Copilot im Unternehmen: Chancen nutzen, Risiken kontrollieren

„Künstliche Intelligenz ist kein Selbstläufer – sie braucht klare Regeln, gute Daten und Menschen, die wissen, was sie tun."

Oliver Krizek, Gründer und Geschäftsführer der NAVAX Unternehmensgruppe, teilt im Gespräch mit Barbara Steininger vom trend. seine wichtigsten Learnings aus der Praxis:

Was darf der Copilot? Was darf er nicht? Wie muss der KI-Assistent für das Unternehmen eingestellt sein, um Datenpannen zu vermeiden und wie sollten Mitarbeitende auf ihren neuen Assistenten vorbereitet werden.

Der Copilot muss viel wissen, um hilfreich zu sein: Wie vermeide ich technisch und organisatorisch, dass er keine Dokumente zeigt, die nicht alle sehen sollen?

Damit Copilot im Unternehmen hilfreich sein kann, muss er auf viele Informationen zugreifen – idealerweise nur auf jene Datenquellen, die für die jeweilige Person auch bestimmt sind. Technisch lässt sich das sicherstellen, indem man die Zugriffsrechte in Microsoft 365, SharePoint, OneDrive und Teams sauber verwaltet. Copilot zeigt in weiterer Folge nur jene Inhalte, die für den Anwender bestimmt sind. Organisatorisch bedeutet das: Es braucht klare Regeln, wer welche Daten sehen darf und regelmäßige Berechtigungsprüfungen.

Als Beispiel: Wenn ein vertrauliches HR-Dokument versehentlich in einem allgemein zugänglichen Ordner liegt, kann Copilot daraus Informationen ziehen. Der Fehler liegt allerdings nicht an Copilot selbst bzw. der KI-Lösung, sondern an der falschen Datenablage.

Tipp: Wer also seine Daten gut strukturiert und Mitarbeitende sensibilisiert, kann Copilot sicher und effektiv nutzen.

Welche Werkseinstellungen müssen unbedingt geändert werden? Wie stelle ich sicher, dass keine Daten nach draußen oder von draußen angesehen werden können?

Einige Werkseinstellungen von Microsoft Copilot M365 sollten unbedingt angepasst werden, um sowohl die Datensicherheit als auch den Datenschutz im Unternehmen zu gewährleisten. Besonders wichtig ist es, den Zugriff auf externe Datenquellen zu beschränken und sogenannte „Cross-Tenant"-Verbindungen zu deaktivieren – also den automatischen Austausch von Informationen mit anderen Organisationen. Zusätzlich sollten Datenschutzfunktionen (z.B.: Microsoft Purview) genutzt werden, um sensible Daten zu klassifizieren und deren Verarbeitung durch Copilot gezielt zu steuern.

Ein Beispiel: Wenn personenbezogene Daten wie Mitarbeiterlisten oder Gesundheitsinformationen nicht korrekt gekennzeichnet sind, könnten sie unbeabsichtigt in eine Copilot-Antwort einfließen. Der Umstand wäre mit Sicherheit datenschutzrechtlich problematisch.

Tipp: Wer also die richtigen Einstellungen im Microsoft 365 Admin Center vornimmt, Datenschutzrichtlinien technisch abbildet und Mitarbeitende entsprechend schult, schafft eine sichere und DSGVO-konforme Grundlage für den produktiven Einsatz von Copilot M365.

Welche neuen Routinen sollte die IT-Abteilung bzw. Sicherheitsbeauftragte beachten dabei?

Mit dem Einsatz von Microsoft Copilot entstehen für IT-Abteilungen und Sicherheitsverantwortliche neue Routinen - nicht nur technisch, sondern auch rechtlich. Besonders im Fokus steht dabei der EU AI-Act, der seit 2025 verbindliche Anforderungen an den Einsatz von KI-Systemen stellt. Unternehmen müssen sicherstellen, dass Copilot nur auf freigegebene Daten zugreift, und gleichzeitig dokumentieren, wie die KI eingesetzt wird. Technisch lässt sich das über Zugriffsrechte, Sensitivitätskennzeichnungen und Audit-Logs steuern. Zusätzlich können bestimmte Abfragen, etwa zu besonders sensiblen Daten wie Gehältern oder Gesundheitsinformationen, gezielt blockiert oder eingeschränkt werden, um Risiken zu minimieren und den Anforderungen des AI-Acts gerecht zu werden.

Beispiel: Ein Unternehmen kann Copilot so konfigurieren, dass Anfragen wie „Zeige mir alle Mitarbeitende mit Burnout-Diagnose“ automatisch unterbunden werden – nicht nur aus Datenschutzgründen, sondern auch, weil der AI-Act vorschreibt, dass Hochrisikoanwendungen besonders geschützt und kontrolliert werden müssen.

Tipp: Wer diese Schutzmechanismen mit einer klaren Governance, regelmäßigen Schulungen und einer internen KI-Richtlinie kombiniert, schafft die Grundlage für einen sicheren, rechtskonformen und produktiven Einsatz von Copilot im Unternehmen.

Wie kann ich den Copilot kontrollieren?

Copilot lässt sich auf mehreren Ebenen kontrollieren – sowohl technisch als auch organisatorisch. Über das Microsoft 365 Admin Center kann die IT genau festlegen, welche Funktionen Copilot nutzen darf, auf welche Daten er zugreifen kann und für welche Nutzergruppen er aktiviert ist. Zusätzlich lassen sich sensible Inhalte mit sogenannten „Sensitivity Labels“ schützen, und über Audit-Logs kann jederzeit nachvollzogen werden, welche Informationen verarbeitet wurden.

Ein Beispiel: In einem Unternehmen wurde Copilot im Marketing-Team eingeführt, aber gezielt so konfiguriert, dass er keine Daten aus dem Finanzbereich analysieren kann – selbst wenn ein Mitarbeitender danach fragt.
So bleibt Copilot ein leistungsstarkes Werkzeug, das produktiv unterstützt, aber immer unter klarer Kontrolle und im Einklang mit Datenschutz und Unternehmensrichtlinien arbeitet.

Gibt es einen speziellen NAVAX-Hack für den sicheren Umgang? Einen Supertipp?

Ein bewährter „NAVAX-Hack“ für den sicheren und produktiven Umgang mit Copilot ist die Kombination aus einer klaren AI-Strategie, einer verantwortlichen Rolle im Unternehmen und dem gezielten Einsatz eigener KI-Modelle in Azure. Statt Mitarbeitenden unkontrollierten Zugang zu externen KI-Diensten wie ChatGPT, Google Gemini oder Claude zu gewähren, empfiehlt NAVAX, geprüfte, unternehmensinterne Lösungen bereitzustellen – etwa über Azure Services, die sich nahtlos in bestehende Microsoft-365-Umgebungen integrieren lassen. So können Mitarbeitende über eine sichere Azure-Instanz auf bis zu 2.000 KI-Modelle zugreifen – mit voller Kontrolle über Datenschutz, Datenstandort und Nutzung. Alle Informationen bleiben im Unternehmen, Compliance und Governance sind gewährleistet.

Ein zentraler Bestandteil dieser Strategie ist der **NAVAX Buddy** – ein unternehmensinterner KI-Assistent, der auf Azure AI Foundry, Copilot Studio Agents und Microsoft 365 basiert. Der Buddy fungiert als sicherer Einstiegspunkt für alle KI-Anfragen im Unternehmen. Er verarbeitet ausschließlich freigegebene interne Datenquellen wie SharePoint, Intranet oder Jira und bietet über spezialisierte Agents (z. B. für HR, IT, Sales oder Engineering) gezielte Unterstützung im Arbeitsalltag. Adaptive Cards und Feedback-Mechanismen sorgen für Transparenz und Nachvollziehbarkeit. So wird verhindert, dass sensible Inhalte in öffentliche Tools gelangen – und gleichzeitig wird Wissen zentralisiert, dokumentiert und wiederverwendbar gemacht.

Supertipp: Nutzung des NAVAX Buddy als Standardzugang für KI im Unternehmen – sicher, integriert und datenschutzkonform.

Wie sollten Mitarbeiterschulungen konzeptioniert sein, damit sie das Potenzial wirklich ausschöpfen?

Damit Mitarbeitende das volle Potenzial von Copilot nutzen können, sollten Schulungen nicht nur praxisnah und rollenbasiert sein, sondern auch den rechtlichen Rahmen berücksichtigen – insbesondere den EU AI-Act. Dieser verpflichtet Unternehmen dazu, sicherzustellen, dass alle, die mit KI-Systemen arbeiten, über ausreichende Kenntnisse verfügen.

Wir empfehlen daher ein gestuftes Schulungskonzept: Zunächst eine Basisschulung für alle mit Grundlagen zu KI, Datenschutz, dem AI-Act, sicheren Prompts und Sensibilisierung beim Arbeiten mit KI-Tools. Darauf aufbauend folgen bereichsspezifische Trainings, z. B. für HR, Vertrieb, Finanzen oder IT, und für fortgeschrittene Nutzer auch vertiefende Module, etwa zur Integration von KI in Workflows oder zur Nutzung eigener Modelle in Azure.

Wir empfehlen, dass in einem Unternehmen alle Mitarbeitenden zunächst mit einem einstündigen E-Learning geschult werden, bevor sie mit etwaigen AI-Modellen in Berührung kommen. Dies soll optimalerweise in den Onboarding-Prozess integriert sein und sorgt für Sicherheit, Akzeptanz und eine gemeinsame Wissensbasis.