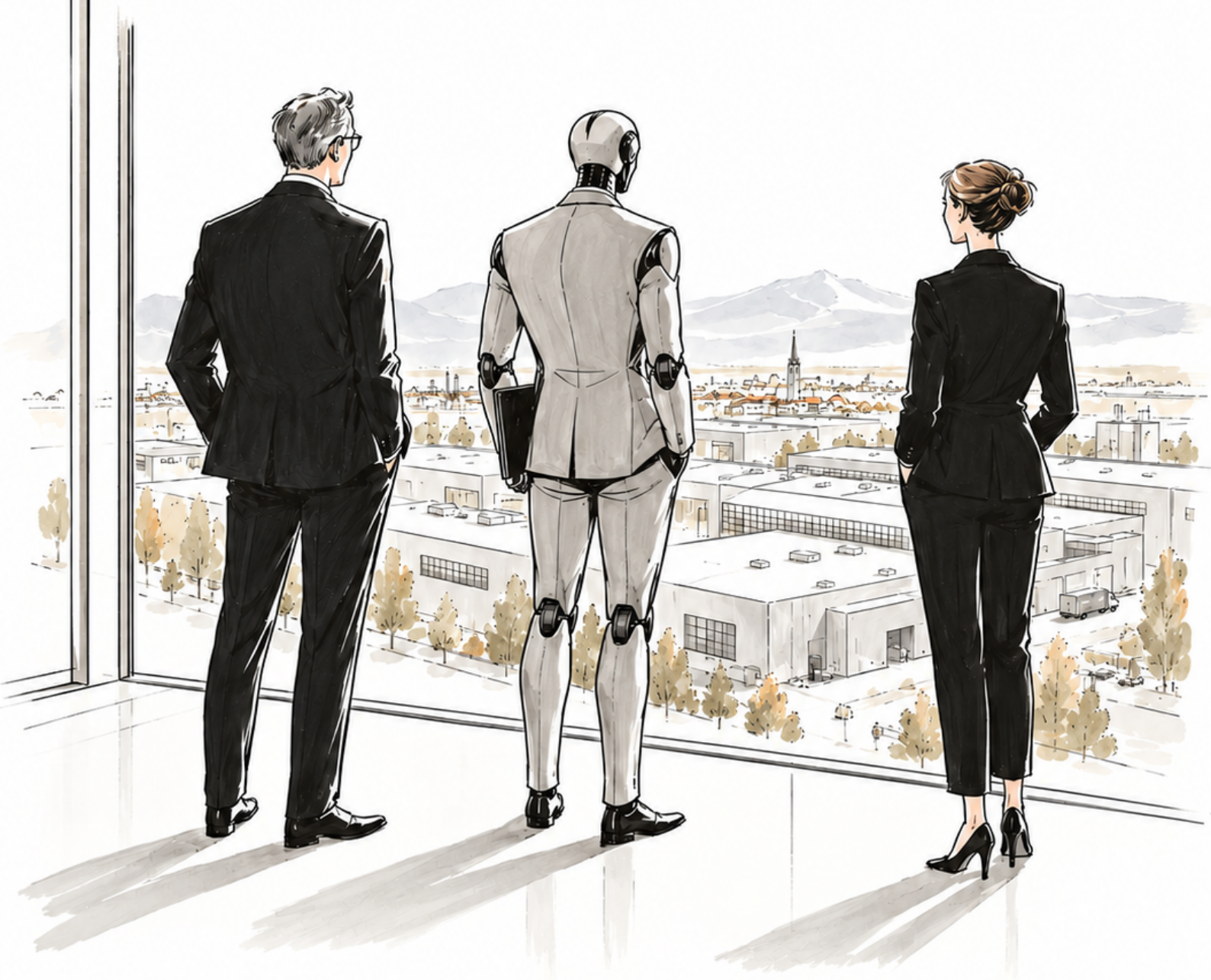


DER Dritte Mann

Wie KI-Agenten die industrielle
Wertschöpfung verändern

KUNDE · UNTERNEHMEN · AGENT



VORWORT · KLAUS WESSING

Der dritte Mann sitzt längst mit am Tisch

Kunde. Unternehmen. Agent. Wer entscheidet künftig, was der Kunde sieht - und von wem er kauft?

Wer über künstliche Intelligenz spricht, spricht oft über Modelle, Werkzeuge und Geschwindigkeit. Für ein Unternehmen ist eine andere Frage entscheidend: Welche Arbeit wird neu verteilt - und wer darf künftig Entscheidungen vorbereiten oder ausführen? Zwischen Kunde und Unternehmen tritt ein digitaler Stellvertreter. Er sucht, vergleicht, prüft und kann, wenn man ihn lässt, auch handeln. Diese Rolle ist nicht Zukunftsmusik in jedem Bereich; sie ist aber auch noch keine flächendeckende Realität.

Wir haben deshalb Befragungen von BCG, KPMG, McKinsey und Deloitte mit Forschung, Unternehmensangaben und internationaler Berichterstattung zusammengeführt. Die Quellen erzählen keine einheitliche Erfolgsgeschichte. Sie zeigen wachsende Experimente, einzelne produktive Anwendungen, erhebliche Unterschiede zwischen Branchen und eine große Lücke zwischen technischer Möglichkeit und belastbarem wirtschaftlichem Nutzen. Diese Unterschiede sind der Ausgangspunkt unserer Auswertung, nicht ein Störfaktor.

Für Unternehmen beginnt die Veränderung nicht erst dort, wo ein Agent selbstständig bestellt oder eine Maschine steuert. Sie beginnt früher: wenn ein System Informationen auswählt, Angebote vorsortiert, Wissen bündelt oder eine Entscheidung vorbereitet. Wer diese Vorstufen nicht gestaltet, überlässt anderen den Zugang zum Kunden und die Ordnung der eigenen Informationen. Wer sie vorschnell automatisiert, riskiert dagegen, Fehler schneller und schwerer nachvollziehbar zu verbreiten.

VORWORT · FORTSETZUNG

Nüchternheit ist eine Voraussetzung für Tempo

Die Industrie braucht keine größere Vision, sondern eine präzisere Grenze zwischen Vorschlag, Entscheidung und Handlung.

Gerade in der Industrie ist deshalb Nüchternheit eine Voraussetzung für Tempo. Ein Agent kann einen Prozess beschleunigen; er kann aber weder fehlende Stammdaten noch unklare Zuständigkeiten wegzaubern. Produktiv wird die Technik erst, wenn Daten, Abläufe, Rechte und menschliche Verantwortung zusammenpassen. Die Frage lautet nicht nur, was ein Modell kann. Sie lautet, was ein Unternehmen ihm anvertrauen darf - und wie es erkennt, wenn die Antwort falsch ist.

Dieses Dossier betrachtet die Entwicklung aus der Perspektive industrieller Wertschöpfung. Es verbindet Befragungen und Studien mit Fachbeiträgen, Medienberichten und konkreten Anbieterangaben. Dabei unterscheiden wir zwischen gemessenen Ergebnissen, Selbstauskünften, technischen Demonstrationen und Prognosen. Wo die Beleglage dünn ist, sagen wir es. Wo ein Nutzen plausibel erscheint, benennen wir die Bedingungen, unter denen er erst nachgewiesen werden muss.

Für die Industrie folgt daraus weder ein Ruf nach maximaler Autonomie noch ein Grund zum Abwarten. Unternehmen sollten ihre Kundenzugänge, Produktinformationen und Arbeitsabläufe so ordnen, dass digitale Akteure sie korrekt verstehen - und nur dort handeln, wo Verantwortung, Grenzen und Rückwege festgelegt sind. Die entscheidende Führungsaufgabe lautet: Produktivität und Wertschöpfung sichern, Wissen in der Arbeit verankern und Robotik und KI wirksam einbetten. Das ist kein Technikprogramm für sich. Es ist eine Führungsentscheidung.

DAS DOSSIER IN SIEBEN SÄTZEN

Was man vor der Lektüre wissen sollte

Der rote Faden führt von der Meta-Nachricht über industrielle Wertschöpfung zur strategischen Zukunftsfrage.

-
1. Agenten verschieben Wertschöpfung von einzelnen Aufgaben zu zusammenhängenden Ergebnissen.
 2. Multi-Agent-Systeme können Abläufe über Funktionen und IT-Systeme hinweg koordinieren.
 3. Menschen wechseln von Routineausführung zu Orchestrierung, Prüfung und Aufsicht.
 4. Schnellere Entscheidungen erhöhen Produktivität nur dann, wenn der Workflow neu gestaltet wird.
 5. Verlässliche Daten, Nachweise und klare Regeln sind die Grundlage für Vertrauen.
 6. Unternehmen sollten mit begrenzten Anwendungsfällen und sichtbaren menschlichen Kontrollpunkten beginnen.
 7. IT und OT müssen zusammenarbeiten, bevor Agenten in der Produktion handeln dürfen.

Der rote Faden: Meta News beschreibt den Eintritt des Agenten in die Marktbeziehung. Wertschöpfung zeigt, wo er bereits Arbeit übernimmt. Zukunft fragt, welche Rechte, Daten und Verantwortlichkeiten Unternehmen jetzt ordnen müssen.

TEIL I · META NEWS

Meta Muse trifft auf die Grenze des Marktplatzes

Die Nachricht ist größer als ein neues KI-Produkt: Ein digitaler Stellvertreter versucht zu handeln – und stößt auf die Regeln des Ortes, an dem der Kunde einkauft.

Meta stellte Muse im September 2026 als persönlichen Agenten vor, der Aufgaben über Apps und Webdienste hinweg übernehmen soll. Die Ankündigung verschiebt die Debatte: Es geht nicht mehr nur darum, ob KI eine Antwort findet. Ein Agent soll im Auftrag eines Menschen recherchieren, vergleichen, Formulare ausfüllen und gegebenenfalls Transaktionen anstoßen. Reuters berichtete zugleich über interne Tests, in denen das Produkt ins Stocken geraten sei und sensible Daten unberechtigt offengelegt worden seien. Produktversprechen und Sicherheitsbefund stehen damit von Beginn an nebeneinander.

Wenige Tage später sperrte Amazon Muse für Einkäufe auf seiner Plattform. Amazon verwies laut Medienberichten auf unerlaubten Agentenzugriff, fehlende Kennzeichnung und Sicherheitsbedenken; Meta hatte zum Start erklärt, sichere Login- und Zahlungsdaten seien dem Agenten nicht zugänglich. Der Streit ist deshalb mehr als ein technischer Fehler. Er legt offen, dass der Nutzer zwar delegieren kann, Plattformen aber weiterhin über Zugang, Identität, Daten und Transaktionsregeln entscheiden.

Eine Messung von DataDome macht die Bewegung sichtbar, ohne sie zu einem Erfolgsnachweis zu machen: Im eigenen Netzwerk registrierte das Unternehmen für Muse 29,1 Millionen Browser-Anfragen in den ersten zwölf Tagen voller Verfügbarkeit. 99,3 Prozent kamen dem Bericht zufolge aus Cloud- und CDN-Infrastruktur; 8,9 Prozent berührten sensible Abläufe wie Login, Warenkorb oder Zahlung. DataDome misst sein eigenes Netzwerk. Anfragen sind weder eindeutige Nutzer noch abgeschlossene Käufe und erlauben keine Hochrechnung auf das gesamte Internet.

Damit ist der Ausgangspunkt des Dossiers gesetzt: Meta News bis Wertschöpfung bis Zukunft. Ein Agent tritt zwischen Kunde und Anbieter; damit verschieben sich Auswahl, Empfehlung und Kundenwissen. Die Zukunftsfrage lautet, unter welchen Regeln digitale Akteure in Unternehmensprozesse eintreten dürfen. Die folgenden Praxisfälle zeigen konkrete Anwendungen - und die Grenzen ihrer Belege.

1 · Research bis 2 · Engineering bis 3 · Procurement bis 4 · Supply Chain 5 · Claims bis 6 · Commerce bis 7 · Payment Sieben operative Felder - keine zwingend lineare Prozesskette.

Der eigentliche Nachrichtenwert liegt damit nicht in der Existenz eines weiteren Assistenten. Neu ist der Anspruch, den Abstand zwischen Absicht und Ausführung zu verkürzen. Aus einer Suchanfrage wird eine Handlungskette; aus einem Interface wird ein wirtschaftlicher Akteur. Der Konflikt mit Amazon zeigt, dass diese Kette nicht im luftleeren Raum entsteht. Sie berührt Eigentumsrechte an Kundenzugängen, Identitätsprüfung, Haftung und die Frage, wer eine Transaktion stoppen darf. Meta News ist deshalb kein Technikprolog. Die Episode ist ein frühes Lehrstück über die kommende Ordnung des digitalen Marktes.

TEIL II · WERTSCHÖPFUNG

Von der Recherche zur Entscheidung und Handlung

Die Agent Journey wird wirtschaftlich relevant, wenn Informationen eine Auswahl verändern und begrenzte Handlungen auslösen.

Der „dritte Mann“ ist der digitale Stellvertreter zwischen Kundenabsicht und Unternehmensangebot. Er kann suchen, vergleichen und handeln; seine Interessen und Rechte sind nicht automatisch dieselben wie die von Kunde oder Anbieter. Die Quellen zeigen erste Verschiebungen bei Recherche, Plattformzugang und Transaktion - noch keine vollständige Übernahme von Kaufentscheidungen. Eine belastbare Journey beginnt nicht beim Modell, sondern bei einer Absicht: ein Ersatzteil finden, eine Maschine qualifizieren, eine Lieferabweichung behandeln. Der Agent muss den Bedarf präzisieren, Kriterien ableiten, Quellen finden und Angaben vergleichen.

Anschließend kann er eine begründete Auswahl vorbereiten, einen Menschen um Freigabe bitten oder eine begrenzte Handlung ausführen. An jeder Übergabe kann der Prozess kippen. Ein unvollständiger Bedarf führt zu einer falschen Suche. Uneinheitliche Produktdaten machen den Vergleich unzuverlässig. Ein abgelaufenes Zertifikat kann eine scheinbar saubere Qualifikation entwerten. Und eine Empfehlung ohne sichtbare Kriterien ist schwer zu prüfen. Die Forschung zu agentischer Lieferkettenplanung untersucht deshalb Aufgabenzerlegung, Werkzeugnutzung und Evidenz - bislang vor allem in begrenzten Modellen und Fallstudien. Unternehmen sollten nicht nur testen, ob ihr Name in einer Antwort erscheint.

Zu prüfen ist, ob das System das Angebot richtig identifiziert, Merkmale der richtigen Variante zuordnet, Quellen beibehält, Unsicherheit sichtbar macht und die Übergabe an Menschen korrekt ausführt.

Damit verschiebt sich auch der Ort, an dem Wertschöpfung beginnt. Bislang war die Website häufig Endpunkt einer Suche: Der Kunde kam an, las, verglich und entschied. In der Agent Journey wird sie zu einer von mehreren Quellen, die ein System bewertet. Unternehmen konkurrieren nicht mehr allein um Aufmerksamkeit, sondern um die Aufnahme in eine begründete Empfehlung. Das verändert Vertrieb und Einkauf zugleich. Wer nur sichtbar ist, kann übergangen werden; wer nur strukturiert ist, kann dennoch unglaublich bleiben. Entscheidend wird die Verbindung aus maschinenlesbarer Information, überprüfbarer Leistung und kontrollierter Handlungsfähigkeit.

VOLLMACHT · STUFEN STATT SCHALTER

Recherche ist nicht Autonomie

„Agent darf arbeiten“ ist keine ausreichende Berechtigung. Rechte müssen zur möglichen Schadenshöhe passen.

Ein Agent kann lesen, sortieren, zusammenfassen, empfehlen, entscheiden oder ausführen. Diese Tätigkeiten benötigen unterschiedliche Daten, Prüfungen und Freigaben. Ein interner Rechercheassistent kann mit einem breiten Leserecht auskommen. Ein System, das Liefermengen verändert, benötigt einen fachlichen Owner, Schwellenwerte, einen Freigabeprozess und eine nachvollziehbare Rücknahme. Die Deloitte-Analyse zur agentischen Supply Chain beschreibt fortlaufende Überwachung und begrenzte Aktionen als mögliches Zielbild. Das ist eine Fachanalyse, kein Beleg, dass Unternehmen solche End-to-End-Abläufe bereits breit produktiv betreiben. Wir übernehmen daraus die Gestaltungsfrage - nicht die Zukunftsbehauptung.

Jede Vollmacht sollte Zweck, Datenklasse, Werkzeuge, Höchstwert, Zeitfenster, menschliche Freigabe, Protokoll und Abschaltweg enthalten. Zahlung, Vertragsänderung, Lieferantenwechsel und Eingriffe in sicherheitsrelevante Produktionsschritte sind eigene Rechte. Sie dürfen nicht aus einer allgemeinen Agentenfreigabe abgeleitet werden.

Vollmacht ist deshalb kein technisches Attribut, sondern eine Managemententscheidung. Sie muss sich auf einen konkreten Prozess, einen zulässigen Wert und eine definierte Situation beziehen. Ein Agent, der Ersatzteile recherchiert, benötigt andere Rechte als ein System, das Liefertermine bestätigt oder Zahlungen auslöst. Die verbreitete Vorstellung, Autonomie lasse sich über einen einzigen Schalter aktivieren, verkennt diese Abstufung. In der Praxis braucht es ein Mandat, das ähnlich präzise ist wie eine Unterschriftenregelung: mit Zweck, Grenze, Eskalation und Widerruf. Erst diese Architektur macht Geschwindigkeit verantwortbar.

BEFUND · KONSUMENTEN

Recherche wird akzeptiert, Kaufdelegation bleibt begrenzt

Die deutsche KPMG-Erhebung hilft, Nutzung, Absicht und tatsächliche Vollmacht auseinanderzuhalten.

Der KPMG Consumer Snapshot, durchgeführt und ausgewertet vom EHI Retail Institute, berichtet: 46 Prozent der Befragten hätten in den zurückliegenden zwölf Monaten häufig oder sehr häufig KI bei Kaufentscheidungen genutzt; 73 Prozent könnten sich einen Agenten für den Vergleich von Produkten, Preisen oder Angeboten vorstellen. Die zentrale Nuance der Studie: Recherche und Vergleich werden eher delegiert als der gesamte Kaufabschluss. Das ist ein starker Beleg für eine frühe Akzeptanzstufe - aber nicht für autonome Kaufentscheidungen in großem Umfang. Es handelt sich um Befragungswerte und geäußerte Bereitschaft.

Sie sagen nicht, wie viele Menschen tatsächlich einen Kaufagenten autorisiert haben, wie oft dieser korrekt handelt oder welche Produktkategorien am ehesten betroffen sind. Reuters berichtete im August über Händler, die Agenten-Traffic gewinnen wollen, zugleich aber Kunden- und Transaktionsdaten auf ihren eigenen Kanälen halten möchten. Zwei Tage später kündigte Walmart Werkzeuge an, mit denen Kunden Agenten Käufe erledigen lassen können. Das sind konkrete Marktbewegungen; ihre Reichweite und Nutzung müssen sich erst zeigen.

Für die strategische Planung ist diese Differenz wichtiger als eine hohe Zustimmungsquote. Zwischen 'ich würde einen Agenten nutzen' und 'ich überlasse ihm einen Kauf' liegen mehrere Vertrauensstufen. Recherche kann bequem sein, ohne dass Menschen Preis, Anbieter oder Abschluss delegieren. Unternehmen sollten daher nicht auf den großen autonomen Sprung warten. Relevanter ist die schrittweise Verschiebung der Vorauswahl. Wenn ein Agent aus hundert Angeboten drei macht, ist wirtschaftliche Macht bereits verlagert - selbst wenn der Mensch den letzten Klick behält.

MARKT · SICHTBARKEIT

Von Auffindbarkeit zu begründeter Empfehlung

Ein maschinenlesbares Angebot ist auffindbar. Ein überzeugendes Angebot ist zusätzlich verständlich und überprüfbar.

Klassische Suche misst oft Impressionen, Klicks und Rankings. Agentische Systeme können mehrere Quellen zusammenführen und mit wenigen Optionen antworten. Dadurch wird die Frage nach maschineller Auswahl wichtiger. Der Begriff „Share of Recommendation“ kann diese Frage beschreiben, ist aber derzeit keine standardisierte Marktkennzahl. Ergebnisse unterscheiden sich nach Modell, Prompt, Nutzerprofil, Datenzugang und Zeit. Der Reuters-Bericht über Händler zeigt, dass Unternehmen ihre Produktseiten bereits für Chatbot-Suche verbessern. Zugleich ringen sie darum, wer die Transaktion und Kundendaten kontrolliert.

Das ist ein guter empirischer Einstieg für die Distributionsfrage; eine einzelne Traffic-Kennzahl ist jedoch kein Beweis für dauerhafte Kanalverschiebung. Für die Praxis sind dokumentierte Testfälle aussagekräftiger als ein allgemeiner Score: Welche Anbieter werden bei klaren Anforderungen gefunden? Werden Modell, Preis, Verfügbarkeit und Bedingungen korrekt wiedergegeben? Welche Quellen werden zitiert? Wo fallen Anbieter heraus - und warum? Jeder Test braucht Datum, System, Prompt und Vergleichsfall.

Die neue Sichtbarkeit ist folglich relational. Ein Angebot wird nicht abstrakt gut oder schlecht gefunden, sondern im Verhältnis zu einem konkreten Bedarf, zu verfügbaren Belegen und zu den Alternativen. Das erschwert einfache Rankings, verbessert aber die strategische Diagnose. Unternehmen können Tests entlang realer Kauf- oder Beschaffungsfragen aufbauen und nachvollziehen, an welcher Stelle sie ausscheiden: bei der Identifikation, beim Variantenbezug, bei fehlenden Nachweisen oder bei unklaren Bedingungen. Aus Sichtbarkeitsmessung wird so eine Prüfung der eigenen Angebotsfähigkeit.

MARKT · MARKE UND VERTRAUEN

Marke braucht überprüfbare Substanz

Eine bekannte Marke kann Orientierung geben. Der Agent muss erkennen können, worauf diese Erwartung beruht.

Marken reduzieren Unsicherheit, weil Kunden Erwartungen an Qualität, Service und Verlässlichkeit mit ihnen verbinden. Im Agentenraum bleibt dieser Wert bestehen, aber er muss in konkrete Informationen übersetzt werden: Welche Leistung gilt für welche Variante? Welche Garantie ist zugesagt? Welche Liefer- und Servicebedingungen sind verbindlich? Welche Quelle bestätigt die Aussage? Die NRF- und IBM-Erhebung zu globalem Einkaufsverhalten beschreibt zugleich eine Vertrauenslücke: Menschen nutzen KI zur Produktrecherche, äußern aber weiterhin erhebliche Datenschutz- und Missbrauchsbedenken. Das mahnt, Vertrauen nicht mit bloßer Nutzungsbereitschaft gleichzusetzen.

Für Hersteller und Händler heißt das: Produktfakten, Serviceversprechen, Rückgaberegeln und Herkunft müssen konsistent sein. Eigene Inhalte sind notwendig, aber kein neutraler Beweis. Eine maschinelle Empfehlung sollte auf nachvollziehbare Informationen zurückführbar sein; Widersprüche zwischen Herstellerseite, Datenfeed und Händlerangebot schaden Menschen wie Agenten.

Das schwächt Marken nicht; es zwingt sie zur Übersetzung. Reputation bleibt ein wichtiges Signal, weil weder Menschen noch Systeme jede Eigenschaft selbst prüfen können. Doch der Wert einer Marke wird künftig stärker daran hängen, ob ihr Versprechen in belastbare Fakten zerlegt werden kann. Herkunft, Service, Garantie, Reparierbarkeit oder Lieferfähigkeit müssen der richtigen Variante zugeordnet und aktuell gehalten werden. Eine Marke, die nur emotional erzählt, verliert maschinell an Kontur. Eine Marke, die nur Daten liefert, verliert menschlich an Bedeutung. Wettbewerbsfähig ist die Verbindung aus Erwartung und Beleg.

MARKT · PLATTFORMMACHT

Wer kontrolliert den Weg zum Kunden?

Agenten können Nachfrage vermitteln. Damit werden Zugang, Daten und Transaktionsregeln zu strategischen Fragen.

Wer den Agenten betreibt, kann bestimmen, welche Quellen genutzt, welche Kriterien gewichtet und welche Händler eingebunden werden. Für Anbieter entsteht ein Abhängigkeitsrisiko, falls ein Vermittler allein über Identität, Nutzungsdaten, Empfehlungen und Zahlungsfluss entscheidet. Reuters beschreibt, wie Händler Agenten-Traffic annehmen, aber die Kundenbeziehung selbst bewahren möchten. Der Walmart-Fall zeigt eine alternative Architektur: Agenten können über einen definierten Zugang an Produktkatalog und Transaktionssystem angebunden werden; Nutzer erhalten Profile, Ausgabengrenzen und Widerrufsmöglichkeiten. Das ist ein konkreter Produktstart, noch kein Beleg für breite Transaktionsnutzung oder ein allgemeines Modell für den B2B-Einkauf.

Unternehmen sollten Daten exportieren, Zugänge widerrufen und alternative Systeme anbinden können. Verträge müssen Ranking, Gebühren, Speicherung, Nutzung von Kundendaten, Reklamation und Haftung abdecken. Offene Schnittstellen allein lösen die Machtfrage nicht; entscheidend sind Rechte und Verhandlungsspielraum.

Der Plattformkonflikt macht zudem sichtbar, dass Interoperabilität nicht automatisch Offenheit bedeutet. Eine Schnittstelle kann technisch zugänglich und wirtschaftlich stark kontrolliert sein. Wer Regeln für Identität, Ranking, Gebühren und Zahlung setzt, beeinflusst die Verteilung von Margen und Kundenwissen. Für Unternehmen entsteht damit eine klassische Make-or-buy-Frage in neuer Form: Welche Teile der Kundenbeziehung dürfen an einen fremden Agenten delegiert werden, welche müssen im eigenen Verantwortungsraum bleiben? Diese Entscheidung gehört in die Geschäftsstrategie, nicht ausschließlich in IT oder Marketing.

TEIL II · INDUSTRIELLE WERTSCHÖPFUNG

Warum der industrielle Fall anders ist

Eine Kaufentscheidung über eine Maschine oder Komponente ist keine Produktrecherche im Endkundenshop.

Industrielle Beschaffung verbindet technische Eignung mit Sicherheit, Qualität, Kapazität, Lieferfähigkeit, Compliance und Lebenszykluskosten. Ein Fehler kann Stillstand, Ausschuss oder eine ungültige Zulassung verursachen. Deshalb ist der sinnvolle Einstieg nicht „Agent kauft ein“, sondern „Agent bündelt Informationen und markiert Abweichungen“. BCG, KPMG und Deloitte sehen Potenzial in Supply Chain, Planung, Beschaffung und Engineering. Ihre Beiträge liefern nützliche Prozessbilder, sind aber teilweise Beratungsperspektiven und Anbieterstudien. Sie belegen, dass Use Cases identifiziert werden - nicht automatisch, dass die Systeme unter realen Fabrikbedingungen zuverlässig, wirtschaftlich und skalierbar laufen.

Die Forschung untersucht konkrete Teilprobleme wie flexible Produktionsplanung und Lieferkettenabstimmung. Sie zeigt, dass spezialisierte Modelle und Simulationen entscheidend sind. Ihre Aussagekraft endet dort, wo aus Experimenten und Simulationsdaten eine allgemeine Aussage über den Serieneinsatz abgeleitet würde.

Im Industriegütergeschäft verschärft sich diese Frage, weil Auswahlfehler nicht nur einen unzufriedenen Käufer erzeugen. Sie können Anlagenstillstand, Qualitätsabweichungen, Vertragsrisiken oder Sicherheitsprobleme auslösen. Der Agent muss deshalb mehr leisten als Ähnlichkeit zu erkennen. Er muss Anforderungen auflösen, Varianten unterscheiden, Gültigkeiten prüfen und Unsicherheit eskalieren. Der industrielle Fall ist damit weniger spektakulär, aber anspruchsvoller: Nicht maximale Autonomie ist das Ziel, sondern eine bessere, schnellere und zugleich prüfbare Entscheidung im Zusammenspiel von Fachwissen, Daten und Prozess.

DATEN · INDUSTRIELLE PRODUKTAKTE

Ein Angebot muss eindeutig sein

Maschinenlesbarkeit beginnt bei Identität und Variantenlogik – die Entscheidung braucht zusätzlich Herkunft und Gültigkeit.

Eine industrielle Produktakte sollte Modell, Ausführung, technische Merkmale, Einheiten, Kompatibilität, Änderungsstand, Zertifikate, Prüfberichte, Ersatzteile und Servicebedingungen verknüpfen. Für jede Angabe braucht es Produktbezug, Quelle, Stand und verantwortliche Stelle. Ohne Variantenbezug kann ein System korrekte Einzelwerte zu einer falschen Gesamtaussage kombinieren. Befragte Unternehmen nennen Daten- und Technologiegrundlagen regelmäßig als Skalierungshemmnis. BCGs gemeinsame Industrieerhebung mit dem Weltwirtschaftsforum beschreibt frühe Erfolge, zugleich aber große Schwierigkeiten beim Übergang von Einzelanwendungen zu Netzwerken. Diese Befunde beziehen sich auf industrielle KI insgesamt, nicht allein auf Agenten. Die Konsequenz ist nicht, zunächst alle Daten im Konzern zu bereinigen.

Beginnen sollte man mit einem kritischen Produktsegment oder Prozess. Für jede Information wird geklärt: Wer erstellt sie? Wer bestätigt sie? Wie wird eine Änderung erkannt? Was passiert, wenn Quelle und ERP voneinander abweichen?

Eine solche Produktakte ist kein zusätzliches Datenprojekt neben dem Geschäft. Sie ist die digitale Form des Angebots selbst. Wenn ein Merkmal nicht eindeutig einem Modell, einer Revision oder einem Gültigkeitszeitraum zugeordnet ist, kann der Agent es nicht zuverlässig verwenden. Das Problem betrifft nicht nur KI. Auch Vertrieb, Service, Ersatzteilwesen und Qualität leiden unter widersprüchlichen Stammdaten. Agent Readiness macht diese Schwäche lediglich früher sichtbar. Wer die Produktakte verbessert, investiert deshalb zugleich in Vertriebsfähigkeit, Prozessqualität und die Senkung späterer Klärungskosten.

BESCHAFFUNG · QUALIFIKATION

Vom Lieferantenverzeichnis zur prüfbaren Auswahl

Agenten können Kriterien bündeln. Sie dürfen fehlende Nachweise nicht als erfüllte Anforderungen behandeln.

Ein Lieferantenvergleich muss technische Eignung, Qualitätsstatus, Kapazität, Kosten, Lieferperformance, Risiko und Compliance unterscheiden. Die Kriterien haben nicht immer denselben Rang. Bei einer kritischen Komponente kann ein niedriger Preis einen ungeklärten Qualitätsnachweis nicht ausgleichen. Bei weniger kritischen Standardteilen kann eine stärker automatisierte Vorprüfung sinnvoll sein. Deloitte und KPMG beschreiben Agenten für RFI- und Angebotsprüfung, Risikoüberwachung und routinebasierte Beschaffung. Das ist ein plausibles Feld für Recherche, Datenabgleich und Ausnahmeerkennung. Eine automatische Lieferantenzulassung bleibt ein anderer Eingriff und verlangt Nachweise zu Datenvollständigkeit, Fairness, Fehlerquote und Eskalation.

Der Prozess sollte fehlende Informationen als „offen“ markieren, nicht als „bestanden“. Lieferanten brauchen einen Korrekturweg, wenn ein Datensatz unvollständig oder falsch ist. Das schützt auch kleinere Anbieter, die nicht dieselbe Daten- und IT-Infrastruktur wie Großkonzerne haben.

Die prüfbare Auswahl verlangt außerdem eine sichtbare Rangordnung der Kriterien. Manche Anforderungen sind Ausschlusskriterien, andere lassen sich gegeneinander abwägen. Ein Agent darf diese Logik nicht aus statistischer Plausibilität erraten. Sie muss aus Beschaffungsstrategie, Qualitätsanforderungen und Risikoklasse abgeleitet werden. Besonders wichtig ist der Umgang mit Nichtwissen: Fehlt ein Zertifikat, ist die Anforderung nicht erfüllt - aber auch nicht widerlegt. Das System muss die Lücke markieren und einen Verantwortlichen ansprechen. Diese nüchterne Behandlung fehlender Evidenz ist ein Kernunterschied zwischen einer hilfreichen Vorauswahl und einer gefährlich selbstsicheren Automatisierung.

BESCHAFFUNG · PILOTDESIGN

Ein Pilot muss eine Investitionsentscheidung ermöglichen

Ein Agentenpilot ist nur dann wertvoll, wenn ein Unternehmen auch begründet stoppen oder umbauen kann.

Vor dem Start werden Prozessgrenze, Baseline, Erfolgskriterium und Sicherheitsgrenze festgelegt. Gemessen werden Durchlaufzeit, Vollständigkeit, Fehlklassifikation, Nacharbeit, Nutzeraufwand und wirtschaftlicher Effekt. Die Zahl der Abfragen oder erzeugten Agenten ist keine Wertkennzahl. Ein aussagekräftiger Pilot verwendet historische Fälle und einen Schattenbetrieb. Er prüft veraltete Daten, widersprüchliche Zertifikate, Lieferantenausfall, ungewöhnliche Nachfrage und manipulierte Dokumente. Ein unabhängiger Fachexperte bewertet dieselben Fälle. Erst danach darf ein begrenzter Live-Einsatz folgen. Die Vollkosten umfassen Integration, Datenpflege, Lizenzen, Modell- und Betriebskosten, menschliche Kontrolle, Fehlerfolgen und Rückfallverfahren. Eine schnelle Sortierung ist kein Produktivitätsgewinn, wenn die Fachprüfung anschließend länger dauert.

Die Baseline muss vor der Einführung erhoben werden.

Ein Pilot ist deshalb kein Schaufenster für technische Möglichkeiten, sondern ein befristeter Investitionsversuch. Er braucht einen Ausgangswert, gegen den sich Wirkung messen lässt, und eine Fehlerklasse, bei der der Versuch abgebrochen wird. Zeitersparnis allein genügt nicht. Wenn Fachkräfte jede Empfehlung umfassend nachprüfen müssen, wandert Arbeit lediglich an eine andere Stelle. Ebenso muss der Aufwand für Datenpflege, Rechteverwaltung und Überwachung in die Rechnung. Ein guter Pilot erzeugt am Ende keine Demo, sondern eine belastbare Entscheidung: stoppen, umbauen oder unter klaren Bedingungen skalieren.

SUPPLY CHAIN · AGENT CHAIN

Eine Lieferkette wird nicht durch APIs allein agentisch

Agenten zwischen Unternehmen brauchen gemeinsame Begriffe, zulässige Daten und abgestimmte Verantwortungsgrenzen.

„Agent Chain“ bezeichnet hier eine mögliche Entwicklung, in der Systeme Abweichungen erkennen, Optionen vergleichen und abgestimmte Schritte vorschlagen oder ausführen. Das ist ein infpro-Analysebegriff, kein etablierter Industriestandard. Die Kette braucht gemeinsame Semantik: Was bedeutet „verfügbar“? Wann beginnt die Lieferzeit? Welche Kapazität ist fest zugesagt? Deloitte skizziert Agenten, die Risiken kontinuierlich beobachten, Alternativen berechnen und begrenzte Aktionen auslösen. Fachmedien mahnen zugleich, dass manche als Agenten vermarktete Funktionen etablierte Prognose-, Optimierungs- oder Workflow-Technik nutzen. Der neue Name macht eine bestehende Fähigkeit nicht automatisch autonom. Die entscheidende Infrastruktur ist deshalb nicht nur ein API-Katalog.

Sie umfasst Identität, Rechte, Datenqualität, Versionierung, Protokoll, Streitbeilegung und vertragliche Regeln. Bei einer Störung muss erkennbar sein, welche Quelle eine Änderung ausgelöst hat, welche Alternativen bewertet wurden und wer die Aktion autorisiert hat.

Die Agent Chain entsteht folglich nicht dadurch, dass mehrere Systeme Nachrichten austauschen. Sie entsteht erst, wenn Bedeutung, Zuständigkeit und Haftung über Unternehmensgrenzen hinweg anschlussfähig werden. Ein Lieferant kann einen Termin bestätigen, ohne die Produktionsfolgen beim Kunden zu kennen; ein Logistikagent kann eine Route optimieren, ohne Qualitätsfreigaben zu verstehen. Die Kette braucht deshalb gemeinsame Referenzen und definierte Übergaben. Jede Übergabe muss zeigen, welche Information übernommen wurde, wer sie bestätigt hat und welche Entscheidung daraus folgen darf. Ohne diese Disziplin skaliert nicht Wertschöpfung, sondern Missverständnis.

ACHT PRAXISFÄLLE · 1/2

Wo Agenten bereits in operative Arbeit eingreifen

Vier Fälle aus Einkauf, Engineering, Supply Chain und Schadenbearbeitung. Die Unternehmen berichten reale Einsätze; Leistungszahlen bleiben als Anbieterangaben gekennzeichnet.

1 · EnBW: Einkauf als Agentenbetrieb. Microsoft stellte am 22. Oktober 2026 EnBW's Ansatz vor. Agenten sollen Lieferketten überwachen, weltweit Lieferanten suchen und Teams bei Verhandlung und Vertragsverwaltung unterstützen. EnBW beschreibt ein neues Operating Model. Die genannten Einsparungen sind jedoch Zielgrößen, keine bereits gemessenen Ergebnisse.

2 · Siemens: Engineering im TIA Portal. Der Eigen Engineering Agent bearbeitet Aufgaben mehrstufig und verbindet sich direkt mit dem TIA Portal. Siemens nennt mehr als 100 Erprobungskunden in 19 Ländern sowie schnellere Beschleunigungs- und Qualitätswerte. Das sind Anbieterangaben; eine vergleichende unabhängige Studie liegt nicht vor.

3 · Microsoft: Agenten in der eigenen Supply Chain. Microsoft berichtet über mehr als 111 spezialisierte Agenten. In fünf monatlichen Planungszyklen sank die durchschnittliche Zykluszeit laut interner Auswertung von rund zehn auf weniger als zweieinhalb Arbeitstage. Belegt ist damit ein definierter Workflow, nicht eine allgemeine Produktivitätswirkung.

4 · Allianz: sieben Agenten im Schadenprozess. Project Nemo bündelt Planung, Deckungsprüfung, Wetterabgleich, Betrugsprüfung, Auszahlungsberechnung und Audit. Allianz meldet bei einfachen australischen Sturmschäden rund 80 Prozent kürzere Bearbeitungszeit. Die Auszahlung bleibt beim Menschen; die Kennzahl stammt vom Anbieter.

Die ersten vier Fälle zeigen den Übergang vom Assistenten zur operativen Rolle. Entscheidend ist ihre Begrenzung: Lieferanten, Engineering-Aufgaben, Planungsläufe und Schadenfälle werden konkret gefasst; Menschen bleiben bei Freigabe, Ausnahme oder Auszahlung sichtbar. So entsteht Produktivität nicht durch allgemeine Autonomie, sondern durch zerlegte Aufgaben und überprüfbare Ergebnisse.

Vom Plattformzugang bis zur Agentenorganisation

Vier weitere Fälle zeigen, wie Handel, Zahlungsfreigabe und Unternehmenssteuerung auf delegierte digitale Arbeit reagieren.

5 · Amazon: Kaufabschluss auf fremden Händlerseiten. Shop Direct zeigt Angebote externer Händler; Buy for Me kann den Kauf auf deren Website im Auftrag des Kunden abschließen. Amazon nennt mehr als 100 Millionen Produkte von über 400.000 Händlern. Reichweite und Nutzung sind Anbieterangaben, der strategische Befund ist dennoch klar: Auswahl, Zahlung und Kundenkontakt können auseinanderfallen.

6 · OpenAI: Checkout mit begrenzter Zahlungsdelegation. Das Agentic Commerce Protocol nimmt strukturierte Produktdaten auf und wickelt einen Checkout mit dem Händler ab. Warenkorb, Preise, Steuern und Bestellstatus müssen autoritativ zurückgemeldet werden. Die Spezifikation zeigt, wie Vollmacht technisch begrenzt und zugleich Händlerverantwortung erhalten werden kann.

7 · Palantir: Agenten im operativen Unternehmensmodell. Der Agent Stack dokumentiert Arbeit in Sessions und führt Kontext, Ereignisse, Werkzeugresultate und Zustandswechsel zusammen. Das ist zunächst Produktarchitektur, kein Wirkungsnachweis. Organisatorisch relevant sind der klare Arbeitsgegenstand, nachvollziehbare Zwischenschritte und prüfbare Übergaben.

8 · Microsoft: mehr als 500.000 Agenten sichtbar. Microsoft berichtete im März 2026 über interne Sichtbarkeit von mehr als 500.000 Agenten. Kurz vor der Veröffentlichung seien mehr als 65.000 Agenten täglich aktiv gewesen. Registry-Sichtbarkeit ist nicht mit Produktivität gleichzusetzen; sie macht vor allem den Governance-Bedarf sichtbar.

Die zweite Fallgruppe erweitert den Blick auf Markt- und Systemarchitekturen. Amazon, OpenAI und Palantir beschreiben Zugänge, Protokolle und Beobachtbarkeit; Microsoft macht den künftigen Verwaltungsbedarf sichtbar. Entscheidend ist nicht die Zahl der Agenten, sondern ob Identität, Auftrag, Datenzugriff, Version und verantwortlicher Owner bekannt sind.

FORSCHUNG · PROTOTYPEN UND FELD

Was wissenschaftliche Arbeiten tatsächlich belegen

Forschung zeigt technische Möglichkeiten unter kontrollierten Bedingungen – und markiert, was vor der Fabrik noch fehlt.

Eine 2025 veröffentlichte Arbeit im Journal of Intelligent Manufacturing beschreibt, wie natürliche Sprache zur Erzeugung von Produktionssimulationsmodellen genutzt werden kann. Getestet wurden 18 Aktionstypen; die Antwortzeiten reichten je nach Aufgabe von Sekunden bis zu mehreren Minuten. Das ist ein technischer Leistungsnachweis eines Forschungsansatzes, kein Serienbetrieb in einer Fabrik. Eine Arbeit in den CIRP Annals 2026 untersucht Multi-Agent-Planung mit Simulations- und Optimierungsverfahren anhand von Daten eines Automobilzulieferers. Die Validierung findet in sieben Simulationsexperimenten statt. Das ist näher an industriellen Daten, bleibt aber eine Simulation und keine produktive Langzeitmessung.

Eine weitere Studie zu agentischer Konsensbildung in Lieferketten testet Lagerbestandsentscheidungen und berichtet reduzierte Bullwhip-Effekte im untersuchten Modell. Auch dieser Befund ist ein Forschungsergebnis unter definierten Bedingungen. Für die Praxis müssen Robustheit, Datenqualität, Anreizkonflikte und menschliche Intervention zusätzlich geprüft werden.

Für Vorstände ist diese Trennung zwischen technischer Möglichkeit und betrieblichem Beleg zentral. Eine Studie kann zeigen, dass ein Modell unter definierten Bedingungen plant oder simuliert. Sie beantwortet damit noch nicht, ob Daten im Werk vollständig sind, ob Ausnahmen rechtzeitig erkannt werden oder ob der wirtschaftliche Nutzen nach Wartung und Kontrolle bestehen bleibt. Forschung liefert Bausteine und Prüfmethoden; sie ersetzt nicht die Feldvalidierung. Unternehmen sollten Ergebnisse daher weder kleinreden noch überdehnen. Der angemessene nächste Schritt ist ein kontrollierter Transfer mit realistischen Störungen, nicht die sofortige Generalisierung.

PRODUKTION · VOM VORSCHLAG ZUR AKTION

In der Fabrik zählt die sichere Grenze

Ein plausibel klingender Text darf keine Produktionsentscheidung auslösen, deren Folgen nicht kontrolliert werden können.

Ein Produktionsagent kann eine Störungsmeldung klassifizieren, Wartungsunterlagen zusammenführen, eine Reihenfolge simulieren oder Energie- und Kapazitätsdaten aufbereiten. Für jede Aufgabe ist festzulegen, ob der Agent nur liest, einen Vorschlag macht oder eine Anlage beziehungsweise ein Produktionssystem tatsächlich verändert. Die WEF- und Accenture-Analyse zu intelligenten Industrieoperationen beschreibt den Übergang von unterstützter Analyse zu stärker vernetzten und adaptiven Betriebsmodellen. Das ist eine strategische Landkarte, kein universeller Reifegradpfad. Für jedes Werk gelten andere Anlagen, Sicherheitsanforderungen und Datenstände. Ein sinnvoller Anfang liegt bei häufigen, gut dokumentierten und nicht sicherheitskritischen Fällen.

Der Agent kann die Meldung einer bekannten Störung mit früheren Fällen und Arbeitsanweisungen abgleichen. Eine Fachkraft bestätigt oder korrigiert. Erst nach Tests im Schattenbetrieb und sauberer Fehlerrückkehr darf eine eng begrenzte automatische Handlung geprüft werden.

In der Produktion muss deshalb jede Agentenfunktion einer klaren Wirkebene zugeordnet werden. Lesen, diagnostizieren, simulieren, empfehlen und ausführen sind unterschiedliche Klassen. Zwischen ihnen liegen technische und organisatorische Schranken. Ein System darf beispielsweise eine Störung priorisieren, ohne selbst eine Anlage abzuschalten. Es kann eine neue Reihenfolge vorschlagen, ohne den Plan freizugeben. Diese Differenzierung wirkt zunächst langsamer als die Vision autonomer Fabriken. Tatsächlich schafft sie die Voraussetzung für Tempo, weil Fehler nicht unkontrolliert in physische Prozesse durchschlagen.

RISIKO · ANGRIFFSFLÄCHE UND FEHLER

Agenten erweitern die Angriffsfläche

Externe Inhalte, interne Daten und Werkzeugrechte treffen in einem Prozess zusammen.

Ein Agent kann manipulierte Dokumente lesen, unberechtigte Daten abrufen, falsche Werkzeuge aufrufen oder seine Aufgabe durch eine fremde Anweisung fehlinterpretieren. Das Risiko liegt nicht allein im Sprachmodell. Es entsteht aus dem Zusammenspiel von Modell, Datenquelle, Werkzeug, Identität und Prozessrecht. NISTs AI Agent Standards Initiative zielt auf sichere Interoperabilität, Vertrauen sowie Forschung zu Agentensicherheit und Identität. Sie ist eine laufende Initiative und kein abgeschlossener Unternehmensstandard. Unternehmen müssen ihre eigenen Schutzregeln weiterhin aus Anwendungsfall und Risiko ableiten.

Red-Team-Prüfungen sollten konkrete Geschäftsabläufe nachstellen: Prompt Injection in Lieferantendokumenten, Rechteausweitung, Datenabfluss, doppelte Buchung, unautorisierte Änderungen und Ketteneffekte über Unteragenten. Jeder Befund braucht Korrektur, Owner und Wiederholungstest. Lieferketten und Fabriken erleben verspätete Teile, Qualitätsprobleme, widersprüchliche Bestände, Nachfragesprünge und kurzfristige Lieferantenwechsel. Ein Agent kann Signale schneller bündeln. Er kann jedoch aus historischen Mustern nicht sicher ableiten, welche neue Ausnahme für ein Werk tragbar ist. Die Financial Times betont bei der Supply Chain, dass Nutzen saubere Daten, standardisierte Abläufe und klare Ziele voraussetzt.

Sie warnt außerdem vor überautomatisierten Reaktionen, schlecht erklärbaren Ergebnissen und Abhängigkeit von Plattformen. Das ist eine wichtige Gegenperspektive zu den Anbieter- und Beratungsszenarien. Ein robustes System eskaliert bei fehlenden Belegen, widersprüchlichen Quellen, unbekannten Fällen und hoher Schadenswirkung. Es sollte Alternativen vergleichen, aber nicht stillschweigend eine einzige Lösung ausführen. Krisentests müssen Ersatzlieferanten, Materialsubstitution, Kapazitätsengpässe und fehlerhafte Stammdaten enthalten.

Die besondere Gefahr agentischer Systeme liegt in ihrer Verbindungskompetenz. Ein Modell allein besitzt oft wenig Handlungsmacht; Werkzeuge, Konten und Schnittstellen machen aus einem Fehler eine Aktion. Sicherheitsarchitektur muss deshalb den gesamten Ablauf betrachten. Welche externen Inhalte darf der Agent lesen? Welche internen Daten darf er kombinieren? Welche Werkzeuge darf er unter welchen Bedingungen aufrufen? Protokollierung ist dabei nicht bloß Dokumentation im Nachhinein. Sie muss eine Entscheidung so sichtbar machen, dass Fachbereich und Sicherheitsteams Abweichungen erkennen und den Prozess rechtzeitig stoppen können.

REALITY CHECK · PHYSISCHE AUTONOMIE

Softwareagent und humanoider Roboter sind nicht dasselbe

Die Debatte über Agenten darf digitale Geschäftsprozesse nicht mit autonomer physischer Arbeit vermischen.

Ein digitaler Agent kann Daten lesen und in Geschäftssystemen handeln. Ein Roboter muss zusätzlich Wahrnehmung, Bewegung, Sicherheit und physische Ausführung beherrschen. Die Fortschritte sind nicht gleich schnell. Reuters berichtete 2026, dass humanoide Roboter trotz hoher Investitionen mit Geschicklichkeit, Zuverlässigkeit und Anpassung an neue Situationen kämpfen; konventionelle Industrierobotik bleibt in vielen Aufgaben günstiger und verlässlicher. Eine weitere Reuters-Meldung zitierte Siemens mit der Einschätzung, KI könne den Automatisierungsgrad einer Fabrik perspektivisch auf bis zu 80 Prozent erhöhen. Das ist eine Managementprognose, keine Messung einer bereits erreichten Fabrikleistung.

Diese Trennung schützt das Dossier vor einer häufigen Übertreibung: Eine agentische Softwarearchitektur ist nicht automatisch eine „autonome Fabrik“. Jede Aussage sollte benennen, ob sie digitale Recherche, Prozessautomatisierung, physische Robotik oder eine Kombination davon betrifft.

Die begriffliche Trennung schützt auch vor falschen Investitionsschlüssen. Fortschritte bei digitalen Agenten lassen sich nicht direkt auf humanoide Robotik übertragen. Physische Arbeit verlangt robuste Wahrnehmung, sichere Bewegung und Verantwortung für unmittelbare Folgen. Umgekehrt kann ein digitaler Agent erhebliche wirtschaftliche Macht entfalten, obwohl er keinen Körper besitzt: Er kann Lieferanten priorisieren, Verträge vorbereiten oder Zahlungen anstoßen. Beide Entwicklungen gehören zusammen gedacht, aber getrennt bewertet. Sonst entsteht entweder technischer Überschwang oder eine falsche Entwarnung.

INFPRO-RAHMEN · SECHS STUFEN

Agent Readiness ist ein Profil, kein Abzeichen

Ein Unternehmen kann für Recherche vorbereitet sein und zugleich keine sichere Handlungsvollmacht besitzen.

Wir prüfen Readiness entlang von sechs Stufen: Auffindbarkeit - wird das Angebot gefunden? Verständlichkeit - werden Produkt, Variante und Bedingungen korrekt interpretiert? Verifizierbarkeit - sind Aussagen belegbar und aktuell? Zugänglichkeit - können erlaubte Systeme die Daten sicher erreichen? Handlungsfähigkeit - kann ein definierter Workflow korrekt ausgeführt werden? Steuerbarkeit - gibt es Owner, Grenzen, Protokolle und Rücknahme? Das ist ein infpro-Prüfraster, kein extern validierter Branchenstandard. Es lehnt sich an die in Deloitte-, BCG- und WEF-Arbeiten wiederkehrenden Voraussetzungen an: Datenbasis, Prozessredesign, Fähigkeiten, Governance und menschliche Verantwortung.

Bewertet wird ein konkretes Produkt und ein konkreter Workflow. Ein Gesamtwert darf keine kritische Schwäche verdecken. Für jede Stufe braucht es einen Beleg - etwa einen Testfall, einen gültigen Nachweis, einen freigegebenen Datenzugang oder einen protokollierten Eskalationstest.

Ein Profil ist aussagekräftiger als eine einzelne Reifegradzahl, weil Unternehmen in verschiedenen Dimensionen unterschiedlich weit sein können. Ein Hersteller kann hervorragend auffindbar sein, aber keine belastbaren Produktnachweise liefern. Ein Werk kann saubere Daten besitzen, aber keine sicheren Aktionsrechte definieren. Die sechs Stufen machen diese Asymmetrie sichtbar. Sie dienen nicht dem Marketing, sondern der Reihenfolge von Investitionen. Erst wenn Verständlichkeit und Verifizierbarkeit stimmen, lohnt es sich, Zugänglichkeit und Handlungsfähigkeit auszuweiten. Steuerbarkeit bleibt dabei keine Abschlussstufe, sondern begleitet jede Erweiterung.

GOOGLE ZERO · DER GRUNDSTEIN

Auffindbarkeit ist die Eintrittskarte, nicht der Wettbewerbsvorteil

Google Zero und KI-Suche beginnen mit verlässlichen, zugänglichen Informationen. Sie garantieren keine Empfehlung.

Wenn Suchsysteme und Agenten Antworten statt Trefferlisten liefern, wird eine klare Quellenbasis wichtiger. Unternehmen sollten ihre Inhalte so strukturieren, dass Marke, Autor, Produkt, Variante, Kernaussage, Datum und Beleg eindeutig zusammengehören. Das stärkt auch klassische Suche und menschliche Beschaffung. Für infpro bedeutet das: Google Zero ist die Grundlage der Informationsarchitektur, nicht das Ende der Strategie. Inhalte müssen auffindbar, verständlich, überprüfbar und aktuell sein. Danach kommt die entscheidende Qualitätsfrage: Wird ein Angebot im konkreten Anwendungsfall als geeignet bewertet - und lässt sich die Bewertung erklären?

Ein Agent kann auf Seiten zugreifen und trotzdem eine falsche Auswahl treffen. Datenzugang, Plattformregeln, Nutzerkriterien und Aktualität wirken gemeinsam. Deshalb sollte jede Organisation externe KI-Antworten mit wiederholbaren Testfragen beobachten, statt sich auf ein einmaliges Sichtbarkeitssiegel zu verlassen. Der technische Check umfasst robots.txt, XML-Sitemap, Canonical-URLs, Statuscodes, interne Verlinkung, Mobile-Auslieferung und strukturierte Daten. Für zentrale Inhalte muss klar sein, welche Seite maßgeblich ist, wann sie aktualisiert wurde und wer dafür verantwortlich zeichnet. Crawling-Zugang ist zudem von Berechtigung für private oder geschützte Daten zu unterscheiden. Schema.org kann Entitäten und Eigenschaften maschinenlesbar beschreiben.

Es verifiziert keine Behauptungen. Eine strukturierte Angabe zur Lieferzeit bleibt falsch, wenn der Datenstand veraltet ist. Ein Agent braucht deshalb Belege und Kontext - nicht nur ein korrektes JSON-LD. Für Infpro sollte jede Themenseite die Kernaussage, verantwortliche Autorenschaft, Veröffentlichungs- und Aktualisierungsdatum, Primärquellen und verwandte Fachbeiträge sichtbar verbinden. Für Unternehmen gilt dasselbe Prinzip bei Produkten und Lieferanteninformationen.

Google Zero ist in diesem Bild weder Endzustand noch Randthema. Es beschreibt die Verlagerung von der Trefferliste zur direkten Antwort und zwingt Unternehmen, ihre Aussagen als belastbare Quellen anzubieten. Das schafft die Eingangsvoraussetzung für Agenten, aber noch keinen Wettbewerbsvorteil. Ein Agent kann eine Quelle finden und sie trotzdem verwerfen, wenn Varianten unklar, Belege veraltet oder Bedingungen widersprüchlich sind. Der technische Grundstein besteht daher aus Zugänglichkeit, Struktur und Autorenschaft. Fachliche Autorität entsteht erst durch Konsistenz, Aktualität und die Bereitschaft, Grenzen offenzulegen.

WERT · WORKFLOW STATT TOOL

Der Workflow ist die Investitionseinheit

Ein Agent auf einen alten Ablauf gesetzt, kann Arbeit nur verschieben.

Wert entsteht durch eine bessere Arbeitsteilung. Vor der Einführung wird dokumentiert, wie lange ein Vorgang heute dauert, wie oft Fehler auftreten, wie viel Nacharbeit entsteht und welche Kosten oder Risiken im Prozess liegen. Nach dem Pilot werden dieselben Werte erhoben. Neben dem Zeitgewinn zählen Datenpflege, Integrationsaufwand, Modell- und Betriebskosten sowie menschliche Kontrolle. BCG und Deloitte argumentieren für End-to-End-Prozessredesign; McKinsey berichtet, dass Unternehmen mit größerem KI-Wert häufiger Abläufe grundlegend neu gestalten. Die Erhebungen zeigen Zusammenhänge in Unternehmensangaben. Sie beweisen nicht, dass Redesign allein den Erfolg verursacht oder dass jedes Unternehmen denselben Effekt erzielt.

Ein belastbarer Business Case enthält Baseline, Vergleichsgruppe oder nachvollziehbare Vorher-nachher-Messung, Gesamtbetriebskosten und Fehlerfolgen. Der Pilot endet mit einer Entscheidung: stoppen, ändern, skalieren. Eine reine Demonstration ohne Abbruchkriterium ist kein Investitionsfall.

Das verändert auch die Investitionslogik. Ein einzelnes Tool kann beeindruckend wirken und dennoch keinen End-to-End-Nutzen erzeugen. Entscheidend ist, ob Wartezeiten sinken, Fehler früher erkannt werden und weniger Nacharbeit entsteht. Dazu muss der gesamte Workflow betrachtet werden - einschließlich der menschlichen Prüfung. Wird nur ein Teilschritt beschleunigt, kann der Engpass an die nächste Station wandern. Der wirtschaftliche Nachweis verlangt deshalb dieselben Kennzahlen vor und nach dem Pilot sowie eine Betrachtung der Vollkosten. Erst dann wird aus individueller Zeitersparnis betriebliche Produktivität.

GOVERNANCE · VERTRAUEN

Vertrauen ist eine technische und organisatorische Kontrollarchitektur

Regeln wirken nur, wenn sie in Zugriffsrechten, Prozessschritten und Eskalationen umgesetzt sind.

Der Agent braucht eine eindeutige Identität, minimal notwendige Rechte, ein begrenztes Werkzeugset und eine dokumentierte Aufgabe. Aktionen und relevante Quellen müssen protokolliert werden. Bei einem Fehler muss rekonstruierbar sein, welche Daten, Regeln und Freigaben galten. NISTs Agenteninitiative arbeitet an sicheren Interoperabilitäts- und Identitätsfragen. Sie bietet keinen universellen Freigabekatalog, den ein Unternehmen einfach übernehmen könnte. Für industrielle Betriebe ist die Verbindung zu OT-Sicherheit, Lieferantenrechten und Business Continuity entscheidend. Ein produktives Agentenregister sollte Zweck, fachlichen Owner, technische Betreiber, Datenzugriffe, Tools, Rechte, Abhängigkeiten, Teststand, Änderungshistorie und Not-Aus enthalten.

Sicherheitsprüfungen finden vor jeder neuen Berechtigung und nach wesentlichen Änderungen erneut statt. Bei Agent-zu-Agent-Prozessen muss sichtbar sein, welcher Akteur eine Aufgabe delegiert hat, welche Rechte weitergegeben wurden und wann sie enden. Schlüsselrotation, Widerruf, Versionskontrolle und getrennte Konten gehören in den Lebenszyklus. Ein Agent ist kein Mitarbeiterkonto mit dauerhaftem Zugriff. Auditprotokolle sollten Eingaben, Quellversionen, Regeln, Werkzeugaufrufe, Freigaben und resultierende Aktionen erfassen. Das bedeutet nicht, dass jede interne Modellberechnung vollständig erklärbar sein muss. Es bedeutet, dass die geschäftlich relevante Entscheidungsspur nachvollziehbar bleibt.

Ein einfacher Betriebstest lautet: Kann das Unternehmen nach einer falschen Bestellung oder Produktionsänderung innerhalb kurzer Zeit rekonstruieren, was der Agent wusste, welche Grenze galt, wer freigab und wie der Prozess zurückgesetzt wurde? Wenn nicht, fehlt die Betriebsreife.

Vertrauen ist unter diesen Bedingungen kein Gefühl, das durch eine gute Benutzeroberfläche entsteht. Es ist das Ergebnis einer Kontrollarchitektur, die Identität, Rechte, Quellen und Eskalation verbindet. Menschen müssen erkennen können, ob eine Aussage aus freigegebenen Daten stammt, welche Werkzeuge eingesetzt wurden und welche Unsicherheit verbleibt. Ebenso wichtig ist der Rückweg: Eine Aktion muss gestoppt, korrigiert oder auf einen sicheren Zustand zurückgeführt werden können. Je näher ein Agent an Geld, Vertrag oder Maschine rückt, desto weniger darf diese Architektur implizit bleiben.

ARBEIT · WISSEN UND KOMPETENZ

Fachwissen wird zur Prüfinstanz

Agenten können Routine verringern und neue Kontroll-, Pflege- und Ausnahmearbeiten schaffen.

Die Quellen erlauben keine pauschale Aussage, wie viele Arbeitsplätze Agenten ersetzen. McKinsey beschreibt individuelle Produktivitätsgewinne und zugleich eine deutlich kleinere Gruppe von Unternehmen, die nennenswerten EBIT-Beitrag angibt. Der Übergang von persönlichem Zeitgewinn zu betrieblichem Ergebnis bleibt eine Managementaufgabe. Mitarbeitende müssen Anforderungen präzisieren, Quellen beurteilen, Ausnahmen erkennen und Entscheidungen eskalieren können. Dieses Wissen lässt sich nicht allein mit Prompt-Schulungen aufbauen. Es braucht Fachkompetenz, Zeit zur Prüfung und das Recht, eine Agentenempfehlung zu überstimmen.

Besonders gefährlich ist eine formale Aufsicht ohne Kapazität: Wenn Menschen Ergebnisse bestätigen sollen, aber weder Zeit noch Fachwissen oder Zugriff auf die Belege haben, wird Human-in-the-Loop zum Stempel. Arbeitsgestaltung muss deshalb Prüfaufwand und Verantwortung explizit berücksichtigen. Ein Agentigramm ordnet jedem produktiven Agenten Ziel, fachlichen Owner, Plattform, Datenzugriff, Werkzeuge, Rechte, Unteragenten und Eskalationsweg zu. Es ergänzt Prozesslandkarten und Organigramm. Es ersetzt weder Verantwortlichkeit noch die rechtliche Zurechnung von Entscheidungen. Das Bild wird besonders wertvoll, wenn ein Agent mehrere Bereiche berührt: Einkauf, Qualität, Produktion und IT.

Dann zeigt die Karte, ob eine End-to-End-Verantwortung existiert oder ob jede Abteilung nur ihren Ausschnitt freigegeben hat. Sie macht auch Plattformabhängigkeiten sichtbar. Das Register ist laufend zu pflegen. Neue Modelle, Tools, Datenquellen und Agentenverbindungen verändern die Berechtigungsfläche. Verantwortlich ist nicht allein die IT; der fachliche Prozessowner muss wissen, welche Entscheidung sein digitaler Akteur vorbereitet oder trifft.

Damit ändert sich die Rolle von Fachwissen. Erfahrung wird nicht überflüssig, sondern zur Voraussetzung für gute Regeln, Ausnahmen und Prüfungen. Wer einen Prozess nicht versteht, kann auch nicht sinnvoll entscheiden, welche Schritte ein Agent übernehmen darf. Gleichzeitig muss Wissen aus Köpfen, Dokumenten und informellen Routinen in überprüfbare Arbeitszusammenhänge überführt werden. Das ist keine vollständige Kodifizierung menschlicher Erfahrung. Es ist eine bewusste Sicherung der Punkte, an denen Qualität, Sicherheit und Lieferfähigkeit hängen. Der produktive Einsatz von Agenten wird so zu einem Programm der Wissensorganisation.

TEIL III · ZUKUNFT · REALITY CHECK

Drei Pfade statt einer Prognose

Szenarien sollen Investitionen robust machen – sie geben keine Eintrittswahrscheinlichkeit vor.

Pfad A - assistierte Auswahl: Agenten recherchieren und vergleichen; Menschen bleiben bei Kauf und Freigabe sichtbar beteiligt. Pfad B - begrenzte Delegation: Agenten erledigen standardisierte, risikoarme Fälle innerhalb von Budget und Regeln. Pfad C - konzentrierte Vermittlung: Wenige Plattformen bündeln Kontext, Suche und Transaktion und gewinnen Verhandlungsmacht. Die Marktberichte 2026 - vom Walmart-Transaktionszugang bis zu Händlerkonflikten um Daten - zeigen, dass verschiedene Architekturen parallel entstehen. Sie belegen nicht, welcher Pfad gewinnt. Die Berichterstattung zu humanoider Robotik zeigt zudem, wie weit physische Autonomie hinter manchen Erwartungen zurückbleiben kann.

Robust über alle Pfade sind: Datenqualität, offene Ausstiegsoptionen, klare Prozesse, kleine Rechte, menschliche Zuständigkeit und Messung. Frühindikatoren sollten konkret sein: tatsächliche delegierte Käufe, belastbare Schnittstellen, operative Agenten außerhalb von Piloten und nachgewiesene Prozesswirkung.

Die drei Pfade sind deshalb keine Vorhersagen, sondern Belastungstests für Entscheidungen. Unternehmen sollten heute so investieren, dass sie in mehreren Entwicklungen handlungsfähig bleiben. Bleibt der Mensch sichtbar in der Auswahl, braucht es vor allem gute Quellen und Assistenzprozesse. Wächst begrenzte Delegation, werden Rechte, Budgets und Protokolle entscheidend. Konzentriert sich Vermittlung bei wenigen Plattformen, gewinnen Datenzugang und Verhandlungsmacht an Gewicht. Robuste Strategie heißt, Abhängigkeiten und Ausstiegsoptionen in jedem Pfad mitzudenken.

DIE DREI HANDLUNGSFELDER

Was wir aus der Deloitte-Dramaturgie übernehmen

Die drei Zukunftsfelder werden mit den Entscheidungen aus „Der dritte Mann“ verbunden – nicht unverändert auf die Agent Journey übertragen.

1. Produktivität und Wertschöpfung sichern. Agenten dort testen, wo Entscheidungslatenz, Suchaufwand oder Abstimmungskosten messbar hoch sind. Wirkung am End-to-End-Prozess prüfen, nicht an Toolnutzung. 2. Wissen in der Arbeit verankern. Kritisches Produkt-, Prozess- und Erfahrungswissen so dokumentieren, dass Menschen und digitale Systeme es prüfen können. Ausnahmen, Grenzen und Quellen müssen mitgeführt werden. 3. Robotik und KI wirksam einbetten. Agenten, Automatisierung und physische Technik nach Risiko und Aufgabenart verbinden. Rechte, Identität, Arbeitsschutz, OT-Sicherheit und menschliche Freigabe gehören in dieselbe Betriebsarchitektur.

Diese Handlungsfelder folgen der in der Deloitte-Referenz gesetzten Logik, Zukunftsfragen mit konkreten Entscheidungsfeldern zu verknüpfen. Für dieses Dossier werden sie auf Kundenzugang, industrielle Wertschöpfung und kontrollierte Handlungsmacht zugeschnitten.

Die drei Handlungsfelder ordnen diese Unsicherheit, ohne sie künstlich aufzulösen. Wertschöpfung fragt nach messbarem wirtschaftlichem Ergebnis. Wissen fragt danach, ob Daten, Erfahrung und Verantwortlichkeit die Entscheidung tragen. Technik und Verantwortung bestimmen, welche Systeme handeln dürfen und wie ihre Grenzen überwacht werden. Keines der Felder kann die anderen ersetzen. Ein technisch sicherer Agent ohne relevanten Prozess bleibt Spielzeug; ein wertvoller Prozess ohne gepflegtes Wissen bleibt fragil; gute Daten ohne Rechtearchitektur können gefährlich breit genutzt werden.

HANDLUNGSFELD 1 · WERTSCHÖPFUNG

Produktivität und Wertschöpfung sichern

Die erste Aufgabe besteht darin, einen wirtschaftlich relevanten Prozess statt eines attraktiven Demos auszuwählen.

Wählen Sie einen Prozess mit hoher Such-, Abstimmungs- oder Nacharbeitslast. Beispiele sind Lieferantenqualifikation, technische Angebotsprüfung, Variantenklärung oder Störungsdiagnose. Vor dem Pilot werden Zeit, Fehler, Kosten, Prüfaufwand und Kundenwirkung gemessen. Ordnen Sie Aufgaben neu: Was kann der Agent parallel sammeln? Was muss ein Fachbereich bewerten? Welche Entscheidungen sind regelgebunden? Wo bleibt eine Ausnahme menschlich? Der neue Ablauf muss eine bestehende Tätigkeit ersetzen oder verbessern - eine zusätzliche KI-Schicht allein schafft noch keinen Wert. Der Pilot endet mit einer dokumentierten Investitionsentscheidung. Geschäftsführung und Fachbereich sehen Baseline, Gesamtkosten, Fehlerfälle, Kontrollaufwand und Skalierungsbedingungen.

BCGs Prozessargument ist hier eine nützliche Hypothese; die eigene Prozessmessung bleibt der Beleg.

Die Auswahl des ersten Prozesses ist damit eine strategische Entscheidung. Attraktive Demos liegen häufig dort, wo Daten leicht verfügbar und Risiken gering sind. Wirtschaftlicher Wert kann jedoch an anderen Stellen entstehen: bei Variantenklärung, Lieferantenqualifikation oder Störungsdiagnose. Der Vorstand sollte deshalb nicht fragen, wo sich ein Agent schnell zeigen lässt, sondern wo eine bessere Entscheidung messbar auf Ergebnis, Lieferfähigkeit oder Kapitalbindung wirkt. Das Ziel ist kein Agentenprojekt, sondern ein verbesserter Wertschöpfungsprozess mit klarer Baseline.

HANDLUNGSFELD 2 · WISSEN

Wissen in der Arbeit verankern

Gute Daten sind nicht nur eine Vorleistung für KI. Sie sichern auch die Kontinuität des Betriebs.

Wählen Sie kritische Produkt- und Prozessinformationen. Halten Sie fest, welche Variante gilt, wer den Nachweis verantwortet, wann er geprüft wurde und welche Ausnahme nicht automatisch entschieden werden darf. Überführen Sie Erfahrungswissen aus Dokumenten, Schichtübergaben und Expertenwissen in prüfbare Arbeitsanweisungen. Die Wissensbasis muss sowohl für den Agenten als auch für den Menschen verständlich sein. Quellenangabe, Gültigkeit und Versionsstand dürfen beim Zusammenfassen nicht verschwinden. Ein Agent sollte zeigen, auf welche Regel oder Messung er sich stützt, statt eine glatte Antwort ohne Herkunft zu liefern. Das schützt gegen den Verlust von Erfahrungswissen und gegen Automatisierungsfehler.

Jede Verbesserung durch Agenten muss mit einer Methode verbunden sein, wie Fachkräfte Fehler korrigieren und Wissen zurück in den Prozess geben.

Wissen muss dabei im Arbeitsablauf verankert werden, nicht in einem zusätzlichen Archiv. Eine Quelle ist nur dann nützlich, wenn Mitarbeitende und Systeme wissen, wann sie gilt, für welche Variante sie gilt und wer Änderungen verantwortet. Besonders kritisch sind Ausnahmen: Sie markieren häufig genau die Erfahrung, die in Standarddokumenten fehlt. Unternehmen sollten deshalb nicht versuchen, alles zugleich zu erfassen. Sie sollten bei den Entscheidungen beginnen, deren Fehler teuer sind, und dort Provenienz, Gültigkeit und fachliche Zuständigkeit sichtbar machen.

HANDLUNGSFELD 3 · TECHNIK UND VERANTWORTUNG

Robotik und KI wirksam einbetten

Digitale Agenten, klassische Automatisierung und physische Robotik brauchen klare Schnittstellen und unterschiedliche Schutzgrenzen.

Definieren Sie den Aktionsraum jedes Systems. Ein Agent darf vielleicht einen Wartungsfall priorisieren, aber keine Anlage stoppen. Ein Robotersystem kann eine freigegebene Bewegung ausführen, aber nicht eigenständig den Produktionsplan ändern. Systemrollen müssen im Prozess sichtbar sein. Verbinden Sie IT- und OT-Sicherheit: Identität, minimale Rechte, Segmentierung, Protokoll, Sicherheitsfreigabe und sicherer Rückfall. NISTs laufende Agenteninitiative unterstreicht die offenen Fragen zu Interoperabilität und Identität; sie nimmt Unternehmen die eigene Risikoanalyse nicht ab. Führen Sie neue Rechte stufenweise ein: Schattenbetrieb, Vorschlag mit Freigabe, begrenzte Aktion, erst danach gegebenenfalls breitere Automatisierung.

Jede Stufe braucht realistische Fehlertests und einen klaren Abschaltweg.

Technische Integration wird wirksam, wenn sie die Grenzen zwischen digitaler Empfehlung, klassischer Automatisierung und physischer Aktion ausdrücklich gestaltet. Ein Agent kann einen Auftrag vorbereiten, ein ERP ihn verbuchen und eine Anlage ihn ausführen - doch Verantwortung darf in dieser Kette nicht verschwinden. Jede Systemrolle benötigt einen definierten Aktionsraum. Neue Rechte werden stufenweise vergeben: zunächst im Schattenbetrieb, dann als Vorschlag mit Freigabe und erst später als begrenzte Aktion. Skalierung folgt dem Nachweis, nicht der Begeisterung.

FRAGEN AUS DEM EXECUTIVE WEBCAST

Fragen, die Entscheidungen öffnen

Die Fragen sind redaktionell formulierte Leitfragen, keine Zitate aus einem tatsächlich geführten Webcast.

Zu Handlungsfeld 1 - Wertschöpfung: Welche Entscheidung im Vertrieb, Einkauf oder Werk ist heute langsam, fehleranfällig oder teuer? Woran würden wir nach 90 Tagen erkennen, dass ein Agent den Ablauf tatsächlich verbessert? Zu Handlungsfeld 2 - Wissen: Welches Wissen hängt an einzelnen Beschäftigten oder unstrukturierten Dokumenten? Wie sichern wir, dass ein Agent Änderungen, Varianten und Ausnahmen korrekt behandelt - und Mitarbeitende die Aussage überprüfen können? Zu Handlungsfeld 3 - Technik: Welche Handlungen dürfen digitale und physische Systeme eigenständig ausführen?

Wer setzt Grenzen, überwacht Ergebnisse und stoppt den Ablauf, wenn Quelle, Situation oder Risiko unklar sind? Querschnitt: Was können wir aus Japan und anderen Hochlohnländern über Produktivität, Standards und Qualifizierung lernen? Welche Elemente sind auf deutsche Werke übertragbar - und welche hängen an dortigen Institutionen, Arbeitsbeziehungen oder Investitionsbedingungen?

Gute Vorstandsfragen verhindern, dass die Diskussion in abstrakte Techniksprache ausweicht. Sie verbinden jeden Vorschlag mit einer Entscheidung, einem Verantwortlichen und einem Beleg. Wo genau entsteht heute Verlust? Welche Daten tragen die Empfehlung? Wer erkennt eine Ausnahme? Welche Aktion bleibt dem Menschen vorbehalten? Und woran wird nach 90 Tagen entschieden, ob der Versuch fortgesetzt wird? Solche Fragen sind unbequem, weil sie aus einer Vision einen überprüfbaren Auftrag machen. Gerade deshalb öffnen sie Entscheidungen, statt sie zu vertagen.

VORSTANDSAGENDA · 12 MONATE

Vom Dossier zur Führungsentscheidung

Drei Programme, ein Verantwortungsmodell und sichtbare Entscheidungspunkte machen die Strategie ausführbar.

Monate 1-3: Agentenregister und Zugriffsinventar anlegen. Zwei bis drei Prozesse auswählen. Baselines und Risikoklassen festlegen. Angebote und kritische Produktdaten auf Varianten, Quellen und Aktualität prüfen. Monate 4-6: Piloten im Schattenbetrieb starten. Fehlerfälle, manipulierte Quellen, fehlende Nachweise und Eskalationen testen. Betriebsrat, Informationssicherheit, Fachbereich und IT/OT früh einbinden. Monate 7-9: Ergebnisse mit der Baseline vergleichen. Kontrollaufwand und Vollkosten einrechnen. Stoppen, ändern oder begrenzt skalieren. Rollen, Schulung und Rückfallverfahren verbindlich machen. Monate 10-12: Nur nach belastbarem Nachweis skalieren. Kundenzugang und Plattformverträge überprüfen. Szenarien und Frühindikatoren aktualisieren.

Der Vorstand erhält ein Profil aus Wert, Risiko, Evidenz und Verantwortlichkeit statt einer allgemeinen Reifegradzahl.

Die Zwölf-Monats-Agenda ist kein Rolloutplan für möglichst viele Agenten. Sie ist ein Führungsprogramm, das Ordnung vor Reichweite setzt. In den ersten Monaten werden Agenten, Zugriffe und Prozesse sichtbar gemacht. Danach folgen Piloten mit realistischen Fehlerfällen. Erst die dritte Phase verbindet Wirkung, Vollkosten und Kontrollaufwand. Skalierung ist die letzte, nicht die erste Entscheidung. Auf diese Weise entsteht eine belastbare Lernkurve: Das Unternehmen gewinnt Geschwindigkeit, ohne die Fähigkeit zu verlieren, einen Prozess zu verstehen, zu stoppen und neu zu gestalten.

QUELLEN UND EINORDNUNG

Die wichtigsten Grundlagen der Auswertung

Ausgewählt nach Relevanz für Marktverschiebung, industrielle Anwendung, Forschung und sichere Einführung.

McKinsey & Company (2026): The State of AI in 2026 - On the Road to ROI. Globale Befragung; Selbstberichte, keine isolierte Agentenwirkung.

KPMG / EHI Retail Institute (2026): Consumer Snapshot: Wenn KI für uns einkauft. Deutsche Verbraucherbefragung zu Nutzung und Kaufdelegation.

Deloitte Insights (2026): Resilient by Design: The Agentic Supply Chain. Architektur- und Use-Case-Rahmen, kein Nachweis breiter Marktreife.

NIST / Center for AI Standards and Innovation (2026): AI Agent Standards Initiative. Primärquelle zu Interoperabilität und Sicherheit.

Meta AI und Reuters (08.09.2026): Produktankündigung und journalistische Einordnung von Muse; Anbieterangaben und Beobachtungen getrennt bewertet.

Reuters (07.08.2026): Retailers Tap AI Shopping Traffic but Fight to Keep Customer Data. Gegenperspektive zu Plattformmacht und Kundenzugang.

Siemens AG (20.04.2026): Launch of the Eigen Engineering Agent. Anbieterquelle zu Status, Einsatz und Leistungsversprechen.

Elbasheer et al. (2025): Natural Language-driven Production Planning. Technischer Prototyp, keine Langzeit-Feldstudie.

Jannelli et al. (2025): Agentic LLMs in the Supply Chain. Peer-reviewte Fallstudie unter definierten Bedingungen.

Microsoft / EnBW (22.10.2026): Agenten als Operating Model im Einkauf. Ziele und Prognosen sind nicht mit bereits erzielter Wirkung gleichgesetzt.

Allianz (03.11.2025): Project Nemo. Anbieterbericht zu sieben Agenten im Schadenprozess; Auszahlung bleibt menschlich kontrolliert.

OpenAI Developers (Abruf 23.10.2026): Agentic Commerce Protocol. Technische Spezifikation, kein Beleg flächendeckender Nutzung.

BEGRIFFE · 1/2

Die Sprache der Agent Journey

Die zentralen Begriffe werden im Dossier in einem klar abgegrenzten Sinn verwendet.

KI-Agent. Softwaresystem, das ein Ziel in Schritte zerlegt, Werkzeuge oder Datenquellen nutzt und Ergebnisse oder Aktionen erzeugt.

Agentic AI. Sammelbegriff für Systeme, die über einzelne Antworten hinaus Aufgaben planen und innerhalb definierter Grenzen ausführen.

Multi-Agent-System. Mehrere spezialisierte Agenten teilen Aufgaben oder prüfen Ergebnisse. Mehr Agenten bedeuten nicht automatisch bessere Ergebnisse.

Workflow. Zusammenhängender Ablauf aus Aufgaben, Daten, Systemen, Freigaben und Verantwortlichen - vom Auslöser bis zum Ergebnis.

Human-in-the-loop. Ein Mensch prüft oder genehmigt einen Schritt. Die Prüfung braucht Zeit, Kompetenz und Zugriff auf Belege.

IT und OT. IT verarbeitet Geschäfts- und Informationsdaten; OT überwacht oder steuert physische Anlagen und Produktionsprozesse.

API. Technische Schnittstelle für Daten und Funktionen. Sie regelt nicht automatisch Bedeutung, Qualität oder Nutzungsrechte.

Digitaler Zwilling. Digitales Modell eines Produkts, einer Anlage oder eines Prozesses; nur so verlässlich wie Daten und Annahmen.

Maschinenlesbarkeit. Informationen sind so strukturiert, dass Software ihre Bedeutung zuordnen kann. Das ist kein Gütesiegel für Wahrheit.

Google Zero. Arbeitsbegriff für eine Suche, in der Antworten direkt in Such- oder KI-Oberflächen erscheinen und der Klick zur Quelle entfällt.

BEGRIFFE · 2/2

Daten, Kontrolle und Nachweis

Wo die Branche mehrere Bedeutungen nutzt, benennt INFPRO die für dieses Dossier verwendete Lesart.

Provenienz. Herkunft und Verlauf einer Information: Urheber, Quelle, Bestätigung und Zeitpunkt der Prüfung.

Grounding / Belegbindung. Eine Antwort wird mit konkreten Quellen oder freigegebenen Daten verknüpft. Das verbessert Prüfbarkeit, beseitigt Fehler aber nicht.

Prompt Injection. Angriff, bei dem Inhalte oder Eingaben einen Agenten dazu bringen sollen, Regeln zu missachten oder unzulässige Aktionen auszuführen.

Schattenbetrieb. Der Agent verarbeitet reale oder historische Fälle, führt aber noch keine produktive Aktion aus.

Red Team. Unabhängiger Test, der Angriffe, Fehlkonfigurationen und unerwünschte Folgen realistisch nachstellt.

Baseline. Messbarer Ausgangswert vor einer Veränderung, etwa Bearbeitungszeit, Fehlerquote, Kosten oder Nacharbeit.

ERP. Unternehmenssoftware für zentrale Abläufe wie Einkauf, Produktion, Lager, Finanzen und Aufträge.

RPA. Regelbasierte Automatisierung wiederkehrender Schritte; nicht identisch mit einem lernenden KI-Agenten.

Agent Readiness. INFPRO-Prüfraster für Auffindbarkeit, Verständlichkeit, Verifizierbarkeit, Zugänglichkeit, Handlungsfähigkeit und Steuerbarkeit.

Agentigramm. INFPRO-Begriff für eine Übersicht über Agenten, Verantwortliche, Datenzugriffe, Werkzeuge, Rechte und Abhängigkeiten.

Supply Chain. Liefer- und Wertschöpfungsnetzwerk aus Lieferanten, Werken, Logistik, Kunden sowie Material- und Informationsflüssen.

SCHLUSS · 1/2

Der dritte Mann ist kein Produkt

Er ist eine neue Rolle in der Beziehung zwischen Kunde, Unternehmen und Entscheidung.

Die Debatte über KI-Agenten leidet darunter, dass sie zu oft bei den Produkten beginnt. Dann stehen Namen, Modelle und Funktionen im Mittelpunkt. Für Unternehmen ist jedoch etwas anderes entscheidend: Ein digitaler Akteur tritt in Abläufe ein, in denen bislang Menschen gesucht, verglichen, verhandelt und freigegeben haben. Seine Bedeutung entsteht nicht aus seiner Oberfläche, sondern aus der Position, die er im Prozess erhält.

Meta Muse macht diese Verschiebung sichtbar. Der Konflikt mit Amazon ist mehr als eine Episode zwischen zwei Plattformen. Er zeigt, dass der Zugang zum Kunden, die Identität eines handelnden Systems und die Kontrolle über die Transaktion neu ausgehandelt werden. Der Agent kann dem Kunden dienen, dem Plattformbetreiber, dem Händler - oder mehreren Interessen zugleich. Gerade deshalb genügt es nicht, ihn als bequemes Werkzeug zu beschreiben.

In der industriellen Wertschöpfung ist die Lage noch anspruchsvoller. Dort entscheidet ein Fehler nicht nur über eine unpassende Empfehlung. Er kann Lieferfähigkeit, Qualität, Vertrag oder Sicherheit berühren. Agenten werden deshalb nicht dadurch wertvoll, dass sie möglichst selbstständig erscheinen. Wertvoll werden sie, wenn sie einen klar bestimmten Teil der Arbeit besser erledigen, ihre Quellen zeigen, Grenzen respektieren und eine Übergabe an verantwortliche Menschen beherrschen.

Der dritte Mann ist somit kein Gast, der eines Tages an die Tür klopft. Er sitzt bereits in Suchergebnissen, Vorauswahlen, Planungsprozessen und Plattformregeln. Die strategische Aufgabe besteht darin, seine Rolle zu benennen, bevor Gewohnheit oder Anbieterarchitektur sie stillschweigend festlegen.

SCHLUSS · 2/2

Verantwortung lässt sich nicht outsourcen

Die Agent Journey verändert die Arbeitsteilung. Sie hebt die Verantwortung des Unternehmens nicht auf.

Die Zukunft der Agenten wird weder als geradliniger Siegeszug noch als kurze Mode verlaufen. Dafür sind Märkte, Datenlagen und Risiken zu verschieden.

Wahrscheinlich ist eine ungleichzeitige Entwicklung: In manchen Prozessen bleiben Agenten Assistenten, in anderen übernehmen sie begrenzte Handlungen, und an wenigen Stellen entstehen weitgehend autonome Ketten. Wer daraus heute eine einzige Prognose ableitet, verwechselt Richtung mit Gewissheit.

Robust ist deshalb keine Strategie, die auf maximale Autonomie setzt. Robust ist eine Strategie, die mehrere Entwicklungen aushält. Sie hält eigene Quellen zugänglich, wahrt den Kundenzugang, ordnet Produkt- und Prozessdaten und definiert Rechte pro Aufgabe. Sie misst nicht, wie viele Agenten eingeführt wurden, sondern ob Entscheidungen besser, Abläufe verlässlicher und Fehler beherrschbarer geworden sind.

Google Zero bleibt dabei der Grundstein, nicht das Gebäude. Maschinen müssen Informationen finden und verstehen können. Doch Sichtbarkeit allein schafft weder Vertrauen noch Wertschöpfung. Entscheidend ist, ob Aussagen einer gültigen Variante, einem Zeitraum, einer Quelle und einem Verantwortlichen zugeordnet werden können. Erst dann entsteht aus digitaler Lesbarkeit eine belastbare Entscheidungsgrundlage.

Die wichtigste Veränderung ist daher organisatorisch. Fachwissen wandert nicht einfach in ein Modell. Es muss Regeln, Ausnahmen und Freigaben prägen. Management wiederum darf Verantwortung nicht an Technik delegieren, nur weil deren Entscheidungen schneller erscheinen. Je näher ein Agent an Geld, Vertrag oder Maschine rückt, desto genauer muss sichtbar sein, wer ihn beauftragt, wer ihn begrenzt und wer ihn stoppt.

Der dritte Mann verändert die Wertschöpfung, weil er zwischen Absicht und Handlung tritt. Ob er zum nützlichen Vermittler oder zum unkontrollierten Machtfaktor wird, entscheidet sich nicht im Modell allein. Es entscheidet sich in der Architektur des Unternehmens.



Weiterdenken. Tiefer einsteigen.

www.infpro.de

INFPRO

INSTITUT FÜR PRODUKTIONSERHALTUNG

© 2026