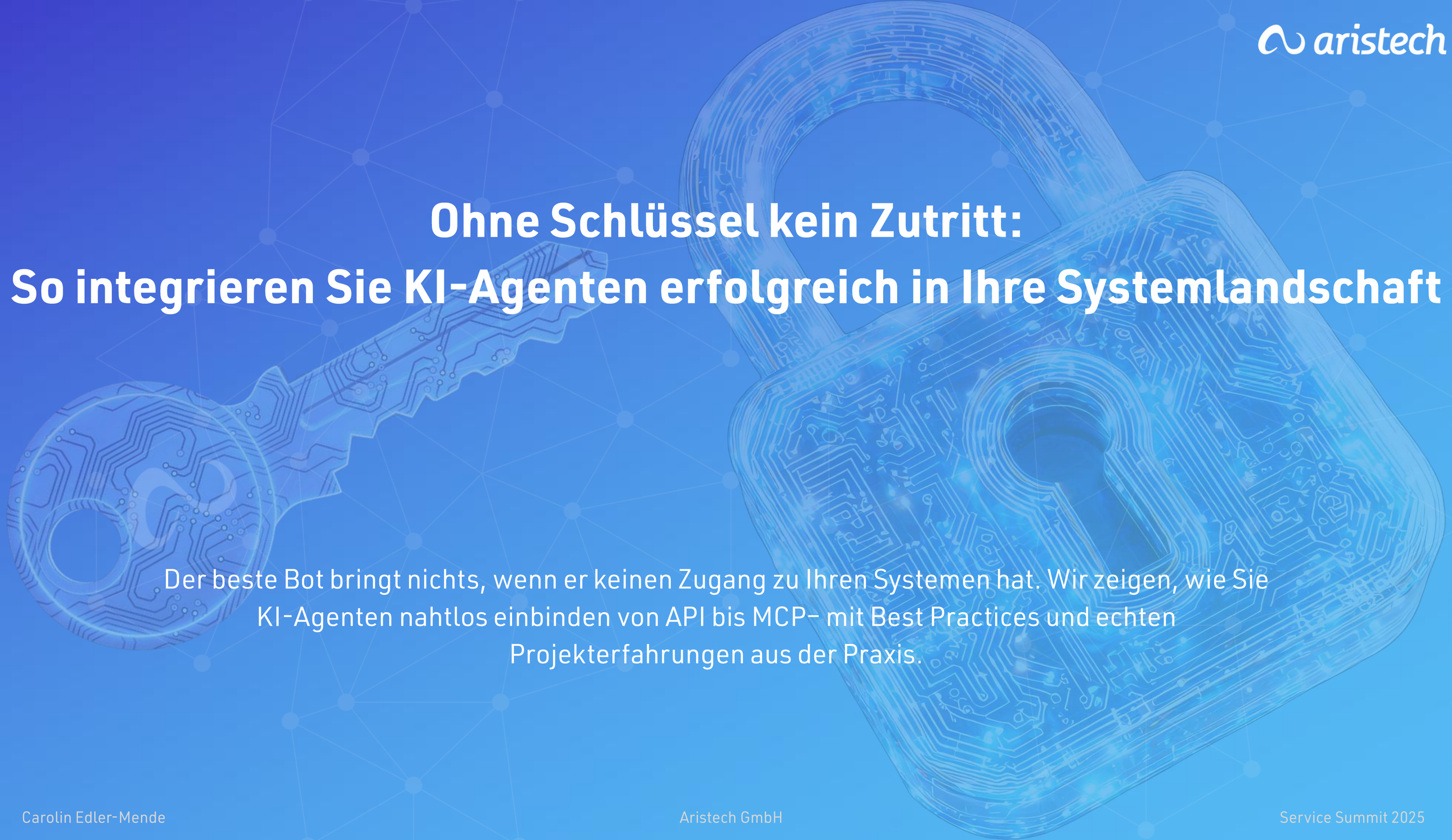
Ohne Schlüssel kein Zutritt:
So integrieren Sie KI-Agenten erfolgreich in Ihre Systemlandschaft

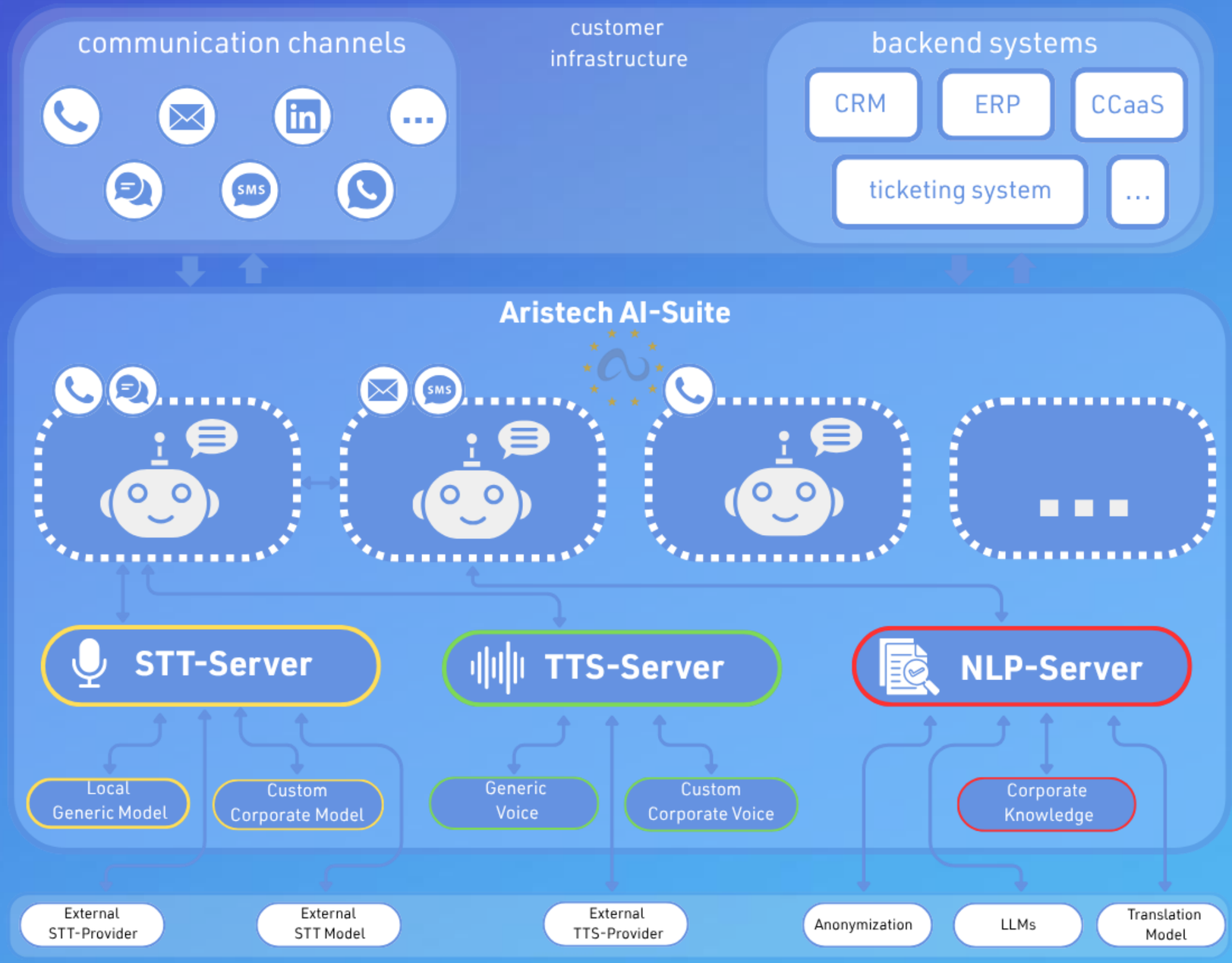


Der beste Bot bringt nichts, wenn er keinen Zugang zu Ihren Systemen hat. Wir zeigen, wie Sie KI-Agenten nahtlos einbinden von API bis MCP– mit Best Practices und echten Projekterfahrungen aus der Praxis.

Carolin Edler-Mende

Aristech GmbH

Carolin Edler-Mende
CEO und Co-Gründerin von Aristech
Vorreiter im Bereich Voice AI
Über 10 Jahre Erfahrung

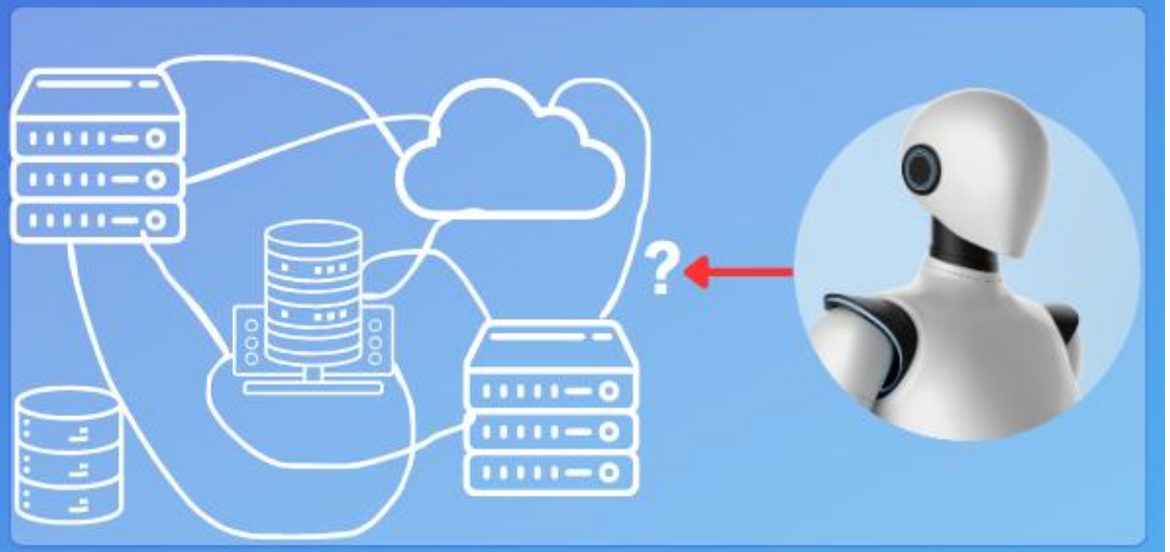

communication channels
customer infrastructure
backend systems
CRM
ERP
CCaaS
ticketing system
...
SMS
Aristech AI-Suite
STT-Server
TTS-Server
NLP-Server
Local Generic Model
Custom Corporate Model
Generic Voice
Custom Corporate Voice
Corporate Knowledge
External STT-Provider
External STT Model
External TTS-Provider
Anonymization
LLMs
Translation Model

KI-Potenzial bleibt oft ungenutzt

- **85 %** versprechen sich Effizienzsteigerung durch KI – nur **39 %** spüren sie im Alltag
- **56 %** nennen fehlende Integration als Hauptproblem

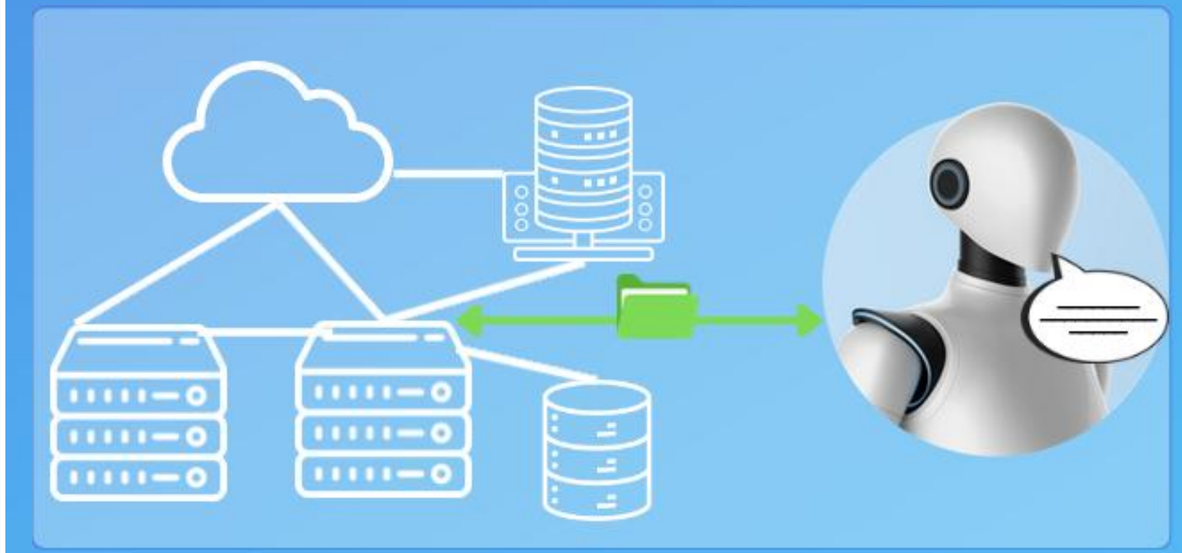
Problem

- Komplexe IT-Umgebung
- Uneinheitliche Daten- & Schnittstellenstrukturen
- Fehlende zentrale Integrationsarchitektur

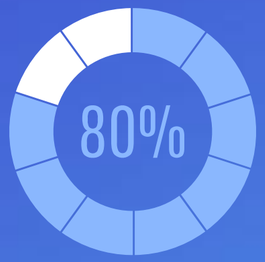


Lösung

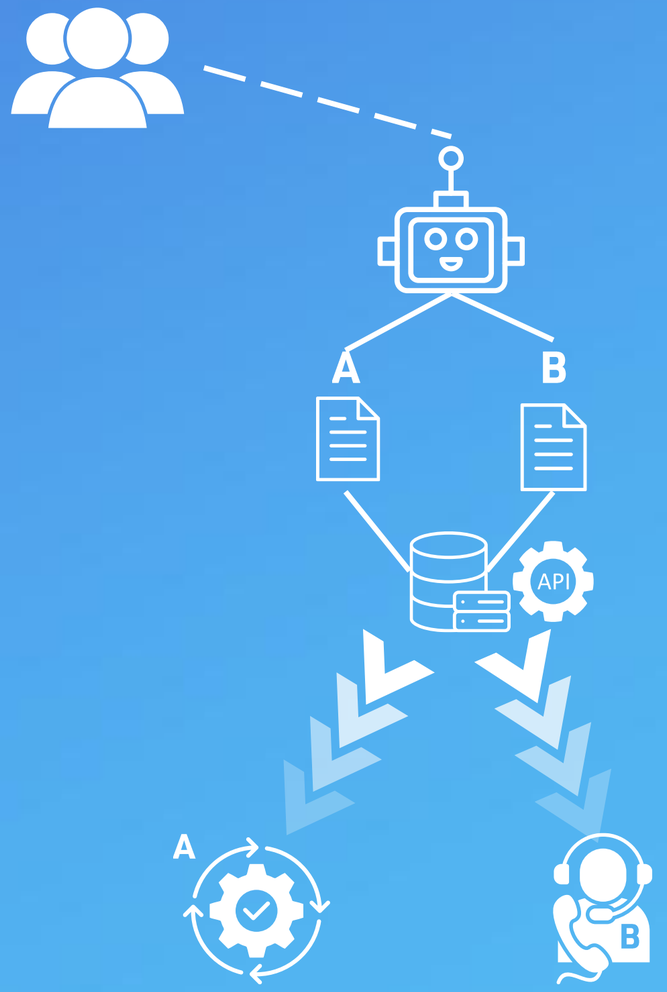
- Struktur schaffen
- Bots an Architektur anbinden
- Integration



Wo Automatisierung heute schon echten Mehrwert bringt



- Zahlungen / Rechnungen
- Technische Probleme
- Vertrags- / Produktfragen



Automatisierung wirkt am besten bei Routinefällen

- schneller
- günstiger
- sicherer

erfordert Zugriff auf Systeme

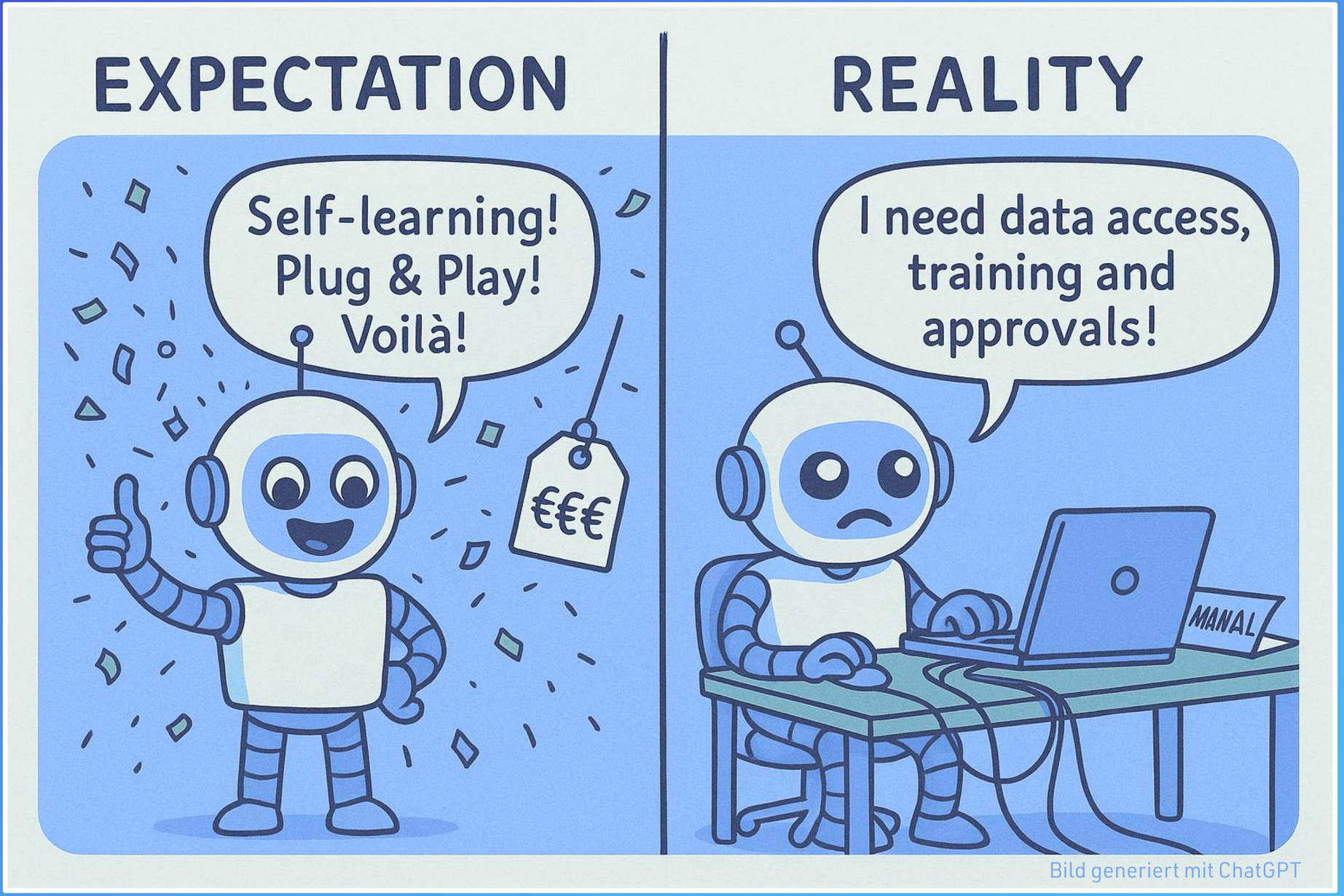
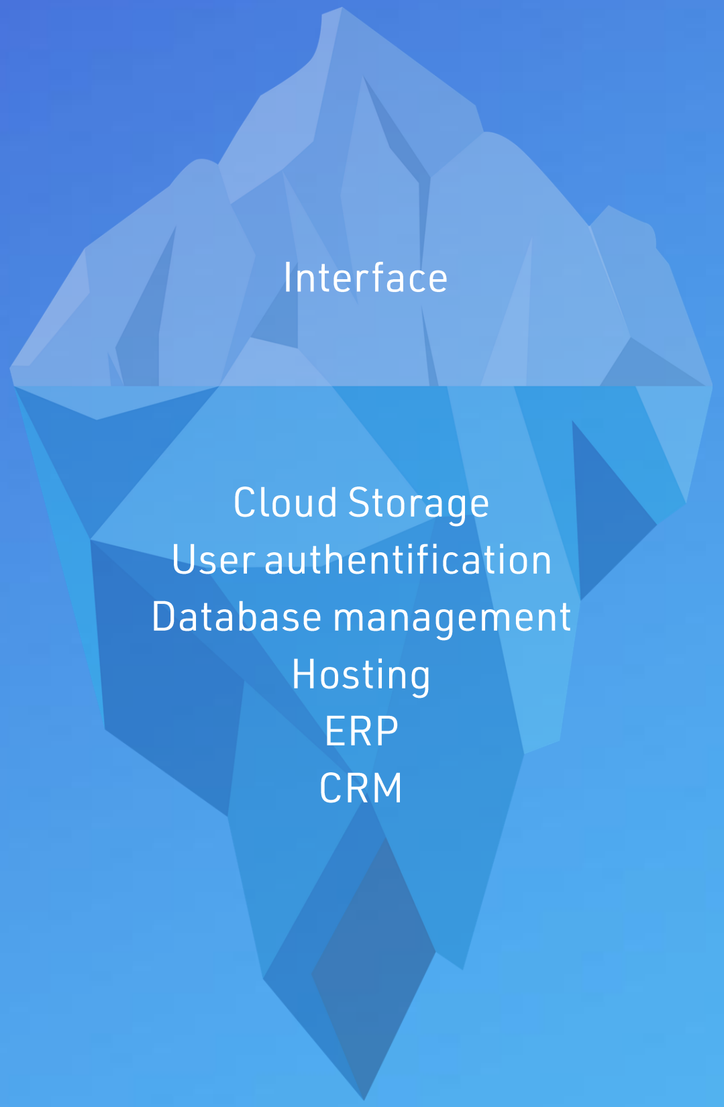


Bild generiert mit ChatGPT

aristech

Mythos

Standardschnittstellen
Plug & Play



Realität

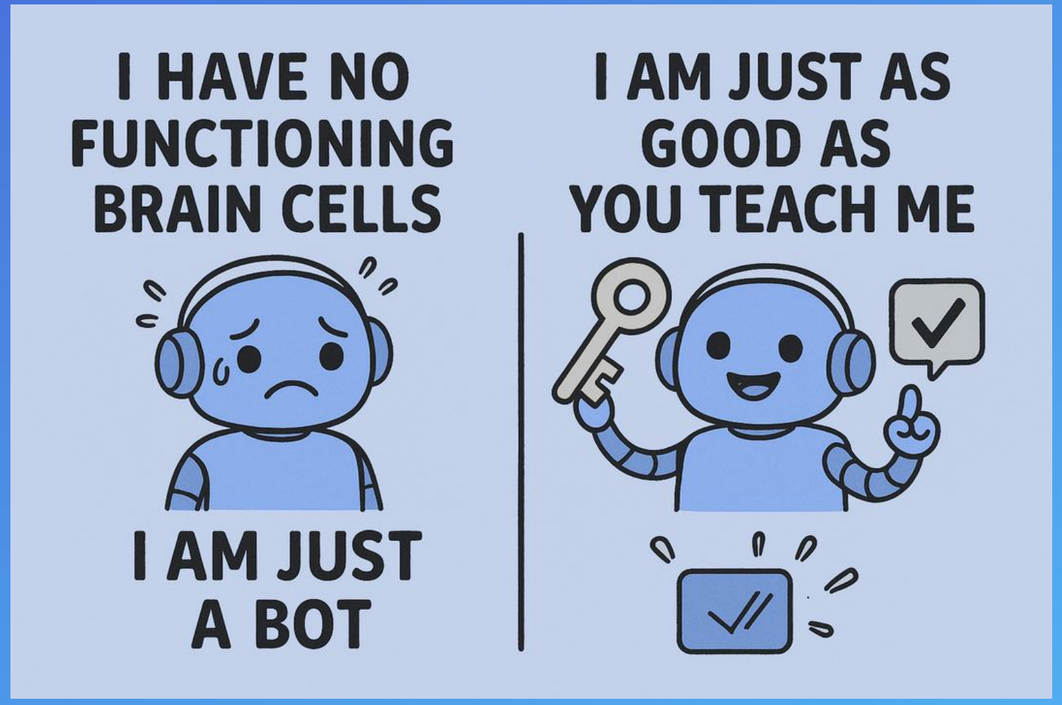
Kein Standardprozess
Systeme, Rechte, Limits variieren

Was ist zu tun?

- Systemanalyse statt Annahmen
- Übersicht über benötigte Systeme und Schnittstellen schaffen
- IT-Ressourcen einplanen
- Rechte & Limits klar definieren
- Verantwortlichkeiten festlegen
- MCP mitdenken

Mythos

Autonom lernende Bots



Realität

Wissen braucht Pflege

Was ist zu tun?

- Wissenskonsolidierung
- Sichten verschiedener Wissensquellen
- Regelmäßige Pflege der Daten
- Redaktionsprozess definieren
- Verantwortlichkeiten klären
- Wissen über Schnittstellen verfügbar machen

Mythos

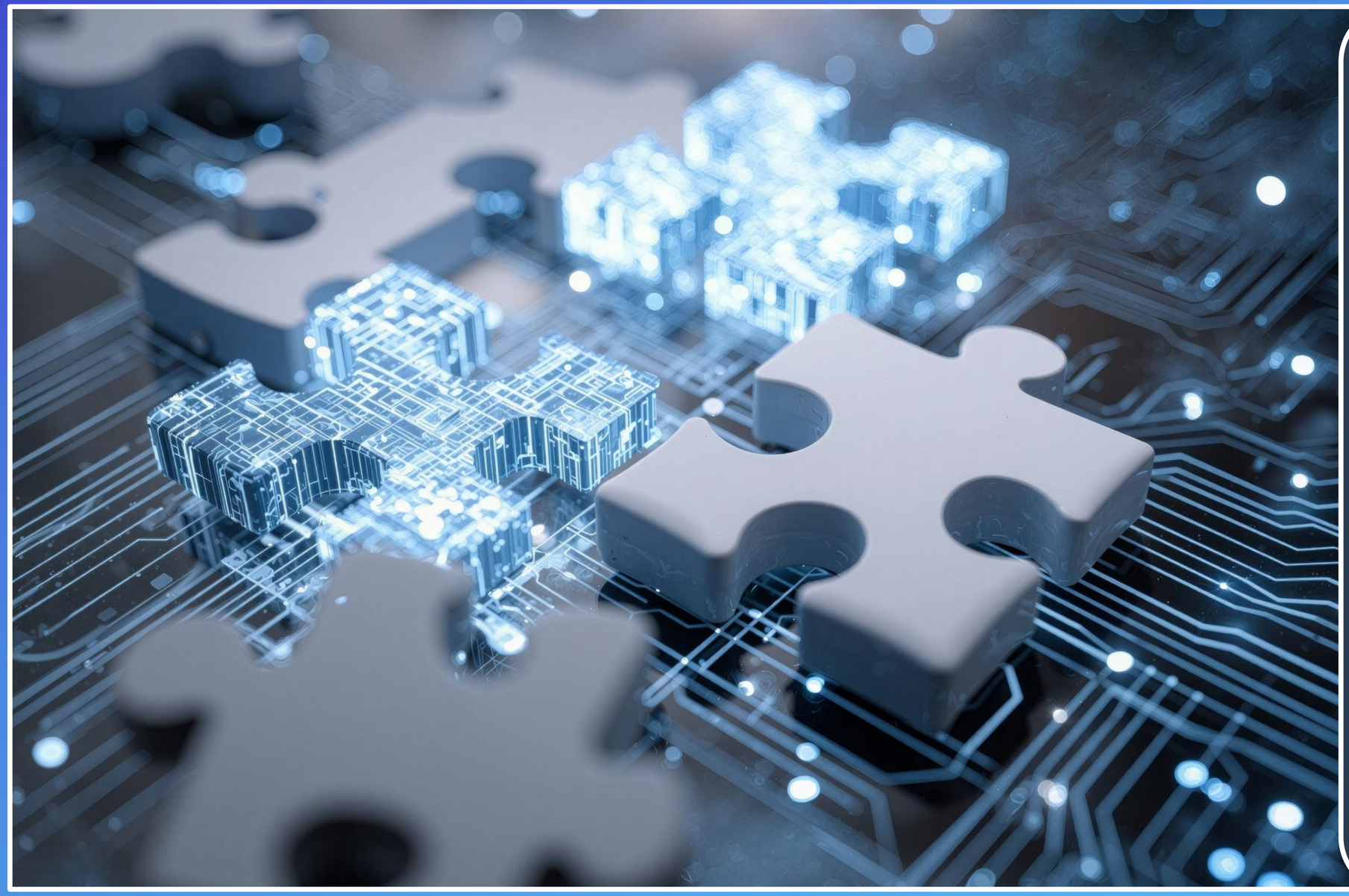
Freigaben erfolgen parallel

Realität

Freigaben brauchen Ownership

Was ist zu tun?

- Klare Verantwortlichkeiten definieren
- IT und Datenschutz von Beginn an einbeziehen
- Früh potentielle Grenzen in Erfahrung bringen
- Transparente Freigabeprozesse etablieren
- Kommunikation zwischen IT-Verantwortlichen direkt gestalten
- Verbindlichkeit schaffen



Die größten Zeitfresser

- Zuständigkeiten
- Zugriffsrechte
- Abstimmungsschleifen
- Wissenskonsolidierung

Untrainiertes LLM (ohne Regeln, ohne Anbindung)

Ich bin total enttäuscht. Mein Service funktioniert seit Tagen nicht und niemand hilft mir...

Oh, das tut mir sehr leid! Ich verstehe völlig, dass Sie verärgert sind. Wir übernehmen selbstverständlich die Verantwortung – Sie bekommen eine Gutschrift.

Echt? Wie viel bekomme ich?

Ich denke, 50 € wären angemessen. Ich veranlasse das sofort

Regelbasiertes LLM ohne Anbindung

Ich bin total enttäuscht. Mein Service funktioniert seit Tagen nicht und niemand hilft mir...

Das klingt wirklich ärgerlich, und ich verstehe, dass Sie eine schnelle Lösung möchten.

(System hat keine Anbindung)

Damit sich eine Servicemitarbeiterin darum kümmern kann, leite ich den Vorgang direkt weiter. Könnten Sie mir bitte Ihre Kundennummer nennen, damit die Weiterleitung korrekt erfolgt?

(Problemerkennung und korrektes Routing)

Regelbasiertes LLM mit Anbindung

Ich bin total enttäuscht. Mein Service funktioniert seit Tagen nicht und niemand hilft mir...

Das tut mir leid zu hören!
Ich prüfe sofort den aktuellen Status Ihres Anschlusses.

(Abfrage läuft im Ticketsystem ...)

Ich sehe, dass in Ihrem Gebiet seit Samstag eine Störung gemeldet ist.
Die Techniker sind informiert, voraussichtliche Behebung: heute bis 18 Uhr.

Okay, immerhin. Aber ich zahle seit Tagen für nichts – bekomme ich da etwas zurück?

Ja, laut unserer Gutschriftenrichtlinie stehtIhnen ab 48 Stunden Ausfall eine anteilige Erstattung zu. Für Ihren Zeitraum ergibt das 8,40 €, die ich direkt gutschreiben kann. Möchten Sie das?

(CRM- und Abrechnungssystem werden verbunden ...)

Ja, bitte.

Erledigt. Die Gutschrift wurde Ihrem Kundenkonto gutgeschrieben und erscheint automatisch auf der nächsten Rechnung.
Sie erhalten gleich eine Bestätigung per E-Mail.

(Aktion & Follow-up ausgelöst, FCR ...)

Wow, das ging schnell. Danke!

Sehr gern – und danke für Ihre Geduld!

(Proaktive Anfragenerkennung...)

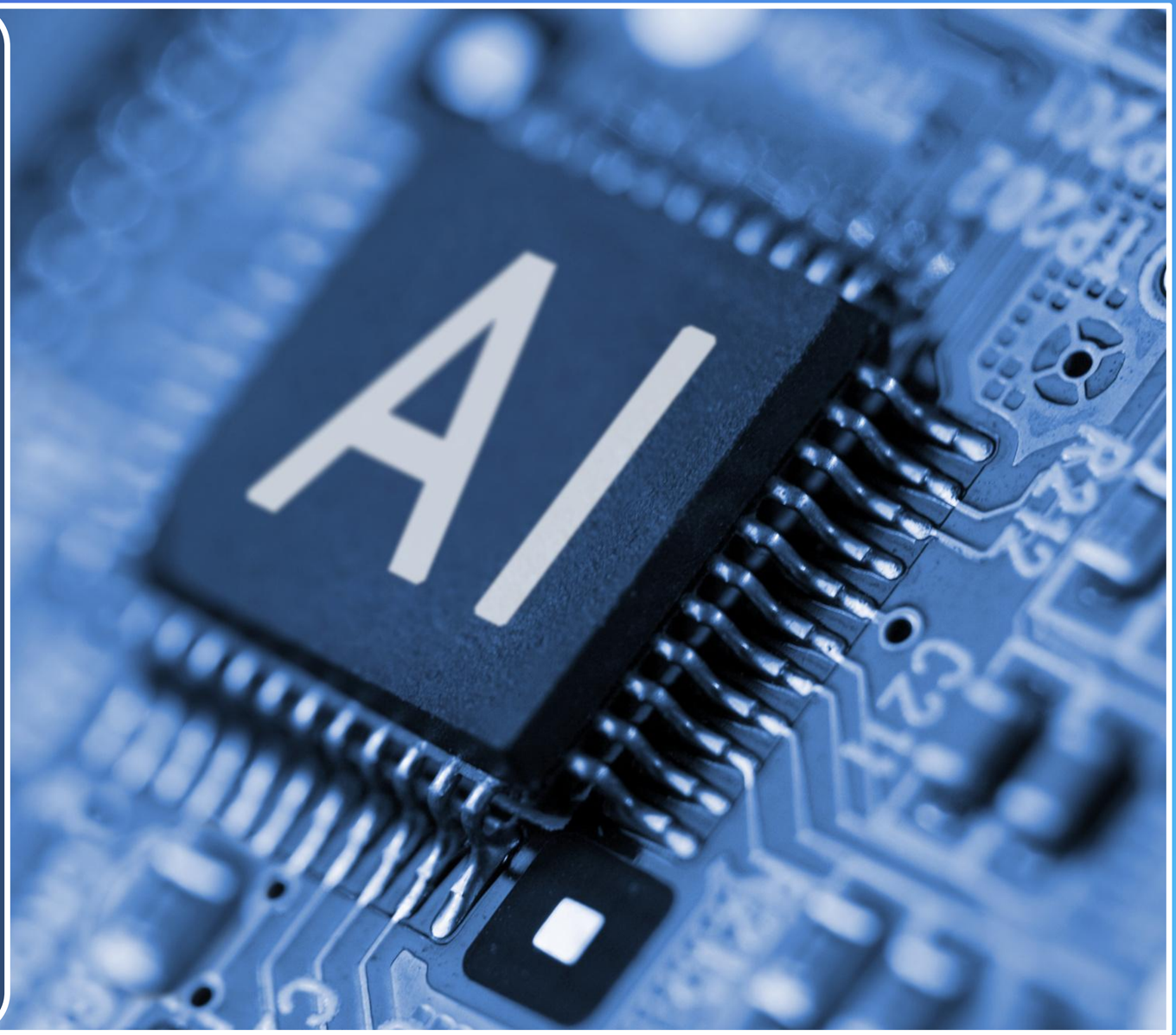
Übrigens sehe ich, dass Ihr Router-Update seit zwei Monaten aussteht.
Möchten Sie, dass ich den automatischen Neustart plane, sobald die Verbindung wieder stabil ist?

Herausforderung: Systemzugriff GenAI

Warum sichere Zugriffe bei GenAI entscheidend sind

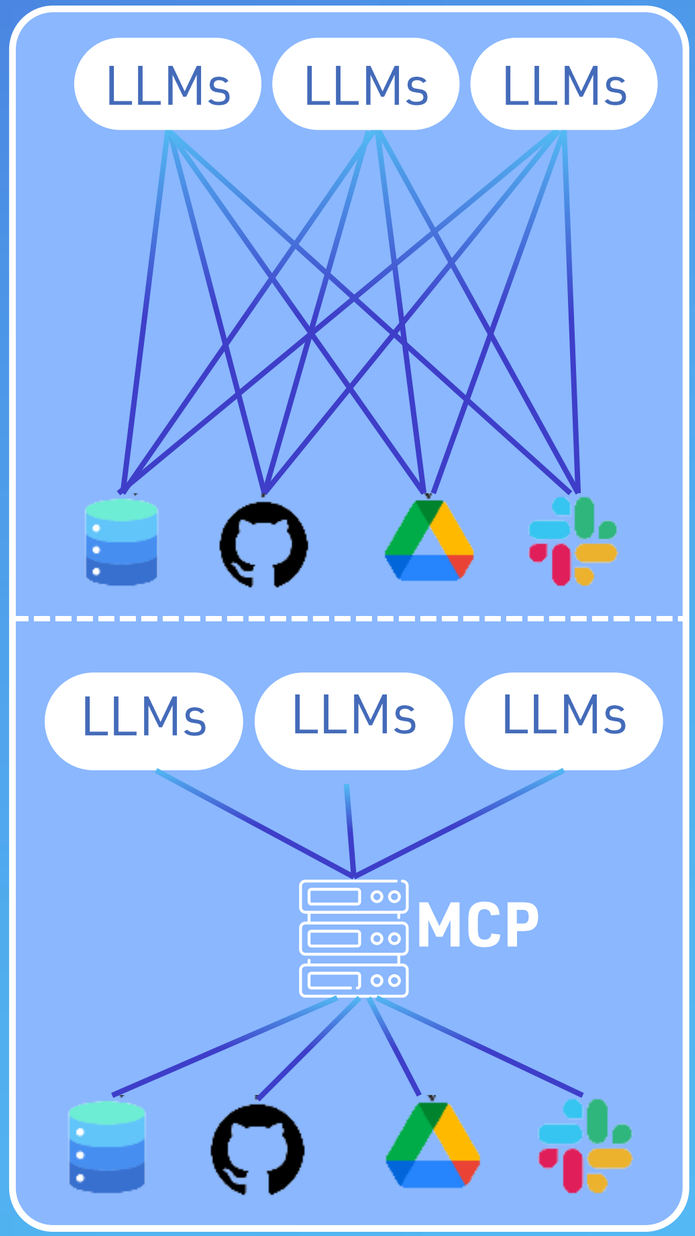
- KI kann nur dann Mehrwert liefern, wenn sie auf relevante Daten zugreifen darf
- Genau dieser Zugriff ist der kritischste Punkt
- Ohne klare Regeln entstehen Risiken und Intransparenz
- Es braucht einen strukturierten, sicheren Vermittlungsweg

GenAI ist nur so gut wie der Zugriff,
den sie bekommt –
und den man kontrolliert.



MCP –Dolmetscher zwischen KI und Unternehmenssystemen

- MCP = Model Context Protocol
- Offener Standard für sicheren, nachvollziehbaren Zugriff von KI auf Systeme
- Funktioniert wie ein „Gatekeeper“ zwischen KI und internen Tools
- Prüft jede Anfrage und gibt nur erlaubte Informationen weiter



Die Vorteile von MCP auf einen Blick

Sicherheit

Effizienz

Skalierbarkeit

Best Practises

Ziele & Architektur klären

Abstimmung mit IT & Systemverantwortlichen

Datenschutz & Governance sicherstellen

Betrieb & Wartung planen

MCP ist das Sicherheitsgeländer für **produktive KI-Integrationen!**

- Keine Automatisierung ohne Integration
- Nie Plug & Play
- Kompetente Partner

Jetzt Termin vereinbaren

SCAN ME

Stand: **L03**

sprache@aristech.de

06221 438590

Galileistraße 1-3,
69115 Heidelberg

Carolin Edler-Mende