isolutions

Künstliche Intelligenz sicher am Arbeitsplatz nutzen

isolutions AG | Bern – Zürich – Basel – Barcelona

Ausgangslage: KI ist überall, auch im Arbeitsalltag

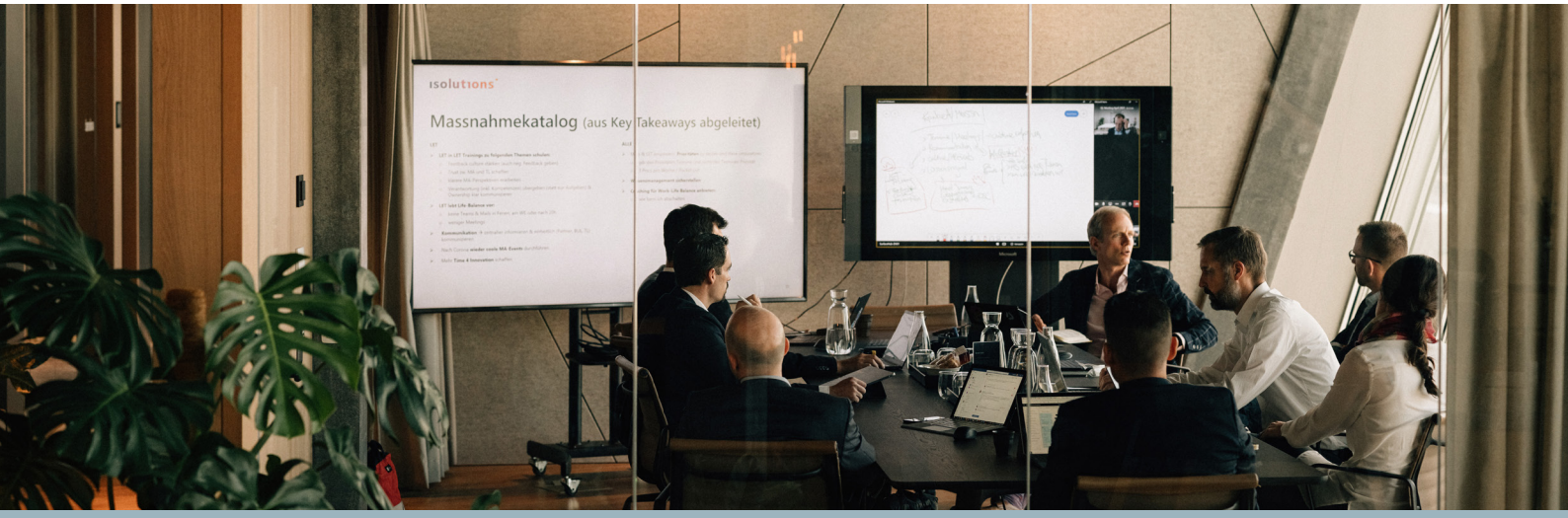
Künstliche Intelligenz hat sich in kurzer Zeit zu einem selbstverständlichen Werkzeug im Arbeitsalltag entwickelt. Mitarbeitende nutzen KI-basierte Anwendungen wie ChatGPT, Google Gemini oder Microsoft Copilot heute ganz selbstverständlich zur Unterstützung ihrer täglichen Aufgaben. Typische Einsatzszenarien sind das Verfassen und Überarbeiten von E-Mails, Übersetzungen, das Zusammenfassen von Dokumenten, Recherchen, Analysen oder die Unterstützung bei der Erstellung von Code und Konzepten.

In vielen Organisationen wächst die KI-Nutzung **organisch und pragmatisch**. Mitarbeitende greifen eigenständig auf verfügbare Tools zurück, um ihre Arbeit effizienter zu gestalten und den steigenden Anforderungen im Arbeitsalltag gerecht zu werden.

KI wird dabei zunehmend als natürliches Hilfsmittel wahrgenommen und weniger als neue Technologie, die aktiv eingeführt werden muss. Für viele Mitarbeitende ist sie bereits ein fester Bestandteil ihres digitalen Werkzeugkastens – vergleichbar mit Suchmaschinen, Kollaborationstools oder Cloud-Services. Die Nutzung von KI ist damit keine Ausnahme mehr, sondern **Teil der gelebten Realität in modernen Arbeitsumgebungen**.

Mit der zunehmenden Verbreitung von KI wächst jedoch auch das Risiko einer unkontrollierten oder unzureichend geregelten Nutzung. Mitarbeitende greifen häufig auf frei verfügbare KI-Dienste zurück, ohne sich der möglichen Auswirkungen auf **Datenschutz, Informationssicherheit, Vertraulichkeit oder regulatorische Anforderungen** bewusst zu sein. Werden sensible Unternehmens- oder Personendaten in ungeprüfte Systeme eingegeben, können erhebliche rechtliche, organisatorische und reputative Risiken entstehen. Um die Vorteile von KI nachhaltig zu nutzen, sind daher klare Rahmenbedingungen, geeignete Kontrollen und ein verantwortungsvoller Umgang mit der Technologie entscheidend.

Damit Sie das Potenzial von KI sicher nutzen können, schaffen wir **Transparenz über Chancen, Risiken und Anforderungen**. Auf Grundlage etablierter Standards wie ISO 42001 analysieren wir Ihre **Prozesse, Rollen und Governance-Strukturen** rund um den Einsatz von Künstlicher Intelligenz. So erkennen Sie frühzeitig Risiken, erfüllen regulatorische Vorgaben und entwickeln einen nachhaltigen Rahmen für den verantwortungsvollen KI-Einsatz.



Herausforderung: Shadow AI ausser Kontrolle

Als Shadow AI bezeichnet man die nicht genehmigte Nutzung von KI-Tools und -An-wendungen durch Mitarbeitende oder Abteilungen, ohne dass die IT- oder Sicherheitsabteilung des Unternehmens davon weiss. Das zentrale Problem von Shadow KI liegt nicht im Einsatz von KI selbst, sondern darin, dass diese Nutzung in vielen Organisationen ohne ausreichende Transparenz und Steuerung erfolgt. KI wird produktiv eingesetzt, jedoch ausserhalb klar definierter organisatorischer und technischer Leitplanken. Dadurch entsteht ein Zustand, in dem die Organisation den Überblick über den tatsächlichen KI-Einsatz verliert.

Folgende drei Leitfragen zeigen typische Anzeichen von Shadow AI:

Wissen Sie, welche KI-Tools in Ihrem Unternehmen genutzt werden – und mit welchen Daten?

In vielen Organisationen fehlt die Transparenz darüber, welche KI-Anwendungen im Einsatz sind, wofür sie genutzt werden und welche Unternehmens- oder Personendaten dabei verarbeitet werden.

Risiko: Ohne Überblick steigt die Wahrscheinlichkeit, dass Mitarbeitende vertrauliche Inhalte (z.B. interne Dokumente oder Kundendaten) in öffentliche KI-Tools eingeben und diese Daten ausserhalb der Kontrolle der Organisation verarbeitet werden.

Gibt es klare Regeln, wie KI im Arbeitsalltag eingesetzt werden darf?

Der Einsatz von KI erfolgt häufig ohne verbindliche Leitplanken. Mitarbeitende entscheiden situativ und individuell, welche Tools sie nutzen und wie sie diese einsetzen.

Risiko: Ohne klare Regeln entstehen Policy-Lücken sowie «Shadow»-Nutzung und gleichzeitig werden KI-Outputs eher ungeprüft übernommen, was zu Fehlern und Fehlinformationen in Prozessen und Dokumentationen führen kann.

Ist eindeutig geregelt, wer für den KI Einsatz verantwortlich ist?

Zuständigkeiten für Freigabe, Risikobewertung und Kontrolle von KI-Tools sind oft nicht klar definiert oder organisatorisch verankert.

Risiko: Wenn Verantwortlichkeiten fehlen, bleiben Governance-Massnahmen, Kontrollen, Audits und Reaktion auf Vorfälle lückenhaft – mit möglichen regulatorischen und reputativen Folgen.

Diese Anzeichen sind typisch für Shadow AI: KI wird produktiv genutzt, aber ausserhalb der formalen Steuerung der Unternehmung.

Lösung: Erkennen – regeln – schützen

Die beste Antwort auf die unkontrollierte Nutzung von KI im Unternehmen ist nicht ein generelles Verbot. Stattdessen sollten Mitarbeitende sichere und freigegebene KI-Lösungen nutzen können, die klare Regeln und Schutzmechanismen bieten. So lassen sich die Vorteile von KI nutzen, ohne Datenschutz, Informationssicherheit oder Compliance zu gefährden.

Ziel ist es, Transparenz darüber zu schaffen, welche KI-Anwendungen eingesetzt werden, klare Vorgaben für deren Nutzung festzulegen und sensible Unternehmensdaten wirksam zu schützen. Im Microsoft-Ökosystem geschieht dies durch einen ganzheitlichen Ansatz, der die Erkennung von KI-Nutzung, deren Steuerung sowie den Schutz von Daten und Zugriffsrechten miteinander verbindet.

Step 1: Discovery Assessment – Transparenz schaffen & Risiken priorisieren

Was wir tun: Wir schaffen systematisch Transparenz darüber, welche KI-Tools und KI-Apps in Ihrem Unternehmen tatsächlich im Einsatz sind, wie intensiv diese genutzt werden und wo potenziell sensible Daten abfliessen. Dafür setzen wir auf die Shadow-IT-/Shadow-AI-Discovery mit **Microsoft Defender for Cloud Apps**, inklusive detaillierter Nutzungsanalysen und integrierter Risikoindikatoren. Die Cloud Discovery ist bereits in **Microsoft 365 E3 bzw. Entra ID P1** enthalten – es entstehen keine zusätzlichen Lizenzkosten für den Einstieg.

Auf Basis dieser Transparenz ermöglichen wir eine klare Priorisierung: von den meistgenutzten KI-Apps über relevante Risikoquellen bis hin zu kritischen Use Cases und KI Agenten. So entsteht eine belastbare Entscheidungsgrundlage, um gezielt Governance, Sicherheitsmassnahmen und Kontrollmechanismen dort zu etablieren, wo sie den grössten Effekt haben.

Output: Eine strukturierte Übersicht der «Top KI-Apps» inklusive Nutzungsintensität, Risikobewertung und priorisierten Handlungsfeldern (z. B. kritische Use Cases und potenzielle Datenflüsse).

Step 2: KI Regelwerk/Policy – Klare Leitplanken erarbeiten

Was wir tun: Auf Basis der gewonnenen Transparenz definieren wir gemeinsam Regeln für den KI-Einsatz in Ihrem Unternehmen: eine kompakte AI Acceptable Use Policy (erlaubt/nicht erlaubt), Datenregeln (welche Inhalte dürfen in KI-Tools eingegeben oder hochgeladen werden) sowie einen pragmatischen Prozess für Ausnahmen und neue Tools.

Rollen und Verantwortlichkeiten (z.B. Tool-Freigabe, Risikobewertung, Betrieb und Kommunikation) werden verbindlich festgelegt und in einer kompakten System-/Prozessbeschreibung dokumentiert.

Output: Abgestimmtes KI-Regelwerk («Acceptable Use Policy» und Datenregeln), definierte Verantwortlichkeiten (RACI) und Ausnahme-/Freigabeprozess für KI-Tools.

Step 3: Technische Umsetzung – Schutzmassnahmen durchsetzen

Was wir tun: Auf Basis Ihrer individuellen Risiken, Use Cases und des gewünschten Reifegrads setzen wir gezielt technische Massnahmen um, damit die in Step 2 definierten Leitplanken im Arbeitsalltag wirksam werden. Im Mittelpunkt stehen die Reduktion von Datenabfluss sowie die kontrollierte Nutzung bzw. Eindämmung nicht freigegebener KI-Tools (Shadow AI).

Baustein 1: Microsoft Defender for Cloud Apps (CASB)
Für die Discovery von Anwendungen, Risikobewertung sowie die Durchsetzung von Kontrollmechanismen auf App-Ebene – z. B. Blockieren, eingeschränkte Nutzung oder Session Controls.

Baustein 2: Microsoft Purview
Für Information Protection (Klassifizierung und Labeling), Data Loss Prevention (DLP) sowie Compliance-Richtlinien auf Inhaltsebene – insbesondere für KI-relevante Datenflüsse und sensible Informationen.

Baustein 3: Microsoft Copilot als «Approved AI Path»
Einführung einer zentral gesteuerten und abgesicherten KI-Lösung, inklusive Tenant- und Sicherheitskonfiguration, Daten- und Berechtigungskonzept sowie begleitender Enablement-Guidance. So erhalten Mitarbeitende eine produktive Alternative zu Shadow-AI-Tools – sicher, integriert und compliance-konform.

Output: Abgestimmtes Massnahmenpaket (z.B. CASB/DLP und/oder Microsoft Copilot als «approved path») inkl. dokumentierter Konfiguration und klaren Betriebs-/Übergabepunkten.

Step 4: Proaktive Überwachung – Sicherheit & Compliance sicherstellen

Was wir tun: Gemeinsam mit unserem Cyber Defense Service etablieren wir eine proaktive Überwachung der KI-Nutzung und der relevanten Kontrollen: laufendes Monitoring, Alerting und regelmässige Reviews (z.B. neue/auffällige KI-Apps, Policy-Verstösse, ungewöhnliche Nutzungsmuster) sowie definierte Incident-Response-Abläufe um Vorfälle schnell einordnen, bewerten und gezielt behandeln zu können.

Output: Monitoring Use-Cases inkl. Alerting, regelmässiges Reporting/Review-Rhythmus und Incident-Response-Runbook für KI-bezogene Findings.

Fazit

Mit einem strukturierten End-to-End-Ansatz bringen wir die KI-Nutzung aus der ‘Schattenzone’ in einen kontrollierten und sicheren Betrieb. Dieser Ansatz kombiniert vier Elemente: Transparenz durch Discovery, klare Governance-Regeln, technisch durchgesetzte Schutzmechanismen (Govern & Protect) sowie eine proaktive Überwachung durch unseren Cyber Defense Service.

Dadurch reduzieren wir Risiken wie Datenabfluss und Compliance-Verstösse. Gleichzeitig fördern wir die Nutzung freigegebener KI-Lösungen und stellen sicher, dass der Produktivitätsgewinn von KI im Arbeitsalltag nachhaltig erhalten bleibt.

Bei einem Erstgespräch besprechen wir gemeinsam, welche Schritte umgesetzt und definiert werden müssen.

isolutions

#weshapethefuture

Im Zivilschutzkeller von drei Berner Oberländer Visionären gegründet, begleitet isolutions seit 1999 als grösster, dedizierter Microsoft One-Stop-Shop in der Schweiz Unternehmen in die digitale Zukunft. Dabei veredeln und integrieren wir die Services von Microsoft so, dass Mehrwert geschaffen und die Unternehmenskultur positiv verändert wird.

Getragen von über 300 passionierten Köpfen bestehend aus Business und Technical Consultants, Change Makers sowie Softwareentwickler, Architekten und Cloud Natives werden wir von unseren Kunden und deren Herausforderungen zu Höchstleistungen angetrieben. Gemeinsam mit Kunden aus unterschiedlichen Branchen, schlagen wir die Brücke zum Tech-Giganten Microsoft. Alle mit einem Ziel: Das beste Mitarbeiter- und Kundenerlebnis zu kreieren, um daraus Wettbewerbsvorteile zu erzielen.

Die Kunden lieben unsere inspirierende Unternehmenskultur, welche ansteckend wirkt. Sie unterstützt und bewältigt erfolgreich organisatorische oder technologische Herausforderungen. Gemeinsam mit ihnen gestalten wir die Zukunft von Teams, Produkten, Unternehmungen und ganzen Industrien.

Standorte

Bern
Schanzenstrasse 4c
3008 Bern

Zürich
The Circle 38
8038 Zürich

Basel
Güterstrasse 144
4053 Basel

Barcelona
Carrer de Trafalgar 6
2a planta, despacho 28
08010 Barcelona

Let's talk

Markus Kaegi
Part-Business Unit Lead
Cyber Security
markus.kaegi@isolutions.ch
+41 44 555 73 53