HDI Cyberstudie 2026

Vom Risiko zur Resilienz: wie sich Cyberrisiken in deutschen KMUs erkennen und abwehren lassen.

Inhaltsverzeichnis

Vorwort

Peter Bertram
Leiter Produktmanagement & Underwriting Cyber,
HDI Versicherung AG

Cyberangriffe sind längst keine abstrakte Bedrohung mehr. Sie sind Realität – für Unternehmen jeder Größe, branchenübergreifend und zunehmend unabhängig vom Digitalisierungsgrad. Die Ergebnisse der vorliegenden HDI Cyberstudie 2026 zeigen deutlich: Das Cyberrisiko hat sich zu einem zentralen unternehmerischen Risiko entwickelt.

Die gute Nachricht: Unternehmen sind heute besser vorbereitet als noch vor wenigen Jahren. Präventive Maßnahmen greifen häufiger, Angriffe werden schneller erkannt und Schäden lassen sich zunehmend begrenzen. Jedoch nimmt die digitale Abhängigkeit immer weiter zu – etwa durch Cloud-Nutzung, vernetzte Prozesse oder den Einsatz Künstlicher Intelligenz. Damit steigt auch die Relevanz von Cybervorfällen für den laufenden Geschäftsbetrieb.

Die Studienergebnisse belegen, dass das Bewusstsein für Cyberrisiken in vielen Unternehmen gewachsen ist und Sicherheitsstrukturen zunehmend professionalisiert werden. Gleichzeitig zeigt sich jedoch, dass Cybervorfälle weiterhin häufig zu Betriebsunterbrechungen führen, der Faktor Mensch ein zentrales Angriffsziel bleibt und präventive Maßnahmen in ihrer Gesamtheit oftmals noch weiter optimiert werden können.

Zugleich verändert sich der Blick auf neue Technologien. Künstliche Intelligenz wird zunehmend als Chance begriffen, nicht zuletzt zur Stärkung der eigenen Cyberresilienz. Dieser Wandel im Mindset ist ein wichtiges Signal – denn moderne Cybersicherheit entsteht nicht durch einzelne Maßnahmen, sondern durch das Zusammenspiel von Technologie, Organisation und Verantwortung.

Mit der HDI Cyberstudie 2026 möchten wir Orientierung geben: Als Versicherer sehen wir eine fortlaufende Auseinandersetzung mit der aktuellen Sicherheitslage als ebenso unerlässlich an wie die Bereitstellung effektiver Assistance-Leistungen. Wir sehen uns hier in der Verantwortung, unser Wissen zu teilen und Zusammenhänge verständlich zu machen – und Unternehmen dabei zu unterstützen, Cyberrisiken realistisch einzuordnen und sich wirkungsvoll abzusichern.

Nicht, um zu alarmieren – sondern, um Handlungsfähigkeit zu stärken. Denn eines zeigt die Studie sehr deutlich: **Cyberrisiken lassen sich nicht vermeiden, aber sie lassen sich beherrschen.**

Wir wünschen Ihnen eine aufschlussreiche Lektüre.

Ihr **Peter Bertram**
Leiter Produktmanagement & Underwriting Cyber,
HDI Versicherung AG

Methodik

Willkommen zur vierten Ausgabe der HDI Cyberstudie, die erneut vom Marktforschungsinstitut Sirius Campus GmbH im Auftrag der HDI Versicherung AG durchgeführt wurde.

Die HDI Cyberstudie 2026 beruht auf einer repräsentativen Onlinebefragung von **1.083 Entscheidenden und Mitentscheidenden** aus kleinen und mittelständischen Unternehmen (KMUs) in Deutschland.

Um die tatsächliche Struktur des deutschen Mittelstands realistisch abzubilden, wurden die Ergebnisse nach Branche und Unternehmensgröße wertschöpfungsgewichtet. Die Stichprobe setzt sich zu etwa gleichen Teilen aus den drei zentralen KMU-Größenklassen zusammen:

- Kleinstunternehmen (0–9 Mitarbeitende)
- Kleinunternehmen (10–49 Mitarbeitende)
- Mittlere Unternehmen (50–250 Mitarbeitende)

Durch diese Gewichtung entspricht die Studie nicht der Anzahl aller KMUs, sondern ihrer wirtschaftlichen Bedeutung. Damit ermöglicht sie eine zuverlässige Hochrechnung auf die gesamte KMU-Wirtschaftskraft in Deutschland.

Die Cyberstudie 2026 setzt die mehrjährige Studienreihe von HDI fort und basiert auf einer Erhebung im Februar 2026. Viele Fragen wurden analog zu den Vorjahren gestellt, sodass Trends, Veränderungen und langfristige Entwicklungen im Cyberrisikoverhalten des Mittelstands klar erkennbar werden.

Die Ergebnisse bieten damit eine **fundierte und differenzierte Momentaufnahme der Cyberlage in deutschen KMUs –** praxisnah, belastbar und datenbasiert.

Die Referenzstudien aus den Jahren 2022, 2023 und 2024 wurden ebenfalls durch das Marktforschungsinstitut Sirius Campus GmbH durchgeführt. Dabei wurden Ende 2021 518, Ende 2022 702 und Ende 2023 1.518 Entscheidende und Mitentscheidende in KMUs befragt.

1.083 Entscheidende und Mitentscheidende aus kleinen und mittelständischen Unternehmen (KMUs) in Deutschland.
Basis: alle; Angaben in %

Zusammenfassung der Ergebnisse

Status der Cybersicherheit in deutschen KMUs.

Cyberkriminalität trifft den Mittelstand immer häufiger.

01 Jedes 3. Unternehmen sieht seine Existenz durch einen Cyberschaden in Gefahr.

- Laut HDI Cyberstudie gab mehr als jedes dritte Unternehmen (35 %) an, dass ein massiver Cyberschaden die eigene Existenz gefährden würde.
- Cybervergessen setzt ein: 49 % der in den letzten zwei Jahren angegriffenen Unternehmen sehen ihre Existenz gefährdet, nach drei bis fünf Jahren nur noch 32 % – trotz unverändertem Risiko.

02 Mehr als die Hälfte der Unternehmen arbeitet inzwischen in der Cloud.

- Insbesondere wissens- und datenintensive Berufsgruppen nutzen die Cloud besonders umfassend.
- Cloud-Lösungen werden von KMUs vor allem aus Sicherheitsgründen genutzt. Knapp die Hälfte der befragten Unternehmen (49 %) nennt die erhöhte IT-Sicherheit als wichtigsten Treiber für den Einsatz von Cloud-Technologien.

03 Cyberangriffe werden für immer mehr Unternehmen zur Realität.

- 35 % der kleinen und mittelständischen Unternehmen wurden in den letzten fünf Jahren mindestens einmal Ziel einer Cyberattacke.
- Der Mensch ist weiterhin Einfallstor Nr. 1. Phishing-Mails und infizierte Dateianhänge waren in den letzten zwölf Monaten die dominierenden Angriffsvektoren bei angegriffenen Unternehmen (64 % bzw. 47 %).

04 Betriebsunterbrechung – das zentrale Risiko eines Cyberangriffs.

- Betriebsunterbrechung ist die häufigste Schadenart infolge eines Cyberangriffs: Unternehmen sind im Schnitt vier Tage arbeitsunfähig.
- Prävention, klar definierte Zuständigkeiten und eine Risikosensibilisierung können die Ausfallzeit reduzieren.

05 Maßnahmen wirken: Prävention ist besser als Reaktion.

- Präventive Maßnahmen können den Durchschnittsschaden um bis zu 33 % reduzieren.
- Präventive Maßnahmen werden von immer mehr Unternehmen umgesetzt.

06 Künstliche Intelligenz – vom Unsicherheitsfaktor zum Stabilitätsanker.

- 55 % der Unternehmen sehen KI als Chance für ihr Unternehmen.
- Unternehmen sehen in der KI eher eine Stärkung ihrer Cyberresilienz (26 %) als eine Schwächung (12 %).

Existenzbedrohung

Risikowahrnehmung trifft
auf Cybervergessen.

Cyberschäden: Jedes dritte Unternehmen ist sich der Gefahr bewusst.

Einige Branchen sehen ihre Existenz durch einen Cyberschaden besonders bedroht.

Cyberangriffe sind im heutigen Arbeitsalltag der Unternehmen angekommen. Täglich gibt es neue Schlagzeilen darüber, dass ein Unternehmen keinen Zugriff mehr auf seine Systeme hat, Daten kopiert wurden oder dass es nicht weiter produzieren kann. Demnach ist es nicht verwunderlich, dass Cyberangriffe für Unternehmen kein theoretisches Risiko mehr sind, sondern eine tatsächliche potenzielle Bedrohung für ihre wirtschaftliche Existenz.

Mehr als jedes dritte Unternehmen (35 %) gibt an, dass ein massiver Cyberschaden die Existenz des eigenen Unternehmens gefährden würde. Demgegenüber sind lediglich 31 % der Befragten der Ansicht, dass dies eher nicht der Fall wäre. Damit sieht eine klare Mehrheit zumindest ein grundsätzliches Existenzrisiko durch Cybervorfälle.

Diese Einschätzung verdeutlicht, wie tiefgreifend die möglichen Folgen von Cyberangriffen inzwischen bewertet werden. Cyberrisiken betreffen nicht nur einzelne IT-Systeme, sondern können gesamte Geschäftsmodelle infrage stellen. Betriebsunterbrechungen, Datenverluste, finanzielle Schäden und Reputationsverluste zählen zu den zentralen Risikofaktoren. Welche Schäden in der Praxis tatsächlich auftreten, wird im Kapitel „Cyberangriffe“ näher beleuchtet.

Die Wahrnehmung der Existenzgefährdung unterscheidet sich je nach Branche und Unternehmensgröße deutlich.

Vor allem kleine Unternehmen mit einem Jahresumsatz zwischen 2,5 Mio. Euro und 10 Mio. Euro zeigen eine erhöhte Sensibilität (39 %): Begrenzte finanzielle Rücklagen, fehlende personelle Redundanzen und eine hohe Abhängigkeit von funktionierenden IT-Systemen können dazu führen, dass Cybervorfälle hier schneller existenzbedrohende Ausmaße annehmen. Die HDI Cyberstudie 2024 hatte hier gezeigt, dass Cyberangriffe insbesondere kleinere Unternehmen überproportional stark treffen, da sie Cyberschäden in der Regel weniger gut kompensieren können als größere Unternehmen.

Auch im Branchenvergleich werden klare Unterschiede sichtbar. Besonders ausgeprägt ist die Sorge vor existenzgefährdenden Cyberfolgen bei:

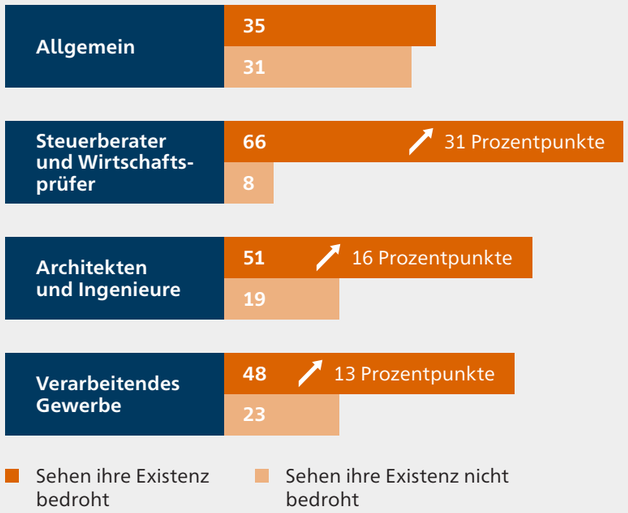
- Steuerberatern und Wirtschaftsprüfern (66 %),
- Architekten und Ingenieuren (51 %)
- sowie im verarbeitenden Gewerbe (48 %).

Demgegenüber nehmen sich **Bauhandwerk** und **Gastgewerbe** deutlich seltener als existenziell gefährdet wahr. So gehen 40 % der befragten Unternehmen aus dem Bauhandwerk sowie 42 % aus dem Gastgewerbe davon aus, dass ein Cyberschaden ihre Existenz **nicht gefährden** würde. Diese Einschätzung der Branchen deutet jedoch nicht zwangsläufig auf ein objektiv niedrigeres Risiko hin, sondern vielmehr darauf, dass Cyberangriffe und deren wirtschaftliche Folgen in diesen Branchen häufig schwerer vorstellbar oder weniger präsent sind.

Besonders deutlich wird dieser Effekt im Zusammenhang mit eigenen Schadenserfahrungen. **Unternehmen, die bereits einen Cyberangriff mit finanziellem Schaden erlitten haben, bewerten die Gefahr als erheblich höher:** 50 % von ihnen sehen ihre Existenz durch einen erneuten Cyberschaden bedroht. Bei Unternehmen ohne bisherige Angriffserfahrung liegt dieser Wert hingegen bei lediglich 28 %. Eigene Betroffenheit schärft damit den Blick für die tatsächliche Tragweite von Cyberrisiken. Dies unterstreicht insbesondere die Tatsache, dass nur 9 % der geschädigten Unternehmen keine existenzielle Bedrohung durch Cyberangriffe sehen.

Ebenso spielen Prävention und Cyberversicherungen eine entscheidende Rolle, um Unternehmen für das Thema zu sensibilisieren. So gaben 49 % der befragten Unternehmen mit einer Cyberversicherung und einem hohen Umsetzungsstand bei präventiven Maßnahmen an, dass ihr Unternehmen durch eine Cyberattacke in existenzielle Schwierigkeiten kommen kann. Welche Maßnahmen hier Unternehmen vor solchen Angriffen schützen können, erfahren Sie im Kapitel „Prävention ist besser als Reaktion“.

Würde ein massiver Cyberschaden die Existenz Ihres Unternehmens gefährden?



Basis: Angaben in %

Kleinere Unternehmen trifft ein Cyberschaden härter, da der finanzielle Schaden nicht so leicht aufgefangen werden kann.

Cybervergessen

Nach einer Attacke steigt das Risikobewusstsein – und nimmt dann wieder nachweislich ab.

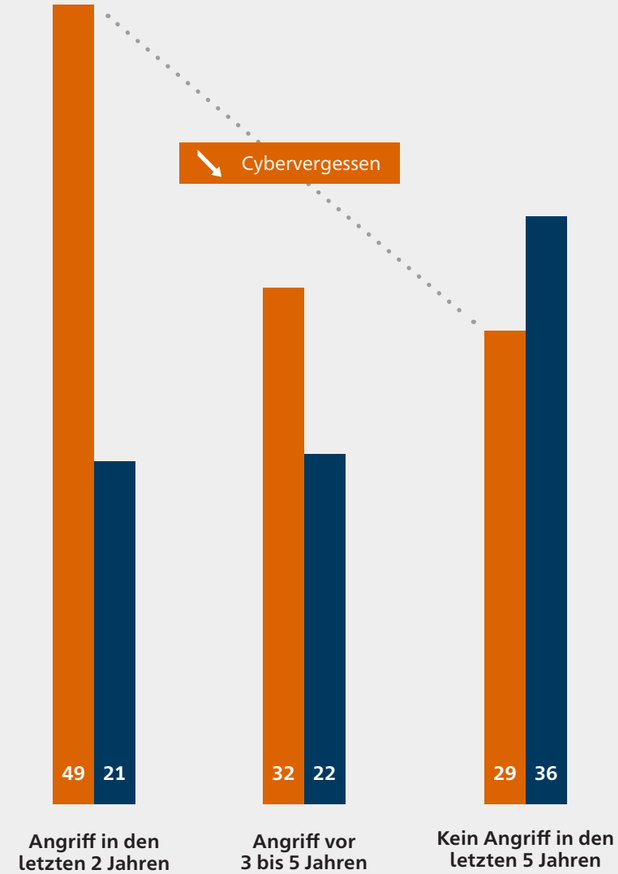
In der HDI Cyberstudie 2024 wurde ein Cybervergessen festgestellt. Das bedeutet, dass Unternehmen direkt nach einem Cyberangriff besonders sensibilisiert sind. Diese Sensibilisierung verliert jedoch bereits innerhalb weniger Jahre spürbar an Intensität. Auch die Einschätzung des eigenen Cyberrisikos folgt diesem Muster und sinkt mit wachsendem zeitlichen Abstand zum letzten Vorfall deutlich.

So geben knapp 49 % der Unternehmen, die in den letzten zwei Jahren angegriffen wurden, an, dass sie ihre Existenz durch einen Cyberangriff gefährdet sehen. Liegt der Angriff bereits drei bis fünf Jahre zurück, so sehen hier nur noch 32 % ihre Existenz gefährdet.

Gerade diese Dynamik ist riskant. Denn Cyberbedrohungen verschwinden nicht – sie verändern sich kontinuierlich. Eine rückläufige Wahrnehmung der Existenzrelevanz kann dazu führen, dass Präventionsmaßnahmen vernachlässigt oder aufgeschoben werden, obwohl die objektive Bedrohungslage unverändert hoch bleibt.

Die Ergebnisse der Cyberstudie 2026 machen damit deutlich: **Cyberschäden haben das Potenzial, Unternehmen in ihrer wirtschaftlichen Substanz zu treffen.** Die Existenzgefährdung durch Cyberangriffe ist kein Randphänomen, sondern ein relevantes Risiko quer durch Unternehmensgrößen und Branchen.

Würde ein massiver Cyberschaden die Existenz Ihres Unternehmens gefährden?



Basis: KMUs mit einer Cyberattacke; Angaben in %

Digitale Abhängigkeit

Potenziale und Risiken
cloudbasierter IT-Strukturen.

Die digitale Abhängigkeit steigt.

Mehr als die Hälfte der Unternehmen arbeitet inzwischen cloudbasiert.

Wie das vorangegangene Kapitel zeigt, bewertet die Mehrheit der befragten Unternehmen Cyberschäden als existenzielle Bedrohung – ein Risikobewusstsein, das eng mit der zunehmenden digitalen Abhängigkeit verknüpft ist. Diese nimmt weiter zu: Mehr als die Hälfte der befragten Unternehmen (54 %) arbeiten inzwischen in der Cloud. Cloudbasierte IT-Strukturen haben sich damit vom Sonderfall zum festen Bestandteil der Unternehmensrealität entwickelt. Insbesondere Geschäftsprozesse, Datenhaltung und Kollaboration verlagern sich zunehmend in externe IT-Infrastrukturen.

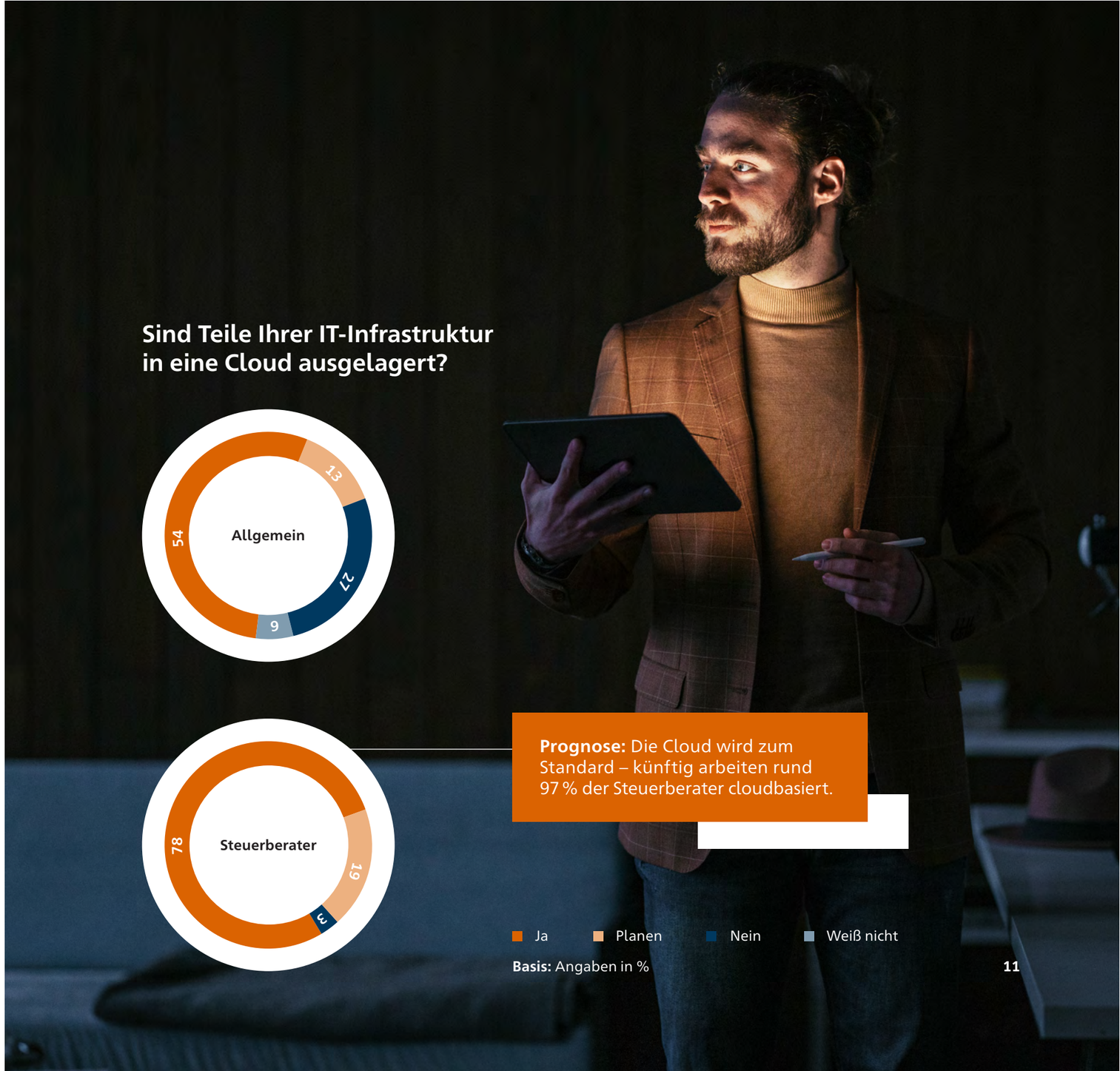
Deutliche Unterschiede je nach Unternehmensgröße.

Besonders stark verbreitet ist die Cloud-Nutzung bei Kleinunternehmen mit einem Jahresumsatz zwischen 2,5 und 10 Mio. Euro, von denen 63 % bereits cloudbasierte Lösungen einsetzen. In diesem Segment treffen zunehmende Digitalisierung, wachsende IT-Anforderungen und der Wunsch nach Skalierbarkeit besonders stark aufeinander.

Demgegenüber verhalten sich Kleinstunternehmen mit einem Jahresumsatz bis 500.000 Euro zurückhaltender: 56 % arbeiten noch nicht in der Cloud. Hier spielen häufig begrenzte IT-Ressourcen, eine geringere Komplexität der Systeme sowie Unsicherheiten bei Sicherheit und Kosten eine Rolle.

Im Branchenvergleich wird sichtbar, dass insbesondere wissens- und datenintensive Berufsgruppen die Cloud bereits sehr umfassend nutzen. **Steuerberater (78 %)** und **Architekten und Ingenieure (77 %)** arbeiten mehrheitlich in der Cloud. Bemerkenswert ist dabei die hohe Dynamik: **Weitere 19 % der Steuerberater planen den Einstieg,** sodass künftig nur noch 3 % dieser Berufsgruppe vollständig ohne Cloud-Nutzung arbeiten würden. Dies unterstreicht den hohen Digitalisierungsgrad dieser Zielgruppe.

Ähnlich zeigt sich das verarbeitende Gewerbe, das ebenfalls verstärkt auf Cloud-Lösungen setzt (65 %), um die Prozesse effizienter zu gestalten, die Kosten zu reduzieren und die Sicherheit zu erhöhen.



Die Cloud: strategisch unverzichtbar.

Chancen und Herausforderungen moderner Unternehmensinfrastrukturen.

Die Ergebnisse der Studie zeigen deutlich: **Cloud-Lösungen werden von KMUs vor allem aus Sicherheitsgründen genutzt.** Knapp die Hälfte der befragten Unternehmen (49 %) nennt die erhöhte IT-Sicherheit als wichtigsten Treiber für den Einsatz von Cloud-Technologien. Cloud-Anbieter verfügen häufig über professionelle Sicherheitsarchitekturen, redundante Rechenzentren, regelmäßige Updates und spezialisierte Sicherheitsteams – Fähigkeiten, die viele Unternehmen im KMU-Segment intern kaum abbilden können. Darüber hinaus spielen **Flexibilität und Mobilität** eine zentrale Rolle: 44 % sehen in der ortsunabhängigen Verfügbarkeit von Daten und Anwendungen einen wesentlichen Vorteil. Auch **Kostenaspekte** sind relevant – 38 % der Unternehmen verbinden Cloud-Nutzung mit einer spürbaren Reduktion von IT-Kosten.

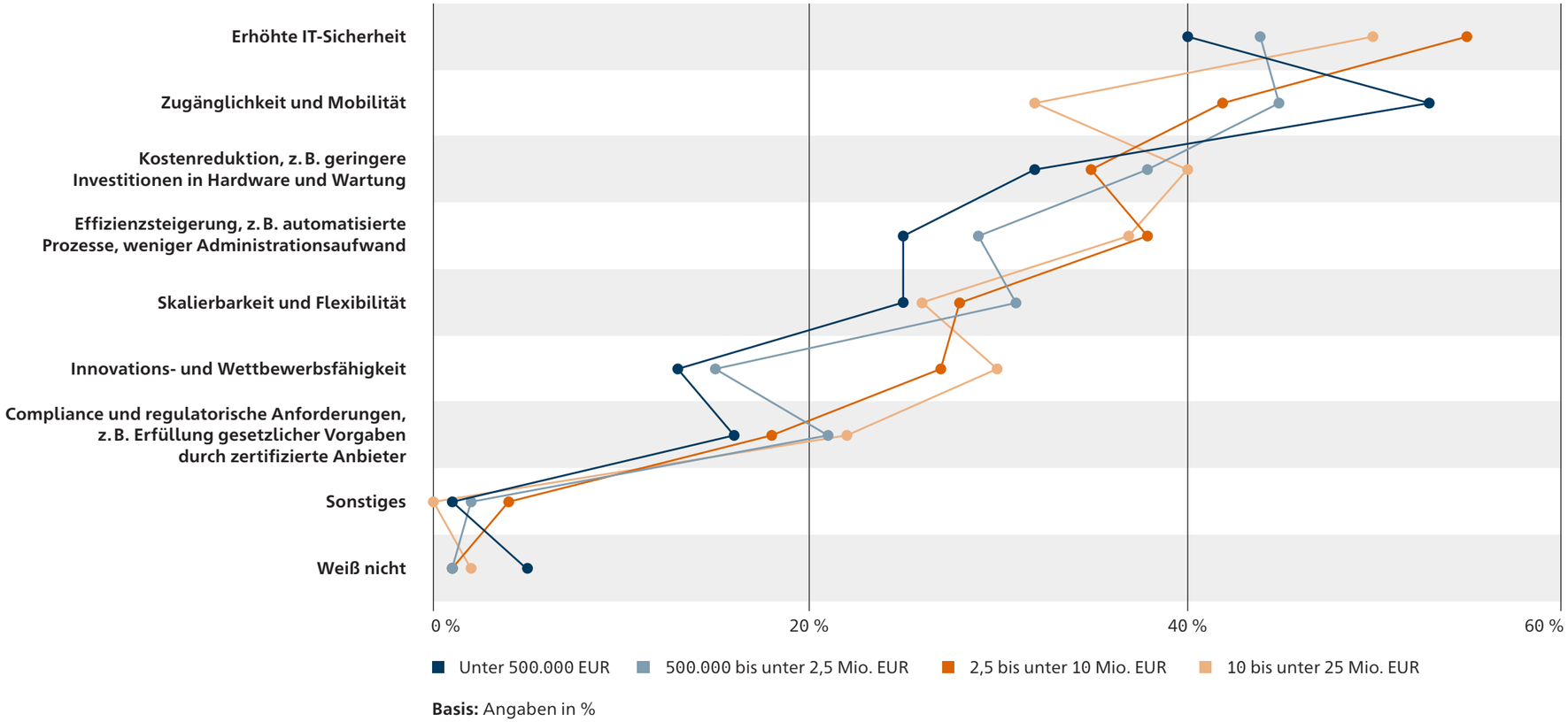
Die Cloud ist für viele KMUs nicht mehr nur eine technologische Option, sondern ein strategischer Baustein, um Sicherheit, Effizienz und Wettbewerbsfähigkeit gleichzeitig zu stärken.

Allerdings birgt diese Einschätzung auch ein Risiko: Cloud bedeutet nicht automatisch Sicherheit. **Die Sicherheit in der Cloud ist kein Produkt, sondern ein Zusammenspiel aus Anbietermaßnahmen und unternehmerischer Verantwortung.** Fehlkonfigurationen, schwache Zugriffskontrollen, unzureichende Nutzerverwaltung oder mangelndes Notfall-Management bleiben auch in der Cloud kritische Schwachstellen.

Gerade für **Kleinstunternehmen,** die eine Cloud vor allem wegen **Zugänglichkeit und Mobilität (53 %)** nutzen, besteht die Gefahr, Sicherheitsaspekte zu unterschätzen. Die einfache Erreichbarkeit von Daten und Anwendungen ist ein Vorteil – sie kann jedoch bei unzureichender Absicherung auch Angriffsflächen vergrößern.

So belegen die Zahlen der HDI Cyberstudie 2026, dass Unternehmen, die ihre IT-Systeme komplett oder zum Teil in die Cloud ausgelagert haben, bei einem Cyberschaden häufiger von einer Betriebsunterbrechung betroffen sind als Unternehmen, die nicht in der Cloud arbeiten (31 % zu 14 %).

Was sind die Hauptgründe dafür, dass Ihr Unternehmen auf Cloud-Lösungen umgestiegen ist oder einen Wechsel plant?



Basis: Angaben in %

Cloud-Nutzung schärft das Risikobewusstsein.

Cloudbasierte Unternehmen sind sich ihrer digitalen Abhängigkeit bewusst – und handeln präventiv.

Die Cloud ist längst ein zentraler Baustein der digitalen Transformation. Mit ihrer zunehmenden Nutzung wächst jedoch auch die Abhängigkeit von einer stabilen und jederzeit verfügbaren IT-Infrastruktur. Positiv zu erwähnen ist hier, dass sich Unternehmen diesem Spannungsfeld zunehmend bewusst sind.

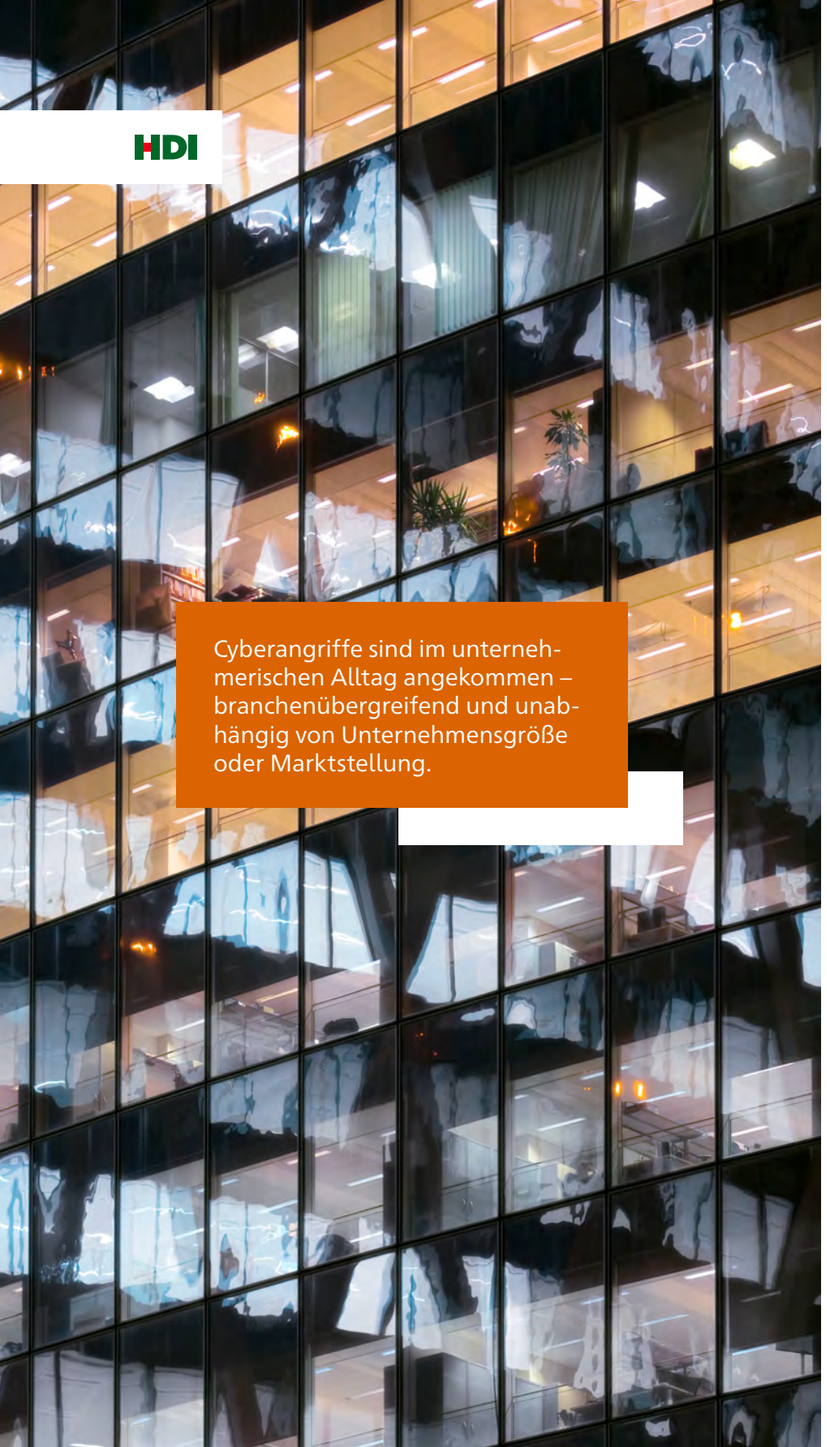
So schätzen Unternehmen mit Cloud-Nutzung ihr eigenes Cyberrisiko deutlich höher ein als Unternehmen, die nicht auf eine Cloud-Lösung setzen. 71 % der cloudnutzenden Unternehmen bewerten ihr Cyberrisiko als hoch – gegenüber lediglich 23 % der Unternehmen, die bislang keine Teile ihrer IT in die Cloud ausgelagert haben. Cloud-Nutzung und Risikowahrnehmung bedingen sich dabei gegenseitig: Wer zentrale Systeme, Daten und Prozesse auslagert, wird sich zugleich der **größeren Angriffsfläche, Abhängigkeiten und potenziellen Ausfallfolgen** bewusster.

Diese erhöhte Risikowahrnehmung bleibt nicht folgenlos. Cloudnutzende Unternehmen investieren deutlich häufiger in **präventive Sicherheitsmaßnahmen: 61 %** von ihnen verfügen über einen hohen Umsetzungsstand an präventiven Maßnahmen. Cloud-Nutzung führt damit nicht zu einer Verharmlosung von Cyberrisiken – im Gegenteil: Sie schärft den Blick für die eigene digitale Verwundbarkeit.

Die Studie macht damit deutlich: **Cloud-Nutzung kann ein Sicherheitsgewinn sein – ist es aber nur dann, wenn sie aktiv gemanagt wird.** Digitale Abhängigkeit erfordert digitale Verantwortung. Entsprechend ergänzen viele Unternehmen ihre Präventionsstrategie um eine zusätzliche Absicherung: Mehr als zwei Drittel der cyberversicherten Unternehmen arbeiten inzwischen zumindest teilweise in einer Cloud (69 %).

Cyberangriffe

Die größte Sicherheitslücke bleibt weiterhin der Mensch.



Cyberangriffe sind im unternehmerischen Alltag angekommen – branchenübergreifend und unabhängig von Unternehmensgröße oder Marktstellung.

Cyberangriffe sind Realität – und sie nehmen weiter zu.

Für Unternehmen stellt sich nicht länger die Frage, ob sie Ziel eines Angriffs werden, sondern wann.

Die Folgen erfolgreicher Cyberangriffe sind erheblich und reichen von finanziellen Schäden und Betriebsunterbrechungen bis hin zu langfristigen Reputations- und Vertrauensverlusten bei Kunden und Geschäftspartnern. Die Ergebnisse der Cyberstudie 2026 unterstreichen diese Entwicklung: **35 % der kleinen und mittelständischen Unternehmen wurden in den letzten fünf Jahren mindestens einmal Ziel einer Cyberattacke.**

Welche Branchen sind gefährdet – und warum?

Besonders betroffen waren in den letzten zwölf Monaten **IT-Dienstleister** (32 %), **Architekten und Ingenieure** (28 %), **Ärzte und Heilberufe** (27 %) sowie das **verarbeitende Gewerbe** (25 %). Diese Branchen eint ein hoher Digitalisierungsgrad, zahlreiche externe Schnittstellen und eine starke Abhängigkeit von IT-gestützten Prozessen.

Im verarbeitenden Gewerbe wächst zusätzlich die Vernetzung von Produktionsanlagen und Steuerungssystemen mit der Unternehmens-IT – häufig auf historisch gewachsenen Systemlandschaften, die nicht für heutige Sicherheitsanforderungen ausgelegt sind. Cyberangriffe können so nicht nur Informationssysteme, sondern direkt auch Produktions- und Fertigungsprozesse treffen.

Besonders im Visier der Angreifer: IT-Dienstleister und Heilberufe.

Der Anteil betroffener **IT-Dienstleister** stieg von 23 % (HDI Cyberstudie 2024) auf 32 % – ein **relativer Anstieg von rund 39 %.** IT-Dienstleister verfügen häufig über weitreichende Zugriffsrechte in Bezug auf Kundensysteme und Kundendaten und nehmen eine zentrale Rolle in digitalen Wertschöpfungsketten ein – das macht sie zu besonders attraktiven Angriffszielen.

Ähnliches gilt für **Ärzte und Heilberufe:** Der Anteil stieg von 23 % auf 27 % – ein **Zuwachs von vier Prozentpunkten.** Angesichts hochsensibler personenbezogener und medizinischer Daten ist dieser Anstieg besonders kritisch zu bewerten. Cyberangriffe können hier nicht nur wirtschaftliche Schäden verursachen, sondern auch die Patientenversorgung gefährden.

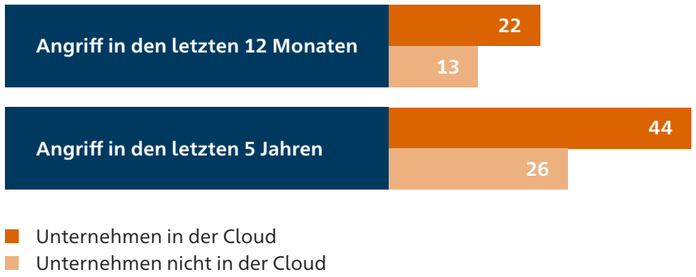
Arbeiten in der Cloud – Sicherheit oder Sicherheitslücke?

Auffällig ist der Zusammenhang zwischen Cloud-Nutzung und Cyberangriffen: **22 % der Unternehmen mit ausgelagerter IT-Infrastruktur berichten von einer Cyberattacke in den letzten zwölf Monaten –** gegenüber 13 % bei den Unternehmen ohne Cloud-Nutzung. Ein deutlicher Unterschied von neun Prozentpunkten.

Über fünf Jahre betrachtet verstärkt sich dieses Bild: 44 % der Unternehmen mit Cloud-Infrastruktur waren mindestens einmal betroffen, bei Unternehmen ohne Cloud-Nutzung waren es 26 %.

Die Ergebnisse verdeutlichen, dass Cloud-Umgebungen trotz ihrer Vorteile hinsichtlich Flexibilität, Skalierbarkeit und Effizienz zusätzliche Angriffsflächen schaffen, die gezielte Sicherheitsmaßnahmen erfordern.

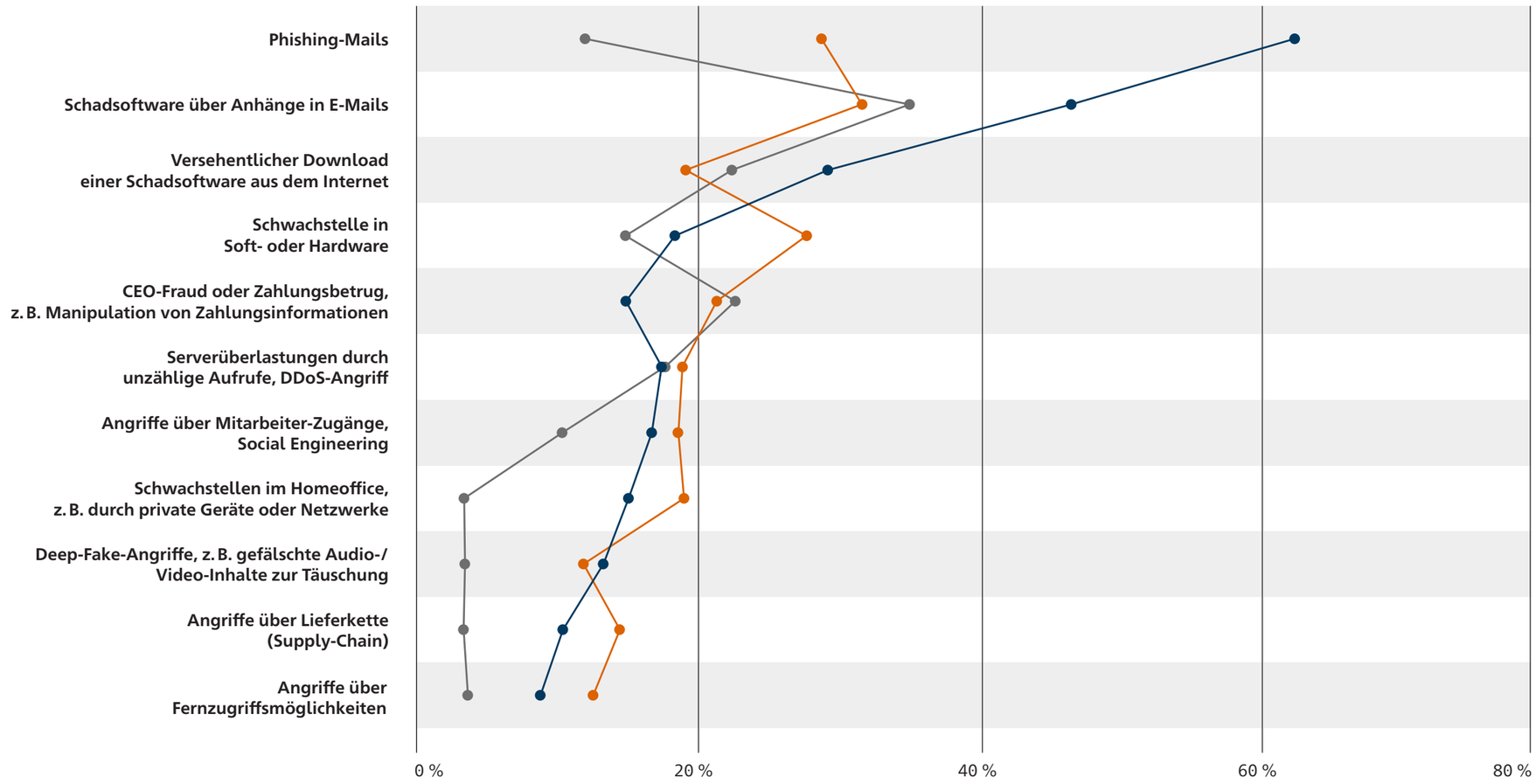
Cloud-Nutzung und Angriffshäufigkeit im Vergleich.



Basis: Angaben in %

Ranking Angriffsart im Zeitverlauf: Kennen Sie die folgenden Formen von Cyberattacken?

(Unternehmen wurde so bereits angegriffen)



Basis: KMUs mit einer Cyberattacke; Angaben in %

Das Vorgehen der Cyberkriminellen: Angriffsmethoden im Überblick.

Auch in diesem Jahr bestätigen die Ergebnisse: Die drei häufigsten Angriffswege zielen auf den Faktor Mensch ab.

Die Auswertung der betroffenen Unternehmen zeigt, dass insbesondere Angriffe über E-Mails im vergangenen Jahr deutlich zugenommen haben. Besonders ausgeprägt ist dabei der weiter **zunehmende Trend bei Phishing-Angriffen: 64 % der betroffenen Unternehmen berichten von entsprechenden Vorfällen** innerhalb der letzten zwölf Monate. Zum Vergleich: Vor drei bis fünf Jahren lag dieser Anteil noch bei lediglich 12 %, was die starke Dynamik und zunehmende Relevanz dieser Angriffsmethode unterstreicht.

Die zweithäufigste Angriffsmethode sind **E-Mails mit Schadsoftware im Anhang.** Wird ein solcher Anhang von Mitarbeitenden unbedacht geöffnet, entsteht unmittelbar ein Einfallstor für Cyberkriminelle. **47 % der betroffenen Unternehmen geben an, diese Form des Angriffs innerhalb der vergangenen zwölf Monate erlebt zu haben,** womit sie Rang zwei der häufigsten Angriffsmuster einnimmt.

Auf **Platz drei folgt der versehentliche Download schädlicher Inhalte aus dem Internet** durch Mitarbeitende, der ebenfalls maßgeblich zur erfolgreichen Kompromittierung von IT-Systemen beiträgt.

Komplexere Angriffsmuster rücken in den Fokus:

Neben den etablierten Angriffsmethoden rücken zunehmend neue Bedrohungsszenarien in den Fokus. CEO-Fraud, Deep-Fake-basierte Täuschungen und Supply-Chain-Angriffe werden im Jahr 2026 erstmals von einem relevanten Anteil der Unternehmen als ernsthafte Risiken wahrgenommen. Dabei zeigen sich deutliche Unterschiede in Abhängigkeit von der Unternehmensgröße: Während **kleinere Unternehmen** mit stärker zentralisierten Entscheidungsstrukturen **besonders häufig von CEO-Fraud** betroffen sind, dominieren in **größeren Organisationen weiterhin Phishing-Angriffe.** Kleinstunternehmen berichten hingegen nur selten von Supply-Chain-Angriffen, da ihre Abhängigkeit von komplexen Liefer- und IT-Dienstleister-Strukturen meist geringer ist.

Welche Schäden daraus entstehen, beleuchtet das nachfolgende Kapitel.

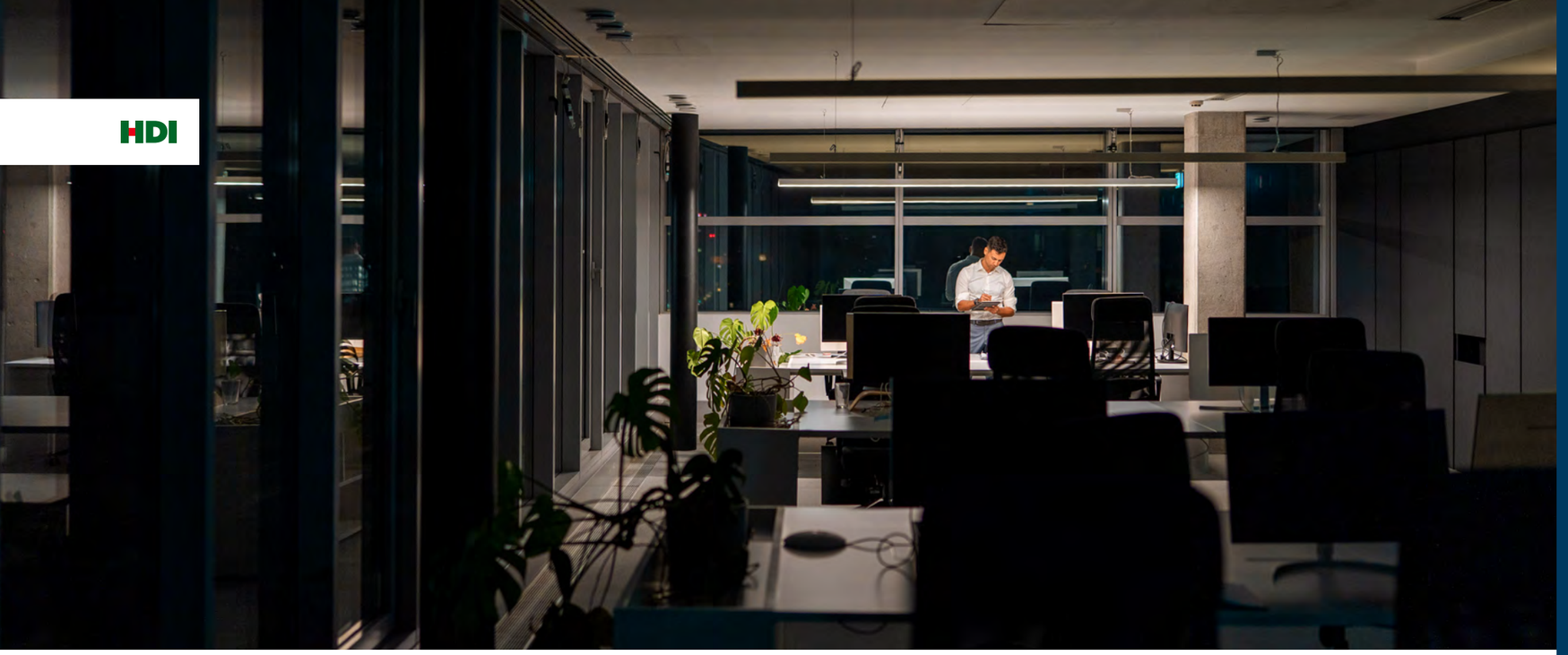
Erfahrung mit Cyberangriffen.

Kennen Sie die folgenden Formen von Cyberattacken?

Basis: alle; Angaben in %
(Ranking nach Top 1: „Unser Unternehmen wurde so bereits attackiert“)

Betriebsunterbrechung

Das zentrale Risiko eines Cyberangriffs.



Unternehmen sind nach einem Cyberschaden durchschnittlich vier Tage arbeitsunfähig.

Trotz verbesserter Präventionsmaßnahmen bleibt die Betriebsunterbrechung auch in der HDI Cyberstudie 2026 die häufigste und folgenreichste Schadenart infolge eines Cyberangriffs. **Rund ein Drittel aller Cybervorfälle (32 %) führt unmittelbar zu einer Betriebsunterbrechung – damit liegt sie klar vor Datenverlust, Reputationsschäden oder Lösegeldforderungen.** Der operative Stillstand erweist sich damit als das Risiko, das Unternehmen am unmittelbarsten trifft.

Im Durchschnitt sind Unternehmen nach einer erfolgreichen Attacke rund vier Tage arbeitsunfähig. Das klingt zunächst überschaubar – die wirtschaftlichen Folgen sind es jedoch nicht.
Bereits wenige Tage ohne Zugriff auf IT-Systeme, Anwendungen, Produktionssysteme oder betriebsrelevante Daten können erhebliche finanzielle Schäden verursachen. **Für viele KMUs wird eine mehrtägige Betriebsunterbrechung so schnell zur existenziellen Bedrohung.**

Unternehmen mit fünf bis neun Mitarbeitenden werden laut Studie besonders häufig erfolgreich angegriffen. Hier treffen hohe operative Abhängigkeiten auf begrenzte personelle und organisatorische Ressourcen, oft ohne vollständig ausgearbeitete Backup-, Notfall- oder Wiederanlaufkonzepte.

Konsequente Prävention hingegen kann Ausfallzeiten verkürzen und Folgeschäden spürbar begrenzen. Welche Maßnahmen dabei entscheidend sind und welchen konkreten Nutzen sie haben, zeigt das Kapitel „Prävention ist besser als Reaktion“.

Besonders gefährdet:
Freiberufler und Selbstständige – mit einem durchschnittlichen Betriebsausfall von sechs Tagen.

Angriffsmethoden, die zu einer Betriebsunterbrechung führen.

Basis: KMUs mit einer Betriebsunterbrechung; Angaben in %

Die Hauptursachen von Betriebsunterbrechungen lassen sich klar benennen. Am häufigsten führen zu einem Stillstand:

- **Schwachstellen in Soft- und Hardware (34 %)**
- **Angriffe über die Lieferkette (33 %)**
- **Versehentlicher Download einer Schadsoftware (25 %)**

Deutlich zugenommen hat vor allem die Ausnutzung von Schwachstellen in Soft- und Hardware: Während diese Angriffsmethode 2024 nur in 29 % der Fälle zu einer Betriebsunterbrechung führte, sind es 2026 bereits 34 %. Dies unterstreicht die Bedeutung eines konsequenten Patch-Managements.

Phishing-Mails und schadhafte Anhänge führen heute seltener zu Betriebsunterbrechungen als noch in der HDI Cyberstudie 2024. Dennoch bleibt Phishing die häufigste Angriffsmethode von Cyberkriminellen. Dass diese Methode seltener zu einem Stillstand führt, deutet darauf hin, dass Unternehmen in den Bereichen Organisation, Technik, Notfallplanung und Sensibilisierung der Mitarbeitenden resilienter geworden sind. Den richtigen Weg haben sie damit eingeschlagen – nun muss er konsequent weiterverfolgt werden.

Cybervergessen verlängert die Ausfallzeiten.

Ein weiterer kritischer Zusammenhang zeigt sich bei der Risikowahrnehmung. **Unternehmen mit einer geringen eigenen Cyberrisikoeinschätzung sind häufiger und länger von Betriebsunterbrechungen betroffen.** Ihre Ausfallzeit liegt im Durchschnitt bei circa fünf Tagen – Unternehmen mit hoher Risikoeinschätzung für ihr eigenes Unternehmen kommen hingegen auf nur drei Tage. Gründe sind fehlende oder nicht getestete Notfallpläne, unklare Zuständigkeiten und unzureichende Wiederanlaufprozesse.

Zusammenfassend lässt sich jedoch sagen: Prävention ist besser als Reaktion. **65 % der Cyberangriffe verursachen inzwischen keinen messbaren Schaden –** 2024 waren es noch 47 %.

Finanzielle Folgen einer Cyberattacke.

Die Schadenhöhe sinkt zwar deutlich – Entwarnung wäre jedoch fatal.

Die durchschnittliche Schadenhöhe pro Cyberangriff liegt 2026 bei rund 25.000 Euro und damit deutlich unter dem Niveau der vorherigen Studie (2024: rund 99.000 Euro). Diese Entwicklung darf jedoch nicht als Entspannung der Bedrohungslage missverstanden werden.

Vielmehr weist sie darauf hin, dass:

- **Präventive Maßnahmen zunehmend greifen**
- **Cyberangriffe häufiger frühzeitig erkannt werden**
- **Schäden schneller eingegrenzt und behoben werden**
- **Cybervorfälle zwar häufiger auftreten, aber seltener zu großen finanziellen Schäden eskalieren**

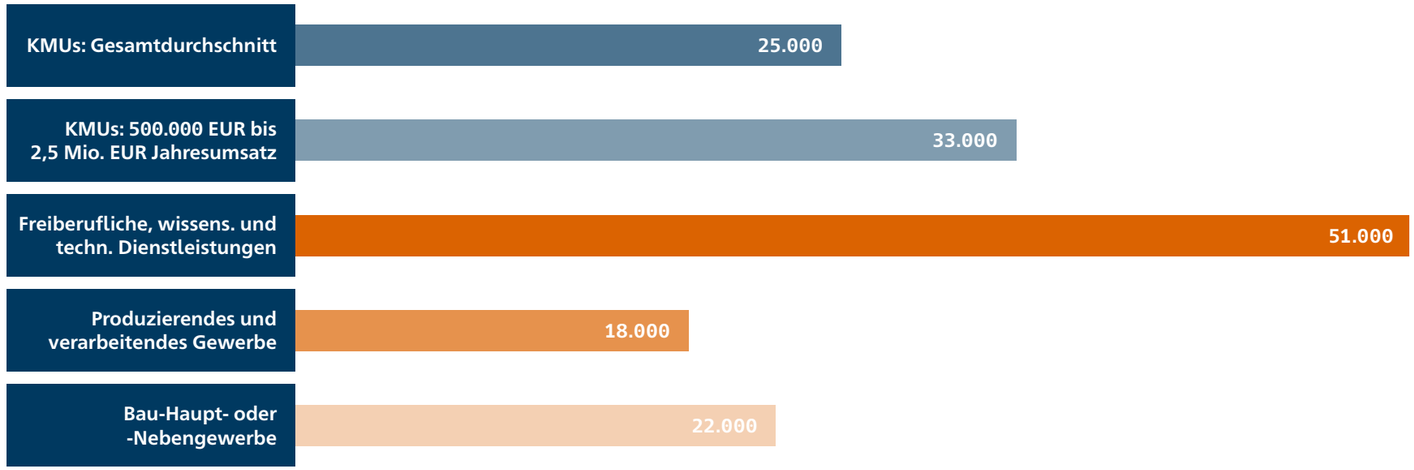
Gleichzeitig zeigt die Studie, dass **einzelne Branchen weiterhin sehr hohe durchschnittliche Schadenhöhen aufweisen:**

- Freiberufliche, wissensintensive und technische Dienstleistungen: rund 51.000 Euro
- Produzierendes und verarbeitendes Gewerbe: rund 18.000 Euro
- Bau-Haupt- oder -Nebengewerbe: rund 22.000 Euro

Besonders kritisch ist zudem die Unternehmensgrößenklasse mit 500.000 Euro bis 2,5 Mio. Euro Jahresumsatz. Hier liegt der durchschnittliche Schaden bei rund 33.000 Euro – eine Größenordnung, die finanzielle Reserven oft deutlich überfordert.

Die ausgewiesenen Schadenssummen stellen Durchschnittswerte dar. Sie verdecken jedoch, dass Cyberangriffe im Einzelfall zu erheblich höheren Schäden bis in den sechsstelligen Bereich führen können.

Durchschnittliche Schadenhöhe.



Basis: KMUs mit einer Cyberattacke; Angaben in EUR

Cyberversicherung als aktiver Resilienzfaktor.

Die Studie zeigt eindeutig: **Unternehmen mit Cyberversicherung nehmen den Geschäftsbetrieb nach einem Cyberangriff schneller wieder auf.** Sie verfügen häufiger über:

- Notfall- und Wiederanlaufpläne
- Strukturierte Incident-Response-Prozesse
- Höhere Präventionsniveaus und klare Verantwortlichkeiten

Die Folge sind kürzere Betriebsunterbrechungen und geringere Folgeschäden. **Die Cyberversicherung wirkt damit nicht nur als finanzieller Schutzmechanismus, sondern als aktiver Stabilitätsfaktor im Krisenfall.**

Resilienz entscheidet über Ausmaß und Dauer.

Die Betriebsunterbrechung bleibt auch 2026 das zentrale Risiko nach Cyberangriffen. Zwar sinken die durchschnittlichen Schadenhöhen, doch Ausfallzeiten, branchenspezifische Abhängigkeiten und organisatorische Schwächen machen einen Betriebsausfall weiterhin zu einem entscheidenden Gefahrenfaktor.

Prävention, klar definierte Zuständigkeiten und eine leistungsfähige Cyberversicherung sind heute zentrale Faktoren dafür, ob ein Cyberangriff lediglich eine kurzfristige Störung bleibt oder sich zu einer existenziellen Krise für das Unternehmen entwickelt.

Prävention ist besser als Reaktion

Ganzheitlich gedachte Cyberresilienz zeigt immer mehr Wirkung.

Cyberschäden begrenzen: So agieren die Unternehmen.

Die Ergebnisse der HDI Cyberstudie 2026 zeigen erneut: Prävention ist ein entscheidender Faktor, um die Schadeneintrittswahrscheinlichkeit zu verringern sowie die Auswirkungen eines Cyberschadens zu minimieren.

In den letzten Jahren haben die Ergebnisse klar darauf hingewiesen, dass präventive Maßnahmen – seien sie technisch oder organisatorisch – das entscheidende Mittel im digitalen Zeitalter sind. Sie können nicht nur Schäden verhindern, sondern auch eintretende Cyberschäden signifikant begrenzen.

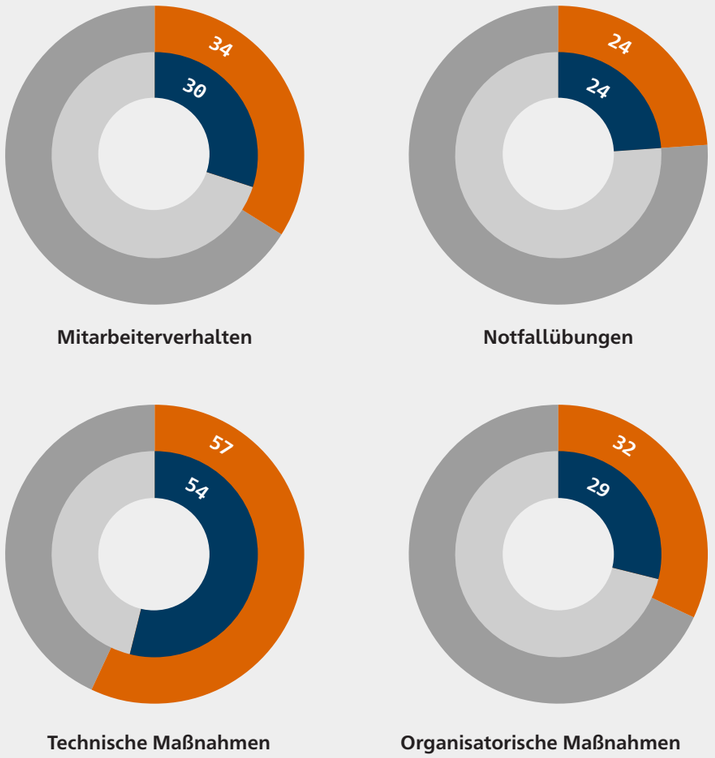
Unternehmen, die frühzeitig, strukturiert und ganzheitlich in ihre Cyberresilienz investieren, sind Angriffen nicht nur seltener schutzlos ausgesetzt – sie erleiden im Ernstfall auch geringere Schäden und können schneller wieder auf ihre Systeme zugreifen. Präventive Maßnahmen – technisch wie organisatorisch – sind im digitalen Zeitalter also kein optionaler Zusatz, sondern ein zentraler Schutzfaktor.

Dass immer mehr Unternehmen präventive Maßnahmen vollständig umsetzen, zeigt bereits Wirkung: Sowohl der durchschnittliche Schaden als auch die Betriebsunterbrechungszeit sind zurückgegangen.

Im Kapitel „Betriebsunterbrechung“ wurde davon berichtet, dass der durchschnittliche Schaden sowie die durchschnittliche Betriebsunterbrechungszeit zurückgegangen sind. Ein Grund dafür ist unter anderem, dass immer mehr Unternehmen präventive Maßnahmen vollständig umgesetzt haben.

Positiv ist zudem, dass Unternehmen der Schwachstelle Nr. 1 – dem Menschen – zunehmend Aufmerksamkeit widmen und versuchen, dieses Einfallstor weiter einzudämmen: Waren es 2024 noch 30 % der Unternehmen, die Maßnahmen zum Mitarbeiterverhalten z. B. durch Schulungen vollständig implementiert haben, sind es nun bereits 34 %. Unternehmen schulen also vermehrt und vor allem regelmäßig ihre Mitarbeiter.

Wie umfangreich haben Sie bereits Präventionsmaßnahmen zur IT-Sicherheit in Ihrem Unternehmen in diesen Bereichen eingerichtet?



Basis: alle; Angaben in % (Top 1: „vollständig umgesetzt“)

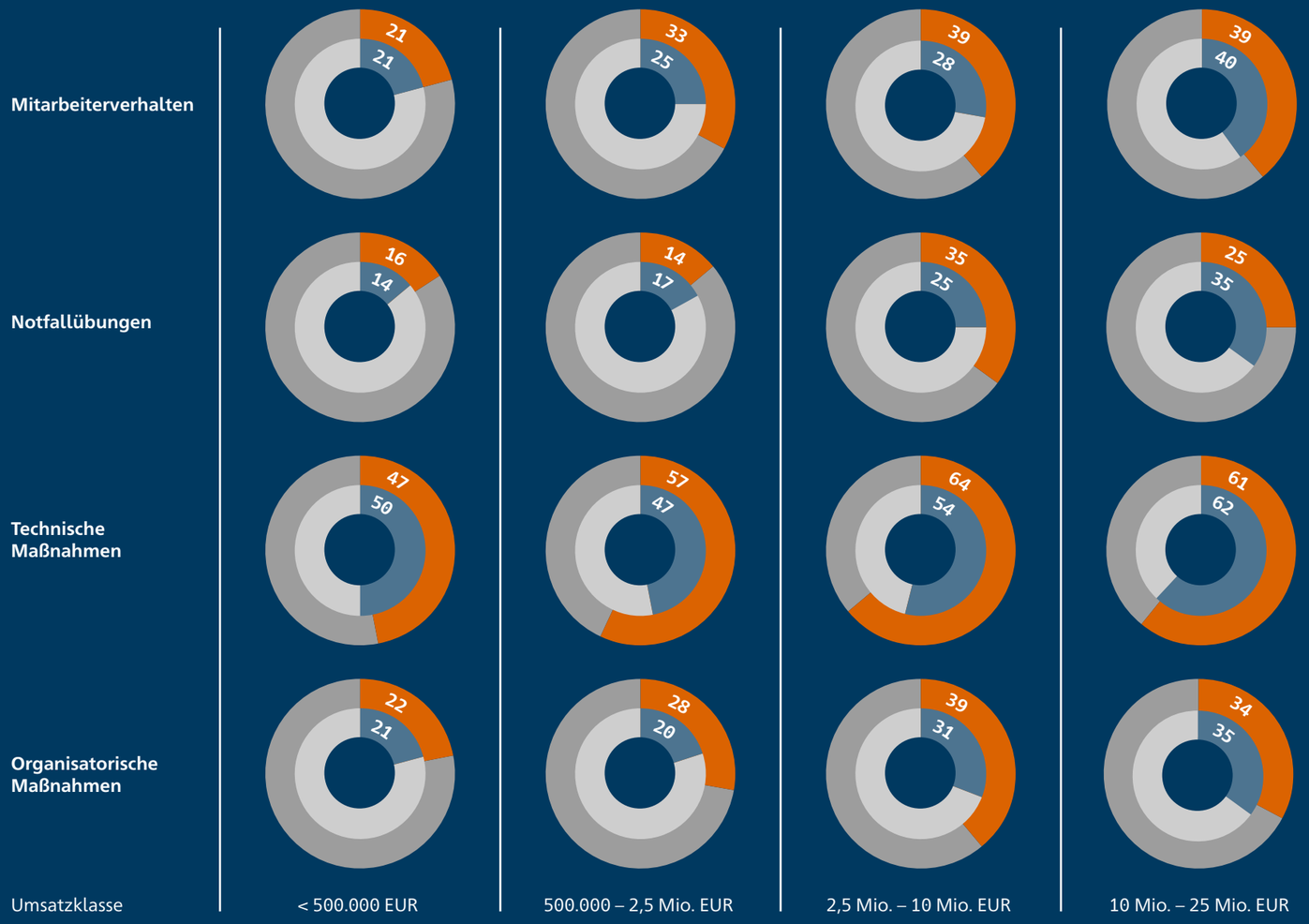
Gezielte Prävention.

Aktives Vorgehen unterscheidet sich deutlich je nach Unternehmensgröße.

Besonders hervorzuheben sind kleine Unternehmen mit einem Jahresumsatz von 2,5 bis 10 Mio. Euro: Der Anteil jener, die Maßnahmen zum Mitarbeiterverhalten vollständig implementiert haben, stieg von 28 % (HDI Cyberstudie 2024) auf 39 % – ein relativer Anstieg von knapp 40 %.

Über alle präventiven Maßnahmen hinweg verzeichnet diese Unternehmensgruppe eine beeindruckende Steigerung von knapp zehn Prozentpunkten.

Wie umfangreich haben Sie bereits Präventionsmaßnahmen zur IT-Sicherheit in Ihrem Unternehmen in diesen Bereichen eingerichtet?



2026 2024 **Basis:** alle; Angaben in % (Top 1: „vollständig umgesetzt“)

Präventive Maßnahmen zahlen sich aus.

Der Erfolg von Sicherheitsmaßnahmen ist eindeutig messbar.

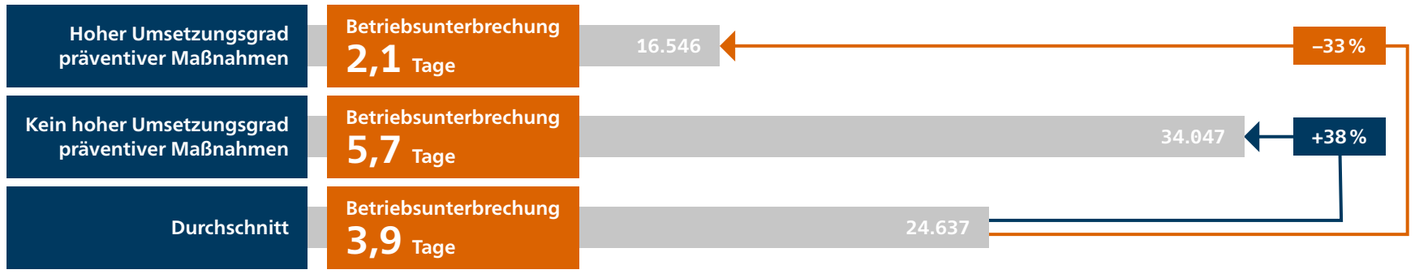
Die Ergebnisse der HDI Cyberstudie 2026 zeigen, dass Unternehmen, die vermehrt in die Informationssicherheit investieren und präventive Maßnahmen vollständig umsetzen, eine signifikant geringere Betriebsunterbrechung aufweisen. So erleiden **Unternehmen mit einem hohen Umsetzungsgrad präventiver Maßnahmen im Durchschnitt nur eine Betriebsunterbrechung von etwa zwei Tagen (2,1 Tage), während Unternehmen ohne entsprechende Maßnahmen fünf bis sechs Tage (5,7 Tage) benötigen, um nach einem Cybervorfall wieder arbeitsfähig zu sein.** Zum Vergleich: Die durchschnittliche Betriebsunterbrechung beträgt circa vier Tage. In vielen Branchen kann ein solcher Unterschied über Vertragsstrafen, Kundenbeziehungen und Liquidität entscheiden.

Prävention ist kein Nice-to-have, sondern ein zentraler wirtschaftlicher Faktor.

Der finanzielle Schaden lässt sich durchschnittlich um 33 % senken, wenn ein Unternehmen der Prävention einen hohen Stellenwert beimisst. Diese weisen einen durchschnittlichen Cyberschaden von lediglich rund 17.000 Euro auf. **Unternehmen, die präventive Maßnahmen nicht so stringent verfolgen, haben einen knapp 38 % höheren durchschnittlichen Cyberschaden.**

Hinzu kommt, dass Unternehmen, die Prävention gegen Cyberrisiken aktiv fördern, Angriffe deutlich häufiger erfolgreich abwehren. Rund 73 % der Angriffe führen bei Unternehmen mit ausgeprägten Präventionsmaßnahmen zu keinem Schaden. Bei Unternehmen mit nicht so hohem Präventionsniveau gelingt dies hingegen nur in circa 53 % der Fälle.

Besonders ausgeprägt zeigt sich der Effekt bei Unternehmen, die mehrere Schutzebenen miteinander kombinieren. **Unternehmen mit einem hohen Präventionsniveau, Cloud-Nutzung und einer bestehenden Cyberversicherung verzeichnen signifikant reduzierte Schadensquoten.** Prävention, technische Infrastruktur und Risikotransfer wirken hier nicht isoliert, sondern verstärken sich gegenseitig.



Basis: KMUs mit einer Cyberattacke; Angaben in EUR

Cybermanagement

Mit klaren Verantwortlichkeiten gegen strukturelle Defizite.

Trotz wachsender Bedrohungslage und klarer Vorteile präventiver Maßnahmen zeigt die Studie weiterhin strukturelle Defizite. **23 % der befragten Unternehmen verfügen über keinen klar definierten Verantwortlichen für IT-Sicherheit.** Besonders betroffen sind Kleinstunternehmen, bei denen Cyberprävention häufig unsystematisch oder rein reaktiv erfolgt.

Dieser Effekt nimmt mit steigender Unternehmensgröße deutlich ab. Während bei Unternehmen bis 500.000 Euro Umsatz noch 43 % keinen klaren IT-Sicherheitsverantwortlichen benennen können, sinkt dieser Anteil bei Unternehmen mit einem Umsatz von 10 bis 20 Mio. Euro auf nur noch 12 %. **Cybersecurity wird erst mit zunehmender Größe als eigenständige Managementaufgabe verstanden.**

Eine weitere wichtige Erkenntnis: **Unternehmen mit einer bestehenden Cyberversicherung haben nur noch in 11 % der Fälle keine klaren Verantwortlichkeiten.** Der Abschluss einer Cyberversicherung wirkt damit nicht nur als finanzieller Schutz, sondern auch als organisatorischer Impuls, sich strukturiert mit Zuständigkeiten, Prozessen und Sicherheitsanforderungen auseinanderzusetzen.

Prävention und Cyberversicherung gehören zusammen.

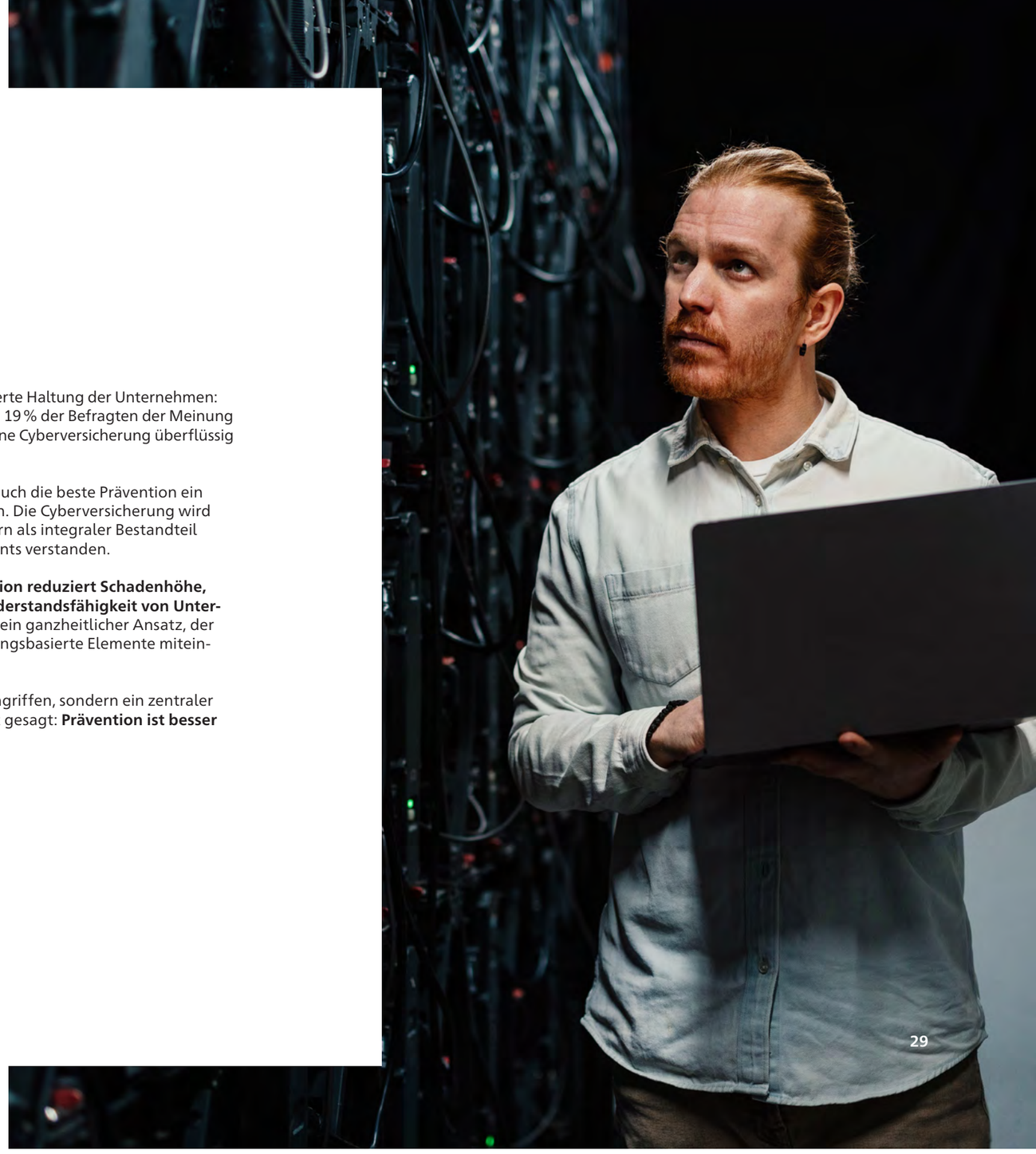
Die Studie zeigt, dass Prävention und Cyberversicherung nicht als Gegensätze verstanden werden, sondern immer mehr als komplementäre Elemente. **Zwar verfügen immer noch 37 % der befragten Unternehmen über keine Cyberversicherung, doch dort, wo das Präventionsniveau hoch ist, ist die Wahrscheinlichkeit für eine bestehende Cyberversicherung deutlich erhöht.**

Bemerkenswert ist insbesondere die veränderte Haltung der Unternehmen: Während bei der HDI Cyberstudie 2024 noch 19 % der Befragten der Meinung waren, dass gute Präventionsmaßnahmen eine Cyberversicherung überflüssig machen, sind es 2026 nur noch 12 %.

Unternehmen erkennen zunehmend, dass auch die beste Prävention ein Restrisiko nicht vollständig eliminieren kann. Die Cyberversicherung wird damit nicht als Ersatz für Prävention, sondern als integraler Bestandteil eines ganzheitlichen Cyberrisikomanagements verstanden.

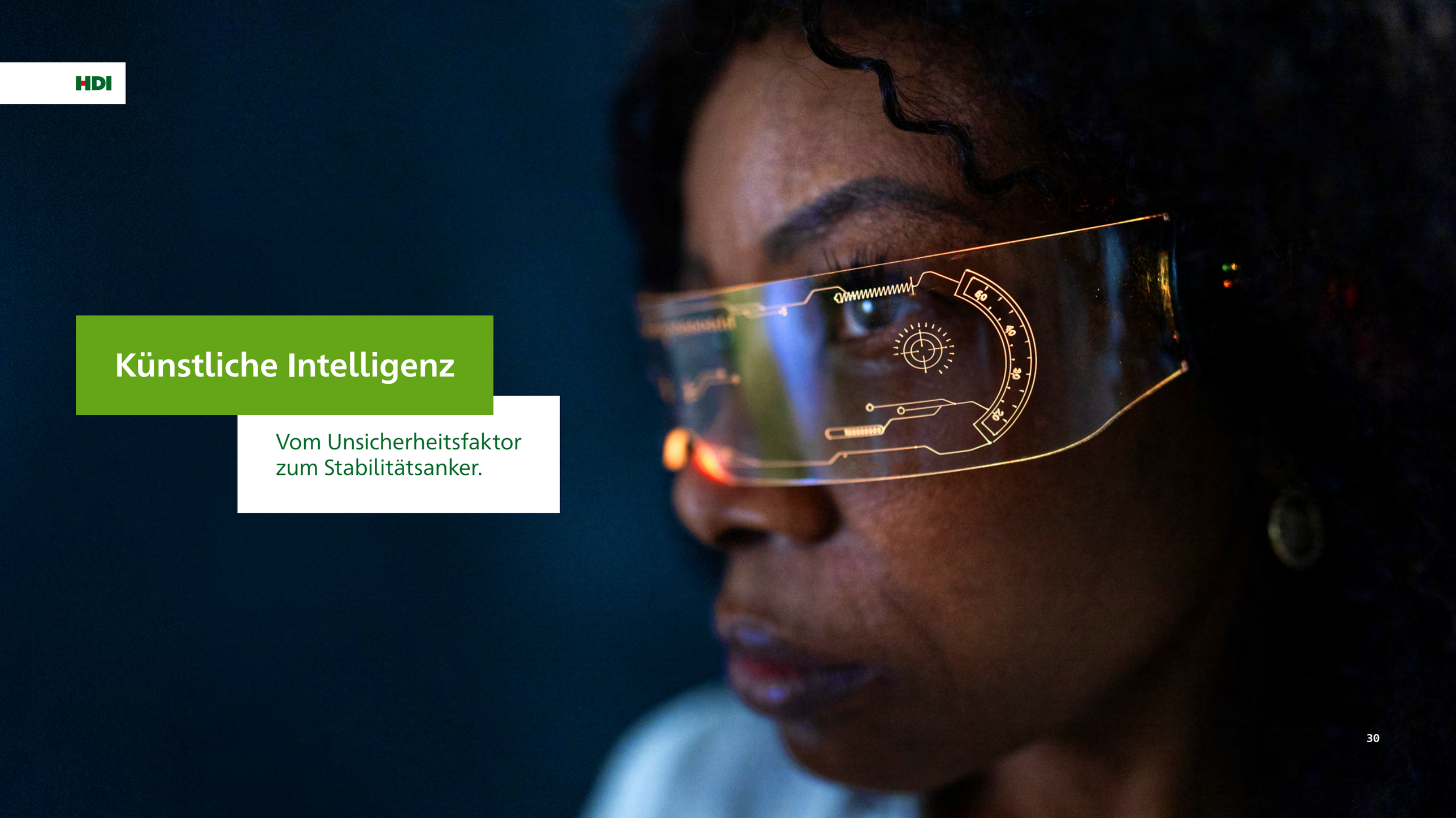
Die HDI Cyberstudie 2026 belegt: Prävention reduziert Schadenhöhe, verkürzt Ausfallzeiten und erhöht die Widerstandsfähigkeit von Unternehmen signifikant. Besonders effektiv ist ein ganzheitlicher Ansatz, der technische, organisatorische und versicherungsbasierte Elemente miteinander verbindet.

Prävention ist damit nicht nur Schutz vor Angriffen, sondern ein zentraler Baustein unternehmerischer Stabilität. Kurz gesagt: **Prävention ist besser als Reaktion.**



Künstliche Intelligenz

Vom Unsicherheitsfaktor
zum Stabilitätsanker.



Kein Hype mehr, sondern Hygiene.

Unternehmen bewerten Künstliche Intelligenz (kurz: „KI“) zunehmend als konkrete Chance zur Stärkung ihrer Cyberresilienz – positiver und differenzierter als noch in der HDI Cyberstudie 2024.

Während KI in der Vergangenheit häufig noch mit neuen Risiken, Kontrollverlusten oder zusätzlicher Komplexität verbunden wurde, rückt nun ihr potenzieller Sicherheitsgewinn stärker in den Fokus. Viele Unternehmen erwarten durch KI bessere Erkennungs-, Analyse- und Abwehrmechanismen im Bereich der IT- und Informationssicherheit.

Wahrnehmung: Chancen überwiegen deutlich.

In der HDI Cyberstudie 2026 hat sich diese Wahrnehmung nochmals verstärkt. Inzwischen bewerten 55 % der Unternehmen KI als Chance, während nur noch 22 % KI als Risiko einschätzen. **KI findet damit zunehmend Anwendung in Unternehmen und wird verstärkt als strategisches Werkzeug verstanden.**

Auffällig ist zudem der Zusammenhang mit der Unternehmensgröße. **Mit steigender Mitarbeiterzahl wächst die Relevanz von KI deutlich:** Lediglich 9 % der Unternehmen mit 50 bis 250 Mitarbeitenden sehen keine Auswirkungen auf ihr Geschäft – bei Kleinstunternehmen ist dieser Anteil rund dreimal so hoch.

Der Wandel zeigt eine zunehmende Reife im Umgang mit KI – und er beschränkt sich nicht auf die IT-Branche.

KI als Chance – nicht nur für IT-Dienstleister.

Auch im klassischen Gewerbe wachsen Akzeptanz und Offenheit gegenüber Künstlicher Intelligenz – mit ein paar Ausnahmen.

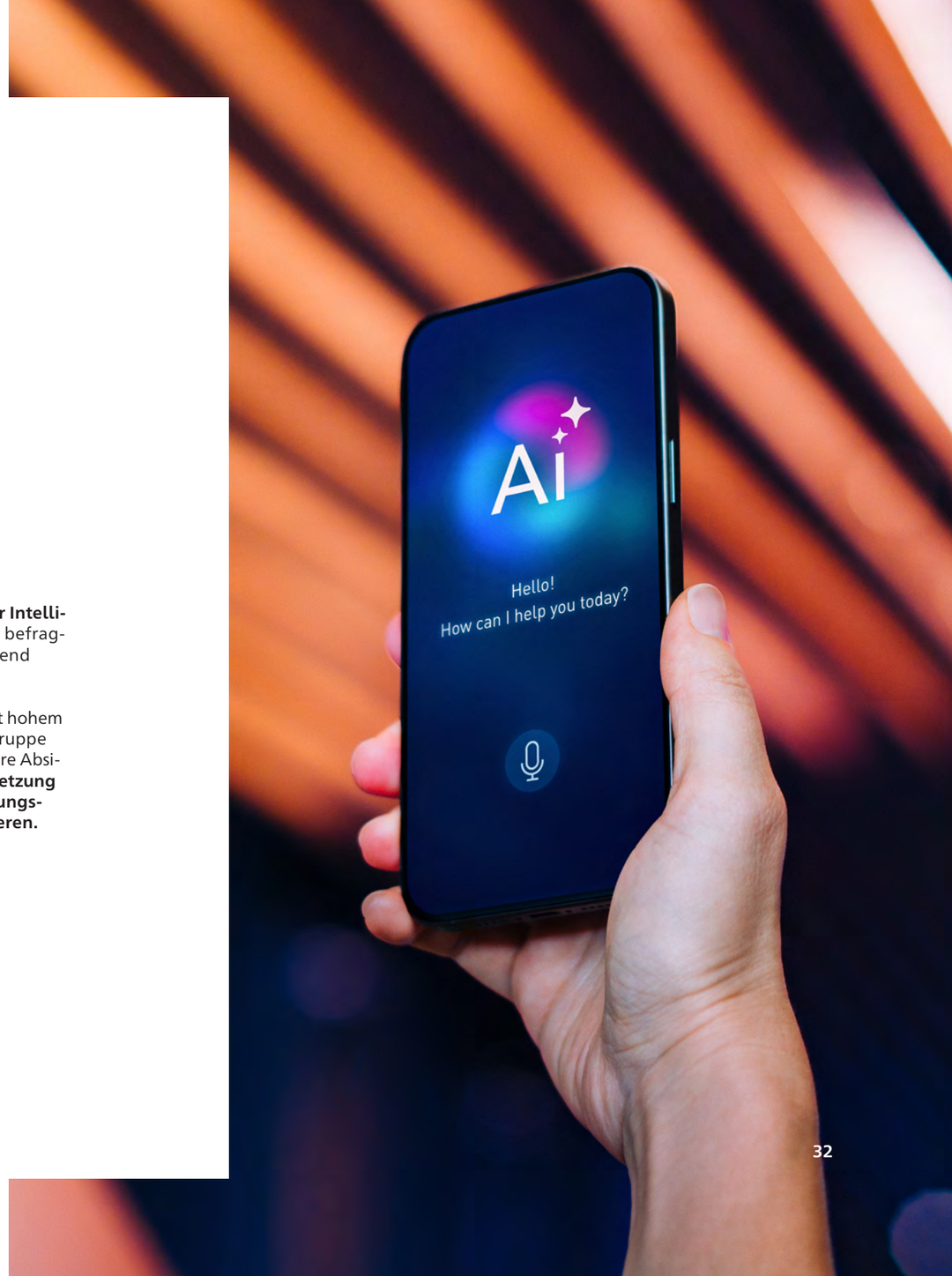
Mit 83 % chancenorientierter Einschätzungen bleiben **IT-Dienstleister zwar die treibende Kraft – gleichzeitig verzeichnen aber auch klassische Wirtschaftsbereiche eine deutlich wachsende Zuversicht** gegenüber KI. Sie gewinnt damit branchenübergreifend an Bedeutung und trägt neben Effizienzgewinnen zunehmend auch zur Stabilisierung digitaler Prozesse und Sicherheitsstrukturen bei.

Lediglich der Sektor Ärzte und Heilberufe vermehrt skeptisch.

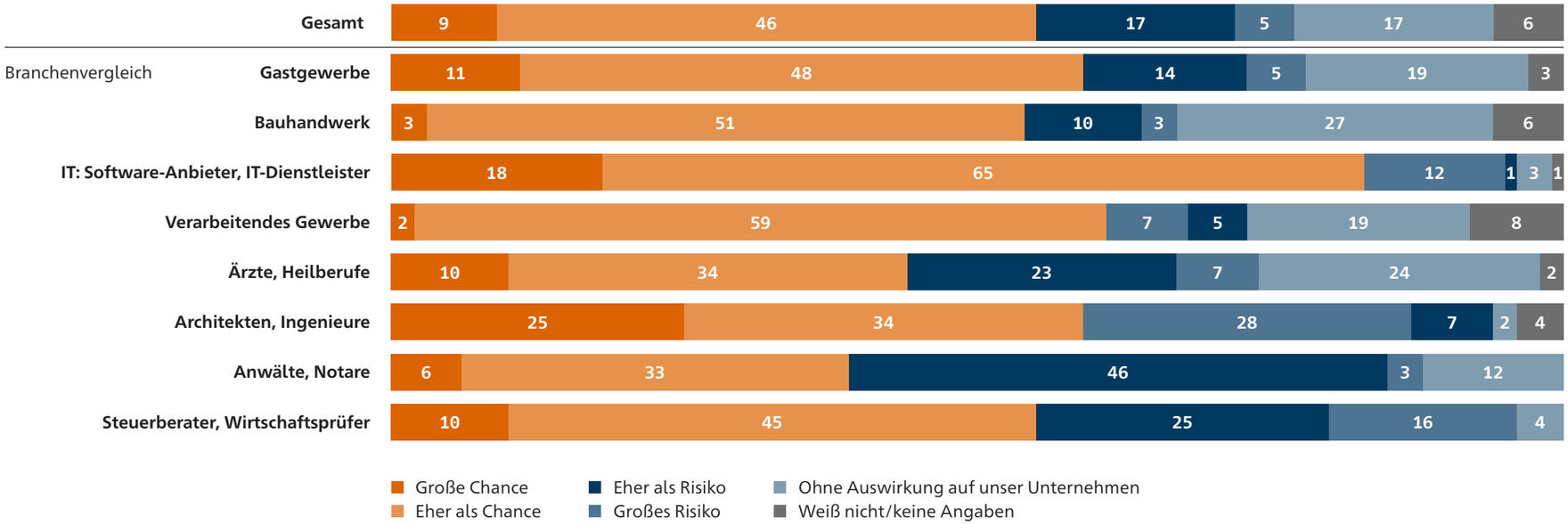
Hier sehen rund 24 % keine nennenswerten Auswirkungen von KI auf das eigene Unternehmen. Dies spricht weniger für Ablehnung als vielmehr für eine noch begrenzte praktische Anwendbarkeit im stark regulierten und sensiblen Umfeld des Gesundheitswesens.

Auch Anwälte und Notare begegnen dem Einsatz von Künstlicher Intelligenz weiterhin mit Zurückhaltung. Insgesamt bewerten 49 % der befragten Kanzleien KI eher als Risiko für das eigene Unternehmen, während lediglich 39 % sie als Chance einschätzen.

Besonders aufschlussreich ist dagegen der Blick auf Unternehmen mit hohem Präventionsniveau und bestehender Cyberversicherung. In dieser Gruppe bewerten 74 % KI als Chance – gegenüber nur 47 % ohne vergleichbare Absicherung. Dies deutet darauf hin, dass **eine intensivere Auseinandersetzung mit digitalen Risiken und das Vertrauen in verlässliche Absicherungsstrukturen die Unsicherheiten im Umgang mit KI spürbar reduzieren.**



Wie bewerten Sie für Ihr Unternehmen die Auswirkungen von Künstlicher Intelligenz für Ihre Unternehmensentwicklung insgesamt?



Basis: alle; Angaben in %

KI als Beitrag zur Cyberresilienz.

Ein besonderer Fokus der Studie liegt auf dem Zusammenhang zwischen Künstlicher Intelligenz und Cybersicherheit. Auffällig ist dabei, dass die Einschätzungen darüber, ob KI zur Verbesserung der Cybersicherheit im eigenen Unternehmen beiträgt, auseinandergehen.

Wird das gesamte Stimmungsbild der befragten Unternehmen betrachtet, zeigt sich eine überwiegend positive Tendenz: **Insgesamt sind 26 % der Unternehmen der Ansicht, dass KI ihre Cyberresilienz stärkt.** Dieser Anteil nimmt mit zunehmender Unternehmensgröße zu.

Demgegenüber geben lediglich 11 % der Unternehmen an, dass KI ihre Cybersicherheit schwächt. Insgesamt überwiegt damit die positive Bewertung des Beitrags von KI zur Cyberresilienz deutlich.

Daraus lässt sich ein klarer Zusammenhang ableiten: Unternehmen, die den Einsatz von KI grundsätzlich als Chance wahrnehmen, kommen auch häufiger zu der Einschätzung, dass KI eine bedeutende Rolle bei der Stärkung der Cyberresilienz spielt.

Vom Trend zum Must-have im Sicherheitskonzept.

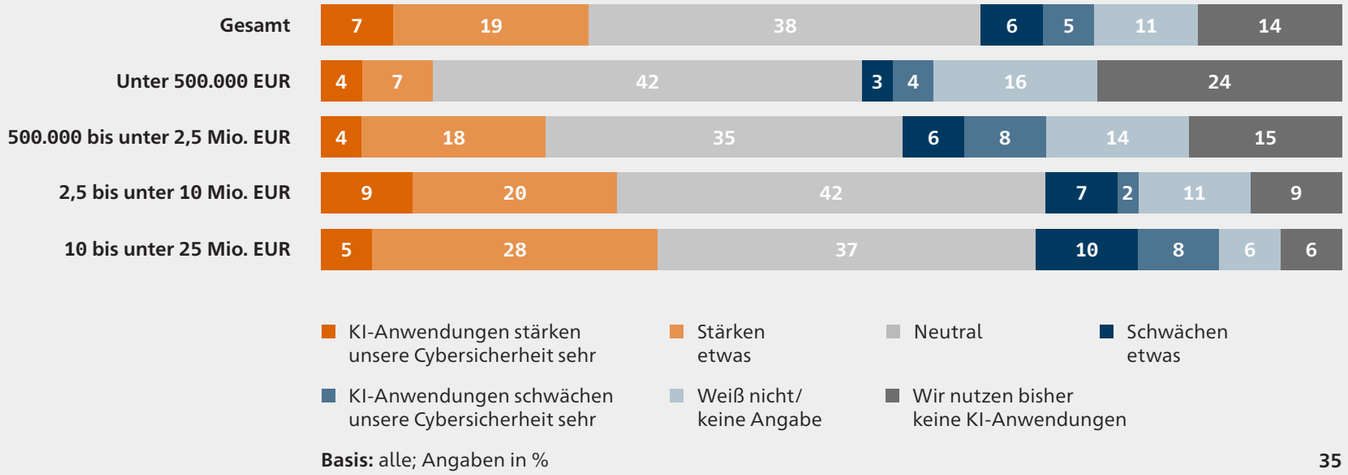
Ähnlich wie bei den Ergebnissen zur generellen Wahrnehmung von KI zeigt sich auch in Bezug auf die Verbesserung der Cybersicherheit ein klares Branchenmuster. **Besonders IT-Dienstleister bewerten den Einsatz von KI hier überdurchschnittlich positiv (47 %).** Ihnen folgen Architekten und Ingenieure mit 44 % sowie das verarbeitende Gewerbe mit 34 %.

Cloud und KI verstärken sich gegenseitig.

Ein weiterer zentraler Befund: **Unternehmen mit cloudbasierter IT-Infrastruktur sehen in KI deutlich häufiger eine Stärkung ihrer IT-Sicherheit (36 %) als Unternehmen ohne Cloud-Nutzung (14 %) –** lediglich 11 % bewerten den Einfluss als schwächend. Eine mögliche Erklärung liegt darin, dass Cloud-Umgebungen häufig mit höherer Standardisierung, besseren Integrationsmöglichkeiten und modernen Sicherheitslösungen einhergehen, in denen KI-Funktionen teilweise bereits integriert sind. Wie das Kapitel „Digitale Abhängigkeit" bereits gezeigt hat, ist Cloud-Technologie dabei mehr als Infrastruktur. **Sie kann ein echter Sicherheitsgewinn sein – allerdings nur, wenn sie aktiv gemanagt wird.**

Die Cyberstudie 2026 zeigt einen klaren Trend: **Künstliche Intelligenz wird zunehmend als Chance gesehen und als Stärkung der Cyberresilienz verstanden.**

Welche Bedeutung messen Sie dem Einsatz von Künstlicher Intelligenz (KI-Anwendungen) für die Verbesserung der Cybersicherheit in Ihrem Unternehmen bei?



Basis: alle; Angaben in %

Sie haben Fragen zum Thema Cyberversicherung?

Moritz Menze

MENZE & MENZE

HDI EXKLUSIV

Obernstraße 42 I 33602 Bielefeld
Tel.: 0521-399061 – 11
Fax.: 0521-399061 – 30
moritz.menze@hdi.de

HDI Versicherung AG
HDI-Platz 1
30659 Hannover
www.hdi.de/cyberversicherung