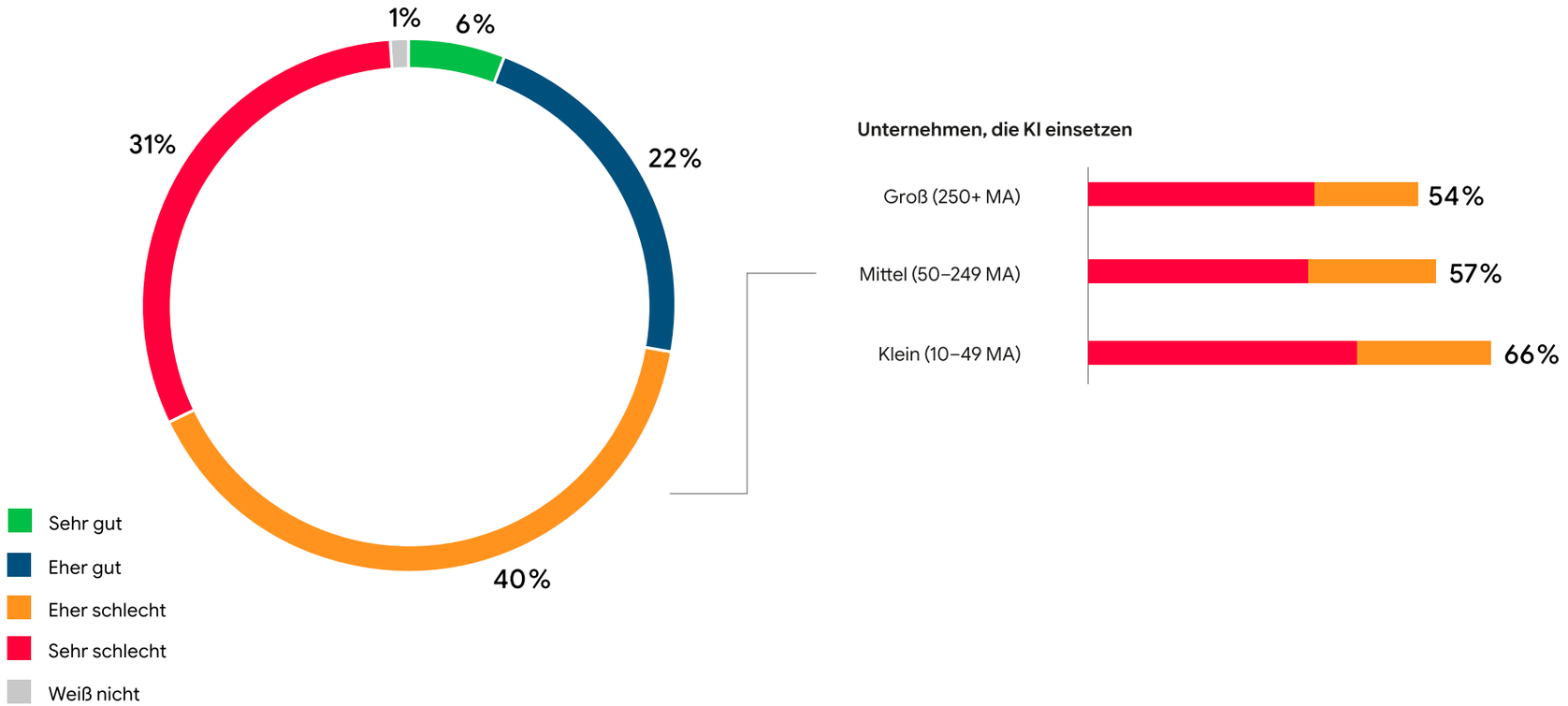
Frage: Ich lese Ihnen nun vier Aussagen vor. Welche trifft am ehesten auf Ihr Unternehmen hinsichtlich des Umgangs mit KI-bezogenen Sicherheitsvorfällen zu?
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen oder die den Einsatz planen (n = 292)

AI Act: Umsetzung und Unterstützungsbedarf

5

Die Mehrheit fühlt sich schlecht informiert

Wie gut fühlen Sie sich über die Anforderungen des AI Act informiert?



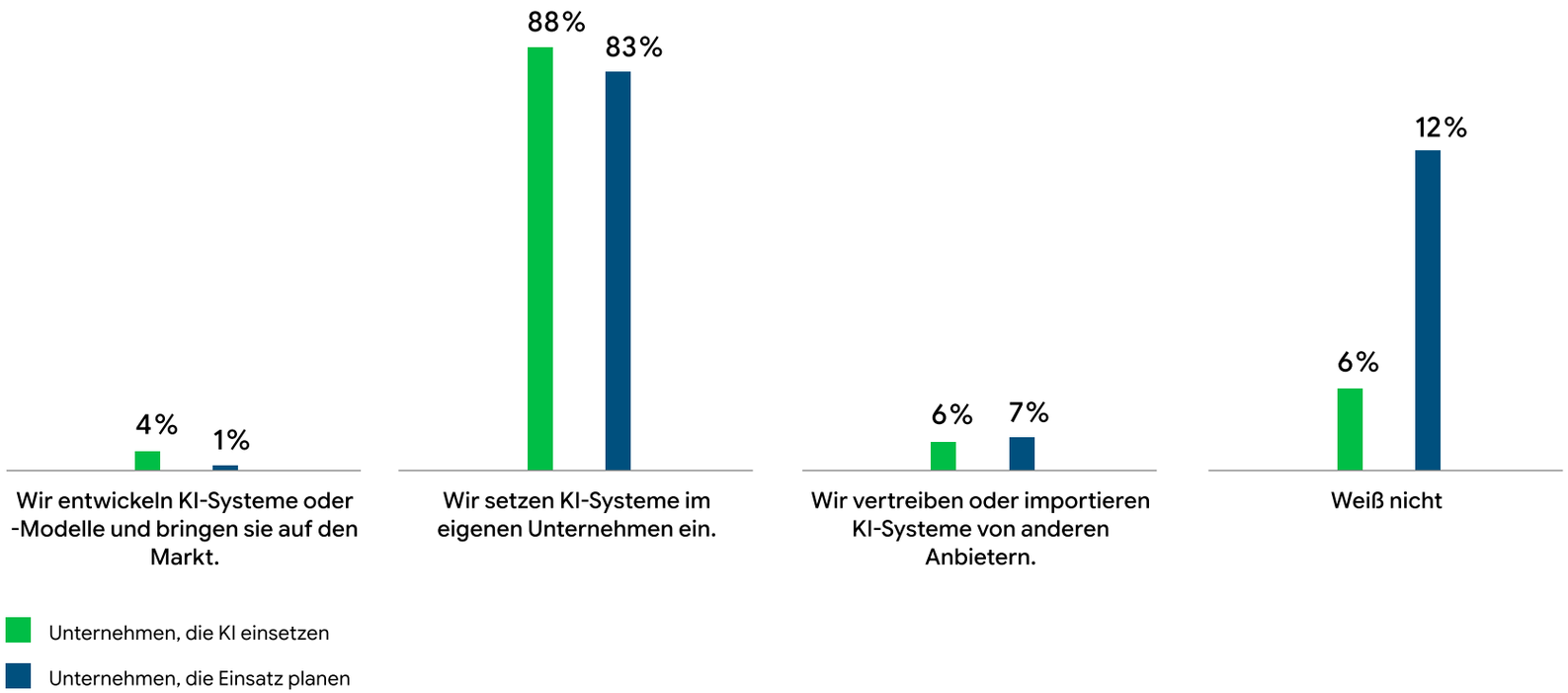
Werden allein Unternehmen betrachtet, die KI nutzen, verbessert sich der Wissensstand spürbar.

Seit 2024 tritt die als AI Act bekannte Verordnung über künstliche Intelligenz der Europäischen Union schrittweise in Kraft. Sie macht nicht nur Vorgaben für die Entwicklung von KI-Anwendungen. Auch Regeln für Anwender und deren Pflichten sind im AI Act festgeschrieben. Was genau zu tun ist, darüber fühlt sich die überwiegende Mehrheit der Befragten schlecht informiert (71 Prozent). Als gut informiert betrachtet sich etwas mehr als ein Viertel (28 Prozent). Werden allein die Unternehmen betrachtet, die KI einsetzen, ist der Wissensstand etwas besser. Bei größeren Unternehmen , mit KI-Nutzung, gibt knapp die Hälfte an, schlecht informiert zu sein (54 Prozent). Bei kleinen Unternehmen ist es rund ein Drittel (66 Prozent).

Frage: Kommen wir nun zur europäischen KI-Verordnung, dem sogenannten ‚AI Act'. Das ist eine EU-Verordnung, die Regeln für die Entwicklung und den Einsatz von KI-Systemen festlegt und seit 2024 schrittweise in Kraft tritt. Wie gut fühlen Sie sich über die Anforderungen des 'AI Act' informiert?
Basis: alle befragten Unternehmen (n = 505) oder Unternehmen, die KI nutzen (n = 246)

AI Act: Die meisten Unternehmen sind KI-Betreiber

Welche der folgenden Rollen treffen auf Ihr Unternehmen zu?
Welche der folgenden Rollen werden auf Ihr Unternehmen voraussichtlich zutreffen?



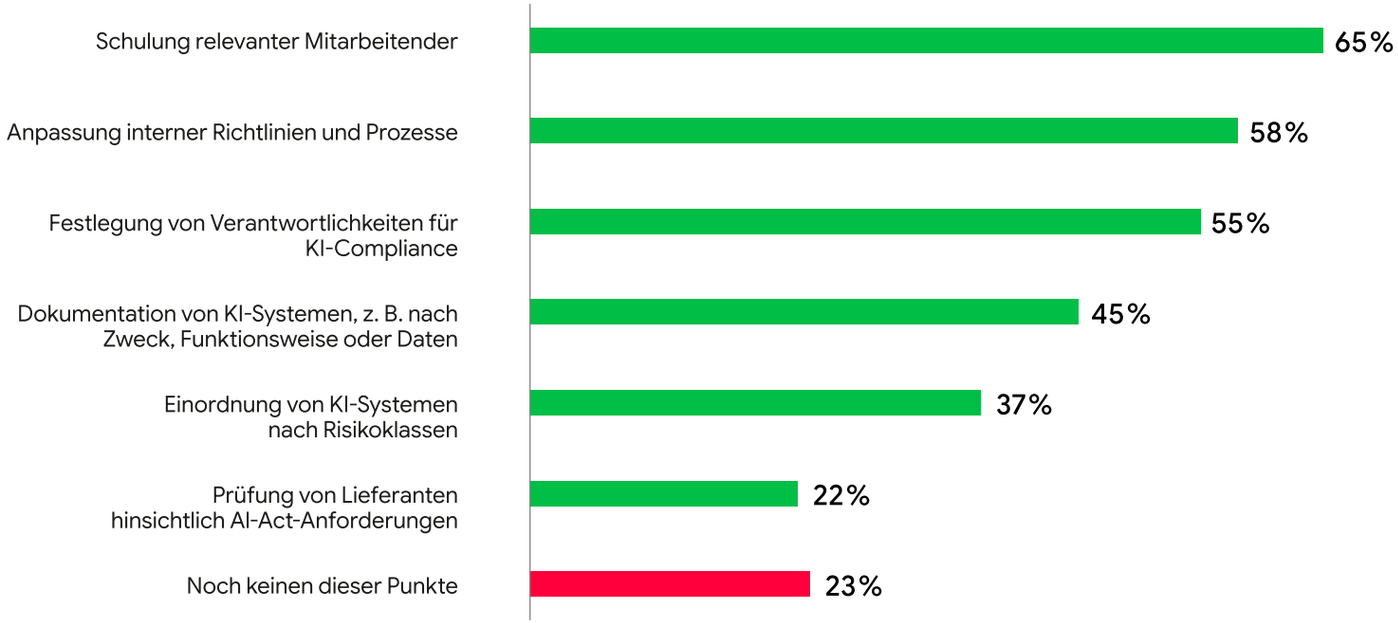
Frage: Der AI Act unterscheidet verschiedene Rollen – je nachdem, ob ein Unternehmen KI entwickelt, einsetzt oder vertreibt. Das hat Auswirkungen darauf, welche Pflichten für die Unternehmen gelten. Welche der folgenden Rollen treffen auf Ihr Unternehmen zu? Welche der folgenden Rollen werden auf Ihr Unternehmen voraussichtlich zutreffen?
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen oder deren Einsatz planen (n = 246 | n = 46)

Nur eine deutliche Minderheit der Befragten entwickelt selbst KI-Systeme oder vertreibt die Anwendungen anderer KI-Anbieter.

Der AI Act unterscheidet bestimmte Rollen für Unternehmen: Wird KI entwickelt, eingesetzt oder vertrieben? Von der Zuordnung hängt ab, welche Regeln und Pflichten gelten. Die große Mehrheit der befragten Unternehmen, die KI einsetzen, ordnen sich den Betreibern zu – sie nutzen also KI (88 Prozent). Jeweils eine Minderheit gibt an, selbst KI-Systeme zu entwickeln und als Anbieter auf den Markt zu bringen (4 Prozent) oder als Distributor die KI-Systeme anderer Anbieter zu vertreiben oder zu importieren (6 Prozent). Bei Unternehmen, die den KI-Einsatz planen, zeigt sich insgesamt ein vergleichbares Bild.

AI Act in der Praxis: Schulungen, Richtlinien, Verantwortlichkeiten

Welche der folgenden Maßnahmen haben Sie in Ihrem Unternehmen bereits umgesetzt oder sind konkret in Arbeit?



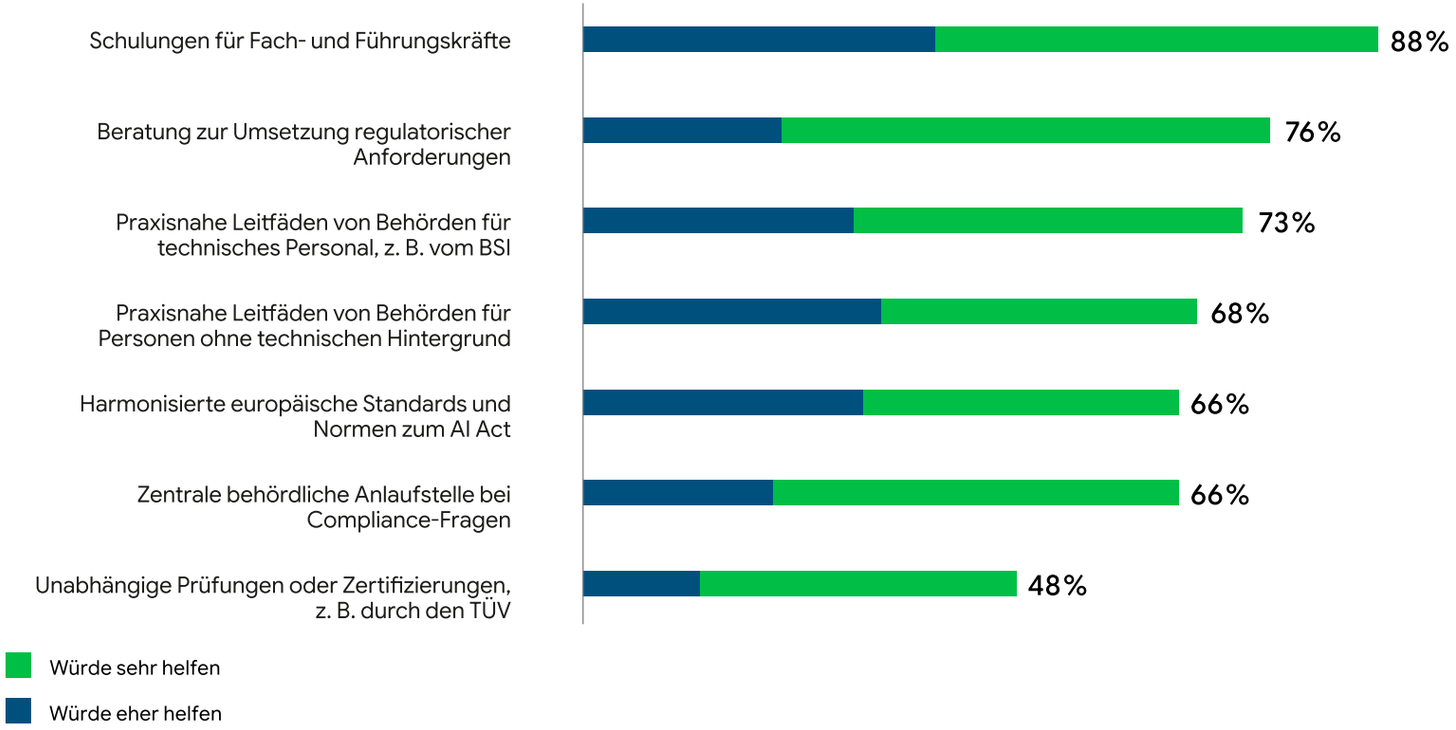
Frage: Der AI Act verpflichtet Unternehmen je nach Rolle und Risikoklasse zu verschiedenen Maßnahmen. Welche der folgenden Maßnahmen haben Sie in Ihrem Unternehmen bereits umgesetzt oder sind konkret in Arbeit? Welche der folgenden Maßnahmen haben Sie in Ihrem Unternehmen in Planung?
Basis: Unternehmen, die KI-Anwendungen aktuell nutzen oder deren Einsatz planen (n = 246 | n = 46)

Mit einer Reihe von Maßnahmen reagieren Unternehmen auf die Anforderungen der Europäischen Union an die KI-Nutzung.

Hochrisiko-KI in medizinischen Geräten oder kritischer Infrastruktur oder niedriges Risiko bei KI in Videospielen? In insgesamt vier Risikoklassen unterteilt der AI Act KI-Systeme abhängig davon, wo sie genutzt werden. Von der Einordnung sowie der Rolle als Anbieter, Betreiber oder Distributor hängt es ab, welche Maßnahmen ein Unternehmen treffen muss. Am häufigsten werden laut Erhebung Beschäftigte geschult (65 Prozent). Befragt wurden Unternehmen, die KI bereits nutzen oder dies planen. Es folgen die Anpassung interner Richtlinien und Prozesse (58 Prozent) und die Festlegung von Verantwortlichkeiten für KI-Compliance (55 Prozent). Knapp die Hälfte setzt auf die Dokumentation von KI-Systemen (45 Prozent). Etwas mehr als ein Drittel (37 Prozent) unterteilt KI-Systeme nach Risikoklassen. Etwa ein Fünftel (22 Prozent) prüft Lieferanten hinsichtlich der AI-Act-Anforderungen. Keine der genannten Maßnahmen umgesetzt hat knapp ein Viertel (23 Prozent). Größere Unternehmen nutzen die Maßnahmen überdurchschnittlich häufig.

Hoher Unterstützungsbedarf beim Umgang mit KI in der Praxis

Wie sehr würden diese Unterstützungsangebote Ihnen helfen, sicher und rechtskonform mit KI umzugehen?



Frage: Ich lese Ihnen nun verschiedene Unterstützungsangebote vor. Wie sehr würden diese Ihnen helfen, sicher und rechtskonform mit KI umzugehen: sehr, eher, eher nicht oder überhaupt nicht? Basis: Unternehmen, die KI-Anwendungen aktuell nutzen oder deren Einsatz planen (n = 292)

Auch die Expertise von Behörden wie dem BSI und unabhängigen Organisationen wie dem TÜV ist gefragt.

In einer Vielzahl von Bereichen zeigen Unternehmen, die KI nutzen oder dies planen, Bedarf an Unterstützung. Besonders gefragt ist diese bei Schulungen für Fach- und Führungskräfte (88 Prozent). Jeweils rund drei Viertel erachten eine Beratung zur Umsetzung regulatorischer Anforderungen (76 Prozent) sowie praxisnahe Leitfäden von Behörden für technisches Personal, etwa vom BSI, als hilfreich (73 Prozent). Rund zwei Drittel zeigen Interesse an Leitfäden von Behörden, die auf Personen ohne technischen Hintergrund abgestimmt sind (68 Prozent). Für harmonisierte Standards und Normen zum AI Act sowie für eine zentrale behördliche Anlaufstelle bei Compliance-Fragen sprechen sich jeweils zwei Drittel aus (66 Prozent). Unabhängige Prüfungen oder Zertifizierungen, etwa durch den TÜV, schätzt rund die Hälfte (48 Prozent) als hilfreich ein für einen sicheren und rechtskonformen Umgang mit KI.

Fazit und Empfehlungen

6

Fazit

KI ist in der Wirtschaft angekommen. Die Mehrheit der Unternehmen nutzt entsprechende Anwendungen oder plant dies binnen eines Jahres. Dabei kommen vor allem fertige Anwendungen wie ChatGPT, Claude oder Canva zum Einsatz. Am weitesten verbreitet ist generative KI zur Erstellung von Texten, Bildern oder Code. Künftig planen Unternehmen allerdings verstärkt, KI-Systeme für interne Zwecke anzupassen. Wer bislang auf KI verzichtet, sieht vor allem keinen erkennbaren Nutzen – oder hat Datenschutz- und Sicherheitsbedenken.

Betrieben werden die Anwendungen überwiegend in einer externen Cloud; kostenpflichtige kommerzielle KI-Anwendungen sind dabei etwas häufiger als Open-Source-Modelle. In der standardmäßigen Integration von KI in Software oder Betriebssysteme sehen viele Befragte Effizienzvorteile, sie befürchten aber zugleich neue Sicherheitsrisiken. Autonom handelnde KI-Agenten setzt erst eine Minderheit ein, vor allem in der Finanzabteilung und der Softwareentwicklung. Noch überwiegt das Misstrauen: Viele befürchten durch KI-Agenten einen Kontrollverlust oder Gefahren für die Sicherheit.

Viele Anwender-Unternehmen erachten KI als wichtig für die gesamten Prozesse und sie haben darauf organisatorisch reagiert. Sie haben mehrheitlich mindestens eine feste Zuständigkeit für KI-Themen geschaffen sowie verbindliche Richtlinien beschlossen. Eine unternehmensweite Strategie gibt es allerdings nur bei einer Minderheit. Beträchtlichen Zuspruch finden unabhängige Prüfungen mit Blick auf die Compliance von KI-Anwendungen. Die breite Mehrheit ist überzeugt, dass Prüfungen etwa durch den TÜV zu einer höheren Sicherheit und einer besseren Einhaltung von regulatorischen Anforderungen beitragen könnten und zudem die Auswahl von KI-Anbietern erleichtern können. Bei der Auswahl von KI-Anwendungen haben IT-Sicherheit und Datenschutz eine sehr große Bedeutung. In der Praxis wird der KI-Einsatz durch eine Reihe organisatorischer Maßnahmen abgesichert: von Schulungen über die Risikobewertung von Anwendungen bis hin zu formalen Freigabeprozessen. Die Mehrheit sieht die Beschäftigten gut auf den Umgang mit KI vorbereitet. Am ehesten Weiterbildungsbedarf erkennen die Unternehmen bei der Anwendungs- und Datenkompetenz sowie der sicheren KI-Nutzung.

Für einen sicheren KI-Einsatz setzen Unternehmen auf unterschiedliche Schutzmaßnahmen und Informationsquellen. Als Vorkehrung lassen viele Firmen mit KI-Nutzung die Ergebnisse noch einmal von Beschäftigten prüfen oder beschränken Zugriffsrechte. Informationen über Risiken oder Sicherheitsmaßnahmen beziehen die Unternehmen besonders oft bei Verbänden und Netzwerken. Eine deutliche Mehrheit hält sich auch beim BSI auf dem Laufenden. Als reale Bedrohung erweisen sich dagegen Cyberangriffe, bei denen Kriminelle selbst KI einsetzen – allen voran Phishing. 17 Prozent der Unternehmen berichten von einem tatsächlichen oder vermuteten KI-gestützten Cyberangriff.

Beim Thema digitale Souveränität zeigt sich ein Spannungsfeld. Europäische und deutsche KI-Anwendungen sind vielen bekannt und jedes dritte der Unternehmen, die KI nutzen, hat sie auch im Einsatz. Darauf verzichtet wird oft aus Bequemlichkeit – man scheut den mit dem Wechsel verbundenen Aufwand – oder zweifelt an der Leistungsfähigkeit europäischer KI-Systeme. Zugleich beschreibt sich ein großer Teil der Unternehmen als abhängig von außereuropäischen KI-Anbietern. Die konkreten Folgen dieser Abhängigkeit können viele jedoch nicht benennen.

Beim AI Act der Europäischen Union besteht Aufklärungsbedarf: Die Mehrheit der Unternehmen fühlt sich schlecht informiert. Weniger häufig ist das in Unternehmen der Fall, die KI nutzen. Als Reaktion auf die Anforderungen des AI Act setzen sie vor allem auf Schulungen, angepasste Richtlinien und festgelegte Verantwortlichkeiten. Dabei äußern die Befragten ein breites Interesse an Unterstützungsangeboten – von Weiterbildung für Fach- und Führungskräfte über Beratung sowie Leitfäden bis hin zu unabhängigen Prüfungen.

Empfehlungen an Unternehmen

Informationspaket des Expertenkreises KI-Sicherheit der Allianz für Cybersicherheit mit konkreten Empfehlungen zum Vorgehen bei der Einführung von KI-Anwendungen oder zur Freigabe zur Nutzung von KI-Diensten

Publikation „Generative KI-Modelle: Chancen und Risiken für Industrie und Behörden“ für Unternehmen, die die Integration generativer KI-Modellen in ihre Arbeitsabläufe planen

Informationen zu Evasion Attacks, die beim Betrieb großer Sprachmodelle stattfinden können, und mögliche Gegenmaßnahmen

Handout „Schutz vor KI-verstärkten Cyberangriffen“ für Inhaberinnen und Inhaber kleiner Betriebe

KI sicher nutzen – Empfehlungen an Unternehmen von BSI und TÜV-Verband

KI soll Unternehmen leistungsfähiger und widerstandsfähiger machen. Viele Unternehmen haben für den KI-Einsatz bereits Zuständigkeiten, Richtlinien und erste Schutzmaßnahmen etabliert. Darauf gilt es aufzubauen: mit klarem betrieblichem Nutzen, anwendungsnaher Qualifizierung und Weiterbildung und wirksamen technischen und organisatorischen Sicherheitsmaßnahmen. Mit der tieferen Einbindung in Geschäftsprozesse, Produkte und IT-Systeme muss die Absicherung von KI weiterentwickelt werden. BSI und TÜV-Verband empfehlen Unternehmen, dabei folgende fünf Prioritäten zu setzen.

1. KI-Kompetenz gezielt aufbauen und für alle Unternehmensprozesse vertiefen

76 Prozent der KI-nutzenden Unternehmen sehen Weiterbildungsbedarf für KI-Anwendung und Integration, 69 Prozent beim sicheren Umgang. Unternehmen sollten die Qualifizierung ihrer Beschäftigten am tatsächlichen und geplanten KI-Einsatz ausrichten: geeignete Aufgaben erkennen, Daten sachgerecht nutzen, Ergebnisse kritisch beurteilen und sensible Informationen schützen. Schulungen sollten regelmäßig aktualisiert und auf die Aufgaben von Fach- und Führungskräften, Entwicklung, IT-Sicherheit, Einkauf oder Compliance zugeschnitten werden. Regelmäßige praktische Übungen sollten auch KI-gestützte Täuschungs- und Betrugsversuche behandeln.

2. KI-Einsatz zur Chef-Sache machen: Governance und Verantwortung verankern

Mit festen Zuständigkeiten bei 63 Prozent und internen Richtlinien bei 59 Prozent der KI-nutzenden Unternehmen bestehen vielfach Grundlagen. Risikobewertungen und Freigabeprozesse nennen jeweils 45 Prozent. KI einzusetzen ist kein Selbstzweck; entscheidend ist ein nachvollziehbarer betrieblicher Nutzen bei beherrschbaren Risiken. KI-Governance sollte Führungsaufgabe sein – ein sichtbares Mandat der Geschäftsleitung ermöglicht eine angemessene Ressourcenplanung und eine an Nutzen und Risiken ausgerichtete Strategie. Ein gepflegtes KI-Inventar sollte Anwendungen, Modelle, Schnittstellen und Verantwortliche erfassen – einschließlich KI-Funktionen in bestehender Software. Klare Nutzungsregeln, Risikobewertungen und Freigaben sollen auch nicht freigegebene KI-Nutzung, sogenannte Schatten-KI, verhindern. Unternehmen sollten ihre Rolle und die einschlägigen Anforderungen nach dem AI Act sowie – je nach Produkt, Tätigkeit und Geltungsbereich – dem Cyber Resilience Act und weiteren Vorschriften prüfen. Zudem sind Verantwortlichkeiten und Nachweise entlang der Lieferkette zu berücksichtigen.

3. KI-Sicherheit priorisieren und unabhängige Prüfungen sowie Zertifikate nutzen

52 Prozent der KI-nutzenden Unternehmen testen KI-Anwendungen vor dem Einsatz; 40 Prozent protokollieren oder überwachen die Nutzung. Unternehmen sollten KI über den gesamten Lebenszyklus absichern: Datenflüsse prüfen, sensible Daten schützen, Zugriffsrechte begrenzen und kritische Ergebnisse kontrollieren. Vor dem Produktiveinsatz sowie nach wesentlichen Modell-, Daten- oder Schnittstellenänderungen sind risikogerechte Sicherheits- und Robustheitstests vorzusehen. Dazu gehören Tests gegen manipulative Eingaben und eingeschleuste Anweisungen (Prompt Injection). Auch fertige Anwendungen und externe Cloud-Dienste sind in diese Bewertung einzubeziehen. Verfügbare unabhängige Prüfberichte und Zertifizierungen sollten die Anbieterauswahl und Compliance-Bewertung unterstützen. Entscheidend ist, welche Version, Eigenschaften und Einsatzbedingungen der Nachweis tatsächlich abdeckt. Bei besonders kritischen Anwendungsfällen bietet sich eine zusätzliche unabhängige Prüfung an. Beim Einsatz von KI-Agenten ist besonders auf technisch begrenzte Rechte, kontrollierte Schnittstellen und geeignete Testumgebungen zu achten. Kritische oder irreversible Aktionen sind durch menschliche Freigaben, Transaktionsgrenzen und technische Abbruchmöglichkeiten proaktiv abzusichern.

4. KI-Gefahren: Sensibilisieren, proaktiv vorbeugen und Notfallprozesse einüben

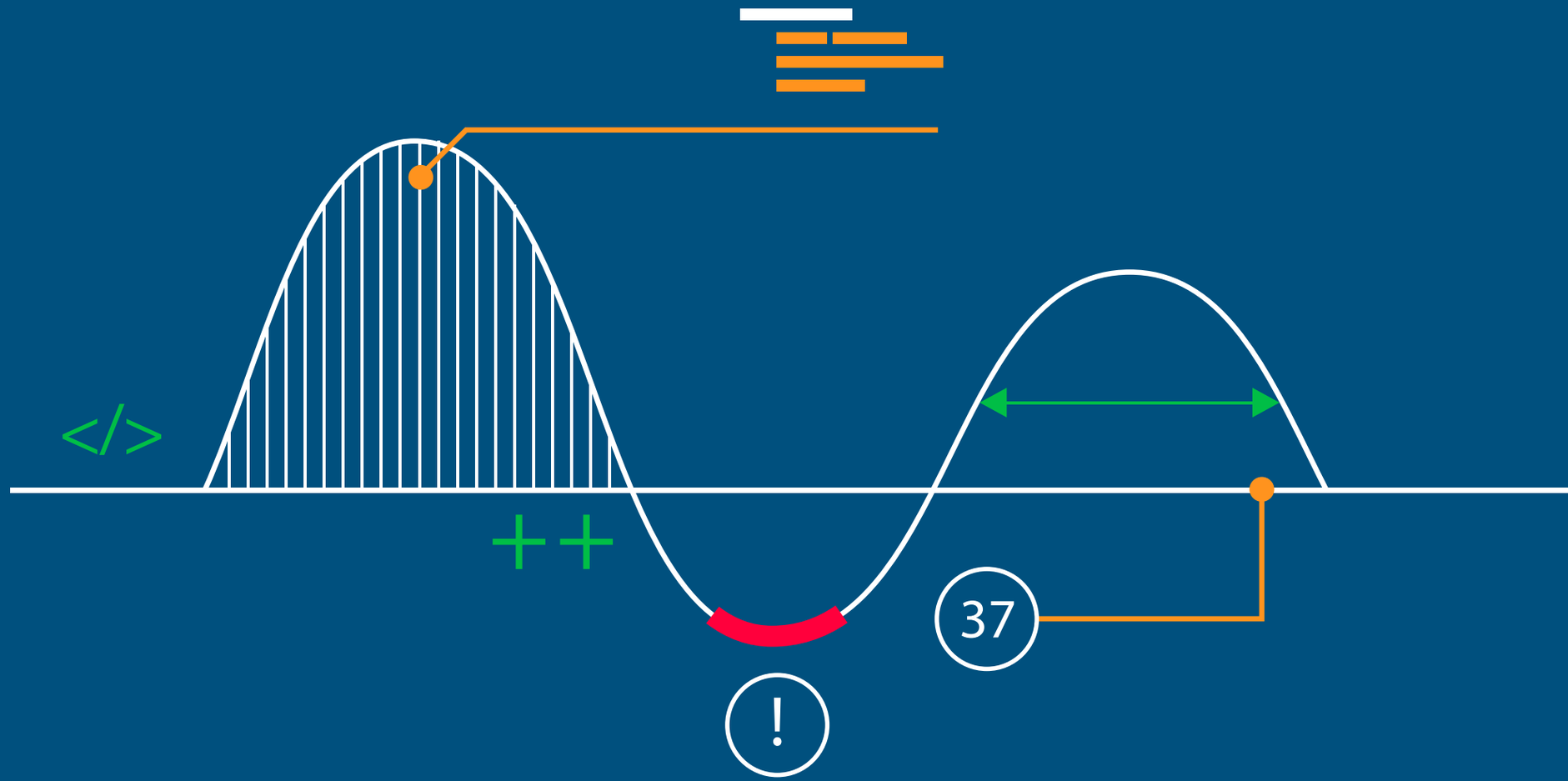
17 Prozent aller Befragten berichten für die vergangenen zwölf Monate bestätigte oder vermutete KI-gestützte Cyberangriffe beziehungsweise Betrugsversuche. Bei 25 Prozent der KI-nutzenden oder -planenden Unternehmen fehlen Regelungen für KI-bezogene Vorfälle. Klassische IT-Sicherheit bleibt das Fundament: Angriffsflächen kennen und verringern, Schwachstellen und Sicherheitsupdates priorisieren, Zugänge absichern und Wiederanlaufverfahren vorbereiten. Alle Unternehmen sollten ihre Beschäftigten gegen KI-Phishing und Betrugsversuche sensibilisieren und sensible Zahlungs- oder Datenfreigaben über einen unabhängigen Kommunikationsweg rückbestätigen. Bestehende IT-Sicherheits- und Notfallprozesse sind um KI-Szenarien wie Datenabflüsse, manipulierte Inhalte und ungewollte Agentenaktionen zu ergänzen. Zugleich sollten mögliche sicherheitskritische Vorfälle beim eigenen KI-Einsatz möglichst frühzeitig erkannt, dokumentiert und ausgewertet werden können. Unternehmen sollten zudem prüfen, wie KI die eigene Abwehr unterstützen kann – etwa beim Erkennen von Schwachstellen in autorisierten Umgebungen, beim Pflegen des IT-Inventars oder Filtern verdächtiger E-Mails. Hierbei sollte ebenfalls auf geeignete technische und organisatorische Sicherheitsmaßnahmen geachtet werden.

5. Digitale Souveränität stärken: Handlungsfähigkeit sichern und Abhängigkeiten reduzieren

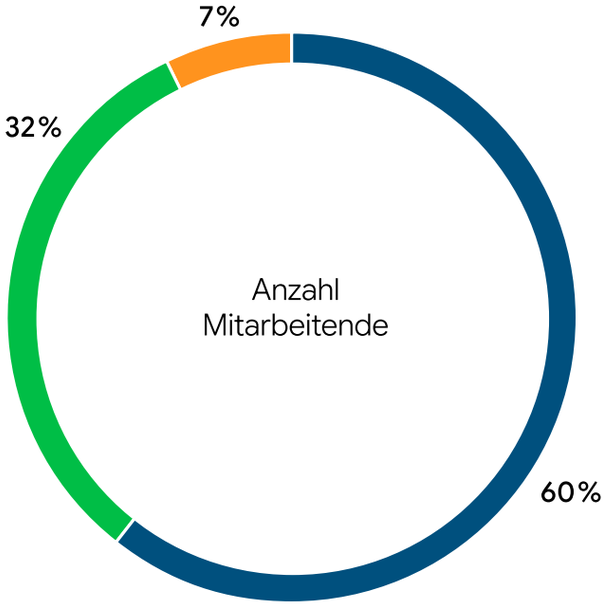
30 Prozent der KI-Nutzenden sehen sich stark von außereuropäischen Anbietern abhängig. Unternehmen sollten die Folgen für Geschäftsprozesse, Datenzugriff und Handlungsfähigkeit bewerten und für kritische Anwendungen Ausweichverfahren vorbereiten. Bei der Beschaffung sind Rechtsraum, Unterauftragnehmer, Datenportabilität, offene Schnittstellen sowie vertragliche Wechselmöglichkeiten zu berücksichtigen.

Europäische und deutsche Angebote sowie Open-Source-Lösungen sollten anhand konkreter Anforderungen an Leistungsfähigkeit, Sicherheit und Integrationsaufwand verglichen und erprobt werden. Maßstab ist selbstbestimmte, sichere Nutzung – nicht allein die Herkunft eines Anbieters.

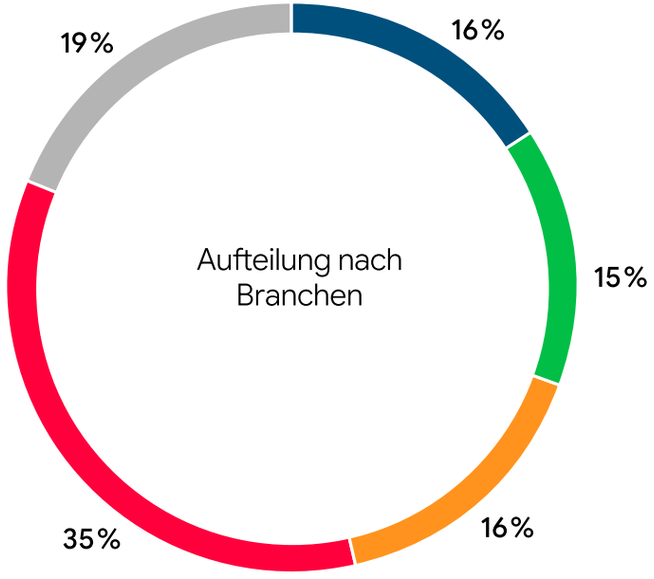
Methodik



Methodik



- Zwischen 20 und bis 49 Mitarbeitern
- Zwischen 50 und 249 Mitarbeitern
- Mehr als 250 Mitarbeiter



- Industrie
- Energie, Bau und Verkehr
- Handel
- Dienstleistungen
- Öffentlicher Bereich/Gesundheit

Die Umfrage wurde von forsa im Auftrag des BSI und des TÜV-Verbands durchgeführt. Die Interviews erfolgten mittels einer telefonischen CATI-Befragung zwischen 22. Juni und 31. Juli 2026. Befragt wurden Verantwortliche für KI-Nutzung, IT-Sicherheit, IT-Leitung oder Geschäftsleitungen. Basis: 505 befragte Unternehmen

Über den TÜV-Verband

Als TÜV-Verband e. V. vertreten wir die politischen Interessen der TÜV-Prüforganisationen und fördern den fachlichen Austausch unserer Mitglieder. Wir setzen uns für die technische und digitale Sicherheit sowie die Nachhaltigkeit von Fahrzeugen, Produkten, Anlagen und Dienstleistungen ein. Grundlage dafür sind allgemeingültige Standards, unabhängige Prüfungen und qualifizierte Weiterbildung. Unser Ziel ist es, das hohe Niveau der technischen Sicherheit zu wahren, Vertrauen in die digitale Welt zu schaffen und unsere Lebensgrundlagen zu erhalten. Dafür sind wir im regelmäßigen Austausch mit Politik, Behörden, Medien, Unternehmen und Verbraucher:innen.

Über das BSI

Das BSI ist die Cybersicherheitsbehörde des Bundes und Gestalter einer sicheren Digitalisierung in Deutschland. Unser Ziel ist der sichere Einsatz von Informations- und Kommunikationstechnik in Staat, Wirtschaft und Gesellschaft. Mit unserer Unterstützung soll Informationssicherheit als Voraussetzung der Digitalisierung verstanden und eigenverantwortlich umgesetzt werden. Wir wollen bewirken, dass Sicherheitsaspekte schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden. Denn Informationssicherheit und Digitalisierung gehören untrennbar zusammen.

TÜV VERBAND

Bundesamt für Sicherheit in der Informationstechnik

Kontakt

Bundesamt für Sicherheit in der Informationstechnik
Pressestelle
Tel.: 0228-999582-5777
E-Mail: presse@bsi.bund.de
Internet: www.bsi.bund.de

TÜV-Verband e. V.
Pressestelle
Tel.: 030-760095-580
E-Mail: presse@tuev-verband.de
Internet: www.tuev-verband.de

Grafik & Design

Nordpunkt Designagentur GmbH