

Shadow Agents: Die neue Compliance-Herausforderung für KMU

MANAGEMENT SUMMARY & KERNAUSSAGE

Shadow Agents sind KI-Systeme, die eigenständig handeln: Sie senden E-Mails, buchen Termine oder lösen Zahlungen aus. Im Gegensatz zu Shadow AI tragen sie eigene rechtliche Verantwortung. Ohne Governance riskierst du Datenschutzverstösse, unkontrollierte Handlungen und Haftung. Der erste Schritt ist eine klare Richtlinie und menschliche Letztentscheidung.

KONTEXT & RELEVANZ FÜR ENTSCHEIDER

Shadow AI war meist ein Vertraulichkeitsproblem: Mitarbeitende gaben manuell Daten in Chatbots ein. Shadow Agents gehen weiter – sie handeln eigenständig. Sie verfassen und versenden E-Mails, buchen Termine, stossen Zahlungen an. Dieser Schritt vom passiven Werkzeug zum aktiven System verändert die Risikolage grundlegend. Wenn [Agenten Zugriff auf Systeme und Daten erhalten]/(ratgeber/ki-agenten-scheitern-am-datenzugriff-so-werden-kmu-agentenbereit), entsteht eine neue Qualität von Verantwortung.

Klassische Kontrollen erfassen vor allem, welche Geräte und Dienste genutzt werden. Sie erkennen aber nicht, was ein Agent tatsächlich tut. Genau hier entstehen neue Angriffsvektoren: Prompt Injection, bei der ein Agent über manipulierte Eingaben zu ungewollten Handlungen verleitet wird, oder die Manipulation ganzer Agentennetzwerke.

KERN-HANDLUNGSEMPFEHLUNGEN

- 01 Inventar erstellen: Welche KI-Agenten oder Automatisierungen sind im Unternehmen aktiv?
- 02 Minimale Governance-Regeln festlegen: Wer darf was? Wo ist menschliche Freigabe Pflicht?
- 03 Zugriffsrechte und Protokollierung einführen: Jede Agentenhandlung muss nachvollziehbar sein.
- 04 Verantwortliche benennen: Für jedes System eine Person, die im Zweifel haftet.

SCHWEIZER UMSETZUNGSKRITERIEN (REVDSG & IT-ARCHITEKTUR)

- ☑ Vollständige Konformität mit dem neuen Schweizer Datenschutzgesetz (revDSG).
- ☑ Keine Abhängigkeiten: Zero Lock-In auf proprietäre geschlossene Modelle.
- ☑ Schnittstellen zu Schweizer ERPs (Abacus, Bexio, M365) im operativen Betrieb.

Unverbindliche Prozess-Analyse

Lass uns in 20 Minuten prüfen, wo KI-Agenten in deinem Unternehmen sofort messbare Entlastung schaffen.

ki-outsourcing.ch