HORNETSECURITY
BY proofpoint

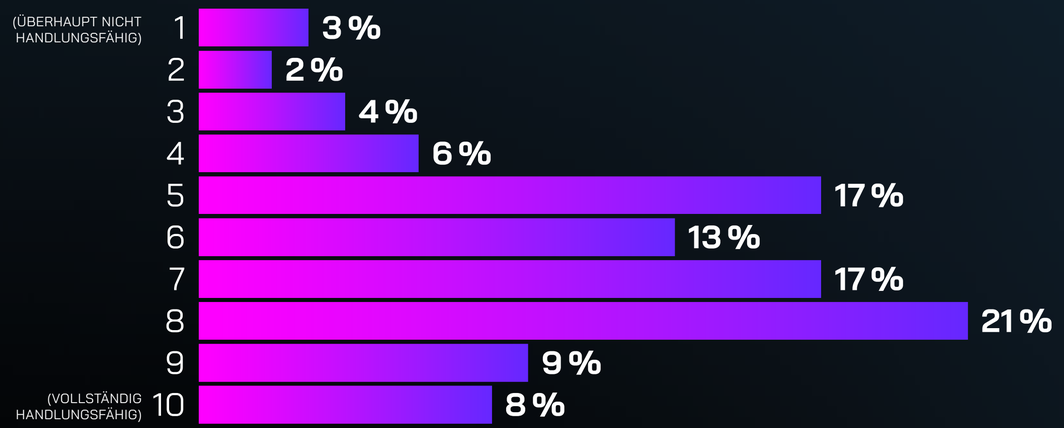
AI RISK

Report 2026 DACH

HORNETSECURITY
BY proofpoint.

Künstliche Intelligenz verändert die Cybersecurity-Landschaft grundlegend – sowohl auf Seiten der Angreifer als auch der Verteidiger. Dieser Report basiert auf aktuellen Umfragedaten einer YouGov-Studie im Auftrag von Hornetsecurity unter 517 Unternehmensentscheidern. Ziel ist es, IT- und Security-Verantwortlichen eine fundierte Grundlage zu bieten, um aktuelle Entwicklungen besser zu verstehen, Risiken realistisch einzuschätzen und strategische Entscheidungen im Umgang mit KI zu treffen.

HORNETSECURITY
BY proofpoint.



Einschätzung der eigenen Handlungsfähigkeit bei Zero-Day-Angriffen der befragten Unternehmen.

5 KEY FINDINGS, DIE SIE KENNEN SOLLTEN

1. KI-Einsatz und Zero-Day-Readiness bleiben begrenzt

Viele Unternehmen stehen weiterhin vor der Herausforderung, neue Sicherheitsanforderungen operativ wirksam umzusetzen.

» So gibt nur rund ein Drittel der Befragten (32 %) an, KI im vergangenen Jahr bereits erfolgreich zur Eindämmung von Cyberbedrohungen eingesetzt zu haben.

Auch die Einschätzung der eigenen Vorbereitung auf Zero-Day-Angriffe fällt überwiegend nur mittelmäßig aus. Die Ergebnisse zeigen damit, dass viele Unternehmen zwar aktiv an ihrer Cybersecurity arbeiten, konkrete operative Reife und belastbare Abwehrfähigkeiten jedoch vielerorts noch im Aufbau sind.

2. Unternehmen betrachten KI nicht als eindeutigen Sicherheitsgewinn

Die Wahrnehmung von KI im Cybersecurity-Kontext bleibt auffallend ambivalent. Nur 9 % der Befragten geben an, dass KI-Sicherheitsbedrohungen ausschließlich gemindert habe, während 24 % ausschließlich eine Verschärfung beobachten. Gleichzeitig sehen 27 % sowohl positive als auch negative Auswirkungen, weitere 27 % erkennen bislang keine Veränderung.

Die Zahlen zeigen deutlich: KI wird derzeit weniger als klarer Sicherheitsgewinn wahrgenommen, sondern vielmehr als Technologie, die bestehende Dynamiken beschleunigt – auf Seiten der Angreifer ebenso wie auf Seiten der Verteidiger.

KI-gestütztes Phishing

(55 %)

KI-gestützte geschäftliche E-Mails

(39 %)

Deepfakes

(41 %)

3. Der Mensch bleibt trotz KI das größte Sicherheitsrisiko

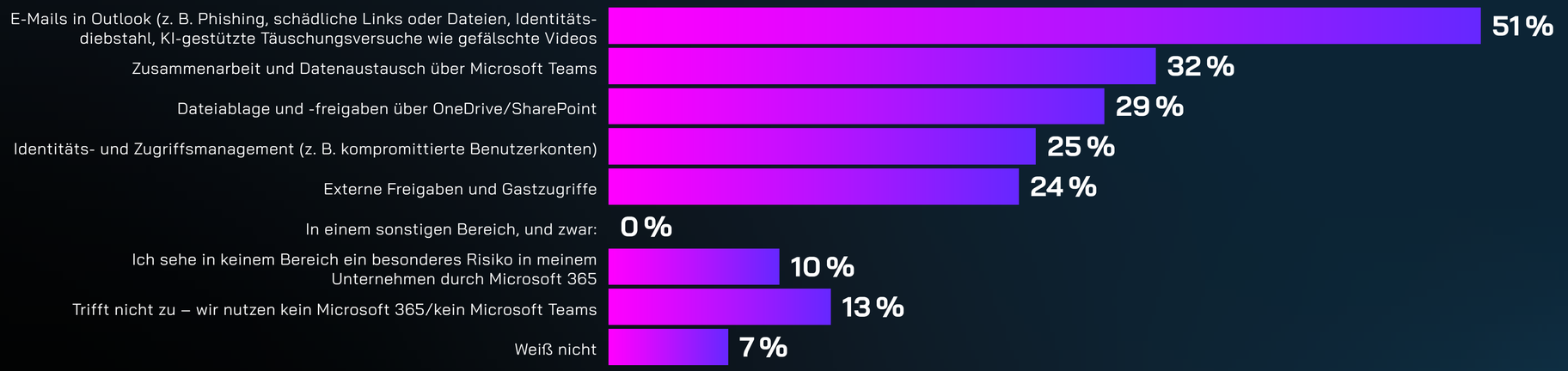
Besonders auffällig ist die Kombination aus wachsender Sorge vor KI-gestützten Angriffen und gleichzeitig begrenztem Vertrauen in die Fähigkeit von Mitarbeitenden, Risiken im Arbeitsalltag sicher zu erkennen und angemessen zu reagieren. Unternehmen fürchten insbesondere KI-gestütztes Phishing (55 %), Deepfakes (41 %) und KI-gestützte geschäftliche E-Mails (39 %) – also genau jene Bedrohungen, die gezielt auf menschliche Schwachstellen abzielen.

Gleichzeitig schätzt nur ein Teil der Befragten die eigenen Mitarbeitenden als sehr gut bis eher gut vorbereitet ein (52 %), Cyberrisiken innerhalb von Microsoft 365 oder Teams zuverlässig zu erkennen und angemessen darauf zu reagieren. Die Ergebnisse machen deutlich: Mit zunehmender Qualität KI-generierter Inhalte wird der Faktor Mensch noch stärker zur kritischen Sicherheitsvariable.

4. Microsoft 365 entwickelt sich zunehmend zur kritischen Sicherheitszone

Die Studie zeigt klar, dass Unternehmen Microsoft 365 und Teams längst nicht mehr nur als Produktivitätsplattformen betrachten. Vielmehr werden sie zunehmend als potenzielle Angriffsfläche wahrgenommen. Besonders relevant ist dabei, dass ein großer Teil der Befragten cloudbasierte Kollaborationsumgebungen mit konkreten Cyberrisiken verbindet.

Das verdeutlicht einen grundlegenden Wandel: Je stärker Kommunikation, Daten und Zusammenarbeit in Cloud-Plattformen verlagert werden, desto stärker verschiebt sich auch der Fokus von Angreifern auf genau diese Systeme.



Die größten KI-gestützten Cyberbedrohungen für Microsoft 365 oder Microsoft Teams aus Sicht der befragten Unternehmen.

HORNETSECURITY
BY proofpoint.

5. Unternehmen priorisieren KI-Investitionen in der Cyberabwehr

Für 19 % der befragten Unternehmen hat KI im Rahmen ihrer Cybersecurity-Investitionen in den kommenden 12–24 Monaten höchste Priorität. Weitere 43 % bewerten Investitionen in KI-gestützte Cybersicherheit als Thema mittlerer Priorität. Die Investitionsbereitschaft deutet darauf hin, dass sie den steigenden Handlungsdruck erkannt haben und KI zunehmend in ihre Sicherheitsplanung einbeziehen, auch wenn die Umsetzung schrittweise erfolgt.

Angesichts zunehmender Sorgen vor KI-gestützten Angriffen wie Phishing, Deepfakes oder manipulierten geschäftlichen E-Mails betrachten sie KI offenbar nicht mehr nur als Innovations- oder Effizienzthema, sondern zunehmend als notwendigen Bestandteil moderner Cyberabwehr.

HORNETSECURITY
BY proofpoint.

KEY ACTIONS: WAS UNTERNEHMEN JETZT TUN SOLLTEN

1. KI-Strategie in konkrete Sicherheitsmaßnahmen übersetzen

Viele Unternehmen haben die strategische Bedeutung von KI erkannt, doch zwischen Priorisierung und operativer Umsetzung besteht weiterhin eine deutliche Lücke. Entscheidend ist jetzt, aus strategischen Absichten konkrete Maßnahmen abzuleiten – etwa durch klar definierte Einsatzbereiche für KI in der Bedrohungserkennung, Analyse oder automatisierten Reaktion auf Vorfälle. Investitionen in KI als Teil der Cybersecurity-Strategie sind dabei ein wichtiger Schritt.

Unternehmen sollten dabei nicht versuchen, KI flächendeckend einzuführen, sondern gezielt dort starten, wo unmittelbarer Sicherheitsmehrwert entsteht.

2. Mitarbeitende gezielt auf KI-gestützte Angriffe vorbereiten

Da Angriffe durch oder mit KI immer glaubwürdiger und schwerer erkennbar werden, reichen klassische Awareness-Trainings zunehmend nicht mehr aus. Unternehmen sollten ihre Schulungsmaßnahmen gezielt an moderne Bedrohungsszenarien anpassen – insbesondere im Hinblick auf KI-generiertes Phishing, Deepfakes und Social Engineering.
Wichtig ist dabei nicht nur Wissen, sondern auch Handlungssicherheit: Mitarbeitende müssen verdächtige Inhalte erkennen, korrekt einordnen und schnell melden können.

HORNETSECURITY
BY proofpoint.

3. Microsoft-365-Umgebungen stärker absichern

Da Microsoft 365 und Teams zunehmend zur zentralen Angriffsfläche werden, sollten Unternehmen ihre Sicherheitsmaßnahmen direkt in diesen Plattformen stärken. Besonders relevant sind dabei E-Mail-Sicherheit, Identitäts- und Zugriffsmanagement sowie die Überwachung ungewöhnlicher Aktivitäten innerhalb der Kollaborationsumgebungen.

» Cloudbasierte Produktivität darf nicht zulasten der Sicherheit gehen – insbesondere dort, wo sensible Kommunikation und Daten zusammenlaufen.

4. Schnellere Reaktionsfähigkeit auf neue Bedrohungen aufbauen

Die Geschwindigkeit KI-gestützter Angriffe erhöht den Druck auf Unternehmen, Sicherheitsvorfälle schneller zu erkennen und einzudämmen. Organisationen sollten daher ihre Incident-Response-Prozesse regelmäßig überprüfen und stärker automatisieren, um auf neuartige Bedrohungen schneller reagieren zu können.

» Dazu gehören unter anderem kontinuierliches Monitoring, automatisierte Alarmierung, klar definierte Eskalationsprozesse, sowie regelmäßige Tests realistischer Angriffsszenarien.

HORNETSECURITY
BY proofpoint.

5. KI realistisch bewerten

Die Ergebnisse zeigen klar, dass KI aktuell weder als reine Gefahr noch als unmittelbare Lösung wahrgenommen wird. Unternehmen sollten deshalb einen pragmatischen Ansatz verfolgen: KI kann Sicherheitsprozesse unterstützen und beschleunigen, ersetzt jedoch keine belastbaren Sicherheitsstrategien, klaren Prozesse oder qualifizierten Mitarbeitenden.

» Entscheidend ist nicht der Einsatz von KI allein, sondern wie sinnvoll sie in bestehende Sicherheitsstrukturen integriert wird.

6. Sicherheitsstrategien kontinuierlich anpassen

Die Dynamik KI-gestützter Bedrohungen macht klassische, statische Sicherheitskonzepte zunehmend unzureichend. Unternehmen sollten Cybersecurity daher nicht als einmaliges Projekt betrachten, sondern als kontinuierlichen Anpassungsprozess.

» Wer Sicherheitsstrategien regelmäßig überprüft, Bedrohungslagen neu bewertet und Technologien flexibel weiterentwickelt, verbessert langfristig seine Widerstandsfähigkeit gegenüber modernen Angriffen.

HORNETSECURITY
BY proofpoint.

FAZIT

Künstliche Intelligenz ist ein zweischneidiges Schwert in der Cybersecurity: Sie erhöht die Schlagkraft von Angreifern – bietet aber gleichzeitig enormes Potenzial für eine effektivere Verteidigung. Die zentrale Herausforderung für Unternehmen liegt nicht darin, ob sie KI einsetzen sollten, sondern wie schnell und wie strukturiert sie dies tun.

Organisationen, die jetzt gezielt in Technologie, Prozesse und Menschen investieren, können sich einen entscheidenden Vorteil verschaffen. Wer zögert, riskiert hingegen, von der Dynamik KI-gestützter Angriffe überholt zu werden.

HORNETSECURITY
BY proofpoint.

ÜBER UNS

Hornetsecurity by Proofpoint ist der Geschäftsbereich von Proofpoint, der die Hornetsecurity-Produktsuite speziell für Managed Service Provider (MSPs) sowie kleine und mittelständische Unternehmen (KMUs) bereitstellt. Das Unternehmen bietet cloudbasierte Sicherheits-, Compliance-, Backup- und Security-Awareness-Lösungen der nächsten Generation, die Unternehmen und Organisationen jeder Größe auf der ganzen Welt unterstützen.

Das Flaggschiffprodukt 365 Total Protection ist die umfassendste Cloud-Sicherheitslösung für Microsoft 365 auf dem Markt. Angetrieben von Innovation und Cybersecurity-Exzellenz, baut Hornetsecurity mit seinem preisgekrönten Portfolio eine sicherere digitale Zukunft und nachhaltige Sicherheitskulturen auf.

Hornetsecurity ist über sein internationales Vertriebsnetz mit über 12.000 Channel-Partnern und MSPs in mehr als 120 Ländern aktiv. Seine Premium-Dienste werden von mehr als 125.000 Kunden genutzt.

Weitere Informationen unter: www.hornetsecurity.com/de/

Die Daten dieser Befragung basieren auf Online-Interviews mit Mitgliedern des YouGov Panels, die der Teilnahme vorab zugestimmt haben. Für diese Befragung wurden im Zeitraum 03. und 11.03.2026 insgesamt 517 Unternehmensentscheider befragt. Die Erhebung wurde quotiert und die Ergebnisse gewichtet. Die Befragten setzen sich repräsentativ nach Beschäftigtenanteil pro Unternehmensgröße, nach Geschlecht und Altersgruppen von Unternehmensentscheidern, nach sechs NACE-Wirtschaftszweigen sowie nach Nielsen-Regionsverteilung von Unternehmen zusammen.