



Microsoft 365
Copilot

Datensicherheit im Zeitalter der KI gewährleisten

Ein Leitfaden für IT-Führungskräfte



E-Book

Dieser Leitfaden richtet sich an IT-Führungskräfte, die die KI-Einführung fördern und gleichzeitig die Sicherheit der Daten in ihrem Unternehmen gewährleisten müssen. Er hilft Ihnen, die Risiken zu verstehen, die KI für Datensicherheit und Datenschutz darstellt, und bietet Ihnen die nötigen Insights, um Ihr Unternehmen souverän durch die KI-Transformation zu führen.

Inhaltsverzeichnis

01

Die neuen Regeln
des KI-gestützten
Arbeitens

02

Auswirkungen von KI
auf die Datensicherheit
verstehen

03

Die Herausforderung
„Schatten-KI“

04

Die BYOAI-Realität

05

Das regulatorische
Labyrinth

06

Ein sicherheits-
orientiertes Framework
zur Bewertung von
KI-Lösungen

07

Microsoft 365 Copilot:
KI, der Sie vertrauen
können

08

Der sichere Weg zur
KI-Transformation

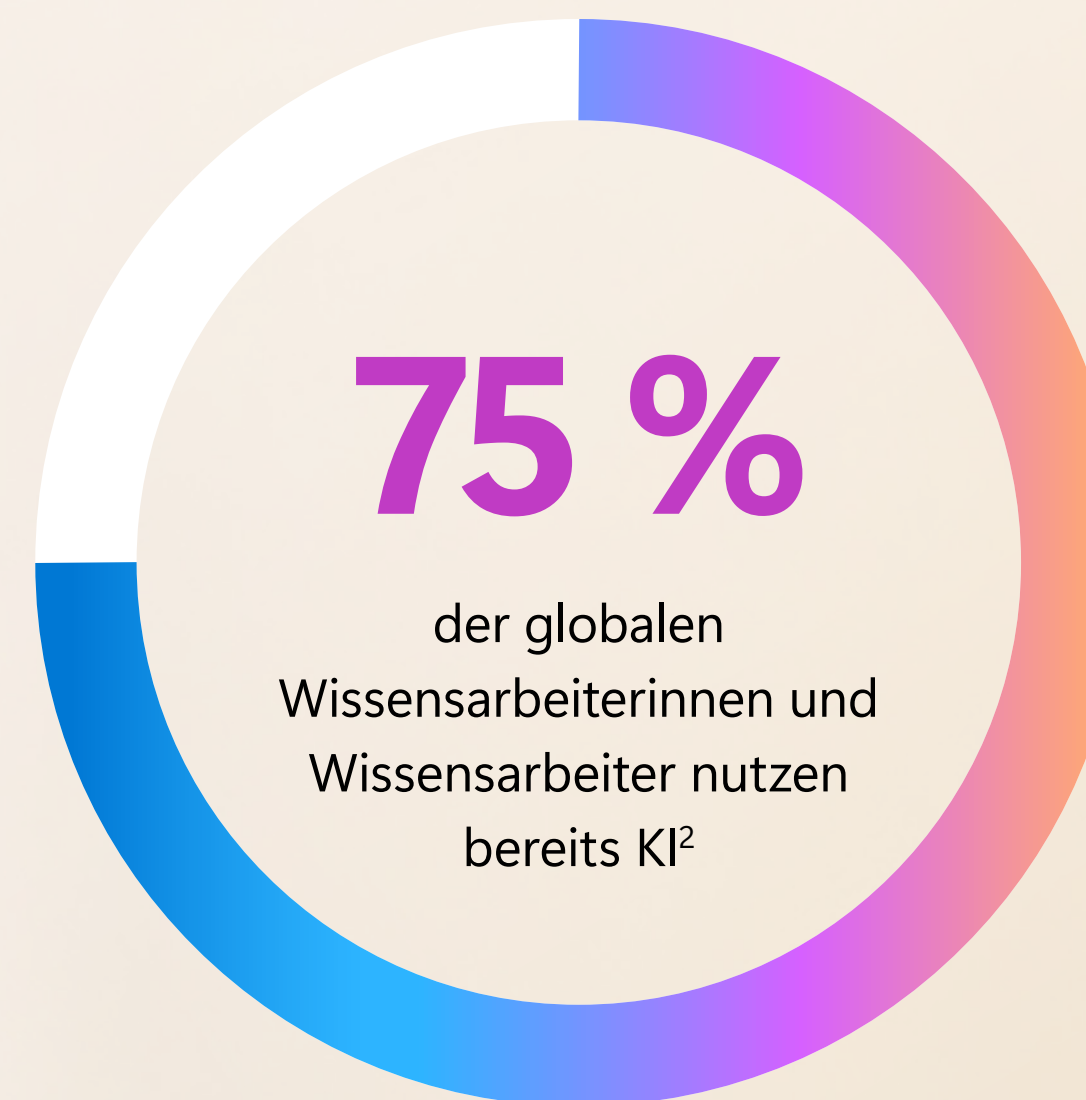
01

Die neuen Regeln des KI-gestützten Arbeitens

Generative KI eröffnet neue Möglichkeiten für Innovationen und hilft Teams, schneller und intelligenter als je zuvor zu arbeiten. Für vorausschauende Unternehmen ist KI nicht nur ein weiterer Technologietrend, sondern eine geschäftliche Notwendigkeit und entscheidend dafür, wie sie ihre Geschäfte betreiben, Mehrwert liefern und Wettbewerbsvorteile aufrechterhalten.

Diese schnelle Einführung bringt jedoch neue und verstärkte Herausforderungen mit sich, die IT-Führungskräfte proaktiv angehen und steuern müssen. KI-Systeme können über die gesamte Dateninfrastruktur hinweg aktiv Informationen suchen und kombinieren, wodurch Sicherheitsrisiken im Vergleich zu herkömmlichen Tools erhöht werden. Trotz der rasanten Verbreitung von KI gibt nur **1 %** der Unternehmen an, KI vollständig mit angemessenen Sicherheitsprotokollen in ihre Workflows integriert zu haben.¹ Durch die Implementierung robuster Sicherheits- und Governance-Maßnahmen bereits zu Beginn Ihrer KI-Reise kann Ihr Team sensible Daten effektiv schützen, Compliance-Anforderungen erfüllen und die Informationen Ihres Unternehmens schützen – und gleichzeitig Innovationen fördern.

Die Einführung von KI ist in vollem Gange



02

Auswirkungen von KI auf die Datensicherheit verstehen

Bevor wir auf spezifische Herausforderungen eingehen, ist es wichtig zu wissen, dass KI die Datensicherheitslandschaft grundlegend verändert. Im Gegensatz zu herkömmlicher Software, die nur auf ausdrückliche Anweisung auf Daten zugreift, verarbeitet, analysiert und erstellt generative KI aktiv Inhalte auf der Grundlage aller erhaltenen Informationen.

Dieser Unterschied ist aus mehreren Gründen signifikant:

- KI-Tools können Zusammenhänge zwischen Daten entdecken, die Menschen möglicherweise entgehen.
- Sie können automatisch Informationen aus verschiedenen Quellen synthetisieren.
- Sie können neue Inhalte generieren, die Elemente aus vertraulichen Eingaben enthalten.

Ihre herkömmlichen Sicherheitstools wurden wahrscheinlich nicht im Hinblick auf diese Fähigkeiten entwickelt. Während herkömmliche Software beim Zugriff auf Daten vorhersehbaren Pfaden folgt, kann KI unerwartete Wege durch Ihre Informationsinfrastruktur nehmen und sensible Daten möglicherweise auf eine Weise offenlegen, die Sie nicht erwartet haben.

Dieser grundlegende Wandel erfordert neue Ansätze für Sicherheit und Data Governance, die sich speziell damit befassen, wie KI mit den Informationsressourcen Ihres Unternehmens interagiert.



03

Die Herausforderung „Schatten-KI“

Unabhängig davon, in welcher Phase der KI-Einführung Sie sich befinden, finden Ihre Mitarbeitenden bereits ihre eigenen Lösungen und schaffen so eine „Schatten-KI“.

Durch diese nicht autorisierte Nutzung entstehen beträchtliche Lücken in Ihrem Sicherheitsstatus. Wenn Mitarbeitende Unternehmensdaten mit externen KI-Systemen teilen, umgehen sie bestehende Sicherheitskontrollen und schaffen Schwachstellen, auf die die meisten Unternehmen nicht vorbereitet sind.

Schatten-KI ist nicht nur ein Sicherheitsproblem – sie könnte ein Symptom für nicht erfüllte Produktivitätsanforderungen in Ihrem Unternehmen sein. Wenn Mitarbeitende auf nicht genehmigte Tools zurückgreifen, signalisieren sie, dass Ihre offiziellen Systeme nicht ihren Anforderungen entsprechen. Der Umgang mit Schatten-KI erfordert sowohl eine stärkere Governance als auch verbesserte Produktivitätslösungen.



der Mitarbeitenden fehlt oft die Zeit und Energie zur Erledigung ihrer Arbeit.³ Wenn sie KI-Tools entdecken, die ihre Produktivität erheblich steigern, werden sie sie nutzen – mit oder ohne Genehmigung der IT.

Warum Schatten-KI entsteht:

- Mitarbeitende sind bestrebt, ihre Produktivität durch die beeindruckenden Fähigkeiten von KI zu steigern.
- Die tägliche Arbeitsbelastung übersteigt zunehmend die verfügbare Zeit und Energie.
- Teams stehen unter wachsendem Druck, mit den gleichen Ressourcen mehr zu leisten.
- Consumer-KI-Tools bieten sofortige Lösungen ohne Genehmigungshürden.
- Offizielle IT-Beschaffungsprozesse können nicht mit dem Innovationstempo Schritt halten.

Die Risiken von Schatten-KI:

- Keine Einsicht in die Unternehmensdaten, die von externen KI-Systemen verarbeitet werden
- Keine Garantie, dass vertrauliche Informationen nicht aufbewahrt werden
- Keine einheitlichen Sicherheitsstandards über verschiedene KI-Plattformen hinweg
- Keine Überprüfbarkeit zu Compliance-Zwecken
- Keine Integration in Ihre bestehende Sicherheitsinfrastruktur



Beispiel-Szenario:

Eine Finanzanalystin, die mit einer komplexen Tabelle zu kämpfen hat, lädt sie in ein nicht autorisiertes KI-Tool hoch, um Hilfe zu erhalten. Diese Tabelle enthält kundenspezifische Finanzdaten, interne Kennzahlen und Prognosen. Während die Analystin die nötige Hilfe erhält, befinden sich die vertraulichen Finanzdaten Ihres Unternehmens nun außerhalb Ihres Sicherheitsperimeters und sind für Ihre Überwachungssysteme völlig unsichtbar.

04

Die BYOAI-Realität

Ohne klare Anweisungen von der Führungsebene nehmen Mitarbeitende die KI-Einführung zunehmend selbst in die Hand: **78 %** der KI-Benutzenden verfolgen einen „Bring Your Own AI“-Ansatz (BYOAI) bei der Arbeit.² Dieser Trend ist in kleinen und mittelständischen Unternehmen noch ausgeprägter, wo **80 %** der Mitarbeitenden BYOAI-Praktiken anwenden.²

Dieser nicht genehmigte Ansatz hat erhebliche Nachteile. Mitarbeitende verschweigen häufig, dass sie KI nutzen: **52 %** geben nur ungern zu, dass sie KI für wichtige Aufgaben verwenden, und **53 %** befürchten, dass die KI-Nutzung sie austauschbar erscheinen lässt.² Diese Geheimhaltung hindert Unternehmen nicht nur daran, die Vorteile einer strategischen KI-Implementierung voll auszuschöpfen, sondern führt auch zu schwerwiegenden Sicherheitslücken in einer Umgebung, in der Führungskräfte Cybersicherheit und Datenschutz als ihre **größte** Sorge nennen.²

Angesichts der umfassenden Nutzung und der unvermeidlichen Weiterentwicklung von KI stellt sich nicht die Frage, ob KI in Ihrem Unternehmen erlaubt werden sollte – sondern wie Sie eine sichere Lösung bereitstellen, die die Anforderungen Ihrer Mitarbeitenden erfüllt und gleichzeitig die Daten Ihres Unternehmens schützt.



05

Das regulatorische Labyrinth

Rahmenbedingungen und Gesetze rund um Datenschutz und Sicherheit schaffen eine weitere Ebene der Komplexität bei der Einführung von KI. Während einige Frameworks speziell für KI-Governance entwickelt wurden, verfügen andere über umfassendere Anwendungen, die sich dennoch auf den Umgang mit Informationen auswirken – und die Strafen bei Verstößen bleiben streng.

Wenn Ihre Mitarbeitenden KI-Tools ohne angemessene Aufsicht verwenden, können sie unbeabsichtigt Compliance-Verstöße verursachen. KI erhöht dieses Risiko, da sie auf regulierte Informationen auf eine Art zugreifen, diese kombinieren und offenlegen kann, wie es herkömmliche Technologien nicht können.

Die wichtigsten Vorschriften, die sich auf Ihre KI-Nutzung auswirken:

DSGVO

Die Datenschutz-Grundverordnung der Europäischen Union gibt Menschen die Kontrolle über ihre personenbezogenen Daten und erfordert eine eindeutige Zustimmung zu deren Verarbeitung

EU AI Act

Das umfassende Framework der Europäischen Union, das speziell zur Regulierung von Systemen für künstliche Intelligenz basierend auf ihren jeweiligen Risikostufen entwickelt wurde

HIPAA

Dieses US-amerikanische Bundesgesetz für das Gesundheitswesen legt strenge Standards für den Umgang mit geschützten Gesundheitsdaten fest.

NIST AI Risk Management Framework

Diese freiwillige US-amerikanische Richtlinie unterstützt Unternehmen dabei, Risiken bei der Konzeption, Entwicklung und Bereitstellung von KI-Systemen anzugehen.

Die Compliance-Risiken mit KI:

- Kundendaten werden auf Servern außerhalb der genehmigten Regionen verarbeitet.
- Personenbezogene Daten werden ohne ordnungsgemäße Zustimmung verwendet.
- Sensible Daten bleiben ohne entsprechende Aufbewahrungskontrollen in Systemen gespeichert.
- Kein Prüfpfad darüber, wie auf geschützte Informationen zugegriffen wird und wie diese verwendet werden
- KI-generierte Inhalte, die gegen branchenspezifische Compliance-Anforderungen verstoßen

Diese Verstöße können schwerwiegende Konsequenzen nach sich ziehen:

- Hohe Geldstrafen (Bußgelder im Rahmen der DSGVO können bis zu **4 %** Ihres weltweiten Umsatzes ausmachen)⁴
- Anforderungen zur Benachrichtigung Betroffener über Datenschutzverletzungen
- Rechtliche Schritte der Betroffenen
- Schädigung des Rufs Ihres Unternehmens und des Kundenvertrauens

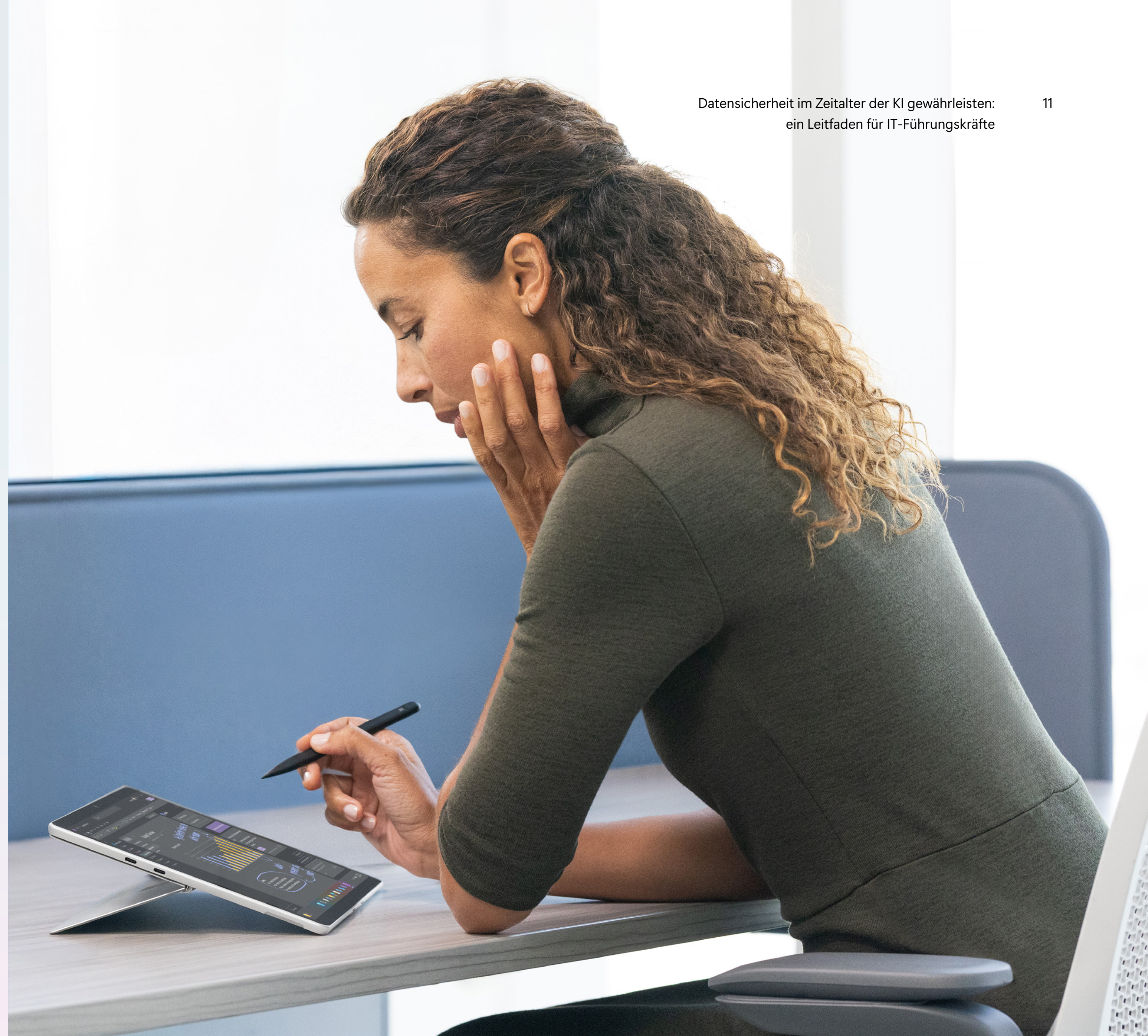
Angesichts des zunehmenden Einsatzes von KI in Ihrem Unternehmen benötigen Sie Governance, die Mitarbeitenden hilft, effizient zu arbeiten, und gleichzeitig sicherstellt, dass Ihr Unternehmen die Vorschriften einhält, die Ihr Geschäft und Ihre Kundschaft betreffen.

06

Ein sicherheits-orientiertes Framework zur Bewertung von KI-Lösungen

Da Schatten-KI, BYOAI und Vorschriften erhebliche Risiken darstellen, benötigen Sie einen strukturierten Ansatz zur Bewertung von KI-Lösungen, der sicherstellt, dass sie Ihrem Unternehmen helfen, Innovationen voranzutreiben – und gleichzeitig sensible Daten schützen und die Einhaltung der sich entwickelnden gesetzlichen Anforderungen sicherstellen.

Das folgende Framework beinhaltet sechs einfache Fragen, mit denen beurteilt werden kann, ob eine KI-Plattform in beiden Bereichen erfolgreich ist.



Frage 1

Bietet sie von Grund auf Sicherheit auf Unternehmensniveau?

Mit der richtigen Lösung stellen Sie sicher, dass sich der Schwerpunkt Ihrer Sicherheit verlagert: von der Reaktion auf Probleme, nachdem sie aufgetreten sind, hin zur proaktiven Suche nach Schwachstellen in den Daten Ihres Unternehmens, bevor diese zu größeren Problemen werden.

Suchen Sie nach Lösungen, die:

- Echtzeit-Transparenz für Ihre gesamte Dateninfrastruktur bieten.
- potenzielle Datenrisiken automatisch identifizieren, bevor sie zu Vorfällen werden.
- vertrauliche Informationen auf allen Ebenen schützen.

Frage 2

Kann sie bestehende Sicherheitskontrollen einfach übernehmen und verbessern?

Die Sicherheitsrichtlinien Ihres Unternehmens sollten nahtlos mit KI zusammenarbeiten. Ihr KI-Lösungsanbieter sollte Ihre vorhandenen Sicherheits-Frameworks respektieren und in diese integrieren – nicht von Ihnen verlangen, völlig neue zu erstellen.

Suchen Sie nach Lösungen, die:

- Ihre vorhandenen Sicherheitsrichtlinien, Vertraulichkeitsbezeichnungen und Informationsschutzeinstellungen nahtlos übernehmen.
- granulare Zugriffskontrollen auf individueller Ebene anwenden, damit Benutzende nicht auf Daten zugreifen können, für die sie keine Berechtigung haben.
- Versuche zur Untergrabung von Zugriffskontrollen aktiv kennzeichnen.

Frage 3

Umfasst sie integrierte Kontrollmechanismen für Governance und Datenschutz?

Da KI-Tools proaktiver arbeiten, müssen auch Ihre Sicherheitsmaßnahmen proaktiv sein. Die Implementierung einer starken Data Governance schafft klare Grenzen, innerhalb derer Ihre Mitarbeitenden sicher Innovationen umsetzen können, ohne vertrauliche Informationen zu gefährden.

Suchen Sie nach Lösungen, die:

- KI-Governance mit automatisierter Richtliniendurchsetzung für alle Aktivitäten zentralisieren.
- die frühzeitige Erkennung einer möglichen übermäßigen Datenfreigabe umfassen.
- auf regulatorische Frameworks abgestimmt sind, um eine konforme KI-Nutzung zu gewährleisten.

Frage 4

Kann sie konsistent im gesamten Unternehmen bereitgestellt werden?

Ihre Mitarbeitenden haben ihren eigenen Arbeitsstil, ihre eigenen Zeitpläne und können überall auf der Welt ansässig sein. KI sollte allen zugute kommen.

Suchen Sie nach Lösungen, die:

- eine nahtlose Einrichtung und eine einfache KI-Einführung in die täglichen Arbeitsabläufe bieten.
- flexiblen Zugriff bieten, vom kostenlosen KI-Chat bis hin zu skalierbaren Agent-Lösungen.
- Mitarbeitenden helfen, KI-Kenntnisse zu entwickeln und in ihre Arbeit zu integrieren.

Frage 5

Kann sie nahtlos in vorhandene Frameworks integriert werden?

Ihr Unternehmen arbeitet derzeit mit einer eigenen digitalen Infrastruktur aus Softwareprogrammen, Apps und mehr.

Suchen Sie nach Lösungen, die:

- sich nahtlos in Ihre Tools und Programme einfügen, um Unterbrechungen zu minimieren.
- ein kontinuierliches KI-Erlebnis über alle Apps hinweg bieten, um einen nahtlosen Arbeitsfluss zwischen Tools sicherzustellen.
- Aufgaben innerhalb bestehender Workflows automatisieren und optimieren.

Frage 6

Erhalten Benutzende die Möglichkeit, Innovationen umzusetzen?

Im Kern sollte KI die Art und Weise verändern, wie Arbeit erledigt wird. Hier geht es nicht nur um Automatisierung, sondern auch um Steigerung der Produktivität und Förderung von Innovationen.

Suchen Sie nach Lösungen, die:

- zeitaufwendige Prozesse in optimierte Abläufe verwandeln.
- repetitive Aufgaben automatisieren.
- es Mitarbeitenden ermöglichen, Zeit zurückzugewinnen und sich auf Prioritäten zu konzentrieren.

07

Microsoft 365 Copilot: KI, der Sie vertrauen können

Microsoft 365 Copilot ist die GenAI-Lösung, die robuste Sicherheits-, Governance- und Zugriffskontrollen bereitstellt und so eine sichere Bereitstellung und nachhaltige Innovation gewährleistet. Microsoft 365 Copilot steigert die Produktivität mit intuitiven Tools wie Copilot Chat, das Sie dort unterstützt, wo Sie arbeiten, und Copilot Studio, mit dem Ihr Team ohne Programmierkenntnisse individuelle KI-Agents entwickeln kann.

Copilot lässt sich nahtlos in Ihre Microsoft 365-Umgebung integrieren und übernimmt die jeweiligen Benutzerberechtigungen, Vertraulichkeitsbezeichnungen, Richtlinien zur Data Loss Prevention und Anforderungen im Hinblick auf die geografische Datenhoheit – ohne zusätzliche Konfiguration. Durch die Einbettung von KI in die Tools, die Ihre Mitarbeitenden bereits verwenden, minimiert Copilot Sicherheitsrisiken, während die Daten in Ihrer vertrauten Microsoft 365-Umgebung bleiben.

Die Verpflichtungen von Microsoft stellen sicher, dass Ihr Unternehmen die Kontrolle behält:

- Ihre Daten sind sowohl im Ruhezustand als auch während der Übertragung sicher.
- Ihre Daten werden nicht zum Trainieren von KI-Modellen verwendet.
- Sie entscheiden, welche Informationen in die Cloud gelangen.
- Sie sind vor KI-Sicherheits- und Urheberrechtsrisiken geschützt.

Speziell entwickelte Governance-Tools wie das Copilot Control System und SharePoint Advanced Management bieten IT-Teams die Transparenz, Kontrollen und Überwachungsprotokolle, die sie für die Aufrechterhaltung der Compliance benötigen.

Mit Microsoft 365 Copilot müssen Sie sich nicht zwischen Innovation und Sicherheit entscheiden – Sie können beides haben.



Der sichere Weg zur KI-Transformation

Die KI-Revolution bietet IT-Führungskräften eine einzigartige Gelegenheit, einen strategischen Wert zu liefern, indem sie Innovationen und Sicherheit in Einklang bringen.

Durch die Implementierung sicherer KI-Tools wie Microsoft 365 Copilot geben Sie Mitarbeitenden Tools an die Hand, mit denen sie ihre Produktivität steigern können, während gleichzeitig die Risiken von Schatten-KI eliminiert werden. Der Weg in die Zukunft besteht darin, auf sichere Weise Innovationen zu ermöglichen. Ihre Führungsrolle bei der sicheren KI-Einführung wird die IT als Wegbereiter der Transformation positionieren. Dies hilft Ihrem Unternehmen, in diesem neuen Zeitalter erfolgreich zu sein und sorgt dafür, dass Datensicherheit und Compliance gewährleistet bleiben.



Erste Schritte mit Microsoft 365 Copilot

Quellen:

¹ „Superagency in the workplace: Empowering people to unlock AI’s full potential“, McKinsey & Company, 28. Januar 2025 <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work>.

² „KI am Arbeitsplatz ist inzwischen Realität. Jetzt kommt der schwierige Teil.“, Microsoft Work Trend Index, 8. Mai 2024 <https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part>

³ „Wird KI die Arbeit erleichtern?“, Microsoft Work Trend Index, 9. Mai 2023 <https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work>

⁴ „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“, Europäisches Parlament und Rat der Europäischen Union, 27. April 2016 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.