Vom Workflow-Agenten zum Persönlichen Assistenten

Wie OpenClaw und co. erneut das Paradigma ändern.

MAI 2026 · PHILIPP KUNTSCHIK

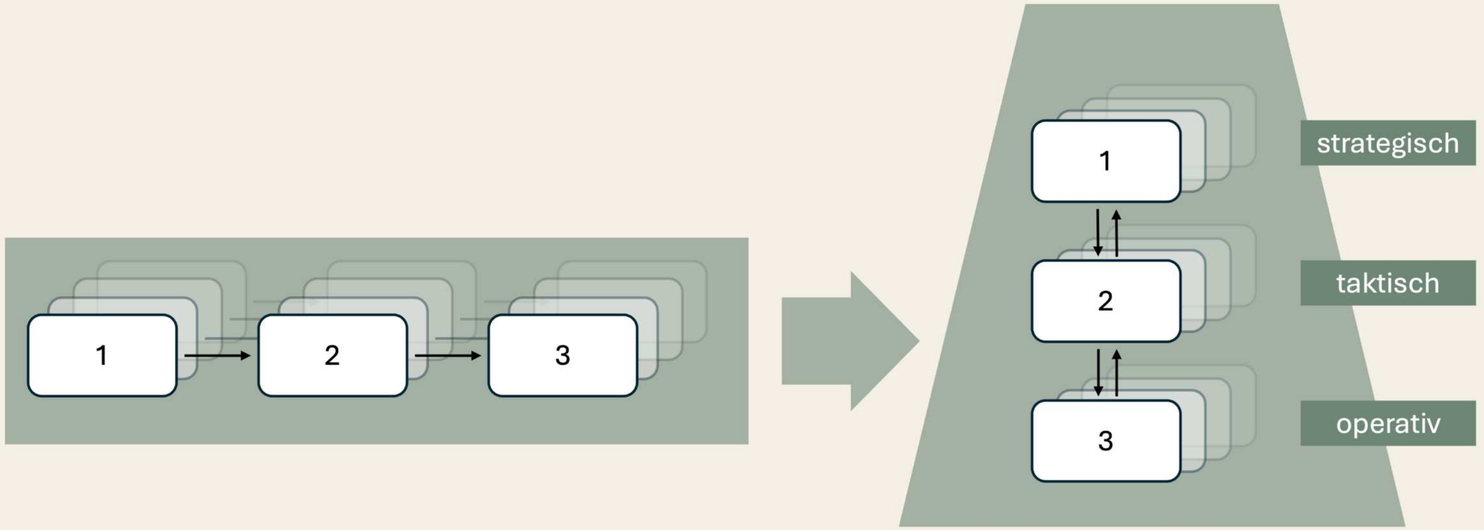
Die unsachgemässe Anwendung kann katastrophale Folgen verursachen.

Diese Präsentation zeigt Inhalte und Software, welche zum heutigen Stand **nicht für den flächendeckenden Einsatz** im Unternehmen geeignet sind.

Eine unsachgemässe Nutzung kann sehr schnell **katastrophalen Schaden** anrichten.

Wir wollen aufzeigen, was im Jahr 2026 / 2027 mit KI möglich wird, und wie sich das auf die IT-Sicherheit auswirkt.

Aus Skalierung wird individuelle Unterstützung.



Workflow-Agenten automatisieren Arbeitsschritte entlang eines Prozesses.

Persönliche AI-Agenten unterstützen Menschen entlang ihrer Tätigkeit - individuell und zielorientiert.

Beide Perspektiven können koexistieren.

LIVE-DEMO

Wie wirkt das in der Praxis?

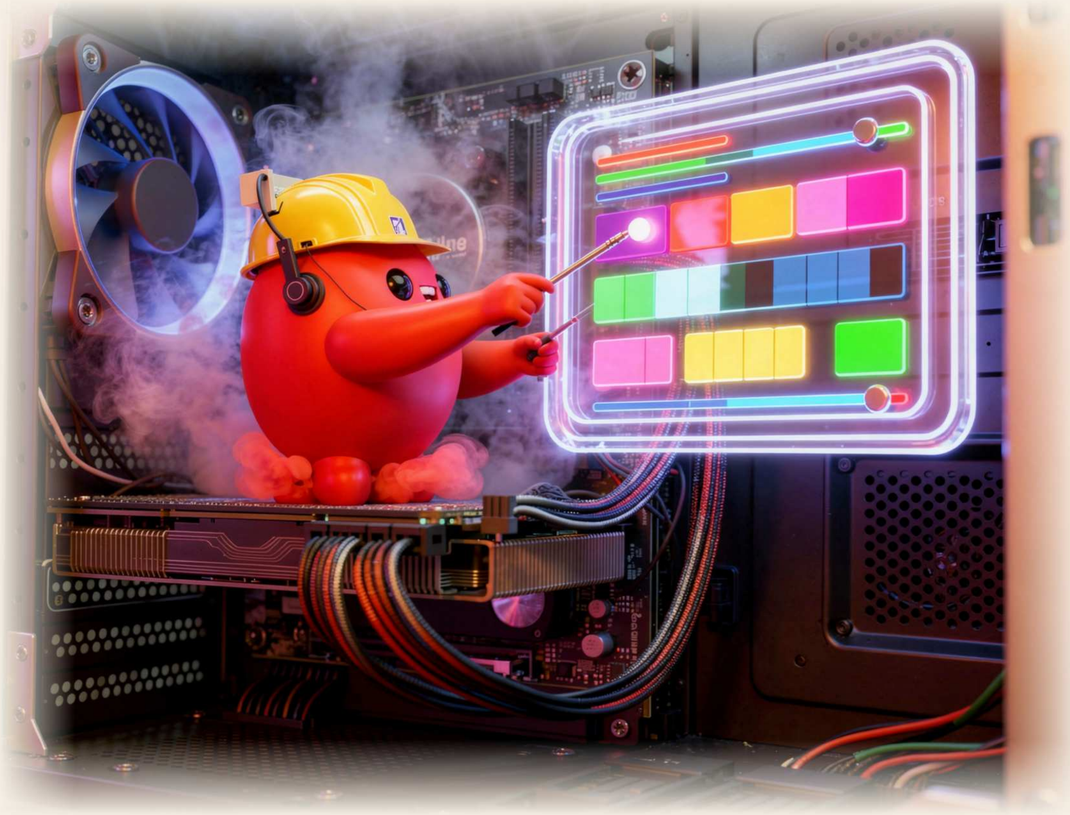
Von Sprachnachricht zu Zeiterfassung.

Situation: Arbeitszeit wird durch ein Online Tool pro Projekt an einem Bildschirm mit Maus und Tastatur erfasst.

Intervention: Statt selbst Arbeitszeit eintzutragen, wird eine Sprachnachricht an OpenClaw versendet. OpenClaw löst das Problem End-to-End.

Effekt: Weniger Aufwand und Kopfschmerzen.

Bedienung und Integration von Hardware.



Situation: Konfiguration und Integration von Hardware setzt Kenntnis vorraus.

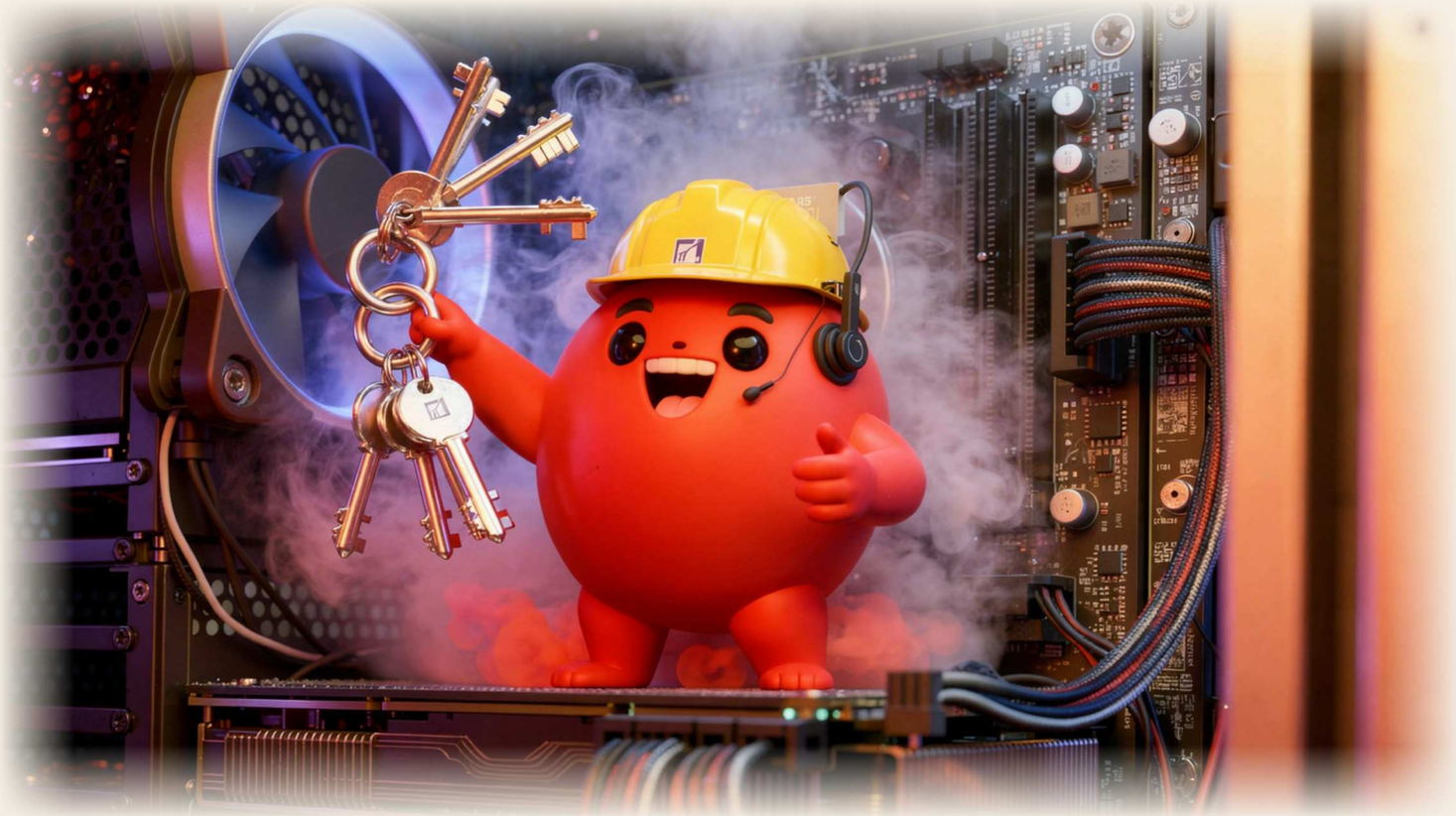
Intervention: Automatische Detektion und Aneignung nötiger Fähigkeiten, mit dem Gerät zu kommunizieren.

Effekt: Volle Kontrolle über das Gerät durch OpenClaw.

TEIL II · RISIKO

Warum sind diese Art von Agenten heute gefährlich?

Gleicher Zugriff wie der lokale Benutzeraccount.



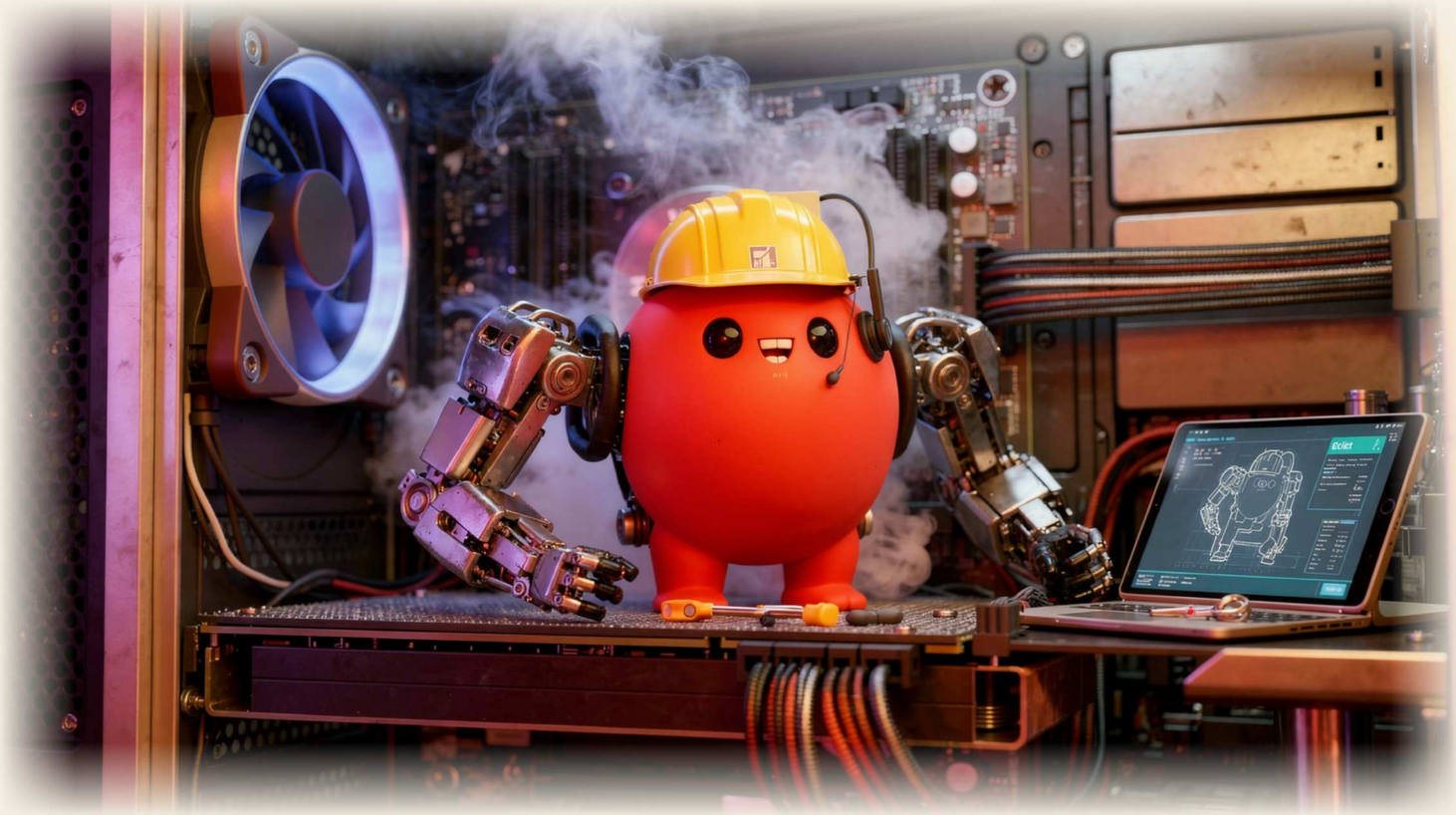
OpenClaw arbeitet mit den Rechten des aktiven Benutzer-Accounts.

Alles, was der ausführende Nutzer darf, kann der Agent ebenfalls ausführen.

Logs analysieren, Cookies auslesen, Zugriff auf Textdateien mit Passwörtern, Interagieren mit Browser-Memory, APIs.

Im Namen des Nutzers beliebige Dokumente öffnen, lesen, verändern oder versenden.

Autonome Weiterentwicklung.



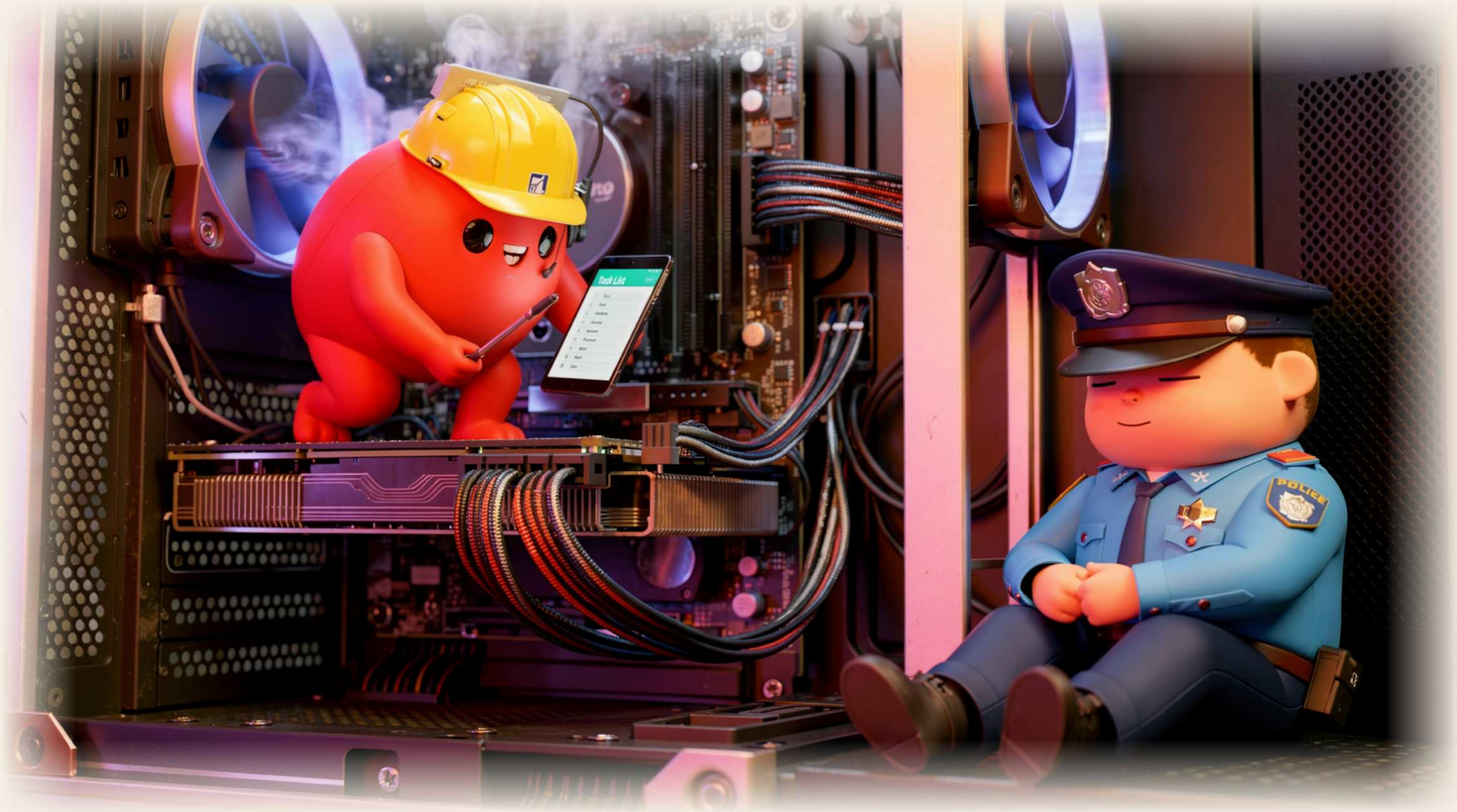
OpenClaw kann den eigenen Werkzeugkasten zur Laufzeit erweitern.

Autonome Entwicklung von Scripts und Programmen direkt auf dem Gerät.

Autonome Installation fremder Tools und Funktionen aus dem Internet.

Prompt-Injection: Eine versteckte Anweisung in einem Dokument, Email oder Websuche, kann den Agenten beeinflussen und fremdsteuern.

Installation ohne Admin-Rechte.



OpenClaw kann via `npm` ohne weitere administrative Rechte installiert werden.

`npm` ist ein JavaScript-Paketmanager mit hoher Verbreitung, der vor allem in der Software Entwicklung eingesetzt wird.

"Experimentierfreudige" Mitarbeitende installieren OpenClaw ohne Kenntnis des Unternehmens.

Supply Chain Angriff: Andere Software installiert OpenClaw als Paket-Abhängigkeit

TEIL III · ABSICHERUNG

Was Unternehmen mindestens tun sollten.

Technisch: Anerkennen und Eindämmen.

Die Nutzung zu verhindern ist nicht realistisch.

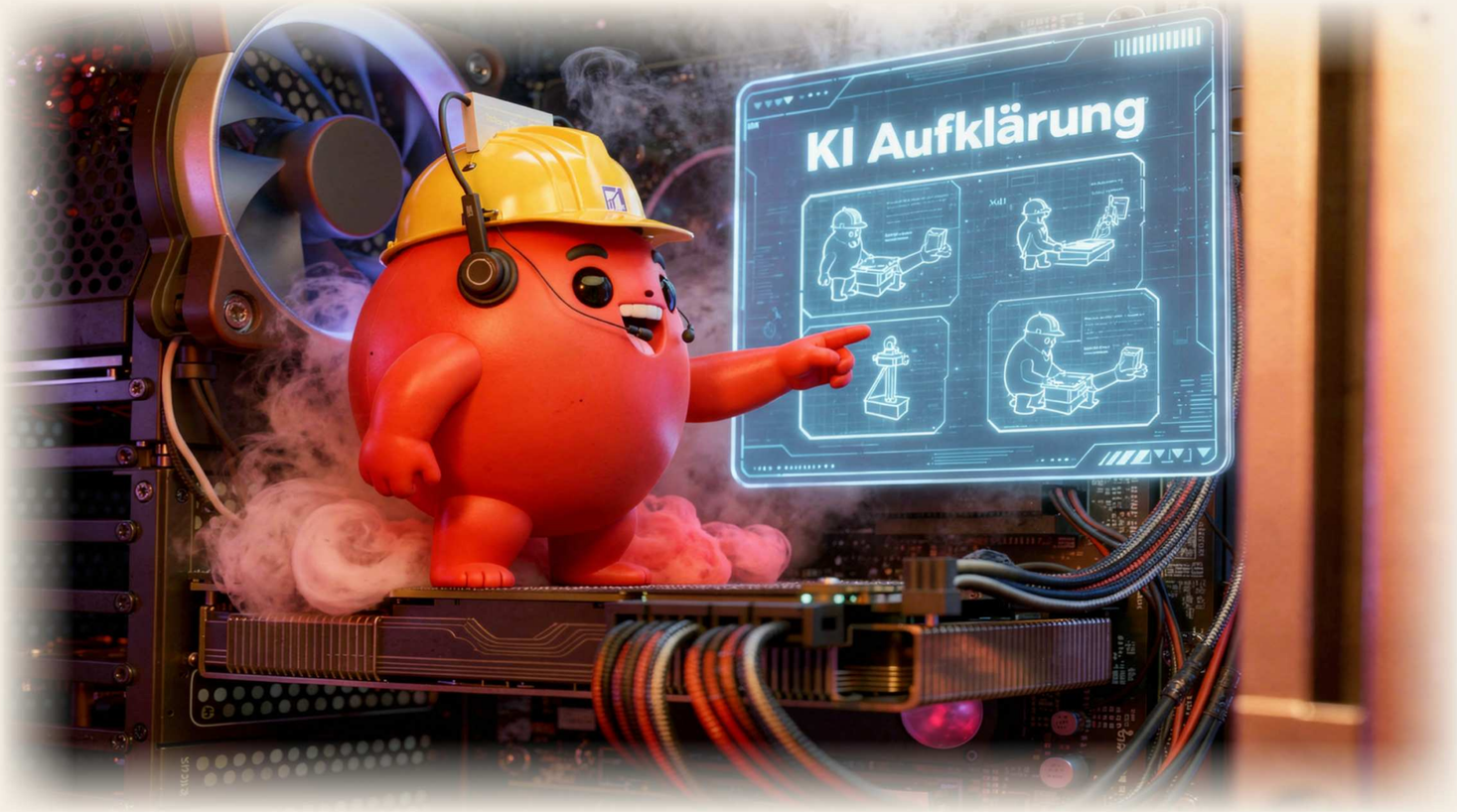
Sinnvoller: gedanklich annehmen, jedes Gerät könnte bereits befallen sein.

Effekt und Ausmass reduzieren durch Hürden, die ein automatisiertes System schwer überspringt.

Isolation durch Zero Trust, RBAC, PAM/MFA etc.

Auf den Ernstfall vorbereitet sein wird zur Pflicht (Playbooks).

Organisatorisch: Aufklärung und Governance.



Vorfälle passieren meist durch Unwissenheit und Unachtsamkeit.

Schulung und Aufklärung entwickeln die Achtsamkeit, und trainieren die Intuition.

Governance, definiert den Rahmen, regelt den Normalbetrieb und macht Abläufe zur dokumentierten Routine.

Drei Sätze zum mitnehmen.

i. KI-Agenten entwickeln sich zum skalierbaren persönliche KI-Assistenten; nicht sicher und meist ausserhalb der IT-Kontrolle.

ii. Die Installation, Nutzung und Weiterentwicklung ist meist bereits mit den vorhandenen Nutzungsrechten möglich.

iii. Sicherheitsstrategien müssen von kompromittierten Systemen und Endgeräten ausgehen. Mechanismen existieren um das Ausmass im Schadensfall zu begrenzen.

Vielen Dank.
Bleiben wir in Kontakt.

Philipp Kuntschik

Fachexperte für autonome KI-Systeme

MAIL: PHILIPP @ KUNTSCHIK.ONLINE

DECK: HTTPS://KUNTSCHIK.ONLINE/OPENCLAW-DEMO

SCAN FÜR LINKEDIN