

Agenten mit Zugriff auf Ihr System – wer steuert wen?

Wenn KI Ihren Rechner selbst bedient, braucht es klare Führung und klare Grenzen.

Immer häufiger tauchen KI-Agenten auf, die nicht nur Texte schreiben oder Analysen liefern, sondern Ihren Rechner direkt bedienen: Dateien öffnen, E-Mails verschicken, Formulare ausfüllen, Buchungen vornehmen. Technisch faszinierend – strategisch heikel.

Die zentrale Frage lautet nicht: „Geht das?“

Sondern: „Wer ist Chef im Ring?“

Was diese Agenten wirklich bedeuten

Ein KI-Agent, der Ihren Rechner steuert, benötigt Zugriff: auf Programme, Dateien, Browser-Sessions – unter Umständen auch auf gespeicherte Passwörter. Das kann Prozesse massiv beschleunigen. Es kann aber auch neue Risiken schaffen.

Pro:

- Automatisierung komplexer Routineabläufe
- Zeitersparnis bei administrativen Tätigkeiten
- Reduzierung menschlicher Tippfehler

Contra:

- Zugriff auf sensible Unternehmensdaten
- Haftungsfragen bei Fehlentscheidungen
- Unklare Verantwortlichkeiten im Team

Ein Praxisbeispiel aus dem Mittelstand

Ein Produktionsbetrieb wollte Angebotsprozesse beschleunigen. Ein externer Dienstleister implementierte einen Agenten, der selbstständig Kundendaten aus E-Mails extrahierte, Kalkulationen öffnete und Angebote direkt versendete.

Was übersehen wurde: Der Agent arbeitete mit einem generischen Admin-Zugang. Nach einem Fehlprompt wurden interne Preiskalkulationen an einen Kunden verschickt. Kein

Hackerangriff – sondern mangelnde Führungsstruktur.

Der Schaden war nicht existenzbedrohend, aber teuer. Und vermeidbar.

Klare Regeln statt Technikbegeisterung

KI ersetzt keine Verantwortung. Sie verschiebt sie. Führung bedeutet hier:

- Rollen- und Rechtenkonzepte definieren
- Keine Admin-Zugänge für Automatisierungen
- Trennung sensibler Datenbereiche
- Protokollierung und menschliche Kontrollschleifen

Meine klare Position: KI darf Prozesse steuern – aber niemals unkontrolliert Zugriff auf alles erhalten. Technologie muss sich Ihrer Organisationsstruktur unterordnen, nicht umgekehrt.

Wenn Sie prüfen möchten, wo in Ihrem Unternehmen Automatisierung sinnvoll ist – und wo klare Grenzen notwendig sind –, lassen Sie uns das strukturiert analysieren.

Vereinbaren Sie ein unverbindliches Strategiegespräch oder buchen Sie einen Impuls-Workshop zum Thema „Kontrollierte KI-Integration im Mittelstand“.

Claudia Blume

KI4U

claudia@ki4u-claudiablume.com