Tech Industry Leadership
KI, Automatisierung und Führung



Unternehmens-KI:

Baue ich mir gerade die nächste IT-Falle?

Drei Strategien für den Aufbau deiner KI-Infrastruktur – und warum die falsche Entscheidung dich in einigen Jahren teuer zu stehen kommen kann.

18. Oktober 2026

Erinnerst du dich noch an die Zeiten, als jedes zweite mittelständische Unternehmen sein eigenes ERP-System entwickeln ließ?

Da gab es den genialen Programmierer, der die Prozesse des Unternehmens kannte wie seine Westentasche. Er entwickelte eine Software, die genau das machte, was das Unternehmen brauchte. Nicht mehr und nicht weniger.

Die Geschäftsführung war begeistert. Endlich keine teuren Standardlösungen mit Funktionen, die sowieso niemand brauchte!

Und dann?

Der Programmierer wechselte den Arbeitgeber. Oder der kleine Softwareanbieter wurde verkauft. Vielleicht ging er auch einfach pleite.

Plötzlich gab es keine Updates mehr. Schnittstellen funktionierten nicht mehr. Neue Anforderungen ließen sich nur mit erheblichem Aufwand umsetzen.

Ich habe selbst erlebt, wie ein ERP-Ausfall ein Unternehmen fast zwei Wochen lahmgelegt hat. Das hätte uns damals die Existenz kosten können.

Warum erzähle ich dir das?

> **Weil ich gerade beobachte, wie sich bei der Einführung von KI in Unternehmen eine ganz ähnliche Entwicklung anbahnt.**

Und ich frage mich ernsthaft, ob wir aus der Vergangenheit eigentlich etwas gelernt haben.

Drei Wege zur eigenen KI – aber welcher führt in die Zukunft?

Wer heute KI im Unternehmen etablieren möchte, hat grundsätzlich drei Möglichkeiten:

1

Ein eigenes Sprachmodell betreiben und intern zur Verfügung stellen.

2

Individuelle KI-Lösungen für das Unternehmen programmieren lassen.

3

Auf eine professionelle KI-Unternehmens-plattform setzen, die Modelle, Agenten und Automatisierung integriert.

Alle drei Ansätze haben ihre Berechtigung. Aber sie unterscheiden sich erheblich darin, wie sicher, flexibel und zukunftsfähig sie sind.

Und genau darum geht es mir heute.

1 Das eigene Sprachmodell: Alles unter Kontrolle. Wirklich?

Eine Strategie, die ich gerade bei sicherheitsbewussten Unternehmen häufiger sehe, ist das Hosting eines eigenen Sprachmodells.

Ein Open-Weight-Modell wird auf der eigenen Infrastruktur installiert. Die Mitarbeiter erhalten einen internen Chatbot und können damit arbeiten.

Der große Vorteil liegt auf der Hand:

Die Daten müssen das Unternehmen nicht verlassen. Man hat die technische Kontrolle über Infrastruktur, Zugriffe und Verarbeitung.

Gerade bei sensiblen Unternehmensdaten ist das ein starkes Argument.

> **Aber Vorsicht: Ein eigener Server ist noch keine Compliance-Strategie!**

Abgesehen davon, dass die dafür notwendige Infrastruktur anspruchsvoll ist, bleiben Datenschutz, Berechtigungen, Protokollierung, Sicherheitsupdates und die Einhaltung regulatorischer Anforderungen ebenfalls weiterhin Aufgaben des Unternehmens.

Und es gibt noch einen zweiten Punkt, der gerne übersehen wird.

Ein Sprachmodell ist zunächst einmal ein Sprachmodell. Es kann Fragen beantworten, Texte analysieren, Inhalte erstellen und vieles mehr. Aber damit hast du noch keine umfassende KI-Infrastruktur.

Was ist mit Agenten, die selbstständig Aufgaben übernehmen? Mit Projekten, dauerhaft verfügbaren Wissensquellen, wiederverwendbaren Skills, Schnittstellen zu ERP und CRM oder automatisierten Workflows?

Natürlich lassen sich solche Funktionen auch um selbst gehostete Modelle herum entwickeln.

Aber sie sind nicht automatisch vorhanden. Du musst sie zusätzlich aufbauen, integrieren und warten. Und jeder einzelne Schritt braucht Zeit und kostet wieder Entwicklungsbudget.

Und während deine IT-Abteilung noch an der nächsten Schnittstelle arbeitet, sind möglicherweise bereits neue Modellgenerationen auf dem Markt.

Das ist die nächste Herausforderung.

> **Ein eigenes Modell bleibt auf dem Entwicklungsstand, auf dem du es betreibst – bis du selbst für ein Update sorgst.**

Neue Versionen müssen bewertet, getestet, gegebenenfalls angepasst und ausgerollt werden. Hardwareanforderungen können sich ändern und zusätzliche Investitionen erforderlich machen. Bestehende Anwendungen müssen erneut geprüft werden.

Du bist also nicht nur Anwender von KI. Du wirst auch zum Betreiber einer eigenen KI-Infrastruktur.

Das kann sinnvoll sein, wenn du über die notwendigen Ressourcen verfügst oder sehr spezielle Sicherheitsanforderungen hast.

Aber für ein mittelständisches Unternehmen, das eigentlich Maschinen bauen, Komponenten entwickeln oder Kunden betreuen möchte?

Da würde ich mir schon die Frage stellen, ob das wirklich zum Kerngeschäft gehört.

2 Individuell programmierte KI-Lösungen: Maßgeschneidert oder maßgeschneiderte Abhängigkeit?

Kommen wir zur zweiten Strategie.

Ein Softwareanbieter entwickelt eine KI-Lösung speziell für dein Unternehmen. Sie schießen wie Pilze aus dem Boden, Startups, die solche Leistungen anbieten.

Und sie machen tatsächlich oft genau das, was du brauchst. Sie integrieren deine Prozesse und berücksichtigen deine Anforderungen. Ihre Lösungen können auf deinen eigenen Servern oder bei den Anbietern selbst betrieben werden. Und sie wagen sich durchaus auch an komplexe, unternehmensspezifische Prozesse heran.

Klingt hervorragend. Darunter sind zweifellos talentierte KI-Spezialisten mit beeindruckendem Know-how. Und tatsächlich können solche Lösungen technisch anfangs sehr leistungsfähig sein.

Nur: **Ein guter Programmierer ist noch lange kein langfristig verlässlicher Technologiepartner.**

Was passiert, wenn dein Anbieter in drei Jahren nicht mehr existiert?

Wenn seine beiden Entwickler das Unternehmen verlassen?

Wenn die nächste Modellgeneration grundlegende Anpassungen erfordert, für die niemand Kapazitäten hat?

Oder wenn du irgendwann den Anbieter wechseln möchtest?

Dann kann aus einer wunderbaren Individuallösung sehr schnell ein ziemlich teures Problem werden.

Deshalb würde ich bei individuell entwickelten KI-Lösungen vor Vertragsabschluss einige unangenehme Fragen stellen:

- **Wem gehört der individuell erstellte Code?** Erhältst du die notwendigen Nutzungsrechte oder gegebenenfalls den Quellcode, um die Lösung selbst weiterentwickeln zu lassen?
- **Ist die Lösung übertragbar?** Kann ein anderer Dienstleister sie übernehmen oder bist du dauerhaft an diesen Anbieter gebunden?
- **Wie gut ist sie dokumentiert?** Kann ein fremder Entwickler die Architektur, Schnittstellen und Abhängigkeiten nachvollziehen?
- **Wie werden Updates organisiert?** Wer sorgt dafür, dass neue Modelle, Sicherheitsanforderungen und Schnittstellen berücksichtigt werden?
- **Was passiert bei einem Ausfall des Anbieters?** Gibt es vertragliche Regelungen, Datenexporte, Übergabekonzepte oder gegebenenfalls eine Quellcode-Hinterlegung?

Und bitte frage nicht nur, ob die Lösung DSGVO-konform ist.

Lass dir erklären, **wie** Datenschutz und Datensicherheit technisch und organisatorisch gewährleistet werden.

Wo liegen die Daten? Welche Unterauftragnehmer sind beteiligt? Wer hat Zugriff? Welche Modelle werden für Embedding, Re-Ranking, Speech-to-Text-Funktionen und andere Verarbeitungsschritte verwendet und kannst du diese frei wählen? Werden Eingaben oder Ergebnisse für das Modelltraining verwendet? Wie werden Sicherheitsvorfälle behandelt?

Eine schöne Präsentation ist kein Sicherheitskonzept. Und ein vertrauenswürdiger Verkäufer ersetzt keine überprüfbare technische Architektur.

3 Professionelle KI-Unternehmensplattformen: Warum ich diesen Ansatz bevorzuge

Jetzt kommen wir zur dritten Möglichkeit, einer Strategie, die ich für viele mittelständische Industrieunternehmen für besonders interessant halte.

Statt einzelne KI-Anwendungen immer wieder neu entwickeln zu lassen, setzt du auf eine professionelle Unternehmensplattform.

Eine Plattform, die verschiedene Sprachmodelle einbinden kann, Agenten verwaltet, Unternehmenswissen kontrolliert zugänglich macht und klassische Automatisierung mit KI kombiniert.

Warum ist mir gerade dieser letzte Punkt so wichtig? Weil nicht jeder Prozess KI braucht!

Stell dir einen technischen Kundenservice vor. Ein Kunde möchte wissen, wann sein Ersatzteil geliefert wird. Dafür muss eine KI nicht kreativ werden.

Die KI muss die Anfrage verstehen, fehlende Angaben erfragen und die Auftragsnummer erkennen. Die Berechtigungsprüfung und die Abfrage des Lieferstatus können dagegen über zuverlässige, regelbasierte Schnittstellen zum ERP-System erfolgen, deren Richtigkeit keiner Wahrscheinlichkeitsrechnung unterliegt. Anschließend kann die KI die Information verständlich und empathisch an den Kunden weitergeben.

> **Die Kunst liegt darin, KI dort einzusetzen, wo sie einen Mehrwert bietet – und klassische Automatisierung dort, wo ein Prozess zuverlässig, sicher und nach festen Regeln funktionieren muss.**

Deshalb bevorzuge ich Plattformanbieter, die nicht erst seit dem KI-Boom Software entwickeln, sondern bereits Erfahrung mit Unternehmensprozessen, Integration und Automatisierung mitbringen.

Solche Plattformen können weitere Vorteile bieten.

Modellunabhängigkeit:	Du kannst unterschiedliche Sprachmodelle für unterschiedliche Aufgaben einsetzen. Ein Modellwechsel muss nicht bedeuten, dass du deine komplette Anwendung neu entwickeln musst.
Zentrale Governance:	Zugriffsrechte, Datenquellen, Protokollierung und Sicherheitsregeln können übergreifend verwaltet werden.
Wiederverwendbarkeit:	Einmal entwickelte Agenten, Integrationen und Workflows können als Grundlage für weitere Anwendungen dienen.
Skalierbarkeit:	Aus einem ersten KI-Agenten im Service können später Anwendungen für Vertrieb, Einkauf, Qualitätssicherung und Entwicklung werden.
Flexibilität:	Prompts in Klartext, die alle einsehbar, durch das Unternehmen anpassbar und beim Unternehmen sicherbar sind. So können Agenten, Compliance-Prompts, Skills und Projekte jederzeit relativ einfach auf andere Standardanbieter umgezogen werden.

Natürlich gilt auch hier: Nicht jede Plattform bietet alle diese Funktionen. Und nicht jede versprochene Modellunabhängigkeit funktioniert in der Praxis problemlos.

Deshalb muss man genau hinsehen.

Ein Modell-Update. Ein Ausfall. Und plötzlich steht dein Prozess still.

Es gibt noch einen Aspekt, den ich für besonders kritisch halte.

Solange du KI nur für gelegentliche Recherchen nutzt, ist ein Modellausfall ärgerlich, aber meistens verkraftbar.

Was passiert aber, wenn deine KI-Agenten wichtige Unternehmensprozesse übernehmen? Wenn Angebote vorbereitet, Kundenanfragen bearbeitet oder Informationen zwischen verschiedenen Systemen automatisch verarbeitet werden?

Und dann fällt das verwendete Sprachmodell aus. Oder ein Update verändert sein Verhalten so stark, dass dein Agent nicht mehr zuverlässig arbeitet.

Genau deshalb halte ich es für gefährlich, eine gesamte KI-Infrastruktur fest an ein einziges Modell zu koppeln.

Eine geeignete Unternehmensplattform sollte es ermöglichen, Modelle und Agenten voneinander zu trennen.

Der Agent bleibt bestehen. Das zugrunde liegende Modell kann bei Bedarf ausgetauscht werden. Natürlich muss auch das Ersatzmodell getestet werden. Ein Wechsel funktioniert nicht bei jeder Anwendung auf Knopfdruck.

Aber eine vorbereitete Ausweichmöglichkeit kann den Unterschied zwischen einer vorübergehenden Einschränkung und einem längeren Prozessstillstand ausmachen.

> **Ausfallsicherheit beginnt nicht erst beim Backup. Sie beginnt bei der Architekturentscheidung.**

Wie groß muss ein verlässlicher KI-Anbieter sein?

Über Größenordnungen kann man sicher streiten. Aber grundsätzlich würde ich bei der Auswahl eines strategischen KI-Plattformpartners durchaus auf eine Unternehmensgröße achten, die am Markt auch schwierige Zeiten überstehen kann.

Für mich sind etwa 25 bis 30 Mitarbeiter eine sinnvolle Orientierungsgröße, wenn ein Anbieter langfristig kritische Unternehmensprozesse betreuen soll.

Nicht, weil kleinere Unternehmen automatisch schlechter wären. Im Gegenteil. Gerade kleine Teams können enorm innovativ sein. Aber Innovation ist nur ein Teil der Aufgabe.

Wer eine unternehmenskritische Plattform betreibt, muss auch dann zuverlässig liefern, wenn zwei Entwickler gleichzeitig krank werden, ein Mitarbeiter kündigt oder mehrere Kunden dringend Unterstützung benötigen.

Dazu braucht es Kapazitäten für Entwicklung, Betrieb, Sicherheit, Support und Weiterentwicklung.

Ein Unternehmen mit fünf Mitarbeitern kann diese Leistungen möglicherweise über ein starkes Partnernetzwerk sicherstellen. Aber was passiert, wenn wichtige Partner wegfallen oder kurzfristig nicht verfügbar sind? Dann ist möglicherweise plötzlich niemand mehr erreichbar, wenn die Agenten ausfallen.

Die Mitarbeiterzahl ist für mich kein abschließender Qualitätsbeweis, aber ein erster Hinweis auf die mögliche Belastbarkeit des Anbieters.

Entscheidend ist, welche Kompetenzen, Vertretungsregelungen und Servicekapazitäten tatsächlich vorhanden sind.

Meine Checkliste: Sieben Fragen, bevor du dich für einen KI-Partner entscheidest

Wenn ich heute als Geschäftsführerin eine strategische KI-Entscheidung treffen müsste, würde ich mir vor allem diese sieben Fragen beantworten lassen.

1 **Wie unabhängig bleibe ich?**

Kann ich Modelle wechseln, meine Daten exportieren und gegebenenfalls zu einem anderen Anbieter umziehen?

2 **Wem gehören meine Anwendungen und mein Wissen?**

Was passiert mit meinen Agenten, Workflows, Prompts, Wissensdatenbanken und Integrationen, wenn ich den Vertrag beende?

3 **Wie wird Sicherheit nachgewiesen?**

Gibt es ein nachvollziehbares Sicherheitskonzept, klare Verantwortlichkeiten, vertragliche Datenschutzregelungen und überprüfbare technische Schutzmaßnahmen?

4 **Wie zukunftsfähig ist die Architektur?**

Können neue Modelle, Funktionen und Schnittstellen integriert werden, ohne jedes Mal bei null anzufangen?

5 **Wie viel Erfahrung hat der Anbieter mit realen Unternehmensprozessen?**

Kann er KI mit klassischer Automatisierung kombinieren? Kennt er die Anforderungen an ERP-Anbindungen, Rollenrechte und stabile Betriebsprozesse?

6 **Wer betreut mich in drei Jahren?**

Wie ist der Support organisiert? Gibt es Vertretungen, verbindliche Reaktionszeiten und einen nachvollziehbaren Entwicklungsplan?

7 **Was passiert, wenn etwas schiefgeht?**

Gibt es Backups, Wiederanlaufpläne, alternative Modelle und ein klares Vorgehen bei Ausfällen oder beim Wegfall des Anbieters?

Mein Tipp: Lass dir die Antworten nicht nur erklären. Lass sie dir demonstrieren und möglichst vertraglich zusichern. Ein Anbieter, der wirklich gut aufgestellt ist, sollte mit solchen Fragen kein Problem haben.

Mein Fazit: Du kaufst keine KI. Du entscheidest über deine zukünftige Handlungsfähigkeit.

Ich bin Maschinenbau-Ingenieurin und habe über 30 Jahre in der technischen Industrie gearbeitet, davon viele Jahre in Führungspositionen.

Und wenn ich eines gelernt habe, dann das: Technische Entscheidungen werden selten nur wegen der Technik teuer. Sie werden teuer, wenn man die langfristigen Konsequenzen nicht ausreichend berücksichtigt.

Eine KI-Lösung, die heute hervorragend funktioniert, kann in wenigen Jahren zu einer kostspieligen Sackgasse werden.

Nicht, weil die Technologie schlecht war. Sondern weil sie nicht weiterentwickelt werden konnte, der Anbieter verschwunden ist oder das Unternehmen sich zu stark von einer einzelnen Lösung abhängig gemacht hat.

Deshalb würde ich beim Aufbau einer KI-Infrastruktur nicht zuerst nach dem günstigsten Angebot oder der beeindruckendsten Demonstration fragen.

Ich würde fragen:

> **Mit welcher Architektur und welchem Partner kann mein Unternehmen auch in fünf Jahren noch flexibel, sicher und wettbewerbsfähig arbeiten?**

Am Ende ist die Wahl eines KI-Partners immer auch eine Vertrauensentscheidung.

Nur sollte dieses Vertrauen nicht auf einem Hochglanzprospekt beruhen, sondern auf überprüfbaren Fakten.

Und wie sieht es bei dir aus?

Hast du dich bereits für eine KI-Infrastruktur entschieden? Oder experimentieren deine Teams noch mit verschiedenen Einzellösungen? Mit welchen Erfahrungen?

Wenn du gerade vor der Entscheidung stehst, wie du KI langfristig in deinem Unternehmen aufbauen möchtest, lass uns darüber sprechen.

Ich unterstütze technische Unternehmen bei der Auswahl geeigneter KI-Plattformen, der Entwicklung sinnvoller Anwendungsfälle und der Implementierung in bestehende Prozesse.

Es geht darum, eine Lösung zu finden, die zu deinem Unternehmen passt und auch morgen noch sinnvoll ist.

Bleib neugierig – aber entscheide mit Weitblick!

Anita Renc



Über die Autorin

Anita Renc

KI-Consultant und Business Coach mit über 30 Jahren Industrie- und Führungserfahrung

info@futuresetup.de · futuresetup.de