Whitepaper KI im Mittelstand

Ein Leitfaden für erfolgreiche Implementierung

Axel Wiemann
kiucon
www.kiucon.com

Patrick Helmig
Omnifact
omnifact.ai

Sebastian Hennerici
Omnifact Academy
https://www.omnifact-academy.de/

Sven-Erik Holm
GvW Graf von Westphalen
GvW.com

kiucon Omnifact Omnifact ACADEMY GvW

INHALTSVERZEICHNIS

Executive Summary 4

Einleitung 6

Ausgangssituation und Marktkontext 7
Die Herausforderung 7
Der Transformationsansatz 8
Aufbau und Methodik des Whitepapers 8
Die Autoren 9

Strategische Betrachtung 14

Geschrieben von Axel Wiemann, kiucon 14
Einleitung 15
Von der Evolution zur Disruption 16
Die strategische Bedeutung von KI für Unternehmen 18
Herausforderungen bei der Integration von KI 18
Entwicklung einer nachhaltigen KI-Strategie 19

Rechtliche Rahmenbedingungen und KI Act 31

Einführung 32
Anwendbare Gesetze und Vorschriften 32
Maßnahmen für die Geschäftsleitung 35
Fazit 36

Mitarbeiter und Operative Einführung 37

Einleitung 38
KI-Kompetenz als strategischer Erfolgsfaktor 38
Bedarfsgerechte KI-Trainings 41
Aufbau und Inhalte von KI-Trainings 44
Kontinuierliche Weiterentwicklung der KI-Readiness und KPIs 46

Software, Technologie und IT-Einführung 48

Technische Architektur 49
KI Rollout als Evolution 53
Security-Framework 54

Fazit und Ausblick 63

Die Transformation als fortlaufender Prozess 64
Die Bedeutung strategischer Entscheidungen 64
Die zentrale Rolle des Menschen 64
Technologische Fundamente für die Zukunft 65
Ausblick in die Zukunft 65

Executive Summary

Die rasante Entwicklung der Künstlichen Intelligenz (KI) stellt Unternehmen vor eine fundamentale Transformation. Moderne generative KI-Modelle haben in den letzten Monaten eine beispiellose Leistungs steigerung erfahren, die neue Anwendungsfälle in bisher unerreichter Komplexität und Effizienz ermöglicht.[1] **Diese Entwicklung erfordert von Unternehmen eine strategische Neuausrichtung, bei der KI nicht mehr als isolierte Technologie, sondern als integraler Bestandteil der Wertschöpfungskette verstanden wird.** Der Fokus muss dabei auf der Schaffung von Strukturen liegen, die die nahtlose Integration von KI in bestehende Systeme und Prozesse gewährleisten.

Die erfolgreiche Implementierung von KI ist eng mit der Fähigkeit verbunden, unternehmensweite Daten effektiv zu nutzen und KI-Systeme sicher und datenschutzkonform zu betreiben. **Eine modulare Architektur, die auf Open-Source-Lösungen und standardisierten Schnittstellen basiert, ist dabei von entscheidender Bedeutung.** Sie ermöglicht es Unternehmen, flexibel auf neue Technologien zu reagieren und Abhängigkeiten von einzelnen Anbietern zu minimieren. Ein durchdachtes Sicherheitskonzept, das sowohl klassische IT-Sicherheitsbedrohungen als auch KI-spezifische Risiken adressiert, ist unerlässlich, um das Vertrauen in KI-Systeme zu stärken und die Einhaltung rechtlicher Vorgaben sicherzustellen. **Agentische Workflows, die bestehende Systeme als Tools verstehen und nutzen, bilden das Fundament für intelligente Automatisierung von komplexen Geschäftsprozessen.**

Zentral für den Erfolg ist die aktive Einbindung der Mitarbeiter in den Transformationsprozess. Der **Kompetenzaufbau im Bereich KI ist nicht nur eine technische, sondern auch eine organisatorische und kulturelle Aufgabe**. Unternehmen müssen ihre Mitarbeiter befähigen, KI-Systeme effektiv zu nutzen, kritisch zu hinterfragen und in ihre Arbeitsabläufe zu integrieren. Durch gezielte Schulungsprogramme und die Etablierung einer Innovationskultur kann die Belegschaft zu einem aktiven Gestalter des Wandels werden. Die Schaffung von interdisziplinären Teams und Kompetenzzentren ist dabei ein Schlüssel, um das Wissen und die Fähigkeiten der Organisation zu bündeln und Synergien zu nutzen.

Die KI-Revolution ist ein fortlaufender Prozess, der eine kontinuierliche Weiterentwicklung von Technologien und Prozessen erfordert. Unternehmen, die die strategischen, technischen und kulturellen Herausforderungen meistern, werden in der Lage sein, die Chancen der KI zu nutzen und sich eine führende Position in einer zunehmend digitalisierten Welt zu sichern. **Die Zukunft gehört dabei denjenigen, die es verstehen, die Potenziale der Künstlichen Intelligenz zum Nutzen ihrer Unternehmen und ihrer Mitarbeiter einzusetzen und dabei die zentrale Rolle des Menschen nicht aus den Augen verlieren.**

1 https://arxiv.org/abs/2309.13059
Bubeck, S., et al. (2023). Sparks of Artificial General Intelligence: Early experiments with GPT-4. (Zugriff 19. Dezember 2023)

Einleitung

Ausgangssituation und Marktkontext

Künstliche Intelligenz transformiert die Arbeitswelt fundamental. Die rasante Entwicklung generativer KI-Modelle, insbesondere von *Agenten*-basierten Systemen, die verschiedene Tools orchestrieren, eröffnet neue Dimensionen der Automatisierung in Unternehmen. ChatGPT markierte mit über 100 Millionen Nutzern [2] in zwei Monaten einen Meilenstein, während McKinsey-Analysen prognostizieren, dass KI-Technologien bis zu 30% der Büroarbeit unterstützen oder automatisieren können.[3]

Diese Entwicklung erfordert vom deutschen Mittelstand eine grundlegende Neuausrichtung der Arbeitsweisen und Prozesse. Die Marktdynamik ist beispiellos, da neue KI-Modelle und Anwendungen in immer kürzeren Abständen erscheinen und deren Leistungsfähigkeit kontinuierlich steigt. Dies bietet ein enormes Potenzial für Effizienzsteigerung und Innovation, erfordert jedoch auch eine strategische und organisatorische Neuausrichtung.

Die Herausforderung

Trotz des Potenzials bleiben die tatsächlichen Effizienzgewinne in Unternehmen hinter den Erwartungen zurück. Die Herausforderung liegt weniger in der KI-Technologie selbst, als vielmehr in der nahtlosen Integration mit bestehenden Unternehmensanwendungen und Datenquellen. Es mangelt an Werkzeugen, die diese komplexe Tool-Integration ermöglichen und dabei höchste Anforderungen an Datenschutz und Sicherheit erfüllen. Neben technischen und rechtlichen Rahmenbedingungen – von der Datensouveränität über den EU AI Act bis hin zu Datenschutzbestimmungen – erfordert die erfolgreiche Implementierung von KI fundamentale Änderungen in der Arbeitsweise und Organisationsstruktur. Diese Transformation muss so gestaltet sein, dass sie die operative Exzellenz nicht gefährdet, sondern systematisch stärkt und die Datensouveränität sicherstellt.

2 https://www.tagesschau.de/wirtschaft/digitales/chatgpt-wachstum-bezahlangebot-abo-101.html
Tagesschau: ChatGPT-Boom: Wachstum, Bezahlabo und Konkurrenz.

3 https://www.mckinsey.de/~/media/mckinsey/locations/europe%20and%20middle%20east/deutschland/news/presse/2024/2024%20-%2005%20-%2023%20mgi%20genai%20future%20of%20work/mgi%20report_a-new-future-of-work-the-race-to-deploy-ai.pdf
McKinsey: A new future of work: The race to deploy AI. (Zugriff Mai 2024)

Der Transformationsansatz

Die erfolgreiche Integration von KI erfordert einen ganzheitlichen Transformationsansatz. Statt punktueller Lösungen braucht es eine systematische Herangehensweise, die technologische, organisatorische und kulturelle Aspekte vereint. Erfolgreiche Organisationen zeichnen sich dadurch aus, dass sie KI nicht als einzelnes IT-Projekt verstehen, sondern als fundamentalen Wandel in der Art, wie sie arbeiten und Wert schaffen.

Zentral ist dabei die Entwicklung einer nachhaltigen Adaptionsfähigkeit: Die Organisation muss in die Lage versetzt werden, kontinuierlich neue KI-Möglichkeiten zu evaluieren, zu integrieren und zu skalieren. Dies erfordert klare Governance-Strukturen, systematischen Kompetenzaufbau und eine Kultur des kontinuierlichen Lernens. Der Fokus liegt dabei nicht auf der Technologie selbst, sondern auf ihrer effektiven Nutzung zur Steigerung der Unternehmensleistung.

Aufbau und Methodik des Whitepapers

Dieses Whitepaper vereint die Expertise aus Technologie, Beratung und Recht, um einen praxisorientierten Leitfaden für die KI-Transformation im Mittelstand zu bieten. Der Aufbau folgt dabei der logischen Sequenz einer erfolgreichen Implementation: von der strategischen Planung über rechtliche und organisatorische Aspekte bis zur technischen Umsetzung. Jedes Kapitel verbindet theoretische Grundlagen mit praktischen Handlungsempfehlungen und konkreten Beispielen aus der Praxis.

Die Expertise der Autoren spiegelt die verschiedenen Dimensionen der KI-Transformation wider: Technologische Kompetenz durch Omnifact, strategische Beratungsexpertise durch kiucon, praktische Implementierungserfahrung durch Sebastian Hennerici sowie rechtliche Expertise durch Graf von Westphalen. Diese Multiperspektivität gewährleistet eine ganzheitliche und praxisorientierte Betrachtung der Herausforderungen und Lösungsansätze.

Die Autoren

Axel Wiemann

Business Angel, Unternehmer und CEO von kiucon
axel.wiemann@kiucon.com

Als Geschäftsführer von kiucon verbindet Axel Wiemann langjährige Erfahrung in der Entwicklung innovativer Technologien mit strategischer Unternehmensführung. Seine Expertise liegt in der Umsetzung maßgeschneiderter Lösungen, die Unternehmen dabei unterstützen, aktuelle Herausforderungen der digitalen Transformation zu meistern.

Als erfahrener Seriengründer und Investor in Bereichen wie Greentech, Energie & Mobilität, Bildung und Deep Tech hat er erfolgreich verschiedene Unternehmen aufgebaut, begleitet und mehrere Exits realisiert. Seine Tätigkeiten in unterschiedlichen Branchen wie Telekommunikation und renewable energy sowie eine Vielzahl an unterschiedlichsten Beratungsprojekten auf CXO-Ebene prägen seinen ganzheitlichen Ansatz in der Unternehmensentwicklung.

Mit kiucon verfolgt er die Mission, Unternehmen durch den Einsatz fortschrittlicher Technologien zukunftsfähig zu machen. Sein besonderer Fokus liegt dabei auf der Entwicklung nachhaltiger Lösungen, die Effizienz und Benutzerfreundlichkeit vereinen und sich nahtlos in bestehende Strukturen integrieren lassen. Vor diesem Hintergrund kommt ihm unter anderem seine über 10-jährige Erfahrung als Interim Manager im Kontext zahlreicher großer Transformationen bei Konzernen zugute. Dazu zählen internationale M&A-Projekte, Post-Merger-Integrationen, Outsourcing, Spinoffs und Carve-outs, die Einführung von Softwareplattformen sowie Nachhaltigkeitsprojekte.

Durch die Gründung von Startups (Big Data/Cloud) im Technology und Dienstleistungsbereich kennt er die Perspektive des Unternehmers. Als Mentor bei Plattformen wie dem e-combinator/Bryck und anderen unterstützt er Start-ups und Entrepreneure bei der Umsetzung ihrer Ideen.

Seine Leidenschaft ist es, Start-ups und Scale-ups dabei zu helfen, erfolgreich zu sein, um einen Beitrag zur Beschleunigung der Nachhaltigkeitstransformation zu leisten, den Klimawandel zu bekämpfen, Bildung zu digitalisieren und technologiegetriebene multimodale Ökosysteme und Plattformen für eine bessere Welt zu etablieren.

In diesem Whitepaper bringt er insbesondere seine Expertise in den Bereichen

- Strategieentwicklung und -aktivierung, Geschäftsmodellentwicklung
- Design und Steuerung hochkomplexer Transformationen in dynamischen Umfeldern
- Technologieentscheidungen für die digitale Transformation vor dem Hintergrund der Entwicklung künstlicher Intelligenz
- Innovation, Entrepreneurship und Organisationsentwicklung
- Entwicklung nutzerzentrierter Lösungen zur Prozessautomatisierung und Effizienzmanagement ein.

Seine Perspektive ist dabei geprägt von der Überzeugung, dass Zukunftsfähigkeit maßgeblich von einer nachhaltigen und ganzheitlichen Strategie, hoher Umsetzungsqualität, klarem Fokus und einem intelligenten Zusammenspiel zwischen Mensch und Technologie, Kultur und Kommunikation abhängt. Künstliche Intelligenz einzuführen bedeutet, heute die richtigen strategischen Weichen zu stellen – von der Auswahl der Anwendungsfelder und Technologiepartner über Aspekte wie Organisation und Governance bis zur Implementierungsstrategie.

Patrick Helmig
CEO & Co-Founder Omnifact
patrick@omnifact.ai

Als CEO von Omnifact verbindet Patrick Helmig langjährige Erfahrung in der Entwicklung von KI-Lösungen, insbesondere für datenschutzsensible und hochregulierte Branchen, mit strategischer Unternehmensführung. Seine Expertise liegt in der Überwindung der technischen und organisatorischen Hürden bei der Integration von KI in bestehende Unternehmensstrukturen, wobei er stets die Notwendigkeit der Vereinbarkeit von intuitiver Nutzbarkeit mit hohen Sicherheitsanforderungen im Blick behält. Er verfügt über mehr als zehn Jahre Erfahrung in der Entwicklung digitaler Lösungen für Branchen wie Banken, Medizin und Pharma.

Nach seinem Studium der Informatik und BWL war er Mitgründer von Rocketloop, einem Unternehmen, das sich auf die Entwicklung digitaler Produkte und individueller KI-Lösungen spezialisierte. Die dort gesammelten Erfahrungen in der Konzeption und Umsetzung komplexer KI-Systeme prägen heute die Entwicklung von Omnifact: Die Plattform verbindet Benutzerfreundlichkeit mit Enterprise-Grade Sicherheit und ermöglicht es Unternehmen, KI-Assistenten zu entwickeln, die sich nahtlos in bestehende Systeme integrieren – und das unter Berücksichtigung strengster Datenschutzbestimmungen.

Mit Omnifact verfolgt er die Mission, Unternehmen die sichere und effektive Nutzung von KI zu ermöglichen. Sein besonderer Fokus liegt dabei auf der Entwicklung von Lösungen, die Datenschutz und Benutzerfreundlichkeit vereinen und es Organisationen ermöglichen, schrittweise und kontrolliert KI-Fähigkeiten aufzubauen.

In diesem Whitepaper bringt er insbesondere seine Expertise in den Bereichen:

- Strategische Technologie-Entscheidungen (Open Source vs. proprietäre Lösungen)
- Nutzerzentrierte Ansätze zur KI-gestützten Automatisierung
- Aufbau zukunftsfähiger KI-Architekturen ohne problematische Abhängigkeiten
- Technische Integration und Skalierung von KI-Systemen
- Datenschutz und -sicherheit in hochregulierten Industrien ein.

Seine Perspektive ist dabei geprägt von der Überzeugung, dass KI eine langfristige Transformation der Arbeitswelt einleitet. Entsprechend wichtig ist es, heute die richtigen strategischen Weichen zu stellen – von der Wahl der Technologie-Partner bis zur Art der Implementation.

Sebastian Hennerici
CEO & Founder Omnifact Academy
sebastian@omnifact-academy.de

Als CEO und Gründer der Omnifact Academy verbindet Sebastian Hennerici langjährige Erfahrung im Aufbau und der Operationalisierung von Enterprise-KI-Strategien mit fundiertem Know-how in der Entwicklung skalierbarer KI-Trainingslösungen. Sein Fokus liegt darauf, Unternehmen bei der nachhaltigen Implementierung zukunftsweisender Technologien zu unterstützen, indem er sowohl strategische als auch operative Herausforderungen adressiert. Er verfügt über mehr als ein Jahrzehnt Erfahrung in der Entwicklung digitaler Produkte, im Management von KI-Ventures und in der Einführung generativer KI-Systeme in hochregulierten Branchen wie Banken, Versicherungen und Finanzdienstleistungen.

Nach seinem betriebswirtschaftlichen Studium an der Goethe Universität Frankfurt sowie der Mitgründung eines KI-Start-ups gewann er wertvolle Erkenntnisse in einem führenden Finanzinstitut, wo er verantwortlich für Konzeption, Pilotierung und Rollout komplexer KI-Anwendungen war. Diese Erfahrungen fließen in die Omnifact Academy ein, deren Angebote von praxisnahen Trainingsformaten bis zur konkreten Begleitung von KI-Einführungsprojekten reichen. So sorgt er dafür, dass Unternehmen ihre Teams gezielt befähigen können, KI-Fähigkeiten aufzubauen, um langfristig Wettbewerbsfähigkeit und Effizienz zu steigern – unter Einhaltung hoher Standards in puncto Regulatorik und Datenschutz.

Mit der Omnifact Academy verfolgt er die Mission, Unternehmen die schrittweise und kontrollierte Entwicklung von KI-Kompetenzen zu ermöglichen. Sein besonderer Fokus liegt dabei auf der Gestaltung von Trainingsformaten, die neben Wissensvermittlung auch höchste Standards im Bereich Aktualität, Praxisrelevanz und regulatorische Konformität erfüllen. So entsteht ein Angebot, das sowohl die strategische Weichenstellung als auch die operative Umsetzung von KI-Initiativen unterstützt.

In diesem Whitepaper bringt er insbesondere seine Expertise folgenden Bereichen ein:

- Mitarbeiterbefähigung durch zielgerichtete Trainingsformate
- Gewinnung von Produktivität am Arbeitsplatz durch effiziente KI-Workflows
- Praxisnahe Umsetzung von KI Use Cases in bestehenden Unternehmensprozessen
- Jahrelang verantwortliche Rolle für das Thema KI in einer Bank
- Governance (Regulatorik und Prozessvorgaben)-konforme Umsetzung von KI-Projekten und Use Cases

Sebastians Perspektive ist dabei von Optimismus geprägt: Er ist überzeugt, dass KI nicht nur neue Effizienzpotenziale und Wachstumsmöglichkeiten schafft, sondern auch den Menschen dabei unterstützt, mehr Freude an ihrer Arbeit zu finden. Durch den Wegfall monotoner Tätigkeiten und die Stärkung kreativer Spielräume gewinnen Mitarbeitende an Selbstbestimmung und Motivation – ein Ansatz, der langfristig nicht nur wirtschaftlichen Erfolg, sondern auch ein erfüllendes Arbeitsleben fördert.

Sven-Erik Holm

Rechtsanwalt bei GvW Graf von Westphalen
S.Holm@gvw.com

Als Rechtsanwalt in einer der führenden deutschen Kanzleien verfügt Sven-Erik Holm über langjährige Beratungserfahrung im Bereich Tech & Data. Seine Beratungsschwerpunkte liegen dabei insbesondere in den Bereichen Datenschutz und IT-Vertragsrecht mit Fokus auf aktuelle EU-Gesetzgebung, wie die EU-KI-Verordnung.

Bereits im Studium hat er sich intensiv mit IT- und Datenschutzrecht im Rahmen seines Schwerpunktstudiums beschäftigt und seine Kenntnisse und Fähigkeiten in diesen Rechtsgebieten durch entsprechende Stationen als Wissenschaftlicher Mitarbeiter sowie als Referendar ausgebaut und vertieft.

Im Rahmen seiner anwaltlichen Tätigkeit berät und begleitet er seit nunmehr rund sieben Jahren Unternehmen aller Art und Größe sowie die öffentliche Hand bei der Planung und Umsetzung von IT-Projekten; er berät insoweit sowohl Kunden- als auch Anbieterseite. Teil der Beratungsleistung ist stets auch die regulatorische Komponente mit Blick auf Datenschutz, IT-Sicherheit und seit 2024 insbesondere die EU-KI-Verordnung.

In diesem Whitepaper bringt er insbesondere seine Expertise in den Bereichen Datenschutz und EU-KI-Verordnung ein. Er ist davon überzeugt, dass die Einführung von KI eine grundlegende Transformation der Wirtschaft- und Arbeitswelt bedeutet, sodass sehr frühzeitig auch die rechtlichen Herausforderungen angegangen werden sollten, um nicht den Anschluss zu verpassen.

Aus einer Vielzahl von Schulungen in den Bereichen Datenschutz und IT-Vertragsgestaltung ist ihm zudem bewusst, worauf es speziell mittelständischen Unternehmen ankommt und mit welchen Herausforderungen sie bei der Einführung neuer Technologien, wie z.B. KI, umzugehen haben.

01

Strategische Betrachtung

Geschrieben von Axel Wiemann, kiucon

KI als strategischer Imperativ: Eine Orientierungshilfe für die erfolgreiche Integration von Künstlicher Intelligenz in Unternehmen

Einleitung

Künstliche Intelligenz hat sich von einer visionären Idee zu einer grundlegenden Basistechnologie entwickelt, die mit atemberaubender Geschwindigkeit in Gesellschaft und Unternehmen Einzug hält. **Sie besitzt das Potenzial, Geschäftsmodelle tiefgreifend zu transformieren, und ist alles andere als ein vorübergehender Trend oder isoliertes Projekt**. Vielmehr stellt sie einen strategischen Imperativ für Unternehmen dar, die ihre Wettbewerbsfähigkeit erhalten und ausbauen möchten.

Aktuelle Studien belegen, dass Unternehmen, die KI erfolgreich integrieren, erhebliche Vorteile in Effizienz, Innovation und Marktposition erzielen. Prognosen zufolge könnte KI bis 2030 einen globalen wirtschaftlichen Mehrwert von mehreren Billionen US-Dollar generieren. **Laut einer McKinsey-Studie aus dem Jahr 2021 nutzen 56 % der befragten Unternehmen bereits damals KI in mindestens einem Geschäftsbereich, Tendenz stark steigend.**[4]

Die rasante Entwicklung KI-basierter technologischer Lösungen in unterschiedlichsten Anwendungsfeldern – von Bildverarbeitung über die Verarbeitung natürlicher Sprache, Objekterkennung und Robotik bis hin zur Prozessautomatisierung – erschwert es Unternehmen jedoch, schnell einen strukturierten Überblick über das komplexe und hochdynamische Feld der Künstlichen Intelligenz zu gewinnen – und zu behalten. **Grenzen und Möglichkeiten, Chancen und Risiken zu erkennen** und **richtig einzuschätzen, stellt eine immense Herausforderung dar, der viele Unternehmen weltweit noch ohne adäquaten Strategie- und Organisationsansatz gegenüberstehen.**

Um nicht von ihrer Konkurrenz abgehängt zu werden, bleibt Unternehmen in vielen Branchen indes keine andere Wahl als **sich mit KI-Technologien wie Large Language Models (LLMs) und ihren Einsatzmöglichkeiten innerhalb von Businessanwendungen intensiv auseinandersetzen**. Heute befinden sich die meisten indes noch ganz am Anfang ihrer Reise und so verwundert es nicht, dass nur wenige angeben, aktuell bereits einen umfassenden Mehrwert durch den Einsatz von KI für ihr Geschäft – spezifische technologische Anwendungen in einzelnen Produktumwelten mal ausgenommen – zu erzielen.

Im Management fehlt es oft an einem klaren Verständnis dafür, welchen Nutzen der Einsatz von KI bietet. Es mangelt an Wissen über die notwendigen Grundlagen für die Umsetzung und die Reihenfolge, in der Herausforderungen angegangen werden sollten. Bestehende, kurzfristig initiierte KI-Projekte sind zwar vorhanden, häufig jedoch nicht in einen strategischen Kontext eingebunden. **Ist man bereits aktiv, ist eine klare Strategie oft nicht erkennbar und in den seltensten Fällen transparent, motivierend und verständlich über alle Instanzen und Ebenen des Unternehmens hinweg kommuniziert und in Köpfen und DNA der MitarbeiterInnen verankert.** Es fehlt an einem gemeinsamen „Big Picture" und einem geteilten Verständnis der der „KI-Strategie" zwischen Management, Mitarbeitern und Stakeholdern. In der Konsequenz bedeutet dies, dass viele Unternehmen sich eher

4 https://www.mckinsey.com/capabilities/quantumblack/our-insights/global-survey-the-state-of-ai-in-2021?
McKinsey: Globale Umfrage: Der Stand der KI im Jahr 2021. (Zugriff 8. Dezember 2021)

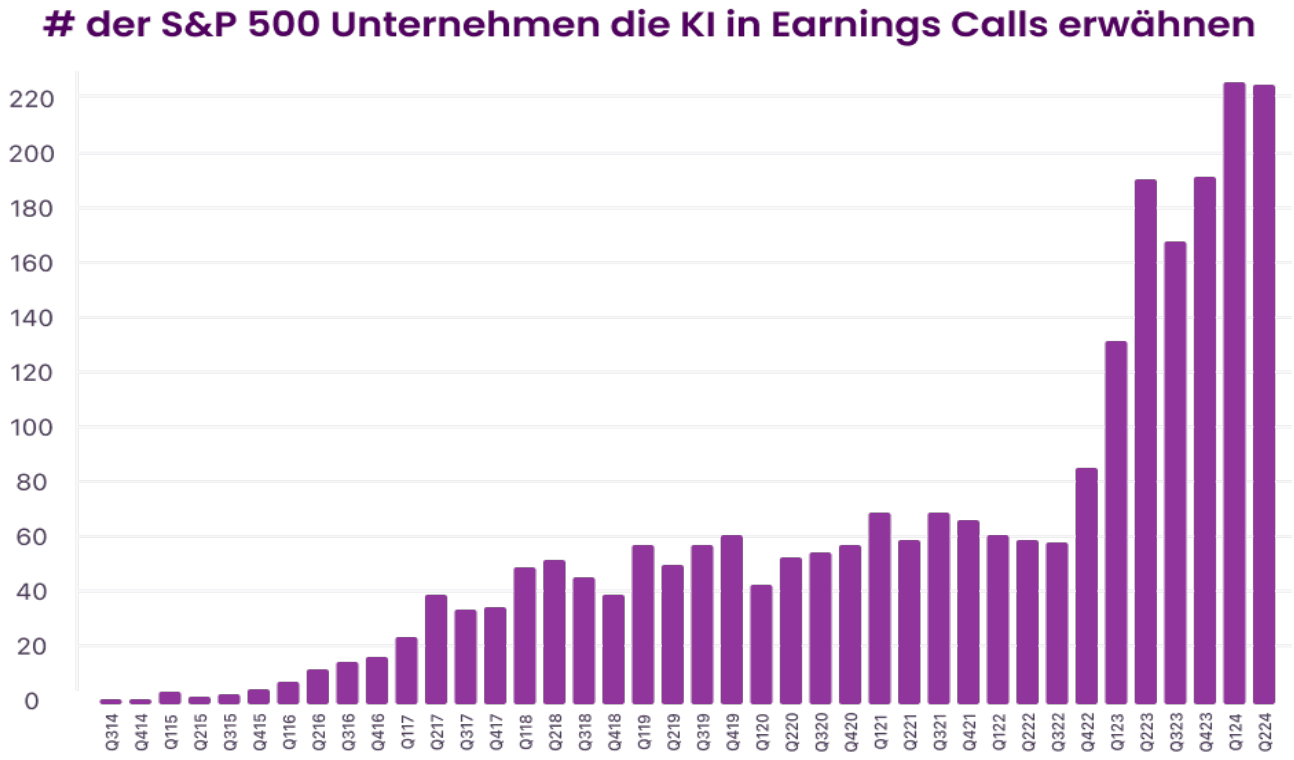


Fig-1 : Anzahl der S&P 500 Unternehmen, die KI in Earnings Calls erwähnen, von Q3 2014 bis Q2 2024. [5]

experimentell, empirisch und wenig planvoll an das „Abenteuer künstliche Intelligenz" herantasten. Ohne Rahmen und Orientierung gebendes Framework. In der Folge mangelt an strukturierten Methoden zur Strategieaktivierung. Zentrale Fragen wie „Welche Bereiche unseres Unternehmens können am meisten von KI profitieren?", „Wie integrieren wir KI in unsere bestehenden Prozesse und Systeme?" oder „Wie schulen wir Mitarbeiter im Umgang mit KI-Technologien?" bleiben unbeantwortet.

Von der Evolution zur Disruption

So unklar die zukünftige Entwicklung der Künstlichen Intelligenz auch sein mag, unstrittig ist, dass Mensch, Gesellschaft und Wirtschaft mit dem Aufkommen dieser Technologie am Beginn einer neuen Ära stehen. Während sich die Fähigkeiten des Menschen – unser Fühlen, Denken und Handeln – über Jahrtausende hinweg kontinuierlich entwickelten, sind die an uns gestellten Anforderungen infolge zunehmender Dynamik, Digitalisierung und Komplexität des Lebens- und Arbeitsalltags zuletzt exponentiell gestiegen.

Konnte man diesen Herausforderungen technologisch, strukturell und methodisch – etwa durch veränderte Arbeitspraktiken, neue Tools und verbesserten Zugang zu Informationen – zunächst oft noch adäquat begegnen, erleben wir heute infolge der fortwährenden Beschleunigung unserer Lebensumwelt eine beständig wachsende Kluft

5 https://insight.factset.com/more-than-40-of-sp-500-companies-cited-ai-on-earnings-calls-for-q2
FactSet: Mehr als 40 % der S&P 500 Unternehmen erwähnten KI in den Earnings Calls für Q2. (Zugriff 13. September 2024)

zwischen Ansprüchen an und Anforderungen von uns auf der einen und unserer individuellen Leistungsfähigkeit auf der anderen Seite. **Die Folgen sind allgegenwärtig: Überforderung,** erlebte **Komplexität und eine infolge zeitlicher Restriktionen oft nur oberflächliche Beschäftigung mit Informationen münden nicht selten in einer mangelnden Outputqualität, Fehlentscheidungen und Frustrationen.**

Auch wenn KI den Menschen heute bei extrem komplexen, ein hohes Maß an Empathie oder Beziehungsfähigkeit erfordernden Tätigkeiten noch – und die Betonung liegt auf noch – nicht vollständig unterstützen oder ersetzen kann, vermag sie doch langwierige Aufgaben mit hohem Datenverarbeitungsbedarf effizient zu übernehmen und weiterzuentwickeln. Sie kann ihre Umwelt wahrnehmen, logisches Denken, Lernen und Planen imitieren, wissenschaftliche Studien oder andere Datenquellen zuverlässig und unermüdlich auswerten und uns Menschen – insbesondere Entscheidern in Unternehmen – durch die Übernahme dieser Arbeiten mehr Zeit für jene Dinge geben, die wir besonders gut oder gerne – oder beides – tun.

Für Unternehmen bedeutet dies, dass Mitarbeiter wieder mehr Zeit haben, sich strategisch mit ihrer Arbeit, der Ausrichtung des Unternehmens, der Kultur, dem Miteinander und anderen „typisch menschlichen Fähigkeiten" zu beschäftigen. Es lohnt sich also, KI dort einzusetzen, wo der Mensch lange braucht oder schlichtweg nicht mehr so gut ist wie eine Maschine. Dass es sinnvoll ist, künstliche Intelligenz im Wirtschaftsleben einzusetzen, ist somit klar.

Die zwei zentralen Fragestellungen, die sich Unternehmen im Umgang mit KI stellen müssen, lauten:

1. **Wie und wo kann KI Unternehmen und Mitarbeiter dabei unterstützen, die zunehmende Komplexität zu bewältigen, Geschäftsprozesse effizienter zu gestalten, den Kundennutzen zu verbessern, Ressourcen optimal einzusetzen, Wichtiges von Unwichtigem zu unterscheiden und wieder Raum für Ruhe, Innovation und die wirklich bedeutsamen Dinge zu schaffen?** Oder anders ausgedrückt: Wie kann KI in die Unternehmensstrategie integriert werden, um echte Effizienzgewinne und nachhaltige Produktivität zu erzielen, Mitarbeiter von Routineaufgaben zu entlasten und somit mehr Zeit für kreative, gestalterische und strategische Unternehmensentwicklung sowie Innovation zu ermöglichen?
2. **Wie lässt sich KI strategisch optimal im Unternehmen einführen?** Wie können zentrale Fehler bei der Implementierung von KI vermieden werden – Fehler, die beispielsweise im Zuge der Digitalisierung der Wertschöpfung zu extrem komplexen, unintegrierten Legacy-Systemlandschaften und immensen Kosten geführt haben? Wie kann die Belegschaft eingebunden, Organisation und Technologie in Einklang gebracht werden? Und wie etabliere ich von vornherein smarte Governance-Strukturen?

Auch wenn diese Fragen an dieser Stelle nur angerissen werden können, bieten sie einen Orientierungsrahmen für strategisch relevante Aspekte, die Entscheider in Mittelstand, Scale-ups und Konzernen bei der Erarbeitung einer KI-Strategie berücksichtigen sollten.

Die strategische Bedeutung von KI für Unternehmen

KI verändert nicht nur Produkte und Dienstleistungen, sondern auch die Art und Weise, wie Unternehmen Wert schöpfen. Sie ermöglicht personalisierte Kundenerlebnisse, optimiert Geschäftsprozesse und eröffnet völlig neue Geschäftsmodelle. Unternehmen, die KI strategisch einsetzen, können Wettbewerbsvorteile erzielen, indem sie effizienter agieren, schneller auf Marktveränderungen reagieren und innovative Lösungen anbieten. **Es bedarf jedoch einer klaren Strategie, die über *isolierte* Pilotprojekte hinausgeht und KI als integralen Bestandteil der Unternehmensvision betrachtet.**

Die Einführung von KI erfordert ein tiefgreifendes Umdenken auf allen Ebenen des Unternehmens. Es geht nicht nur darum, eine (beliebige) neue Technologie zu implementieren, sondern darum, die eigene Geschäftsstrategie entsprechend anzupassen. Die Prämisse dabei: **KI sollte als Katalysator für Transformationen dienen, der es ermöglicht, bestehende Prozesse neu zu gestalten und völlig neue Geschäftsmodelle zu entwickeln.** Voraussetzung dafür ist indes, dass Unternehmen die Potenziale von KI erkennen und gezielt nutzen. Künstliche Intelligenz soll hierbei den Menschen als solches nicht ersetzen, sondern vielmehr ergänzen. **Daher gilt es, neuartige Strategien für eine effektive Zusammenarbeit zwischen Mensch und KI zu entwickeln und die Mitarbeiter von Anfang an sowohl kognitiv als auch emotional mitzunehmen.** Gelingt dies, entsteht eine innovationsfreundliche Kultur, die die Grundlage ist, langfristig die Potenziale der KI vollends auszuschöpfen und gleichsam die Belegschaft des Unternehmens emotional und motivational mitzunehmen. Dass dies nicht einfach ist, zeigen Hunderttausende gescheiterter oder nur teilweiser erfolgreicher Transformations- und Changeprojekte (auf anderen Feldern weltweit). Doch wie bereits gesagt, KI ist vieles, aber kein Projekt.

Herausforderungen bei der Integration von KI

Eine der größten Hürden bei der Integration von KI ist die Bereitschaft und Fähigkeit des Überwindens von organisatorischen Silos und einer Unternehmenskultur, die den Wissensaustausch nicht fördert. KI-Projekte erfordern bereichsübergreifende Zusammenarbeit. Doch häufig verhindern interne Strukturen und Prozesse eine **effektive Kommunikation**. Wertvolles Wissen bleibt isoliert, Synergien werden nicht genutzt. Um dieses Problem zu lösen, müssen Unternehmen eine Kultur des Teilens und der offenen Kommunikation etablieren. Dies kann durch die Einführung interdisziplinärer Teams, regelmäßiger Workshops und einer Unternehmenskultur erreicht werden, die Kollaboration belohnt. Mehr dazu an anderer Stelle.

Ein weiteres entscheidendes aktuelles Hindernis im Kontext der Einführung von Künstlicher Intelligenz in Unternehmen ist der derzeitige **Mangel an Expertise und Talent im Bereich KI**. Der Wettbewerb um qualifizierte Fachkräfte ist intensiv, und so haben viele Unternehmen Schwierigkeiten, die notwendigen Kompetenzen aufzubauen. Anstatt ausschließlich auf externe

Rekrutierung zu setzen, sollten Unternehmen in die **Weiterbildung ihrer bestehenden Mitarbeiter investieren**. Durch gezielte Schulungsprogramme und Kooperationen mit Bildungseinrichtungen kann das notwendige Know-how intern entwickelt werden.

Ferner fehlt es oft an einer klaren strategischen Ausrichtung. Viele Unternehmen starten KI-Initiativen ohne **konkrete Ziele** oder ohne Abstimmung mit der Gesamtstrategie. Dies führt zu Fragmentierung und begrenztem Mehrwert. Um dies zu vermeiden, ist es entscheidend, eine **umfassende KI-Strategie zu entwickeln**, die mit den Unternehmenszielen harmoniert und konkrete Maßnahmen definiert.

Entwicklung einer nachhaltigen KI-Strategie

Der Aufbau einer nachhaltigen KI-Strategie beginnt mit der **Ziel- und Bedarfsanalyse** sowie der **Identifikation der Kernwertschöpfungsprozesse** des Unternehmens. Diese Prozesse sind zentral für das Geschäftsmodell und bieten das größte Potenzial für Wertsteigerung durch KI. Eine gründliche Analyse dieser Prozesse ist unverzichtbar.

Analytische und kreative Ansätze zur Potenzialerkennung

Die Identifikation von KI-Potenzialen in Geschäftsprozessen erfordert sowohl analytische als auch kreative Ansätze. Process Mining ist ein effektives Werkzeug, um Prozessdaten aus IT-Systemen zu analysieren und tatsächliche Abläufe zu verstehen. Durch die Visualisierung von Prozessvarianten lassen sich Engpässe und Ineffizienzen aufdecken. Data Analytics und Machine Learning ermöglichen es, Muster und Zusammenhänge in großen Datenmengen zu erkennen, was Vorhersagen unterstützt und Entscheidungsprozesse optimiert. Workshops und Experteninterviews bieten wertvolle Gelegenheiten, das Wissen von Fachexperten und Mitarbeitern zu nutzen, um konkrete **Pain Points und Prozesse zu identifizieren, die optimiert werden können**. Durch diesen Austausch lassen sich praktische Erfahrungen und Ideen zur Verbesserung oder Automatisierung ressourcenintensiver Abläufe in der Wertschöpfungskette gewinnen.

In **Transformationsprojekten** kann KI beispielsweise als treibende Kraft für Veränderungen dienen. Ein Beispiel hierfür ist die Digitalisierung von Geschäftsprozessen, bei der KI nicht nur Prozesse digitalisiert, sondern grundlegend optimiert. Im Supply-Chain-Management etwa erlaubt der Einsatz von KI die Optimierung von Lagerbeständen und Lieferketten durch prädiktive Analysen. Auch im Kundenservice können KI-gestützte Chatbots und Sprachassistenten Anfragen effizient bearbeiten und die Kundenzufriedenheit steigern. Bei Fusionen und Übernahmen (M&A-Prozessen) leistet KI ebenfalls wertvolle Dienste. Sie beschleunigt Due-Diligence-Prozesse und minimiert Risiken durch die automatisierte Auswertung großer Datenmengen, sodass Verträge und rechtliche Dokumente schneller und präziser analysiert werden können.

Im Bereich Outsourcing und Shared Services steigert KI die Effizienz und Qualität, indem sie Back-Office-Prozesse automatisiert und die Servicequalität überwacht. Die Kombination von Robotic Process Automation (RPA) und KI ermöglicht die Automatisierung von Routineaufgaben, während KI-basierte Qualitätskontrollen die Serviceleistung kontinuierlich verbessern.

Fig-2 : Zuordnung von Anwendungsfällen zur Technologie im Unternehmen, dargestellt nach Wert und Komplexität. Datenquelle: Writer.com [6]

6 https://writer.com/blog/mapping-generative-ai-use-cases/
Writer.com: Mapping Generative AI Use Cases.

Bewertung und Priorisierung von KI-Anwendungsfällen

Nach der Identifikation der Kernprozesse sollten diese hinsichtlich ihres **Potenzials für KI-Anwendungen bewertet werden**. Datenverfügbarkeit und -qualität spielen dabei eine entscheidende Rolle, denn Prozesse mit umfangreichen und hochwertigen Daten eignen sich besonders gut für den KI-Einsatz. Ebenso wichtig sind die **Wiederholbarkeit und Standardisierung der Prozesse**, da KI besonders effektiv ist, wenn Muster erkannt und automatisiert werden können. Auch der geschäftliche Einfluss – wie die potenzielle Steigerung von Effizienz, Kostenreduktion, Qualitätsverbesserung oder Kundenzufriedenheit – sollte bei der Bewertung berücksichtigt werden.

Integration in die Gesamtstrategie und Ressourcenplanung

Auf dieser Grundlage können **konkrete KI-Anwendungsfälle entwickelt werden**, die in die Gesamtstrategie des Unternehmens integriert werden sollten. Dabei ist ein **Problem-Mapping-Dokument** hilfreich, das eine Übersicht über die größten Herausforderungen bietet, die sich durch KI lösen lassen, inklusive möglicher Hindernisse, geschätzter Kosten sowie der Verfügbarkeit von Systemen und Daten.

Die **Use Cases werden mit den Unternehmenszielen abgeglichen**, und es wird eine Ressourcenplanung vorgenommen sowie ein realistischer Zeitrahmen für die Umsetzung geschätzt. Jeder Use Case wird auf seinen potenziellen geschäftlichen Mehrwert analysiert, was eine grobe Berechnung der erwarteten Einsparungen oder Umsatzsteigerungen beinhaltet. **Finanzanalysen** wie Cost-Benefit- und Break-Even-Analysen sowie Sensitivitätsanalysen unterstützen die Bewertung. Speziell auf die KI-Transformation zugeschnittene Business-Case-Frameworks strukturieren und erleichtern die Erarbeitung gemeinsam mit internen und externen Partnern.

Nach Abschluss des vorherigen Schritts werden die **bewerteten Use Cases nach ihrem Aufwand und potenziellem Mehrwert priorisiert**. Eine Priorisierungsmatrix, die Umsatzpotenzial und Implementierungskomplexität gegenüberstellt, unterstützt diese Entscheidung und hilft, Projekte mit hoher Wirkung und niedriger Komplexität zu bevorzugen.

Nach der Priorisierung erfolgt die **Auswahl der relevanten KI-Use-Cases**. Hierbei sollten sowohl kurzfristige Quick Wins als auch langfristige strategische Projekte berücksichtigt werden, die zur Unternehmensstrategie passen und durch erste Pilotprojekte empirische Erfahrungen bieten. Diese Pilotierungen zeigen den potenziellen Nutzen der KI-Anwendungen im Unternehmen auf und machen diese erfahrbar.

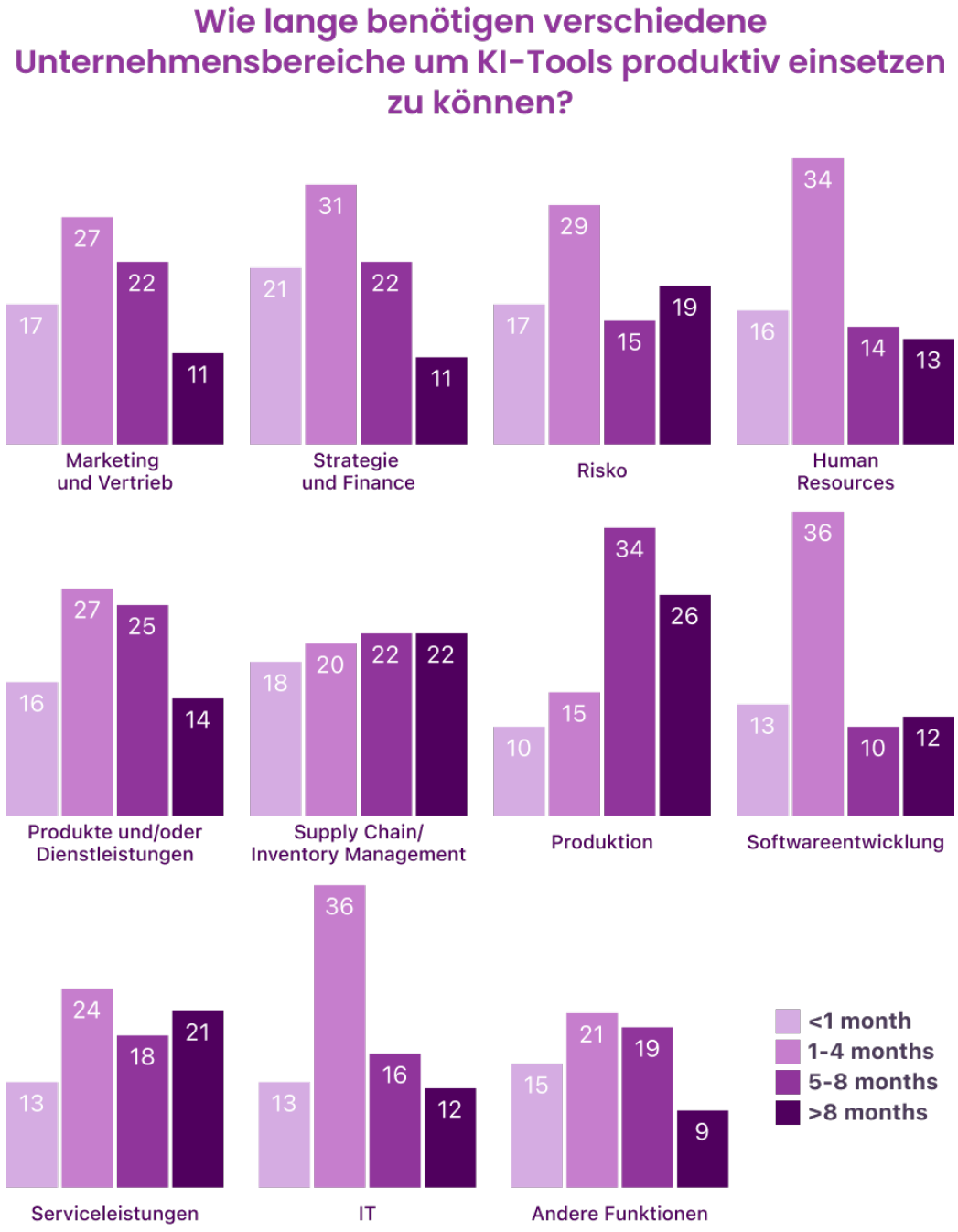


Fig-3 : Zeit, die verschiedene Unternehmensbereiche benötigen, um KI-Tools produktiv einzusetzen. [7]

Entwicklung einer flexiblen Roadmap und KPIs

Basierend auf der Auswahl und Priorisierung wird eine **flexible Roadmap,** bspw. in Gestalt eines **ganzheitlichen AI Strategy Frameworks**, entwickelt, welche Reihenfolge und Zeitpläne der Umsetzung der ausgewählten Cases vorgibt. Diese Roadmap enthält klar definierte Meilensteine und bleibt flexibel genug, um auf neue Erkenntnisse eingehen zu können.

7 https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai
McKinsey: The state of AI in 2023. (Zugriff 30. Mai 2024)

Für jeden Use Case werden **spezifische KPIs** wie Return on Investment (ROI), Time-to-Value (TTV), Einsparungen pro Einheit, Effizienzsteigerung und Kundenzufriedenheit **festgelegt**, um den Erfolg messbar zu machen. Dies ist von zentraler Bedeutung, um jederzeit vollständige Transparenz über Ertrag und Sinnhaftigkeit der Maßnahmen zu behalten. Eine klare Ressourcenallokation legt fest, welche Teams an welchen Projekten arbeiten und welche externen Ressourcen benötigt werden. Projektmanagement-Tools wie Atlassian JIRA oder Azure DevOps unterstützen bei der Planung und Umsetzung.

Aufbau der technischen Infrastruktur

Die erfolgreiche Integration von KI in Unternehmensprozesse erfordert weit mehr als den isolierten Einsatz von Large Language Models. Der wahre Mehrwert und signifikante Return on Investment entstehen erst **durch die nahtlose Verbindung von KI-Systemen mit bestehenden Datenquellen und Unternehmensanwendungen**. Anders als bei klassischen Big-Data-Infrastrukturen, die primär auf die Analyse historischer Daten ausgerichtet sind, müssen moderne KI-Systeme in der Lage sein, in Echtzeit auf verschiedenste Systeme zuzugreifen, Aktionen auszuführen und dabei komplexe Geschäftsregeln zu berücksichtigen.

Die technischen Anforderungen an eine KI-Infrastruktur unterscheiden sich fundamental von traditionellen IT-Architekturen. Während klassische Systeme meist auf klar definierte Prozesse und strukturierte Daten ausgerichtet sind, müssen **KI-Systeme flexibel mit unterschiedlichsten Datenformaten und Anwendungsfällen umgehen können**. Dies erfordert eine Architektur, die sowohl robust genug für den produktiven Einsatz als auch flexibel genug für die kontinuierliche Integration neuer Fähigkeiten ist.

Die beispiellose Entwicklungsgeschwindigkeit im Bereich der KI macht deutlich, dass diese Technologie zunehmend zum integralen Bestandteil der Unternehmens-IT wird. Strategische Entscheidungen bei der Infrastrukturgestaltung müssen daher von Anfang an **die Vermeidung von Lock-in-Effekten und die Gewährleistung des Datenschutzes** berücksichtigen. Eine zukunftsfähige Architektur zeichnet sich durch **Anbieterunabhängigkeit, standardisierte Schnittstellen und robuste Datenschutzmechanismen** aus. Nur so können Unternehmen die rapiden Fortschritte im Bereich der KI nutzen, ohne dabei Kompromisse bei der Datensicherheit einzugehen oder sich langfristig an einzelne Technologien oder Anbieter zu binden.

Pilotphase und Proof of Concept (PoC)

In einer **Pilotphase** werden ein bis zwei priorisierte Use Cases als **Proof of Concept (PoC)** umgesetzt. Diese PoCs dienen dazu, die Machbarkeit und den Nutzen der KI-Anwendung zu testen und bieten eine Evaluierungsgrundlage vor größeren Investitionen. Basierend auf den PoC-Ergebnissen können, falls notwendig, Anpassungen vorgenommen werden, sodass erfolgreiche Ansätze die Grundlage für die weitere Skalierung bilden, während problematische Aspekte vor dem Rollout optimiert werden.

Organisatorische Maßnahmen

Organisatorisch ist es sinnvoll, ein **KI-Kompetenzzentrum** aufzubauen, das die KI-Initiativen steuert und den Abteilungen als Ansprechpartner dient. Dieses Zentrum fördert den Austausch von Best Practices und die kontinuierliche Optimierung der Prozesse.

Die Einführung von **Kompetenzzentren für Künstliche Intelligenz** ist für Unternehmen, die in einem zunehmend datengetriebenen Wettbewerb bestehen wollen, mit vielen Vorteilen verbunden. In diesen spezialisierten Einheiten wird unternehmensweit technologische und organisatorische Expertise gebündelt, um den Einsatz von KI strategisch und effizient zu steuern, maximale Wertschöpfung zu erzielen und Innovationshemmnisse zu minimieren.

Strategische Zielausrichtung und Governance

Die weltweit besten Unternehmen richten ihre KI-Kompetenzzentren dabei direkt an den strategischen Unternehmenszielen aus. Sie etablieren klare Governance-Strukturen, die sicherstellen, dass KI-Projekte nicht isoliert ablaufen, sondern auf zentralen Geschäftsprioritäten wie Kostensenkung, Umsatzsteigerung oder Prozessoptimierung basieren. Diese Kompetenzzentren sind regelmäßig in der Unternehmensleitung verankert, um Top-Down-Unterstützung zu sichern und Silodenken zu vermeiden.

Identifikation und Priorisierung von KI-Anwendungsfällen

Um jene Geschäftsbereiche mit dem höchsten Automatisierungs- oder Optimierungspotenzial zu identifizieren, ist das regelmäßig systematische Assessment Kernwertschöpfungsprozesse des Unternehmens unerlässlich, wobei vor allem auf datengetriebene Tools und Frameworks gesetzt werden sollte, um Anwendungsfälle zu priorisieren, die sowohl technologisch realisierbar als auch wirtschaftlich sinnvoll sind. Typische Beispiele sind predictive Maintenance, Supply-Chain-Optimierungen oder die Automatisierung von Kundenservice-Prozessen.

Aufbau einer skalierbaren Infrastruktur

Technologisch wird vor allem auf skalierbare Cloud-Architekturen und modulare KI-Plattformen gesetzt, die eine schnelle Iteration und den unternehmensweiten Rollout von KI-Lösungen ermöglichen. Modere Frameworks wie TensorFlow, PyTorch oder OpenAI-APIs und Data Lakes, die eine zentrale Datenverfügbarkeit und -analyse fördern, kommen hier zum Einsatz. Die Automatisierung durch MLOps (Machine Learning Operations) stellt sicher, dass KI-Modelle nicht nur entwickelt, sondern auch erfolgreich in den operativen Betrieb integriert werden können.

Aufbau interdisziplinärer Teams

Bei der Besetzung der Kompetenzzentren ist **Interdisziplinarität** ein zentraler Schlüssel zum Erfolg. Dies bedeutet, dass Experten aus verschiedenen Disziplinen wie Data Science, Softwareentwicklung, Change Management und spezifischen Businessbereichen, hier ihre Expertise vereinen, um gemeinsam crossfunktional optimale Lösungen zu entwickeln und sicherzustellen, dass technische Lösungen auch auf die realen Herausforderungen der Organisation abgestimmt sind. Unternehmen wie Google,

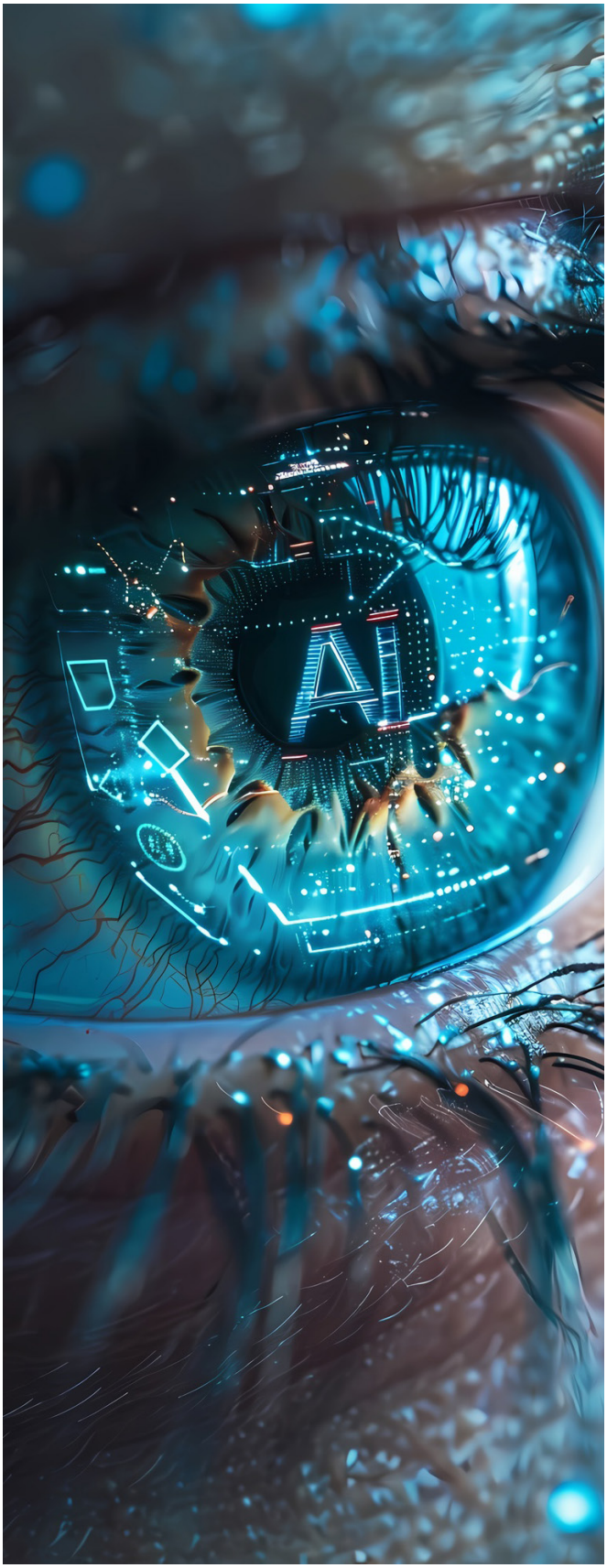
Bosch oder Siemens fördern zusätzlich "Citizen Data Scientists" oder "Data Stewards" und "KI-Ambassadors" – Mitarbeiter ohne technischen Hintergrund, die mit Self-Service-Tools eigenständig KI-Anwendungen entwickeln können, zentral im Querschnitt zur organisatorischen Linienfunktion das Thema Digitalisierung und Datenqualität weiterentwickeln oder den KollegInnen als zentrale Ansprechpartner bei Fragen aller Art rund um das Thema KI zur Verfügung stehen. Im Austausch dazu erhalten sie priorisiert Informationen oder auch finanzielle Anreize für die Wahrnehmung der zusätzlich eingenommenen Matrixfunktion.

Förderung einer KI-Kultur

Ein entscheidender Faktor für die erfolgreiche Einführung von künstlicher Intelligenz in Unternehmensstrategie und -prozessen ist die Schaffung einer datengetriebenen Unternehmenskultur. Hier setzen die besten Unternehmen auf umfassende Weiterbildungsprogramme, die Mitarbeiter auf allen Hierarchieebenen befähigen, KI zu verstehen und anzuwenden. Change-Management-Initiativen oder besser eine vollumfängliche **Strategieaktivivierung** begleiten die Einführung, um Akzeptanz zu fördern und Ängste vor Automatisierung abzubauen.

Partnerschaften und Open Innovation

Von besonderer Bedeutung für dien Erfolg der Arbeit der Kompetenzzentren sind zudem Kooperationen mit externen Partnern wie Universitäten, Start-ups und innovativen Technologieanbietern. Diese Zusammenarbeit ermöglicht Zugang zu neuesten Forschungsergebnissen und Innovationen. Idealerweise - hier lassen sich zahlreiche Unternehmen als Beispiele finden - bauen Unternehmen komplette Ökosysteme auf, in denen sie KI-Entwicklung und -Anwendung gemeinsam mit Partnern vorantreiben.



Warum Unternehmen Kompetenzzentren einführen sollten

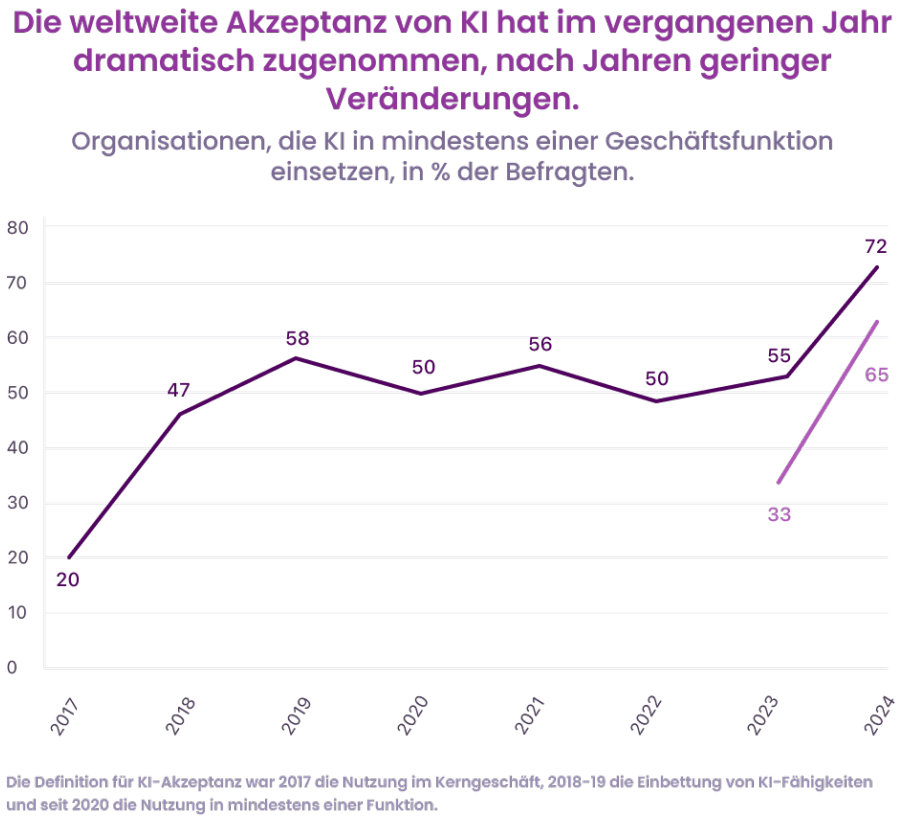


Fig-4 : Weltweite Akzeptanz von KI in Unternehmen, dargestellt als Prozentsatz der Unternehmen, die KI in mindestens einer Geschäftsfunktion einsetzen. Daten aus der McKinsey Global Survey on AI, mit 1.363 Teilnehmern auf allen Organisationsebenen, vom 22. Februar bis 5. März 2024 [8]

Ein gut geführtes KI-Kompetenzzentrum bietet Unternehmen eine Reihe messbarer Vorteile. Es reduziert die Kosten für die Entwicklung und Skalierung von KI-Lösungen durch standardisierte Prozesse, minimiert Risiken durch zentralisierte Governance und erhöht die Geschwindigkeit der Wertgenerierung durch effiziente Ressourcennutzung. Darüber hinaus stärkt es die Innovationskraft und macht Unternehmen zukunftsfähig in einer immer digitaleren und datengetriebenen Welt. Unsere Erfahrung zeigt, dass Unternehmen, die solche Kompetenzzentren erfolgreich aufbauen, nicht nur operativ effizienter werden, sondern auch signifikante Wettbewerbsvorteile erzielen – sei es durch schnellere Markteinführung neuer Produkte, verbesserte Kundenbindung oder gesteigerte operative Exzellenz.

Schließlich kommt einer umfassenden **Change-Management-Strategie** im Sinne einer **Strategieaktivierungslogik** – mit Schulungen, Workshops und transparenter Kommunikation – eine zentrale Bedeutung für die erfolgreiche Einführung künstlicher Intelligenz zu. Abstrakte Unternehmensziele durch eine gemeinsame entwickelte und von einer breiten Basis getragenen Operationalisierungsvision zu unterfüttern, greif- und verstehbar zu machen, unterstützt die Akzeptanz einer neuen Technologien und minimiert potenzielle Widerstände.

8 https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai
McKinsey: The state of AI in 2023. (Zugriff 30. Mai 2024)

Skalierung und Governance

Nach erfolgreichen Pilotphasen kann die **KI-Implementierung schrittweise auf weitere Abteilungen und Prozesse ausgeweitet** werden, wobei bewährte Methoden angewendet werden. KI-Modelle und -Prozesse müssen kontinuierlich überprüft und verbessert werden, um die Qualität der Anwendungen sicherzustellen. Über spezifische, gemeinsam entwickelte **Dashboards**, beispielsweise auf Basis der Palantir Suite, Power BI, Tableau oder spezifischen mit Technologiepartnern entwickelten Custom-Lösungen, können die definierten KPIs in Echtzeit überwacht werden, und regelmäßige Prüfungen gewährleisten, dass die Zielvorgaben erreicht werden. Machine-Learning-Modelle unterstützen, um frühzeitig auf Abweichungen zu reagieren und notwendige Anpassungen vorzunehmen.

Schließlich kommt einer effektiven **Governance-Struktur** eine existenzielle Bedeutung im Kontext einer erfolgreichen KI-Einführung auf unterschiedlichen Ebenen zu. Will man vermeiden, dass technologisch – ähnlich wie man es in der Vergangenheit im Umfeld einer organisch wachsenden IT-Landschaft oft gesehen hat – eingesetzte Applikationen, Datenhaltung oder Skalierbarkeit der Lösungslandschaft in einem unstrukturierten Chaos enden, organisatorisch und kulturell Ownership, Aufgabenerledigung oder auch Identifikation der MitarbeiterInnen mit dem Thema leiden, die Kosten aus dem Ruder laufen oder zunächst unvorhersehbare Wechselwirkungen einzelner Maßnahmen mit anderen Aktivitäten, Vorgaben und Zielen das Gesamtvorhaben in Zweifel stellen, braucht es eine klare, fokussierte Überwachung und Steuerung der **AI Journey**. **Bedürfnisse und Ziele** müssen beständig über alle Ebenen des Unternehmens (nach)geschärft und weiterentwickelt werden. Hierbei sind nicht zuletzt sehr **persönliche Ziele und Wünsche** – also sehr menschliche Komponenten – der handelnden Personen (nach Sicherheit, Kontrollierbarkeit, Wachstum, Entwicklung …) adäquat zu berücksichtigen.

Ein hilfreiches Instrument zur unternehmensinternen wie externen Kommunikation ist die Entwicklung eines gemeinsamen **„Big Pictures“**, mit dem sich alle identifizieren können und das das Unternehmen on track hält. In diesem Kontext sind Verantwortlichkeiten klar zu definieren, Richtlinien und Standards zu entwickeln und Kontrollmechanismen zu etablieren.

Ein Aufwand, der sich lohnt, sieht man doch in einer Vielzahl großer Transformationsvorhaben, dass initiale Fehlanlagen in Projekten, Strukturen und Kultur sich im Nachhinein kaum mehr korrigieren lassen.

Schlaglicht: Überwindung kultureller Barrieren und Förderung von Kollaboration

Die Einführung von KI erfordert einen kulturellen Wandel innerhalb des Unternehmens. Um eine Kultur des Teilens zu etablieren, ist die Förderung von Wissensaustausch und Kollaboration entscheidend. Interdisziplinäre Teams (siehe Kompetenzzentren), in denen Mitglieder aus verschiedenen Abteilungen zusammenarbeiten, ermöglichen den Austausch unterschiedlicher Perspektiven und fördern innovative Lösungen. **Wissensmanagement-Systeme** erleichtern den Zugang zu Informationen und Best Practices. Regelmäßige **Kommunikationsformate** wie Meetings oder Workshops unterstützen den kontinuierlichen Dialog.

Führungskräfte spielen eine zentrale Rolle. Sie müssen die Vision und Bedeutung von KI für die Zukunft des Unternehmens klar kommunizieren und als Vorbilder agieren. Durch aktives Engagement in KI-Initiativen und Offenheit für Neues fördern sie eine

Kultur, die Innovation und Veränderung positiv aufnimmt. Die Schaffung eines Umfelds, in dem Experimente erlaubt sind und Fehler als Lernchancen gesehen werden, ist essenziell. In diesem Kontext ist es von herausragender Bedeutung, **realistische Erwartungen** an die Leistungsfähigkeit von MitarbeiterInnen, Organisation und Technologie zu stellen, um Frustrationen zu vermeiden.

Nicht selten fehlt es Unternehmen an wichtigen Voraussetzungen, die KI-Transformation effizient anzugehen; einer agilen, nachhaltigen und smarten Umsetzung ihrer Digitalisierungsstrategie, der Planung, Umsetzung und Finalisierung von Datenqualitätsvorhaben oder auch dem **Abschluss zentraler organisatorischer, technologischer und kultureller (New Work) Initiativen**, welche die notwendige **Basis für eine Inangriffnahme und erfolgversprechende Umsetzung einer KI-Strategie-Einführung** im Unternehmen bilden.

Schlaglicht: Ethische und rechtliche Aspekte berücksichtigen

Der verantwortungsvolle Einsatz von KI erfordert die Berücksichtigung ethischer und rechtlicher Aspekte. Unternehmen müssen einen ethischen Rahmen entwickeln, der Transparenz, Fairness und Datenschutz gewährleistet.

- **Transparenz**: Offenlegung, wie KI-Modelle Entscheidungen treffen.
- **Fairness**: Vermeidung von Diskriminierung durch Verzerrungen in Daten oder Algorithmen.
- **Datenschutz**: Einhaltung gesetzlicher Vorgaben und Schutz personenbezogener Daten.

Compliance mit gesetzlichen Anforderungen ist unerlässlich. Unternehmen müssen regulatorische Entwicklungen aktiv überwachen und sicherstellen, dass ihre KI-Anwendungen aktuellen Gesetzen entsprechen. Eine ausführliche Dokumentation der KI-Systeme und ihrer Funktionsweisen ist wichtig, um Transparenz und Rechenschaftspflicht zu gewährleisten.

Schlaglicht: Aufbau von Partnerschaften und Ökosystemen

Die erfolgreiche Integration von KI erfordert oft Expertise und Ressourcen, die über die eigenen Möglichkeiten hinausgehen. Die Zusammenarbeit mit Technologieanbietern ermöglicht den Zugang zu fortschrittlichen KI-Lösungen und externem Know-how. Kooperationen mit Forschungseinrichtungen und Universitäten fördern den Wissenstransfer und halten Unternehmen an der Spitze technologischer Entwicklungen.

Die Teilnahme an Brancheninitiativen und Netzwerken fördert den Austausch von Best Practices und die Entwicklung gemeinsamer Standards. Dies erhöht die Akzeptanz von KI in der Branche und hilft, gemeinsame Herausforderungen zu bewältigen. Ein starkes Ökosystem ermöglicht es Unternehmen, ihre Innovationsfähigkeit zu steigern und neue Märkte zu erschließen.

Schlaglicht: Effizientes Risikomanagement bei der Einführung von KI in Unternehmen

Die Einführung von Künstlicher Intelligenz (KI) kann Unternehmen signifikante Wettbewerbsvorteile verschaffen, birgt jedoch auch Risiken, die es zu managen gilt. Zu den

Hauptgefahren gehören Fehlinvestitionen in unwirksame oder nicht zukunftsfähige Lösungen sowie das Risiko eines Vendor Lock-ins. Um diese Risiken zu minimieren und KI intelligent in die Geschäftsstrategie einzubetten, sind unter anderem folgende Aspekte beachtlich.

Risiko von Fehlinvestitionen vermeiden

Fehlinvestitionen in KI-Lösungen entstehen oft durch mangelnde strategische Planung oder eine unklare Zielsetzung. Unternehmen sollten vor der Investition eine gründliche Bedarfsanalyse und Bewertung der potenziellen Anwendungsfälle durchführen. Wie bereits zuvor betont, ist es empfehlenswert, auf eine **agile Herangehensweise mit Proof of Concepts** (PoCs) zu setzen. Diese ermöglicht es, den Mehrwert einzelner KI-Projekte zu testen, bevor erhebliche Ressourcen gebunden werden. Die Integration von Pilotprojekten in die übergeordnete Unternehmensstrategie stellt sicher, dass KI-Projekte nicht isoliert, sondern im Gesamtzusammenhang betrachtet und bewertet werden.

Vendor Lock-in vermeiden

Der sogenannte Vendor Lock-in tritt auf, wenn ein Unternehmen abhängig von einem einzigen Anbieter wird, was zukünftige Flexibilität einschränkt und zu höheren Kosten führen kann. Um dies zu vermeiden, sollten Unternehmen auf **hybride und modulare Architekturen** setzen, die eine spätere Integration anderer Anbieter ermöglichen (vergleiche hierzu auch Kapitel V Software, IT-Integration). Ein Weg, Vendor Lock-ins zu vermeiden, besteht im Einsatz von Open-Source-Lösungen und -Standards, die die Unabhängigkeit von proprietären Systemen sichern bzw. auf Vendoren zu setzen, die offene Plattformlogiken verfolgen, um ihren Kunden jederzeit die Möglichkeit zu geben, auf unterschiedliche Zukunftslösungen zu setzen. Schließlich können „Multi-Vendor"-Strategien verfolgt werden, bei denen verschiedene Anbieter für unterschiedliche Komponenten der KI-Infrastruktur eingesetzt werden. Dies minimiert die Abhängigkeit von einzelnen Anbietern und erleichtert zukünftige Anpassungen.

Intelligentes Abhängigkeitsmanagement und strategische Differenzierung

Ein effektives Abhängigkeitsmanagement im KI-Bereich umfasst neben der Wahl flexibler Architekturen auch die kontinuierliche Weiterentwicklung interner KI-Kompetenzen. Dadurch kann das Unternehmen eigenständiger agieren und bleibt langfristig handlungsfähig. Die strategische Differenzierung durch KI ergibt sich, wenn KI-Lösungen nicht nur Prozesse automatisieren, sondern auch neue Wertschöpfungsmöglichkeiten schaffen und Wettbewerbsvorteile eröffnen. Hierbei spielt die **kontinuierliche Überprüfung der KPIs sowie eine iterative Optimierung der KI-Anwendungen** eine wichtige Rolle. Es ist empfehlenswert, KI-Initiativen eng mit den Unternehmenszielen zu verknüpfen, um eine differenzierte Positionierung im Markt zu erreichen und das volle Potenzial der KI auszuschöpfen.

Kontinuierliche Verbesserung und Innovation

Die KI-Transformation ist ein fortlaufender Prozess, der kontinuierliche Verbesserung und Innovation erfordert. Die Etablierung eines systematischen Innovationsmanagements unterstützt die Generierung, Bewertung und Umsetzung von Ideen. Digitale Ideenmanagement-Plattformen ermöglichen

es Mitarbeitern, Vorschläge einzubringen und gemeinsam weiterzuentwickeln. Klare Prozesse für die Entwicklung und Umsetzung von Innovationen sowie die Bereitstellung von Budgets für Innovationsprojekte fördern diesen Ansatz. Eine **lernende Organisation** fördert die Fähigkeit, Wissen zu generieren und zu teilen. Eine Feedback-Kultur, regelmäßige Reflexionen und die Etablierung von Wissensnetzwerken tragen dazu bei, dass das Unternehmen agil und anpassungsfähig bleibt. Kontinuierliche Investitionen in die Qualifikation der Mitarbeiter sind entscheidend, um mit technologischen Entwicklungen Schritt zu halten.

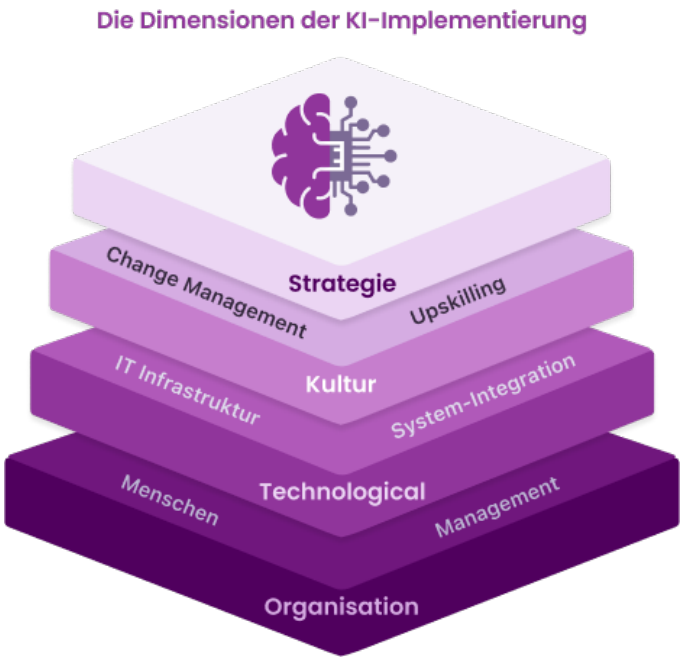


Fig-5 : Ein Überblick über die verschiedenen Dimensionen, die bei der KI-Implementierung berücksichtigt werden müssen.

Fazit

Die Integration von Künstlicher Intelligenz in Unternehmen ist ein komplexer, jedoch unverzichtbarer Prozess, um in einer zunehmend digitalen Welt wettbewerbsfähig zu bleiben. Sie erfordert eine ganzheitliche Strategie, die Technologie, Organisation und Kultur miteinander verbindet. Durch die Identifikation von Kernwertschöpfungsprozessen, die Entwicklung konkreter KI-Anwendungsfälle und die Einbettung von KI in die Unternehmensstrategie können Unternehmen das Potenzial von KI voll ausschöpfen.

Die Überwindung kultureller Barrieren, die Förderung einer lernenden Organisation und der verantwortungsvolle Umgang mit ethischen und rechtlichen Aspekten sind entscheidende Erfolgsfaktoren. Unternehmen müssen bereit sein, in ihre Mitarbeiter zu investieren, neue Wege zu gehen und Partnerschaften aufzubauen.

Die Zeit zum Handeln ist jetzt. Unternehmen, die die Chancen von KI proaktiv nutzen, werden Innovationen vorantreiben, Effizienzgewinne realisieren und ihre Marktposition nachhaltig stärken können. Die erfolgreiche Integration von KI ist kein kurzfristiges Projekt, sondern eine langfristige strategische Entscheidung, die die Zukunftsfähigkeit des Unternehmens sichert.

02

Rechtliche Rahmenbedingungen und KI Act

Geschrieben von Sven-Erik Holm, GvW Graf von Westphalen

KI und Recht: Ein Überblick zu den rechtlichen Rahmenbedingungen inkl. Handlungsempfehlungen für Entscheider

Einführung

Künstliche Intelligenz (KI) revolutioniert viele Branchen und bietet Unternehmen erhebliche Vorteile. Gleichzeitig stellt der Einsatz von KI-Systemen Unternehmen vor komplexe rechtliche Herausforderungen. Diese betreffen insbesondere Datenschutz, Haftung, Urheberrecht und die Einhaltung regulatorischer Vorgaben.

Anwendbare Gesetze und Vorschriften

EU-Datenschutz-Grundverordnung (DSGVO)

Die EU-Datenschutz-Grundverordnung (DSGVO) ist eine der wichtigsten gesetzlichen Grundlagen, die beim Einsatz von KI in Unternehmen zu beachten ist. Sie regelt den Umgang mit personenbezogenen Daten und stellt sicher, dass diese Daten geschützt und nur rechtmäßig verarbeitet werden. Unternehmen müssen sicherstellen, dass ihre KI-Systeme die geltenden und jeweils einschlägigen Datenschutzanforderungen erfüllen, insbesondere in Bezug auf Transparenz, Datenminimierung und die Rechte der betroffenen Personen.

Transparenz: Unternehmen müssen klar und verständlich darlegen, dass und wie personenbezogene Daten durch KI-Systeme verarbeitet werden. Dies umfasst die Information der betroffenen Personen über die Art der Datenverarbeitung und deren Zweck. Mangels eigener Informationen wird vor allem dieser Aspekt vielen Unternehmen in der Praxis schwerfallen. Es ist daher essentiell, die entsprechenden Informationen beim jeweiligen Anbieter des KI-Systems anzufragen.

Datenminimierung: Es dürfen nur die Daten erhoben und verarbeitet werden, die für den jeweiligen Zweck notwendig sind. Dies bedeutet, dass Unternehmen ihre Datenverarbeitungsprozesse regelmäßig überprüfen und anpassen müssen, um sicherzustellen, dass keine unnötigen Daten verarbeitet werden. Bezogen auf den Einsatz von KI-Systemen bedeutet dies, dass stets geprüft werden muss, auf welche Daten des Unternehmens das KI-System tatsächlich Zugriff benötigt, um den gewünschten Zweck erreichen zu können. Die pauschale Zugriffsgewährung auf alle Systeme wir in den seltensten Fällen zulässig sein.

Rollenverteilung: Sofern die eingesetzten KI-Systeme personenbezogene Daten verarbeiten, muss zudem geprüft werden, wie die datenschutzrechtlichen Rollen verteilt sind. Oft werden die Unternehmen, die KI-Systeme einsetzen, die Verantwortlichen für die Datenverarbeitung sein und die Anbieter der KI-Systeme als Auftragsverarbeiter agieren.

In diesen Fällen muss entsprechend eine Auftragsverarbeitungsvereinbarung geschlossen werden. In jedem Fall sollte die datenschutzrechtliche Rollenverteilung genau geprüft und mit dem betrieblichen Datenschutzbeauftragten besprochen werden. Sollten die personenbezogenen Daten außerhalb der EU bzw. des EWR verarbeitet werden, ist überdies zu prüfen, ob und wie dieser Drittlandtransfer datenschutzrechtlich zu rechtfertigen ist.

Rechte der betroffenen Personen: Die DSGVO gewährt den betroffenen Personen verschiedene Rechte, wie das Recht auf Auskunft, Berichtigung, Löschung und Widerspruch. Unternehmen müssen sicherstellen, dass diese Rechte gewahrt werden und entsprechende Prozesse

zur Verfügung stehen, um Anfragen der betroffenen Personen zeitnah zu bearbeiten. Auch diesbezüglich wird es entscheidend sein, sich vorab mit den Anbietern der KI-Systeme zu verständigen, ob und wie und in welcher Zeit die Berichtigung, Löschung aber auch die Auskunftserteilung und weitere Betroffenenrechte technisch umsetzbar sind, um böse Überraschungen zu vermeiden.

EU-KI-Verordnung (AI Act)

Die EU hat mit der KI-Verordnung (AI Act) eine spezielle Verordnung für die Entwicklung und Nutzung von KI erlassen, die seit August 2024 in Kraft ist. Die KI-Verordnung legt klare Regeln für Hersteller, Betreiber sowie Nutzer von KI-Systemen fest. Die KI-Verordnung verfolgt dabei einen risikobasierten Ansatz, sodass entscheidend ist, in welche Risikokategorie ein konkretes KI-System bzw. dessen Nutzung fällt.

Klassifizierung von KI-Systemen: Die KI-Verordnung sieht eine Klassifizierung von KI-Systemen in verschiedene Risikokategorien vor. Hochrisiko-KI-Systeme, wie solche, die z.B. in kritischen Infrastrukturen, im Gesundheitswesen oder in der Strafverfolgung eingesetzt werden, unterliegen grundsätzlich strengeren Anforderungen. Gleiches kann auch für bestimmte Einsatzszenarien im Bereich HR gelten. Eine genaue Prüfung des KI-Systems in Kombination mit dem konkreten Einsatzzweck muss daher zwingend vorab durchgeführt werden.

Fig-6 : Darstellung der Risikostufen in der KI-Architektur eines Unternehmens. [9]

9 https://www.1arabia.com/2024/05/eu-enacts-groundbreaking-legislation.html
1arabia.com: Die EU erlässt bahnbrechende Gesetze zur Regulierung künstlicher Intelligenz. (Zugriff 21. Mai 2024)

Anforderungen an Hochrisiko-KI-Systeme: Für Hochrisiko-KI-Systeme gelten besondere Anforderungen, wie die Durchführung von Risikobewertungen, die Implementierung von Maßnahmen zur Risikominderung und die regelmäßige Überprüfung der Systeme. Unternehmen müssen stets sicherstellen, dass diese Anforderungen auch tatsächlich erfüllt werden.

Transparenz- und Dokumentationspflichten: Die KI-Verordnung sieht vor, dass Unternehmen umfassende Dokumentationen über die Entwicklung, den Einsatz und die Überwachung von KI-Systemen führen müssen. Diese Dokumentationen sollen sicherstellen, dass die Systeme nachvollziehbar und überprüfbar sind. Darüber hinaus müssen die Nutzer sowie die betroffenen Personen, deren Daten durch KI-Systeme verarbeitet werden, transparent über die zum Einsatz kommende KI informiert werden. Zudem muss Personen, die mit dem KI-System interagieren, zu jedem Zeitpunkt bewusst sein und ggf. bewusst gemacht werden, dass sie mit einer KI interagieren und nicht mit einem Menschen.

Urheberrecht

Vor allem beim Einsatz von KI-Systemen, die Inhalte generieren, wie z.B. Texte, Bilder oder Musik, müssen Unternehmen das Urheberrecht beachten. Es ist wichtig sicherzustellen, dass die KI-Systeme keine urheberrechtlich geschützten Werke ohne entsprechende Lizenzen verwenden oder reproduzieren. Sofern Unternehmen selbst keinen Einfluss darauf haben, mit welchen Daten und Werken das KI-System trainiert wurde, ist eine vertragliche Absicherung gegenüber dem Anbieter des KI-Systems in der Regel das Mittel der Wahl.

Schutz von KI-generierten Inhalten: Es stellt sich die Frage, ob und inwieweit KI-generierte Inhalte (Output) urheberrechtlich geschützt sind. Derzeit gibt es (noch) keine einheitliche Regelung oder gefestigte Rechtsprechung. Unternehmen sollten sich daher stets vorab rechtlich beraten lassen, um sicherzustellen, dass ihre KI-generierten Inhalte geschützt sind und gleichzeitig keine Urheberrechte Dritter verletzen.

Lizenzierung und Nutzung von Trainingsdaten: Unternehmen müssen sicherstellen, dass die Daten, die zur Schulung von KI-Systemen verwendet werden, rechtmäßig erworben und lizenziert sind. Dies umfasst sowohl die Datenquellen als auch die spezifischen Daten, die für das Training verwendet werden.

Haftungsfragen

Die Haftung für Schäden, die durch KI-Systeme verursacht werden, ist ein komplexes rechtliches Thema. Unternehmen müssen klären, wer für Fehler oder Schäden verantwortlich ist, die durch die Entscheidungen oder Handlungen eines KI-Systems entstehen. Dies kann sowohl die Hersteller der KI-Systeme als auch die Unternehmen betreffen, die diese Systeme einsetzen.

Herstellerhaftung: Hersteller von KI-Systemen können bei Vorliegen der jeweiligen Voraussetzungen haftbar gemacht werden, wenn ihre Systeme fehlerhaft sind und dadurch Schäden entstehen. Dies umfasst sowohl materielle Schäden als auch immaterielle Schäden, wie z.B. Datenschutzverletzungen.

Betriebshaftung: Unternehmen, die KI-Systeme einsetzen, können ebenfalls haftbar gemacht werden, wenn diese Systeme Fehler machen oder Schäden verursachen und die

weiteren Voraussetzungen für eine solche Haftung vorliegen. Dies gilt insbesondere, wenn das Unternehmen die Systeme nicht ordnungsgemäß eingesetzt, überwacht oder gewartet hat.

Vertragliche Haftung: Unternehmen sollten vor diesem Hintergrund klare vertragliche Vereinbarungen mit den Herstellern und Anbietern von KI-Systemen treffen, um die Haftungsfragen eindeutig und verbindlich zu regeln. Dies umfasst die Festlegung von Haftungsumfang (inhaltlich), Haftungsgrenzen (finanziell), Gewährleistungen und Entschädigungen im Falle von Schäden inkl. der Geltendmachung von Ansprüchen durch Dritte.

Maßnahmen für die Geschäftsleitung

Risikobewertung und -management

Die Geschäftsleitung sollte eine umfassende Risikobewertung durchführen (lassen), um potenzielle rechtliche Risiken zu identifizieren, die mit dem Einsatz von KI-Systemen verbunden sind. Dazu gehört insbesondere die Bewertung der Datenschutzrisiken, der Haftungsrisiken und der Risiken im Zusammenhang mit der Einhaltung gesetzlicher Vorschriften, z.B. aus der KI-Verordnung.

Identifikation von Risiken: Unternehmen sollten alle potenziellen Risiken identifizieren, die mit dem Einsatz von KI-Systemen verbunden sind. Dies umfasst sowohl technische als auch rechtliche Risiken.

Bewertung der Risiken: Nach der Identifikation der Risiken sollten diese bewertet und priorisiert werden. Dies umfasst die Bewertung der Wahrscheinlichkeit und der potenziellen Auswirkungen der Risiken.

Risikominderungsmaßnahmen: Unternehmen sollten Maßnahmen zur Risikominderung implementieren, um die identifizierten Risiken zu minimieren. Dies umfasst technische Maßnahmen, wie die Implementierung von Sicherheitsprotokollen, sowie organisatorische Maßnahmen, wie die Schulung der Mitarbeiter.

Implementierung von Compliance-Programmen

Ein effektives Compliance-Programm ist entscheidend, um sicherzustellen, dass alle rechtlichen Anforderungen erfüllt werden. Dies umfasst die Schulung der Mitarbeiter, die Implementierung von KI- und Datenschutzrichtlinien sowie die regelmäßige Überprüfung der KI-Systeme auf ihre Rechtmäßigkeit und Sicherheit.

Schulung der Mitarbeiter: Mitarbeiter müssen regelmäßig geschult werden, um sicherzustellen, dass sie die rechtlichen Anforderungen und die internen Richtlinien verstehen und einhalten.

KI- und Datenschutzrichtlinien: Unternehmen müssen klare KI- und Datenschutzrichtlinien implementieren, die den Umgang mit KI-Systemen regeln, insbesondere, wenn personenbezogene Daten durch die KI-Systeme verarbeitet werden. Diese Richtlinien sollten regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass sie den aktuellen gesetzlichen und behördlichen Anforderungen entsprechen.

Überprüfung der KI-Systeme: Unternehmen sollten ihre KI-Systeme regelmäßig überprüfen, um sicherzustellen, dass sie weiterhin den rechtlichen Anforderungen entsprechen und sicher sind. Dies umfasst sowohl technische Überprüfungen als auch rechtliche Bewertungen.

Zusammenarbeit mit Rechtsexperten

Die Geschäftsleitung sollte eng mit spezialisierten Juristen (intern oder extern) zusammenarbeiten, um sicherzustellen, dass alle rechtlichen Aspekte des KI-Einsatzes berücksichtigt werden. Dies kann die vorherige Einholung von rechtlichen Einschätzungen, die Beratung durch den betrieblichen Datenschutzbeauftragten und die Zusammenarbeit mit weiteren externen Beratern umfassen. Darüber hinaus kann es Sinn ergeben, einen KI-Beauftragten im Unternehmen zu etablieren, bei dem alle Fäden zusammenlaufen und der als Single Point of Contact fungiert, auch für die Geschäftsleitung.

Fazit

Der Einsatz von KI in Unternehmen bietet viele Chancen, bringt aber auch erhebliche rechtliche Herausforderungen mit sich. Durch die Beachtung der relevanten Gesetze und Vorschriften, die Durchführung einer gründlichen Risikobewertung und die Implementierung eines robusten Compliance-Programms können Unternehmen diese Herausforderungen erfolgreich meistern und die Vorteile der KI-Technologie voll ausschöpfen.

03

Mitarbeiter und Operative Einführung

Geschrieben von Sebastian Hennerici, Omnifact Academy

Der Mensch als Schlüssel für die erfolgreiche KI Transformation

Einleitung

Die erfolgreiche Einführung von KI im Unternehmen hängt entscheidend von den Menschen ab, die diese Technologie im Alltag nutzen sollen. Zwar stehen häufig technische und rechtliche Fragen im Zentrum der Planungen, **doch letztlich ist es die Akzeptanz und Kompetenz der Mitarbeitenden, die über den nachhaltigen Erfolg der Transformation entscheide**t. Unternehmen, die über „hohe" bzw. „sehr hohe" Kompetenzen im Bereich KI verfügen, setzen KI-Initiativen deutlich schneller um und erzielen Wettbewerbsvorteile in wesentlich größerem Umfang als Unternehmen mit einem geringeren Kompetenzniveau. [10]

Die Integration von KI erfordert weit mehr als reine Technologie-Schulungen. **Es geht um einen grundlegenden kulturellen Wandel in der Art, wie Menschen arbeiten, Entscheidungen treffen und mit neuen Tools interagieren**. Mitarbeitende müssen nicht nur lernen, KI-Tools effektiv zu nutzen, sondern auch deren Potenziale und Grenzen verstehen. Erst wenn sie die Technologie als Chance statt als Bedrohung begreifen, können sie zu aktiven Gestaltern des Veränderungsprozesses werden.

Ein strukturierter, zielgruppenorientierter Ansatz zur Mitarbeiterqualifizierung bildet dabei den Schlüssel zum Erfolg. **Dieser muss die unterschiedlichen Bedürfnisse und Voraussetzungen verschiedener Mitarbeitergruppen berücksichtigen.** Neben praktischen Fertigkeiten ist es entscheidend, eine offene und innovationsfreundliche Haltung zu fördern, um die Basis für eine langfristige Transformation zu legen. Die folgenden Kapitel zeigen auf, wie Unternehmen ihre Belegschaft systematisch auf eine KI-gestützte Arbeitswelt vorbereiten und dabei das volle Potenzial ihrer wertvollsten Ressource – der Menschen – erschließen können.

KI-Kompetenz als strategischer Erfolgsfaktor

Die Fähigkeit, KI-Tools und -Software sinnvoll in bestehende Arbeitsabläufe zu integrieren, entscheidet über den Mehrwert, den ein Unternehmen aus seinen KI-Initiativen zieht. **Mitarbeitende müssen lernen, die von KI-Systemen gelieferten Ergebnisse kritisch zu hinterfragen, deren Qualität zu beurteilen und regelmäßig Verbesserungen vorzunehmen.** Auch das Bewusstsein für mögliche Risiken und rechtliche Vorgaben ist wesentlich, um den Einsatz der Technologie sicher und verlässlich zu gestalten. Wer diese Kompetenzen aufbaut, kann aktiv an der Weiterentwicklung von Use Cases mitwirken, Einsatzmöglichkeiten von KI im eigenen Arbeitsumfeld erkennen und neue Impulse für die unternehmensweite KI-Strategie liefern.

Darüber hinaus hat der gezielte Kompetenzaufbau positive Auswirkungen auf die Unternehmenskultur und das Employer Branding. Mitarbeitende, die sich im Umgang mit KI sicher fühlen und deren Nutzen für ihre Arbeit erkennen, empfinden

10 https://www2.deloitte.com/de/de/pages/technology/articles/studie-kuenstliche-intelligenz-in-unternehmen.html
Deloitte: Studie: Künstliche Intelligenz in Unternehmen: Einsatz, Strategien, Kompetenzen.

die digitale Transformation eher als Chance denn als Bedrohung. **Dies fördert eine innovationsfreundliche Grundhaltung, steigert Motivation und Zufriedenheit und macht das Unternehmen attraktiver für qualifizierte Fachkräfte.** So wird KI-Kompetenz zu einem strategischen Faktor, der nicht nur kurzfristige Effizienzvorteile, sondern auch langfristige Wettbewerbsfähigkeit und Arbeitgeberattraktivität stärkt.

Es empfiehlt sich, Erfolge im Kompetenzaufbau zu dokumentieren und regelmäßig zu kommunizieren, etwa in Berichten oder Zielvereinbarungen für Führungskräfte. Auf diese Weise rückt die Bedeutung der KI-Qualifizierung in den Fokus der gesamten Organisation und beeinflusst strategische Entscheidungen nachhaltig.

Unmittelbare Produktivitätsgewinne

Neben den langfristigen Effekten zeigen KI-Befähigungen bereits kurzfristig einen positiven Impact auf die Produktivität eines jeden Büroarbeitsplatzes. Sobald Mitarbeitende in der Lage sind, KI-Tools nutzenstiftend einzusetzen, lassen sich Routinetätigkeiten effizienter gestalten. **Beispiele sind die automatische Erstellung von Standarddokumenten, die Beantwortung häufig wiederkehrender Anfragen oder die intelligente Auswertung großer Datenmengen**. Die dadurch gewonnene Zeit kann für komplexere und kreativere Aufgaben genutzt werden, was die Wertschöpfung an jedem einzelnen Arbeitsplatz unmittelbar steigert.

Auch das beschleunigte Erschließen von Wissensbeständen gehört zu den Vorteilen: Mithilfe von KI lassen sich vorhandene Datenbestände durchforsten, relevante Informationen extrahieren und nutzbar aufbereiten. **Das ermöglicht schnellere Entscheidungen, fundierte Analysen und somit eine verbesserte Reaktionsfähigkeit auf Markt- und Kundenanforderungen**. Zudem kann KI den Mitarbeitenden als Ideengeber dienen, indem sie alternative Lösungswege oder neue Perspektiven vorschlägt. Auf diese Weise erweitert die Technologie den kreativen Spielraum der Beschäftigten, fördert Innovation und eröffnet neue Potenziale in Produkt- und Prozessentwicklung.

Handlungsempfehlung: KI-Trainings sofort angehen

Fig-7 : Prozentsatz der US-amerikanischen Befragten, die verschiedenen Aussagen über KI-Tools zustimmen. Befragt wurden 1249 US-Erwachsene [18-64 Jahre] im Zeitraum Aug - Sep 2024. [11]

Unternehmen sollten nicht darauf warten, bis ihre KI-Strategie im Detail ausgearbeitet ist, bevor sie mit der Qualifizierung ihrer Mitarbeitenden beginnen. Ein frühzeitiger Start der Schulungsmaßnahmen ermöglicht es, die Potenziale von KI möglichst schnell zu erschließen und die Akzeptanz der Mitarbeitenden für den technologischen Wandel von Anfang an zu erhöhen. So lassen sich unmittelbare Produktivitätsgewinne erzielen, Hemmschwellen abbauen und wertvolle Rückmeldungen aus der Praxis für die weitere Strategieentwicklung sammeln.

11 https://www.statista.com/
Statista: Meinungen gegenüber KI sind vielfältig.

Der Kompetenzaufbau sollte als fortlaufender Prozess verstanden werden, da sich KI-Technologien beständig weiterentwickeln. Unternehmen benötigen flexible, modulare Lernangebote, die sich zeitnah an neue Anforderungen anpassen lassen. **Gleichzeitig gilt es, eine Lernkultur zu etablieren, in der Weiterqualifizierung als selbstverständlicher Bestandteil des beruflichen Alltags verankert ist.** Nur so können die Mitarbeitenden Schritt halten mit dem schnellen Fortschritt im Bereich KI und weiterhin souverän mit neuen Tools und Anwendungen umgehen.

Darüber hinaus ist es wichtig, dass sich KI-Schulungen nicht auf rein technisches Wissen beschränken. **Die Teilnehmenden sollten ein ganzheitliches Verständnis dafür entwickeln, wie KI ihre Arbeitsabläufe, Entscheidungsstrukturen und Interaktionen mit Kunden und Kolleginnen beeinflusst.** Nur wenn sie erkennen, dass KI nicht als Bedrohung, sondern als sinnvoller und unterstützender Partner fungiert, werden sie aktiv an der Gestaltung der Transformation mitwirken.

Eine frühzeitige, kontinuierliche und umfassende Qualifizierung im Bereich KI ist somit eine strategische Investition in die Zukunftsfähigkeit jedes Unternehmens. Sie sichert die nachhaltige Ausschöpfung der KI-Potenziale, fördert eine innovationsfreundliche Unternehmenskultur und stärkt die Wettbewerbsfähigkeit im digitalen Zeitalter. **Eine KI-kompetente Belegschaft ist der Schlüssel, um KI nicht nur erfolgreich einzuführen, sondern auch langfristig im Unternehmen zu verankern.**

Bedarfsgerechte KI-Trainings

Die erfolgreiche Einführung von KI im Unternehmen setzt voraus, dass die Mitarbeitenden in der Lage sind, die Technologie sicher und effektiv in ihren Arbeitsalltag einzubinden. **Anstatt auf einheitliche Schulungen für alle zu setzen, müssen Lernangebote auf die spezifischen Anforderungen unterschiedlicher Zielgruppen zugeschnitten werden.**

Nur wenn einzelne Anwendungsszenarien, Aufgabengebiete und Kompetenzprofile differenziert betrachtet werden, lassen sich Weiterbildungsmaßnahmen entwickeln, die den Mitarbeitenden genau das Wissen und die Fähigkeiten vermitteln, die sie für den zielführenden Einsatz von KI benötigen. Auf diese Weise ist gewährleistet, dass Investitionen in Qualifizierung einen größtmöglichen Nutzen stiften und die angestrebten Effizienz- und Qualitätssteigerungen tatsächlich eintreten.

Das Vorgehen bei der Entwicklung passgenauer KI-Trainings hängt maßgeblich vom Reifegrad des Unternehmens in Bezug auf KI ab. **Insbesondere die Verfügbarkeit von Enterprise-Lösungen für Large Language Models (LLMs) ist dabei ein entscheidender Faktor.** Steht noch kein Enterprise-Zugang zu marktführenden Sprachmodellen zur Verfügung, sollte dieser zunächst etabliert werden. Durch die Anbindung mehrerer LLMs können Mitarbeitende lernen, mit unterschiedlichen Modellen umzugehen und ein breiteres Verständnis für deren Möglichkeiten und Grenzen entwickeln.

Organisatorische Voraussetzungen

Um bedarfsgerechte Trainings konzipieren zu können, ist es wichtig, es ante konkrete Einsatzpotenziale von KI in den verschiedenen Unternehmensbereichen zu identifizieren. **Workshops mit Demo Use Cases sind eine Möglichkeit, um Entscheidungsträger von den Potenzialen der Technologie zu überzeugen und die erforderliche Aufmerksamkeit sowie Unterstützung zu gewinnen.**

Parallel dazu müssen technische Voraussetzungen geschaffen werden. Die Bereitstellung geeigneter KI-Modelle – insbesondere moderner LLMs – bildet dafür das Fundament. **Darüber hinaus sind Aspekte wie Datensicherheit, Datenschutz und Compliance von Anfang an zu berücksichtigen.** Eine frühzeitig entwickelte KI-Richtlinie gibt dabei den rechtlichen und ethischen Rahmen vor und sollte in die Schulungsinhalte integriert werden.

Basis-Schulungen für den Einsatz im Arbeitsalltag

Fig-8 : Fig-8 : Die 100 wichtigsten Einsatzgebiete für generative KI, aufgeteilt in 5 Kernbereiche. [12]

12 https://learn.filtered.com/thoughts/ai-now-report
Filtered.com: The AI Now Report.

Aufbauend auf den identifizierten Einsatzfeldern lassen sich zunächst niederschwellige Basisschulungen entwickeln, die allen Mitarbeitenden ein grundlegendes Verständnis für Funktionsweise und Potenziale

von Sprachmodellen vermitteln. **Diese Einführungsformate zeigen, wie KI-Tools in alltäglichen Arbeitsabläufen integriert und gewinnbringend genutzt werden können.**

Ein besonderer Schwerpunkt liegt auf der Interaktion mit den Sprachmodellen über natürliche Sprache. Die Teilnehmenden üben, präzise Anweisungen zu formulieren, um verlässliche und relevante Antworten zu erhalten. **Darüber hinaus lernen sie, die Stärken der KI zu nutzen, aber auch deren Grenzen zu erkennen und kritisch zu hinterfragen.**

Praxisnahe Übungen und fallbezogene Beispiele helfen dabei, das Gelernte zu vertiefen und den Transfer in den individuellen Aufgabenbereich zu erleichtern. Durch die Verwendung verschiedener Sprachmodelle bekommen die Teilnehmenden ein Verständnis für deren jeweilige Stärken, Einsatzmöglichkeiten und Kombinationspotenziale.

Weiterführende Trainings für spezifische Use Cases

Aufbauend auf den Basiskompetenzen folgen spezialisierte Schulungen, die auf konkrete Anwendungsbereiche mit hohem Mehrwert zugeschnitten sind. Hier lernen die Mitarbeitenden, KI-Tools für spezifische Aufgaben zu konfigurieren und zu optimieren.

Je nach Use Case stehen unterschiedliche Schwerpunkte im Vordergrund. **Bei der Automatisierung von Korrespondenzen geht es beispielsweise darum, Vorlagen zu erstellen und Sprachmodelle mit unternehmensrelevanten Daten anzulernen.** Für die Wissensextraktion erarbeiten sich die Teilnehmenden Strategien, um relevante Informationen präzise zu identifizieren und nutzbar zu machen.

Wesentlich ist zudem die Fähigkeit, die Qualität von KI-generierten Inhalten fortlaufend zu prüfen und bei Bedarf anzupassen. Dieser anwendungsnahe Ansatz gewährleistet, dass die Lerninhalte sofort in den Arbeitsalltag einfließen und so einen unmittelbaren Nutzen generieren.

Aufbau eines Expertenteams und interner Wissenstransfer

Um die neugewonnenen Kompetenzen nachhaltig im Unternehmen zu verankern, empfiehlt sich der Aufbau eines internen Expertenteams. **Diese Fachleute fungieren nicht nur als Ansprechpartner und Treiber für den KI-Einsatz, sondern bringen ihr Know-how gezielt in ihre Bereiche ein.**

In vertiefenden Trainings erwerben die Experten umfassende Kenntnisse über Auswahl, Implementierung und Feinjustierung unterschiedlicher Sprachmodelle, lernen Best Practices kennen und machen sich mit technischen Grundlagen sowie typischen Herausforderungen vertraut. Rechtliche und ethische Aspekte stehen dabei ebenso im Fokus wie die technische Umsetzung.

Darüber hinaus benötigen diese Expertinnen und Experten didaktische und methodische Fähigkeiten, um ihr Wissen weiterzugeben. Durch individuelles Coaching „on the job“ sorgen sie dafür, dass ihr Know-how skaliert und in der gesamten Organisation fest verankert wird. **So entsteht ein selbsttragendes System, in dem KI-Kompetenz langfristig gepflegt, weiterentwickelt und optimal genutzt werden kann.**

Aufbau und Inhalte von KI-Trainings

Um den effektiven Einsatz von KI im Arbeitsalltag zu unterstützen, empfiehlt es sich, Schulungen auf Fähigkeiten auszurichten, die für eine kompetente Nutzung von Sprachmodellen erforderlich ist. **Statt reiner Theorievermittlung ist dabei ein praxisorientiertes Vorgehen ratsam, bei dem die Teilnehmenden ausreichend Gelegenheit erhalten, das Gelernte direkt anzuwenden.**

Grundlegendes Verständnis für LLMs

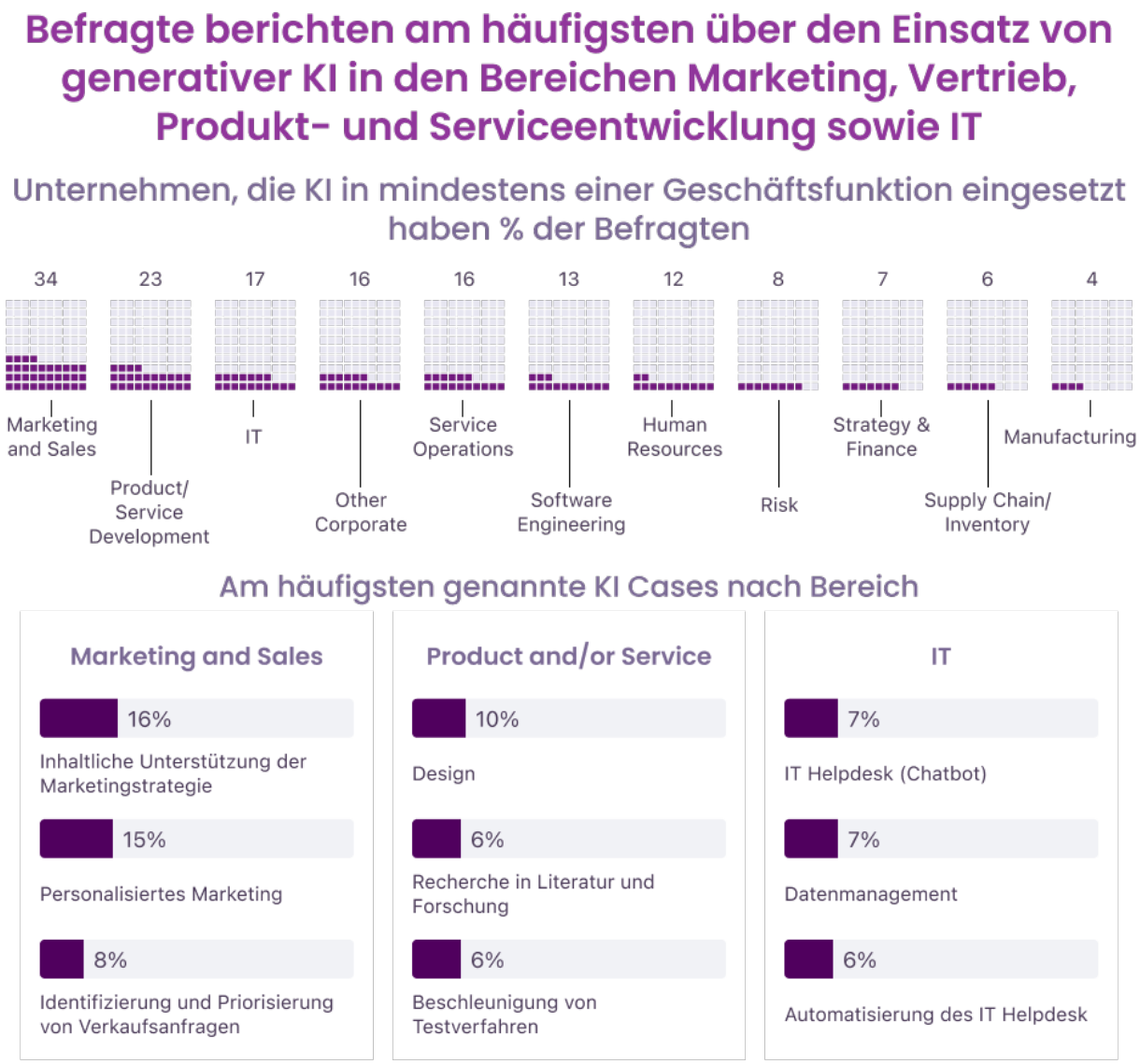


Fig-9 : Fig-9 : Einsatz von generativer KI in verschiedenen Unternehmensbereichen, mit den am häufigsten genannten KI-Anwendungsfällen. [13]

13 https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai?linkId=593691992
McKinsey: Der Stand der KI im Jahr 2023.

Zu Beginn steht die Vermittlung eines soliden Basiswissens über die Funktionsweise, Möglichkeiten und Grenzen von Large Language Models (LLMs). **Ziel ist es, ein Verständnis dafür zu schaffen, dass diese Modelle Muster in umfangreichen Datenbeständen erkennen, jedoch kein tiefgreifendes Weltverständnis besitzen.** Dadurch wird deutlicher, in welchen Einsatzbereichen LLMs hilfreich sind und an welchen Stellen ihr Output kritisch reflektiert werden sollte.

Praxisnahe Beispiele und Übungen bieten dabei einen geeigneten Zugang, um abstraktes Wissen in erfahrbare Lerninhalte zu übersetzen. **Durch eigenständiges Ausprobieren unterschiedlicher Modelle können die Teilnehmenden deren Stärken, Schwächen und spezifische Anwendungsgebiete kennenlernen.**

Prompt Engineering

Aufbauend auf dieser Grundlage empfiehlt es sich, den Schwerpunkt auf das sogenannte "Prompt Engineering" zu legen. Dieses umfasst die gezielte Formulierung von Anweisungen an das LLM, um präzise und verlässliche Ergebnisse zu erhalten. Hierbei spielen vier Schlüsselelemente eine wichtige Rolle:

- **Rolle:** Die Festlegung, in welcher Funktion oder Persona das LLM agieren soll (z. B. als Übersetzer oder Analytiker).
- **Aufgabe:** Die klare Beschreibung der erwarteten Leistung (z. B. Zusammenfassung eines Textes, Beantwortung einer Fragestellung).
- **Format:** Die Definition des gewünschten Ergebnisformats, etwa hinsichtlich Länge, Struktur oder Datentyp.
- **Kontext:** Die Bereitstellung relevanter Hintergrundinformationen und Eingabedaten, die das LLM zur Erfüllung der Aufgabe benötigt.

Eine präzise Formulierung der Prompts bildet die Grundlage für verlässliche Resultate. Gleichzeitig sollte jedoch ausreichend Freiraum für die Kreativität des Modells bestehen. Iteratives Testen und Anpassen ist dabei unerlässlich, um die Eingaben schrittweise zu verfeinern und die Ergebnisse kontinuierlich zu verbessern.

Die Erprobung verschiedener Modelle bietet zudem einen Mehrwert, da so erfahrbar wird, wie sich Prompts je nach Modell anpassen lassen. Ein enger Wechsel zwischen theoretischer Einführung und praktischen Anwendungen unterstützt diesen Lernprozess und erleichtert die Übertragung des Wissens in den beruflichen Alltag.

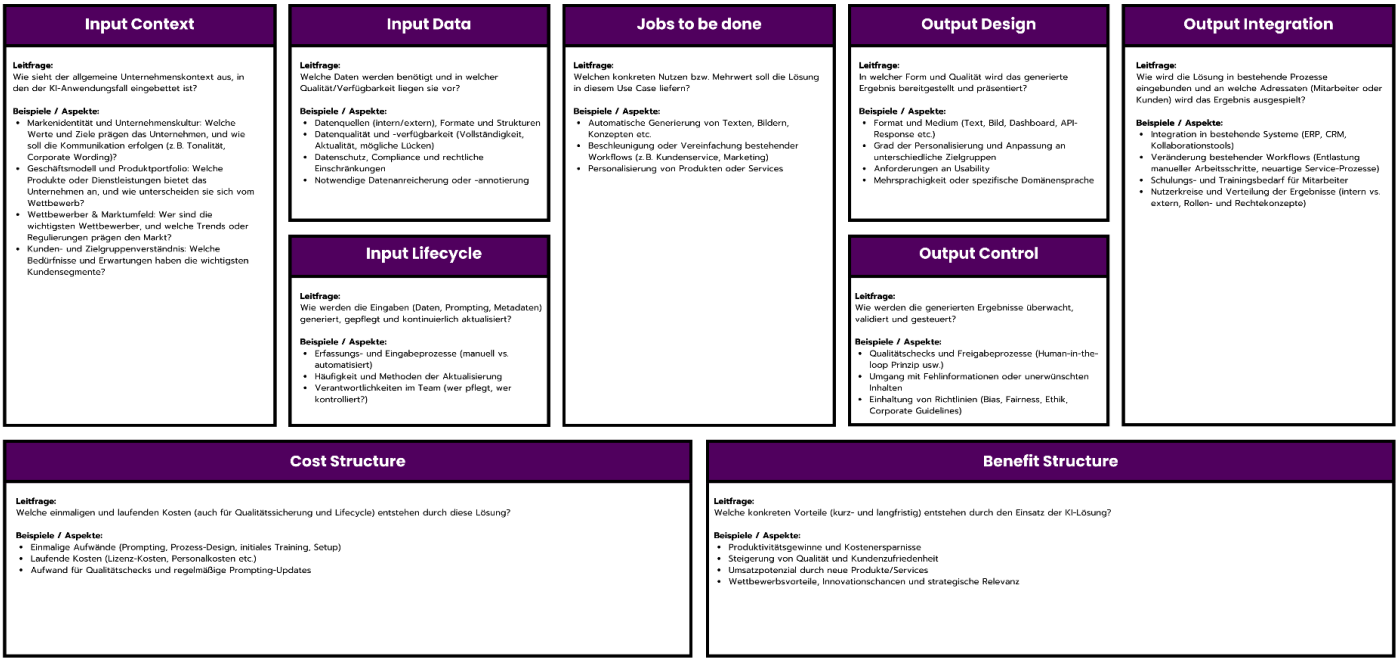


Fig-10 : In Use Case Canvas zur Planung der Anwendung von KI, erstellt von uns.

Systematisches Vorgehen für komplexe Use Cases

Während sich einfachere Anwendungsfälle oft schon durch solide Prompt-Engineering-Fähigkeiten bewältigen lassen, sind bei komplexeren Szenarien systematischere Vorgehensweisen empfehlenswert. Hier kann ein dreistufiges Modell sinnvoll sein:

- **Strukturierung des Use Cases:** Eine präzise Beschreibung des Anwendungsfalls, einschließlich Zielgruppen, Datenquellen, Prozessintegration und Verantwortlichkeiten, bildet die Grundlage für alle weiteren Schritte. Beispielhaft für eine mögliche Strukturierung ist das beigefügte Use Case Canvas (Abbildung 10).
- **Ableitung von Prompt-Strukturen:** Auf Basis dieser Analyse werden Eingaben, Anweisungen und Kontext so definiert, dass das LLM optimale Ergebnisse liefern kann.
- **Iterative Optimierung:** Die entwickelten Prompts werden mehrfach getestet, bewertet und Schritt für Schritt angepasst. Eine stetige Verfeinerung der Formulierungen, die Ergänzung fehlender Informationen und die Berücksichtigung von Sonderfällen tragen dazu bei, die Qualität der Ergebnisse kontinuierlich zu erhöhen.

Die dabei gewonnenen Erkenntnisse lassen sich im Unternehmen dokumentieren und in Form von Best Practices und Erfahrungswerten weitergeben, um die langfristige Entwicklung von KI-Kompetenzen zu unterstützen.

Kontinuierliche Weiterentwicklung der KI-Readiness und KPIs

Der Weg hin zu einem reifen Umgang mit KI ist ein fortlaufender Prozess, der regelmäßig hinterfragt und weiterentwickelt werden sollte. **Dazu bietet sich der Einsatz ausgewählter Kennzahlen an, um den Fortschritt im Kompetenzaufbau sowie die praktische Nutzung von KI im Unternehmen messbar zu machen.** Diese Daten lassen sich zudem für interne Zielformulierungen und externe Berichte, etwa im Geschäftsbericht, verwenden.

Mögliche Indikatoren sind unter anderem:

- **Teilnehmerzahlen an Schulungen:** Diese zeigen, in welchem Umfang sich die Belegschaft mit KI-Inhalten auseinandersetzt.
- **Aktive Nutzer von KI-Tools:** Die Anzahl der Personen, die erworbenes Wissen im Arbeitsalltag anwenden, liefert Hinweise auf die tatsächliche Wirksamkeit der Maßnahmen.
- **Anzahl und Qualität der KI-Use-Cases:** Die Menge und Güte konkreter Anwendungsfälle in verschiedenen Bereichen lassen Rückschlüsse auf den Grad der Verankerung von KI im Unternehmen zu.
- **Häufigkeit von KI-Workshops:** Die Resonanz auf solche Formate gibt Aufschluss über das Interesse und die Bereitschaft, sich mit KI-Themen auseinanderzusetzen.
- **Ausgebildete KI-Multiplikatoren:** Ein steigender Anteil an internen Fachexperten, die ihr Wissen weitergeben können, ist ein Indiz für die nachhaltige Verankerung von KI-Kompetenzen.
- **Mitarbeiterumfragen:** Regelmäßige Befragungen helfen, die subjektive Einschätzung der Belegschaft hinsichtlich ihrer eigenen Fähigkeiten, Unterstützungsbedarfe und Prioritäten zu erfassen.

Solche Kennzahlen sollten stets im Gesamtzusammenhang interpretiert werden. Erst in Kombination mit qualitativen Rückmeldungen, praktischen Projekterfahrungen und einer langfristigen Beobachtung des Entwicklungsverlaufs ergibt sich ein differenziertes Bild der erreichten KI-Readiness.

Fig-11 : Sechs Merkmale von KI-Power-Usern. [14]

14 https://www.proserveit.com/blog/ai-at-work-a-comprehensive-summary-of-microsofts-findings
ProServeIT: KI am Arbeitsplatz – Eine umfassende Zusammenfassung der Ergebnisse von Microsoft. (Zugriff 31. Juli 2024)

04

Software, Technologie und IT-Einführung

Geschrieben von Patrick Helmig, Omnifact

KI Revolution - In großen Schritten von KI Assistenten zu autonomen KI Agenten

Technische Architektur

Generative KI

Die Entwicklung generativer KI-Modelle hat **seit 2021 eine beispiellose Dynamik** erreicht. Diese Modelle, trainiert auf gewaltigen Datenmengen, können heute natürliche Sprache verstehen, kontextuell relevante Antworten generieren und komplexe Aufgaben bewältigen. Zwei wichtige Benchmarks verdeutlichen diese Entwicklung:

Der "Solving World Problems" (SWE) Benchmark misst die Fähigkeit von KI-Modellen, komplexe Programmieraufgaben zu lösen. Die **Leistung der Modelle in diesem Test hat sich von 1% erfolgreicher Lösungen Anfang 2023 auf über 40% Ende 2024 gesteigert**. [15]

Der MMLU (Massive Multitask Language Understanding) Benchmark testet KI-Sprachmodelle in 57 verschiedenen akademischen und beruflichen Fachgebieten mittels Multiple-Choice-Fragen auf Universitätsniveau, um ihre Fähigkeit zum Verständnis und zur Anwendung von Fachwissen zu bewerten.. Auch hier zeigt sich eine beeindruckende Entwicklung: Die Erfolgsquote stieg v**on 60% auf über 90% innerhalb von 18 Monaten.** [16] [17]

Diese rapide Entwicklung hat direkte Auswirkungen auf die praktische Anwendbarkeit: **Use Cases, die vor sechs Monaten noch nicht realisierbar erschienen, sind heute problemlos umsetzbar**. Für Unternehmen bedeutet dies, dass eine regelmäßige Neubewertung von Anwendungsfällen essentiell ist. Die Frage ist nicht mehr ob, sondern wann bestimmte Prozesse durch KI unterstützt oder automatisiert werden können.

Die Rapide Verbesserung von KI Modellen: Entwicklung der Performance seit Ende 2022

Fig-12 : Die Entwicklung der Performance von KI-Modellen seit Ende 2022, basierend auf MMLU-Scores. Daten wurden im Dezember 2024 erhoben.

15 https://www.swebench.com/
SWE Bench: Website. (Zugriff Dezember 2024)

16 https://paperswithcode.com/sota/multi-task-language-understanding-on-mmlu
Papers With Code: Multitasking-Sprachverständnis auf MMLU. (Zugriff Dezember 2024)

17 https://openai.com/index/learning-to-reason-with-llms/
OpenAI: Lernen, mit LLMs zu argumentieren. (Zugriff September 2024)

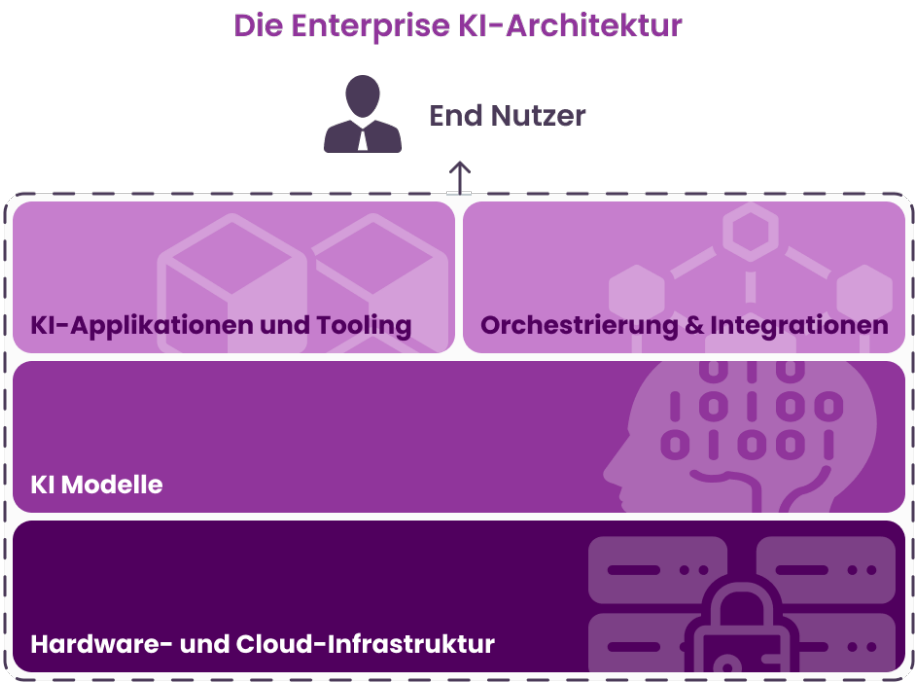


Fig-13 : Darstellung der Enterprise KI-Architektur, erstellt von uns.

Der Enterprise KI Stack

Während Chat-Interfaces den einfachsten Zugang zu KI-Modellen bieten, erfordern unternehmenskritische Anwendungsfälle eine tiefere Integration in bestehende Systeme und Prozesse. Ob Automatisierung im Kundenservice, KI-gestützte Wissensdatenbanken oder intelligente IT-Operations - der wirtschaftliche Mehrwert entsteht durch die Verbindung von KI-Fähigkeiten mit Unternehmensdaten und -systemen.

Die erfolgreiche Implementation von KI im Unternehmenskontext erfordert eine durchdachte Architektur, die weit über einzelne Chat-Anwendungen hinausgeht. **Der wirtschaftliche Mehrwert entsteht erst durch die nahtlose Integration von KI-Fähigkeiten in bestehende Unternehmenssysteme und -prozesse**, was eine mehrschichtige technische Infrastruktur voraussetzt. Diese reicht von der grundlegenden Hardware- und Cloud-Infrastruktur über die eigentlichen KI-Modelle bis hin zu anwendungsspezifischen Komponenten und Integrationsschichten.

Die vier Kernebenen des Enterprise KI Stacks bilden dabei ein kohärentes Gesamtsystem, das Flexibilität und Skalierbarkeit mit den hohen Sicherheits- und Compliance-Anforderungen von Unternehmen vereint. Während die unteren Schichten die technische Basis mit Cloud- oder On-Premise-Infrastruktur sowie verschiedenen KI-Modellen bereitstellen, ermöglichen die oberen Schichten die praktische Nutzung durch Fachanwender und die Integration in bestehende Geschäftsprozesse. Besonders die Integrationsschicht spielt eine zentrale Rolle, da sie durch standardisierte Schnittstellen und robuste Sicherheitsmechanismen die Verbindung zwischen KI-Technologie und operativem Geschäft herstellt.

Der Agenten-Loop: Grundlagen intelligenter Automatisierung

Die Grundlage erfolgreicher KI-gestützter Automatisierung bildet der Agenten-Loop - ein Prozess, der bewusst der menschlichen

Herangehensweise an komplexe Aufgaben nachempfunden ist. **Durch die systematische Kombination von Analyse, Ausführung und Kontrolle können KI-Systeme nicht nur einzelne Aufgaben ausführen, sondern ganze Arbeitsprozesse intelligent steuern und optimieren**. Dabei spielt die Fähigkeit, verschiedene Werkzeuge und Systeme zu orchestrieren, eine zentrale Rolle.

Die erste Phase der Analyse und Planung bildet das Fundament für erfolgreiche Automatisierung. Hier zeigt sich eine zentrale Stärke moderner KI-Systeme: **Die Fähigkeit, komplexe Aufgabenstellungen zu verstehen, in bearbeitbare Teilschritte zu zerlegen und einen strukturierten Handlungsplan zu entwickeln**. Ähnlich wie Menschen analysiert der Agent zunächst die verfügbaren Werkzeuge und Informationsquellen, um dann die effektivste Kombination für die Aufgabenlösung zu wählen.

In der Ausführungsphase wird der besondere Mehrwert der Tool-Integration deutlich: **Der Agent fungiert als intelligenter Orchestrator, der verschiedene Unternehmenssysteme und externe Dienste gezielt miteinander verbindet**. Durch standardisierte Schnittstellen kann er Daten aus dem CRM abrufen, Analysetools nutzen oder Aktionen in anderen Systemen auslösen - ganz ähnlich wie ein erfahrener Mitarbeiter verschiedene Programme und Ressourcen für seine Arbeit kombiniert. Die abschließende Kontroll- und Feedback-Phase gewährleistet dabei die Qualität und kontinuierliche Verbesserung des Prozesses.

Ein entscheidender Vorteil dieses Ansatzes ist seine Skalierbarkeit über verschiedene Autonomie-Level hinweg. **Unternehmen können den Grad der Automatisierung flexibel an ihre Anforderungen und ihr Vertrauensniveau anpassen** - vom vollständig überwachten Modus, bei dem jeder Schritt menschliche Bestätigung erfordert, bis hin zur autonomen Ausführung innerhalb definierter Grenzen. Die Tool-basierte Architektur ermöglicht dabei eine schrittweise Erweiterung der Funktionalität: Neue Systeme und Fähigkeiten können einfach als weitere Tools integriert werden, ohne die grundlegende Logik des Agenten-Loops zu verändern.

Die flexible Gestaltung des Autonomiegrades ist ein Schlüsselelement für die erfolgreiche Integration von KI-Agenten in Unternehmensprozesse. **Je nach Sensibilität der Aufgabe, Erfahrungswerten und Compliance-Anforderungen können Unternehmen den optimalen Grad menschlicher Kontrolle definieren**. Im vollständig überwachten "Supervised Mode" agiert der Agent als vorbereitender Assistent, der jeden geplanten Schritt zur Freigabe vorlegt - ideal für die initiale Einführungsphase oder besonders kritische Prozesse.

Der "Semi-Autonomous Mode" bietet einen ausgewogenen Mittelweg: **Routine-Aufgaben werden selbstständig ausgeführt, während bei kritischen Entscheidungen oder unerwarteten Situationen menschliche Expertise einbezogen wird**. Dies entspricht einem natürlichen Delegationsprozess, bei dem erfahrene Mitarbeiter eigenständig arbeiten, aber bei wichtigen Weichenstellungen Rücksprache halten. Im "Fully Autonomous Mode" kann der Agent schließlich innerhalb klar definierter Parameter vollständig selbstständig agieren - ähnlich einem erfahrenen Team, das in seinem Kompetenzbereich eigenverantwortlich handelt. Entscheidend ist dabei, dass die Grenzen der Autonomie präzise definiert und technisch durchgesetzt werden, etwa durch Budgetlimits, Berechtigungseinschränkungen oder regelbasierte Kontrollen.

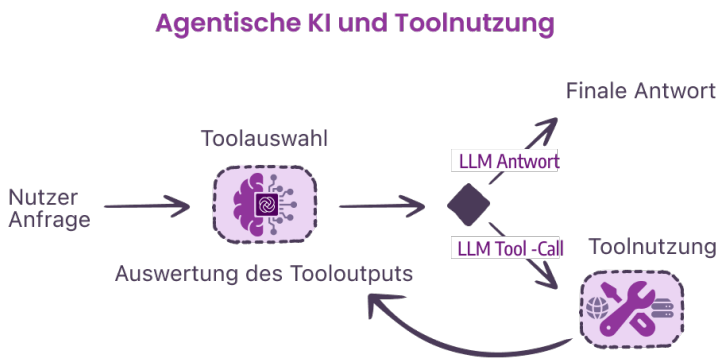


Fig-14 : Veranschaulichung der agentischen KI und Toolnutzung.

Agentenbasierte Automatisierung am Beispiel

Betrachten wir einen typischen Geschäftsprozess: **Die personalisierte Kommunikation eines Produktlaunches an Bestandskunden**. Diese Aufgabe demonstriert das Zusammenspiel aller Architekturkomponenten in einem agentenbasierten Workflow.

Die Aufgabe:

"Informiere alle regionalen Kunden über unser neues Produkt mit personalisierten E-Mails, die Produktdetails aus unserem Wiki, Kundeninformationen aus dem CRM und aktuelle Marktentwicklungen berücksichtigen."

Der Agenten-Loop in Aktion:

1. **Planung und Dekomposition**

- Der Agent analysiert die Aufgabe und erstellt einen strukturierten Plan:
  - **Informationssammlung**
    - Produkt-Details aus Wiki abrufen
    - Kundenliste aus CRM extrahieren
    - Kundenrecherche durchführen **2. E-Mail-Erstellung pro Kunde**
    - Personalisierung basierend auf CRM-Daten
    - Integration von Produktinformationen
    - Anreicherung mit Marktkontext **3. Review und Versand**
    - Qualitätsprüfung der E-Mails
    - Freigabeprozess
    - Versand und Dokumentation

2. **Tool Calling und Ausführung**

- Für jeden Schritt ruft der Agent spezifische Tools auf:
  - RAG-System für Produktdokumentation
  - CRM-API für Kundendaten
  - Web-Search-Tool für Marktrecherche
  - E-Mail-Template-Engine
  - E-Mail-Versand-System

3. **Nutzer-Interaktion und Kontrolle**

- Der Agent holt an kritischen Punkten Feedback ein:
  - Bestätigung des Gesamtplans
  - Review der ersten E-Mail-Templates
  - Freigabe vor Massenversand
  - Eskalation bei Unklarheiten

Besonderheiten des Tool-basierten Ansatzes:

Die besondere Stärke des Tool-basierten Ansatzes liegt in seiner modularen Architektur. **Jedes Unternehmenssystem wird als eigenständiges "Tool" mit klar definierten Fähigkeiten und Schnittstellen in die Automatisierung eingebunden**. Diese Modularität ermöglicht es, die Funktionalität des Systems schrittweise zu erweitern, ohne bestehende Prozesse zu gefährden. Neue Tools - seien es interne Systeme oder externe Dienste - können dank standardisierter Schnittstellen einfach integriert werden, wodurch das Automatisierungspotenzial kontinuierlich wächst.

Die kontrollierte Autonomie bildet einen weiteren zentralen Baustein des Konzepts. **Für jedes Tool werden präzise Regeln und Grenzen definiert, die festlegen, welche Aktionen der Agent ausführen darf und welche nicht**. Eingebaute Sicherheitsprüfungen und konfigurierbare Autonomie-Level gewährleisten dabei, dass die Automatisierung stets in kontrollierten Bahnen verläuft. Dies schafft das notwendige Vertrauen für den produktiven Einsatz in geschäftskritischen Prozessen und ermöglicht eine schrittweise Ausweitung der automatisierten Aufgaben.

Der planungsbasierte Charakter der Ausführung sorgt für maximale Transparenz und Kontrolle. **Bevor der Agent Aktionen ausführt, legt er einen detaillierten Plan vor, der alle geplanten Schritte und deren Abhängigkeiten aufzeigt**. Menschen können diese Pläne prüfen, bei Bedarf anpassen und die Ausführung überwachen. Die lückenlose Dokumentation aller Aktionen und Entscheidungen macht den gesamten Prozess nachvollziehbar und auditfähig - ein entscheidender Vorteil für regulierte Umgebungen und komplexe Geschäftsprozesse.

KI Rollout als Evolution

Die Implementation von KI in Unternehmen folgt typischerweise einer evolutionären Entwicklung. Statt einer revolutionären Umstellung etablierter Prozesse, ermöglicht ein schrittweiser Ansatz sowohl schnelle Erfolge als auch nachhaltige Transformation.

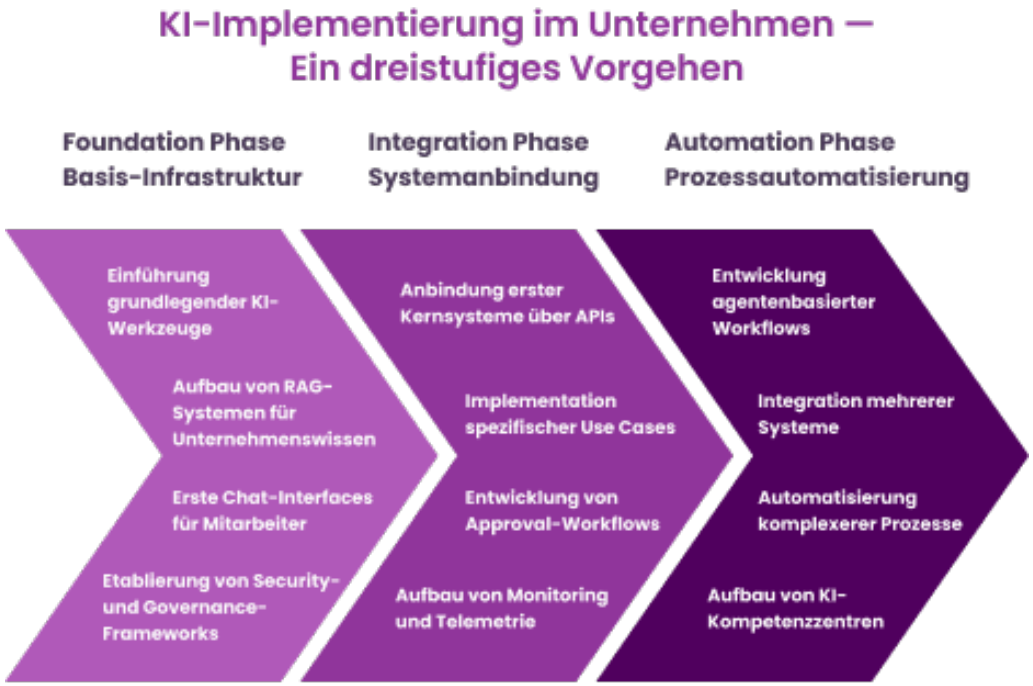


Fig-15 : Darstellung des KI-Implementierungsprozesses in drei Phasen

Exponentielles Wachstum durch modularen Ansatz

Mit jeder integrierten Komponente steigt der potenzielle Automatisierungsgrad überproportional:

- Jedes neue Tool erweitert die Handlungsmöglichkeiten der Agenten
- Kombinationen verschiedener Tools ermöglichen komplexere Workflows
- Bestehendes Wissen kann für neue Use Cases genutzt werden

Security-Framework

Datensouveränität als Grundprinzip

Datensouveränität bedeutet, dass Unternehmen **zu jedem Zeitpunkt die vollständige Kontrolle über ihre Daten behalten**. Dies ist besonders relevant bei der Nutzung von KI-Systemen, die oft auf externe Modelle und Dienste zugreifen.

Kontrolle über Datenflüsse

Die Kontrolle über Datenflüsse bildet das Fundament der Datensouveränität. Eine transparente und lückenlose Dokumentation ermöglicht es Unternehmen, jeden Aspekt der Datenverarbeitung nachzuvollziehen. Dies umfasst die automatische Erfassung aller Datenübertragungen, eine detaillierte Klassifizierung nach Sensitivität sowie umfassende Reporting-Funktionen für Compliance-Anforderungen.

Die **granulare Steuerung der Datenflüsse erfolgt über ein regelbasiertes System, das verschiedene Datentypen differenziert behandelt** und kontextabhängige Zugriffsrechte vergibt. Durch Versionierung

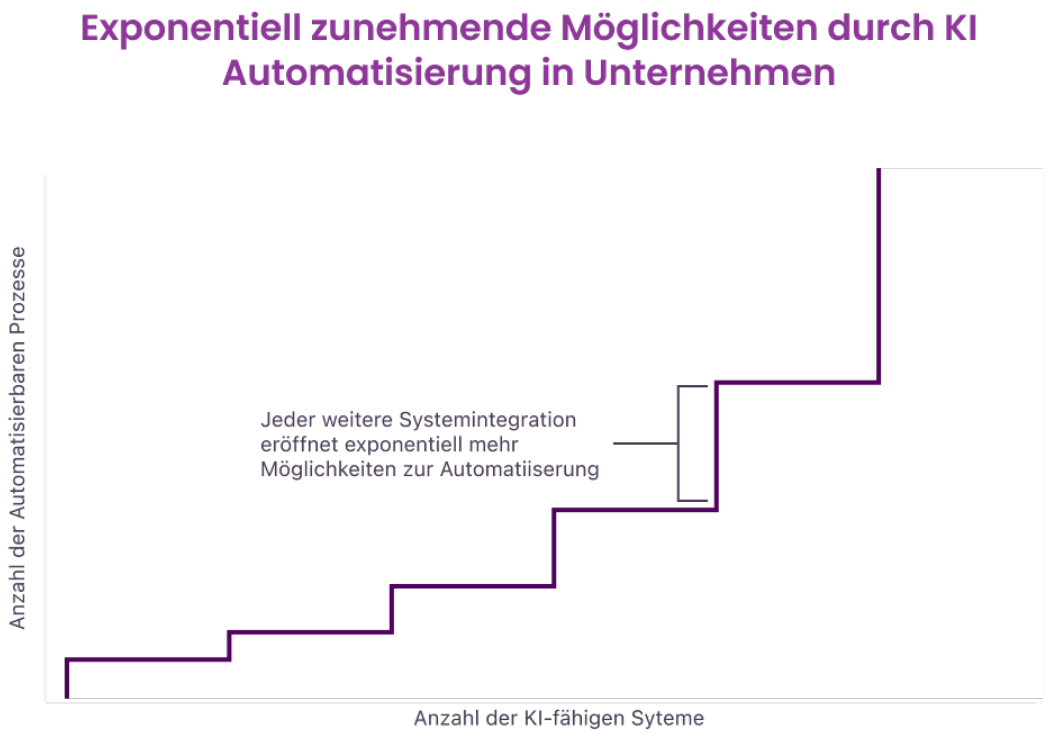


Fig-16 : Darstellung der exponentiell zunehmenden Möglichkeiten durch KI-Automatisierung in Unternehmen

und Historisierung bleibt jede Änderung nachvollziehbar und reversibel.

Ein besonders **mögliches Element sind Privacy Filter, die in Echtzeit sensible Informationen erkennt und filtern.** Dieser automatisierte Prozess identifiziert personenbezogene Daten (PII) und wendet konfigurierbare Maskierungsregeln an. Die Effektivität dieser Filterung wird kontinuierlich überwacht und validiert.

Das Data Lineage Tracking vervollständigt die Kontrolle über Datenflüsse, indem es die gesamte Nutzungshistorie der Daten dokumentiert. Dies ermöglicht nicht nur die Verfolgung von Datentransformationen, sondern auch detaillierte Impact-Analysen und eine auditfähige Protokollierung aller Vorgänge.

Modell- und Anbieter-Strategie

Eine zukunftsfähige KI-Strategie erfordert einen durchdachten Ansatz bei der Auswahl und Integration von Modellen und Anbietern. Mit **zunehmender Abhängigkeit von KI-Systemen in geschäftskritischen Prozessen steigt dabei auch das Risiko von strategischen Fehlentscheidungen** bei der Modellauswahl erheblich.

Hybride Ansätze spielen dabei eine zentrale Rolle: Sie kombinieren verschiedene Modelltypen und ermöglichen eine optimale Balance zwischen Leistungsfähigkeit und Kontrolle. Dabei gewinnen Open-Source-Modelle zunehmend an Bedeutung. Sie bieten nicht nur eine Alternative zu proprietären Lösungen, sondern ermöglichen auch eine tiefere Kontrolle über die eingesetzte Technologie. Die rasante Entwicklung von Modellen wie Mistral oder Llama zeigt, dass Open-Source-Lösungen in vielen Anwendungsfällen bereits mit kommerziellen Anbietern konkurrieren können. Gleichzeitig erfordern sie jedoch auch spezifische Kompetenzen und Ressourcen für Deployment und Wartung.

Die Vermeidung von Vendor Lock-in wird mit steigender KI-Adoption zu einem kritischen Erfolgsfaktor. **Je tiefer KI-Systeme in Unternehmensprozesse integriert werden, desto schwerwiegender werden die Auswirkungen einer zu starken Abhängigkeit** von einzelnen Anbietern. Durch standardisierte Schnittstellen und modellunabhängige Architekturen bleiben Unternehmen flexibel und können bei Bedarf alternative Anbieter oder Open-Source-Lösungen integrieren. Dokumentierte Wechselstrategien stellen sicher, dass ein Anbieterwechsel jederzeit möglich ist - ein Aspekt, der angesichts der dynamischen Entwicklung des Marktes und potenzieller Änderungen in Geschäftsmodellen oder Preisstrukturen der Anbieter nicht zu unterschätzen ist.

Die Nutzung externer Dienste wird durch klare Richtlinien und kontinuierliches Monitoring gesteuert. Dabei müssen Unternehmen zunehmend auch die langfristigen Implikationen ihrer Modellauswahl berücksichtigen: **Wie entwickeln sich Trainings- und Inferenzkosten? Welche Daten sammeln Anbieter über die Nutzung? Wie transparent sind Modellaktualisierungen und deren Auswirkungen auf bestehende Anwendungen?** Service Level Agreements und regelmäßige Compliance-Checks gewährleisten, dass die Dienstleistungen den Unternehmensanforderungen entsprechen.

Ergänzend dazu sichern durchdachte Exit-Strategien die langfristige Handlungsfähigkeit: Sie umfassen detaillierte Datenmigrationspläne, alternative Lösungswege und transparente Kostenanalysen für verschiedene Szenarien. Mit der zunehmenden Integration von KI in kritische Geschäftsprozesse wird die Fähigkeit, Modelle und Anbieter flexibel zu wechseln, zu

einem entscheidenden Faktor für die digitale Souveränität eines Unternehmens.

Ein besonderes Augenmerk sollte dabei auf der Balance zwischen Cloud-basierten Diensten und selbst-gehosteten Lösungen liegen. Während Cloud-Anbieter oft die neuesten Modelle und einfache Skalierbarkeit bieten, ermöglichen selbst-gehostete Open-Source-Modelle eine größere Kontrolle über Datenschutz und Kosten. Eine zukunftsfähige Strategie berücksichtigt beide Optionen und schafft die Voraussetzungen, um je nach Anwendungsfall und regulatorischen Anforderungen die optimale Lösung wählen zu können.

Security Framework für KI-Systeme

Die Integration von KI in Unternehmensprozesse schafft **neuartige Sicherheitsanforderungen**, die sich deutlich von traditionellen IT-Sicherheitskonzepten unterscheiden. Dies lässt sich am Beispiel eines typischen Retrieval Augmented Generation (RAG) Systems veranschaulichen: Ein Unternehmen möchte seinen Mitarbeitern ermöglichen, mittels KI-gestützter Assistenten auf das gesammelte Unternehmenswissen zuzugreifen.

Bereits dieser scheinbar einfache Anwendungsfall offenbart die komplexen Sicherheitsherausforderungen moderner KI-Systeme: Das RAG-System muss Zugriff auf interne Dokumente erhalten, diese inhaltlich verstehen und relevante Informationen an große Sprachmodelle übermitteln. Dabei entstehen neuartige Risiken: **Wie verhindert man, dass sensitive Informationen unbeabsichtigt in Prompts eingebettet werden?** Wie stellt man sicher, dass Nutzer nur auf Dokumente zugreifen können, für die sie berechtigt sind - auch wenn die Informationen über verschiedene Dokumente hinweg kombiniert werden? Wie kontrolliert man die Weitergabe von Unternehmenswissen an externe KI-Modelle?

Diese Fragen verdeutlichen, dass klassische Zugriffskontrollen und Verschlüsselungsmechanismen zwar weiterhin wichtig, aber nicht mehr ausreichend sind. **Ein zeitgemäßes Security Framework muss die gesamte Verarbeitungskette von KI-Systemen berücksichtigen** - von der Datenvorbereitung über die Modellinteraktion bis zur Ergebnispräsentation. Das RAG-Beispiel zeigt dabei exemplarisch die verschiedenen Sicherheitsebenen, die adressiert werden müssen:

- Die Dokumentenzugriffe müssen nicht nur auf Dateiebene, sondern auch auf semantischer Ebene kontrolliert werden
- Privacy-Filter müssen in Echtzeit sensitive Informationen erkennen und maskieren
- Die Interaktion mit externen KI-Modellen muss kontinuierlich überwacht und protokolliert werden
- Die generierten Antworten müssen auf unbeabsichtigte Weitergabe von sensitivem Wissen geprüft werden

Technische Sicherheitsmaßnahmen für KI-Systeme

Die Integration von generativer KI und autonomen Agenten in Unternehmensprozesse schafft neue Sicherheitsanforderungen, die über traditionelle IT-Sicherheitskonzepte hinausgehen. Besonders die Fähigkeit von KI-Systemen, im Namen von Nutzern zu handeln und auf verschiedene Unternehmenssysteme zuzugreifen, erfordert eine Neubetrachtung etablierter Sicherheitsmechanismen.

Zugriffsmanagement für KI-Agenten

Die Delegation von Berechtigungen an KI-Agenten erfordert ein erweitertes Zugriffskonzept. Während traditionelle Systeme primär die Rechte menschlicher Nutzer verwalten, müssen bei KI-Systemen zusätzliche Kontrollebenen eingeführt werden. Auch wenn ein Nutzer umfangreiche Berechtigungen besitzt, muss sichergestellt werden, **dass KI-Agenten, die in seinem Namen agieren, nur innerhalb definierter Grenzen operieren** können.

Dies wird durch ein mehrstufiges Berechtigungssystem erreicht, das spezielle Berechtigungsprofile für KI-Agenten definiert. Diese Profile sind unabhängig von den Nutzerrechten und ermöglichen eine granulare Steuerung erlaubter Operationen. Zusätzliche kontextabhängige Einschränkungen, etwa basierend auf Zeitfenstern, Ressourcenverbrauch oder spezifischen Geschäftsregeln, bieten weitere Kontrollebenen.

Human-in-the-Loop Integration

Ein zentrales Element der Sicherheitsarchitektur ist die **systematische Integration menschlicher Kontrolle.** Moderne KI-Systeme erfordern ein durchdachtes Gleichgewicht zwischen Automation und menschlicher Überwachung. Das System muss klar definieren, welche Aktionen einer expliziten Freigabe bedürfen und wie diese Freigabeprozesse gestaltet sind.

Die Implementierung erfolgt über ein System von Kritikalitätsstufen, die verschiedene Aktionen nach ihrem Risikopotenzial kategorisieren. Darauf aufbauend werden mehrstufige Genehmigungsprozesse für kritische Operationen definiert. Notfall-Stopp-Mechanismen ermöglichen die sofortige Unterbrechung laufender Agenten-Prozesse, während umfassende Audit-Trails alle Freigaben und Interventionen dokumentieren.

KI-spezifische Bedrohungsszenarien

Mit der Einführung von KI-Systemen entstehen neue Angriffsvektoren, die spezifische Schutzmaßnahmen erfordern. Prompt Injection Attacks stellen dabei eine besondere Herausforderung dar. Diese werden durch strikte **Validierung und Sanitization aller Eingaben sowie kontextuelle Analyse von Prompts** auf versteckte Befehle adressiert. Eine konsequente Trennung von Systeminstruktionen und Nutzerinput verhindert unbeabsichtigte Befehlsausführungen. Die Kontrolle von Ressourcen gewinnt ebenfalls an Bedeutung. Durch präzise Budgetierung von API-Aufrufen und Rechenzeit sowie die Implementierung von Kostenlimits pro Agent und Workflow werden wirtschaftliche Risiken minimiert. Gleichzeitig schützen erweiterte Masking-Mechanismen und kontextsensitive Filterung vor unbeabsichtigter Datenexfiltration.

Nachvollziehbarkeit und Attribution

Die Zuordnung von Aktionen zu verantwortlichen Personen wird bei KI-Systemen komplexer. Jede **Agenten-Aktion muss eindeutig mit dem initiierenden Nutzer verknüpft** werden, wobei auch mehrstufige Entscheidungsketten nachvollziehbar dokumentiert werden müssen. Dies erfordert erweiterte Logging-Mechanismen, die nicht nur die Aktionen selbst, sondern auch deren Kontext und Entscheidungsgrundlagen erfassen.

Systemübergreifende Integration

Die Integration von KI-Agenten in bestehende Systemlandschaften erfordert eine Anpassung der Sicherheitsarchitektur auf mehreren Ebenen. Authentifizierungslösungen wie OAuth 2.0 gewährleistet die sichere Rechteweitergabe an Agenten und Diensten sowie die durchgängige Authentifizierung über Systemgrenzen hinweg. Die Identity Federation vereinheitlicht dabei die Identitätsverwaltung für Menschen und Agenten, während temporäre Zugriffstoken mit minimalen Rechten das Prinzip der geringsten Privilegien umsetzen.

Diese erweiterten Sicherheitsmaßnahmen müssen als dynamisches System verstanden werden, das kontinuierlich an neue Entwicklungen im Bereich der KI angepasst wird. Die schnelle Evolution von KI-Fähigkeiten erfordert ein agiles Sicherheitskonzept, das neue Bedrohungsszenarien frühzeitig erkennt und entsprechende Schutzmaßnahmen implementiert. Nur durch diesen ganzheitlichen Ansatz können Unternehmen die Vorteile von KI-Systemen nutzen, ohne dabei ihre Sicherheitsstandards zu kompromittieren.

Datenschutz in KI-Systemen

Der Schutz sensibler Daten erhält im Kontext von KI-Systemen eine neue Dimension. In den vergangenen zwei Jahren haben KI Systeme bereits zu verherenden Datenpannen geführt, die tausende Personen und Unternehmen betroffen haben [Excibit A - WotNot Chatbot data leak, Excibit B - Open AI Data Leak, Excibit C - Permissions issues with Microsoft CoPilot] Anders als bei traditionellen Anwendungen müssen nicht nur Datenzugriffe, sondern auch die Verarbeitung und potenzielle Weitergabe von Informationen durch KI-Modelle kontrolliert werden. Ein mehrschichtiges Privacy-Konzept kombiniert dabei klassische Verschlüsselungsmechanismen mit KI-spezifischen Schutzmaßnahmen.

Hilfreich ist die Implementation eines Privacy-Filters, der sensitive Informationen bereits vor der Übergabe an KI-Modelle erkennt und maskiert. Dieser proaktive Ansatz **verhindert, dass personenbezogene oder vertrauliche Unternehmensdaten unbeabsichtigt in Modell-Prompts oder Trainingsdaten** gelangen. Die Klassifizierung und entsprechende Behandlung verschiedener Datenkategorien erfolgt dabei automatisiert und regelbasiert. Ein intelligentes Retention Management steuert nicht nur die Speicherdauer von Rohdaten, sondern auch von abgeleiteten Informationen in Modell-Caches und Inferenzlogs.

Monitoring & Audit für KI-Workflows

Die Überwachung von KI-Systemen erfordert erweiterte Monitoring-Konzepte, die über traditionelles System-Monitoring hinausgehen. Ein ganzheitlicher Monitoring-Ansatz erfasst dabei nicht nur **technische Metriken, sondern auch die Qualität und Plausibilität von KI-generierten Ergebnissen**. Real-time Monitoring identifiziert dabei ungewöhnliche Muster sowohl in der Systemnutzung als auch in den Modellausgaben, die auf potenzielle Sicherheitsvorfälle oder Qualitätsprobleme hinweisen können.

Besondere Bedeutung kommt der Überwachung von KI-Agenten zu, die eigenständig Aktionen ausführen. Hier müssen sowohl der Ressourcenverbrauch als auch die Aktionssequenzen kontinuierlich analysiert werden. Detaillierte Audit-Logs dokumentieren dabei nicht nur einzelne Aktionen, sondern

auch deren Kontext und Begründung. Dies ermöglicht sowohl die nachträgliche Analyse von Vorfällen als auch die kontinuierliche Optimierung der Sicherheitsmaßnahmen. Automatisierte Compliance-Reports fassen sicherheitsrelevante Ereignisse zusammen und ermöglichen eine effiziente Nachweisführung gegenüber Auditoren und Regulierungsbehörden. Die Integration von KI-spezifischen Metriken in bestehende Security Information and Event Management (SIEM) Systeme gewährleistet dabei eine ganzheitliche Sicherheitsüberwachung über alle Systemebenen hinweg.

Operative Sicherheit

Die operative Sicherheit von KI-Systemen erfordert eine kontinuierliche und proaktive Herangehensweise, die sowohl präventive Maßnahmen als auch effektive Reaktionsmechanismen umfasst. Im Zentrum steht dabei die Frage, wie der sichere Betrieb von KI-Systemen im Unternehmensalltag gewährleistet werden kann.

Incident Response

Die Behandlung von Sicherheitsvorfällen bei KI-Systemen erfordert spezialisierte Prozesse und Kompetenzen. Anders als bei traditionellen IT-Systemen können Vorfälle hier auch durch **unerwartetes Verhalten der KI-Modelle oder durch die Kombination scheinbar harmloser Einzelaktionen** entstehen. Ein effektives Incident Response System muss daher sowohl technische als auch KI-spezifische Expertise vereinen.

Klar definierte Eskalationsprozesse stellen sicher, dass Vorfälle schnell erkannt und an die richtigen Stellen weitergeleitet werden. Dabei spielen Emergency Response Teams eine zentrale Rolle, die sowohl über das notwendige technische Verständnis als auch über Entscheidungskompetenz verfügen. Diese Teams müssen in der Lage sein, die Auswirkungen von Vorfällen schnell einzuschätzen und geeignete Gegenmaßnahmen einzuleiten.

Recovery-Prozeduren müssen dabei die Besonderheiten von KI-Systemen berücksichtigen. Dies betrifft insbesondere die Wiederherstellung von konsistenten Systemzuständen nach Vorfällen, **bei denen KI-Agenten möglicherweise mehrere verknüpfte Systeme beeinflusst haben**. Klare Kommunikationsrichtlinien stellen sicher, dass alle betroffenen Stakeholder zeitnah und angemessen informiert werden.

Kontinuierliche Überwachung

Die kontinuierliche Überwachung von KI-Systemen geht weit über klassisches System-Monitoring hinaus. Security Metrics müssen dabei sowohl technische Aspekte als auch das Verhalten der KI-Modelle selbst erfassen. Die Analyse von Nutzungsmustern und Modellausgaben ermöglicht es, potenzielle Sicherheitsrisiken frühzeitig zu erkennen und präventiv einzugreifen.

Performance Monitoring spielt eine zentrale Rolle bei der Gewährleistung der operativen Sicherheit. Dabei geht es nicht nur um technische Leistungskennzahlen, sondern auch um die **Qualität und Zuverlässigkeit der KI-generierten Ergebnisse**. Usage Analytics liefern wichtige Einblicke in die tatsächliche Nutzung der Systeme und helfen dabei, Anomalien oder missbräuchliche Verwendung zu identifizieren.

Die Kostenkontrolle gewinnt mit der zunehmenden Nutzung von KI-Systemen an Bedeutung. Anders als bei traditionellen IT-Systemen können hier durch **automatisierte Prozesse und Modellaufrufe schnell**

erhebliche Kosten entstehen. Ein proaktives Kostenmanagement muss daher Teil der operativen Sicherheitsstrategie sein.

Governance & Compliance

Die Governance von KI-Systemen stellt Unternehmen vor neue Herausforderungen, die weit über traditionelle IT-Governance-Frameworks hinausgehen. Mit der zunehmenden Integration von KI in geschäftskritische Prozesse wird die Etablierung klarer Strukturen und Verantwortlichkeiten zu einem entscheidenden Erfolgsfaktor.

Richtlinien & Standards

Die Entwicklung und Durchsetzung von KI-spezifischen Richtlinien erfordert ein tiefgreifendes Verständnis sowohl der technologischen Möglichkeiten als auch der damit verbundenen Risiken. Security Policies müssen dabei die besonderen Eigenschaften von KI-Systemen berücksichtigen, etwa die Fähigkeit zur autonomen Entscheidungsfindung oder die Verarbeitung sensibler Unternehmensdaten. Diese Policies definieren **nicht nur technische Rahmenbedingungen, sondern auch ethische Leitplanken** für den Einsatz von KI.

Nutzungsrichtlinien müssen klar kommunizieren, wie KI-Systeme im Unternehmenskontext eingesetzt werden dürfen. Dies umfasst sowohl die erlaubten Anwendungsfälle als auch klare Grenzen der Nutzung. Besonders wichtig ist dabei die Definition von Prozessen für die Einführung neuer KI-Anwendungen, die sowohl technische als auch rechtliche und ethische Aspekte berücksichtigen.

Die Integration in bestehende Compliance-Frameworks erfordert oft deren Erweiterung um KI-spezifische Aspekte. Dokumentationsstandards müssen dabei sicherstellen, dass **Entscheidungen und Aktionen von KI-Systemen nachvollziehbar und überprüfbar** bleiben. Dies ist besonders wichtig im Kontext regulatorischer Anforderungen wie dem EU AI Act oder branchenspezifischen Vorschriften.

Training & Awareness

Die Sensibilisierung und Schulung von Mitarbeitern gewinnt im Kontext von KI-Systemen eine neue Dimension. **Mitarbeiter-Schulungen müssen dabei über die reine Bedienung der Systeme hinausgehen und ein grundlegendes Verständnis für die Möglichkeiten und Grenzen von KI** vermitteln. Dies umfasst auch das Bewusstsein für potenzielle Risiken und die Fähigkeit, problematische Situationen zu erkennen.

Security-Guidelines für den Umgang mit KI-Systemen müssen regelmäßig aktualisiert werden, um neue Entwicklungen und Erkenntnisse zu berücksichtigen. Die Vermittlung von Best Practices spielt dabei eine zentrale Rolle. Diese sollten auf konkreten Erfahrungen im Unternehmenskontext basieren und praktische Handlungsempfehlungen für typische Situationen bieten.

Regelmäßige Updates der Schulungsinhalte sind angesichts der schnellen Entwicklung im Bereich KI unerlässlich. Diese Updates müssen sowohl technologische Fortschritte als auch neue Erkenntnisse zu Risiken und Sicherheitsmaßnahmen berücksichtigen. Die **kontinuierliche Weiterbildung der Mitarbeiter wird damit zu einem integralen Bestandteil** der KI-Governance.

Die Etablierung einer effektiven

Governance-Struktur für KI-Systeme erfordert dabei die enge Zusammenarbeit verschiedener Unternehmensbereiche. IT-Sicherheit, Compliance, Datenschutz und Fachabteilungen müssen gemeinsam an der Entwicklung und Umsetzung entsprechender Richtlinien arbeiten. Nur durch diesen integrierten Ansatz können Unternehmen sicherstellen, dass ihre KI-Systeme sowohl effektiv als auch compliant betrieben werden.

Die regelmäßige Überprüfung und Anpassung der Governance-Strukturen ist dabei von entscheidender Bedeutung. Die dynamische Entwicklung im Bereich KI erfordert eine kontinuierliche Evaluation der bestehenden Richtlinien und Prozesse. Unternehmen müssen in der Lage sein, neue regulatorische Anforderungen oder technologische Entwicklungen zeitnah in ihre Governance-Strukturen zu integrieren.

Zukunftssicherheit

Die rasante Entwicklung von KI-Technologien stellt Unternehmen vor die Herausforderung, ihre Sicherheitskonzepte zukunftsfähig zu gestalten. Eine **vorausschauende Sicherheitsstrategie** muss dabei nicht nur aktuelle Bedrohungen adressieren, sondern auch flexibel genug sein, um auf neue Entwicklungen und Herausforderungen reagieren zu können.

Adaptive Sicherheit

Die Implementation einer adaptiven Sicherheitsarchitektur bildet das Fundament für langfristige Zukunftsfähigkeit. Regelmäßige Security-Assessments müssen dabei über klassische Penetrationstests hinausgehen und spezifische Aspekte von KI-Systemen berücksichtigen. Dies **umfasst etwa die Evaluation von Prompt-Injection-Risiken, die Analyse von Modell-Schwachstellen oder die Überprüfung der Effektivität von Privacy-Filtern**.

Die Anpassung an neue Bedrohungsszenarien erfordert ein tiefes Verständnis der technologischen Entwicklung im KI-Bereich. Während klassische IT-Sicherheitsbedrohungen gut verstanden sind, entstehen durch die **zunehmende Autonomie und Komplexität von KI-Systemen ständig neue Angriffsvektoren**. Die systematische Beobachtung der Threat Landscape und die proaktive Evolution der Sicherheitsmaßnahmen werden damit zu einem kontinuierlichen Prozess.

Compliance-Evolution

Die regulatorische Landschaft im Bereich KI befindet sich in ständiger Entwicklung. Das kontinuierliche Monitoring regulatorischer Änderungen wird damit zu einer zentralen Aufgabe. Unternehmen müssen in der Lage sein, neue **Anforderungen wie den EU AI Act** oder branchenspezifische Regularien zeitnah in ihre Sicherheitskonzepte zu integrieren.

Die Anpassung an neue Standards erfordert dabei oft grundlegende Änderungen in der Art, wie KI-Systeme betrieben und überwacht werden. Die Implementation proaktiver Compliance-Maßnahmen hilft Unternehmen dabei, auch auf kurzfristige regulatorische Änderungen vorbereitet zu sein. Dies umfasst etwa die Entwicklung flexibler Monitoring-Systeme oder die Implementation erweiterbarer Dokumentationsstrukturen.

Die Nachweisführung gewinnt mit zunehmender Regulierung an Bedeutung. Unternehmen müssen in der Lage sein, die Compliance ihrer KI-Systeme jederzeit nachzuweisen. Dies erfordert eine lückenlose Dokumentation nicht nur der Systeme selbst, sondern auch aller Anpassungen und

Sicherheitsmaßnahmen. Die Implementation entsprechender Prozesse und Tools muss dabei von Anfang an die Möglichkeit zukünftiger Anforderungserweiterungen berücksichtigen.

Die Zukunftssicherheit von KI-Systemen erfordert damit einen ganzheitlichen Ansatz, der technische, organisatorische und regulatorische Aspekte vereint. Unternehmen müssen ihre **Sicherheitsarchitektur als evolutionäres System verstehen, das sich kontinuierlich weiterentwickelt.** Die Fähigkeit zur schnellen Adaptation wird dabei zum entscheidenden Erfolgsfaktor – sowohl im Hinblick auf neue Bedrohungen als auch auf sich ändernde Compliance-Anforderungen.

05

Fazit und Ausblick

Künstliche Intelligenz ist kein Projekt, sondern erfordert ein langfristiges Umdenken in allen Unternehmensbereichen

Die Transformation als fortlaufender Prozess

Die Integration von Künstlicher Intelligenz in Unternehmen ist kein einmaliges Projekt, sondern ein kontinuierlicher Transformationsprozess. Die vorangegangenen Kapitel haben gezeigt, dass es nicht ausreicht, lediglich in einzelne Technologien zu investieren. Vielmehr erfordert eine erfolgreiche KI-Strategie einen ganzheitlichen Ansatz, der technische, organisatorische, rechtliche und kulturelle Aspekte gleichermaßen berücksichtigt. Die Implementierung einer flexiblen, modularen Architektur bildet hierbei das technologische Fundament, welches es Unternehmen ermöglicht, neue KI-Fähigkeiten schrittweise zu integrieren und sich an die dynamische Entwicklung des Marktes anzupassen. Die Etablierung einer Kultur, die kontinuierliches Lernen und offene Kommunikation fördert, ist indes genauso wichtig, um die Akzeptanz der Mitarbeitenden für die technologische Transformation zu gewinnen und diese zu einem aktiven Teil des Transformationsprozesses zu machen.

Die Bedeutung strategischer Entscheidungen

Die strategischen Entscheidungen, die Unternehmen heute im Hinblick auf KI treffen, werden deren Wettbewerbsfähigkeit in den kommenden Jahren maßgeblich bestimmen. Die Wahl der Technologiepartner, die Ausgestaltung der KI-Infrastruktur, die Definition klarer Governance-Strukturen und die kontinuierliche Weiterbildung der Mitarbeitenden sind dabei nur einige von vielen Einflussfaktoren. Unternehmen, die KI lediglich als isoliertes IT-Projekt betrachten, laufen Gefahr, ihr Potenzial zu verschenken. Die wahre Wertschöpfung entsteht erst durch die nahtlose Integration von KI in die bestehenden Geschäftsprozesse und durch die gezielte Nutzung ihrer Potenziale zur Optimierung von Abläufen, zur Verbesserung der Kundenerlebnisse und zur Erschließung neuer Geschäftsmodelle.

Die zentrale Rolle des Menschen

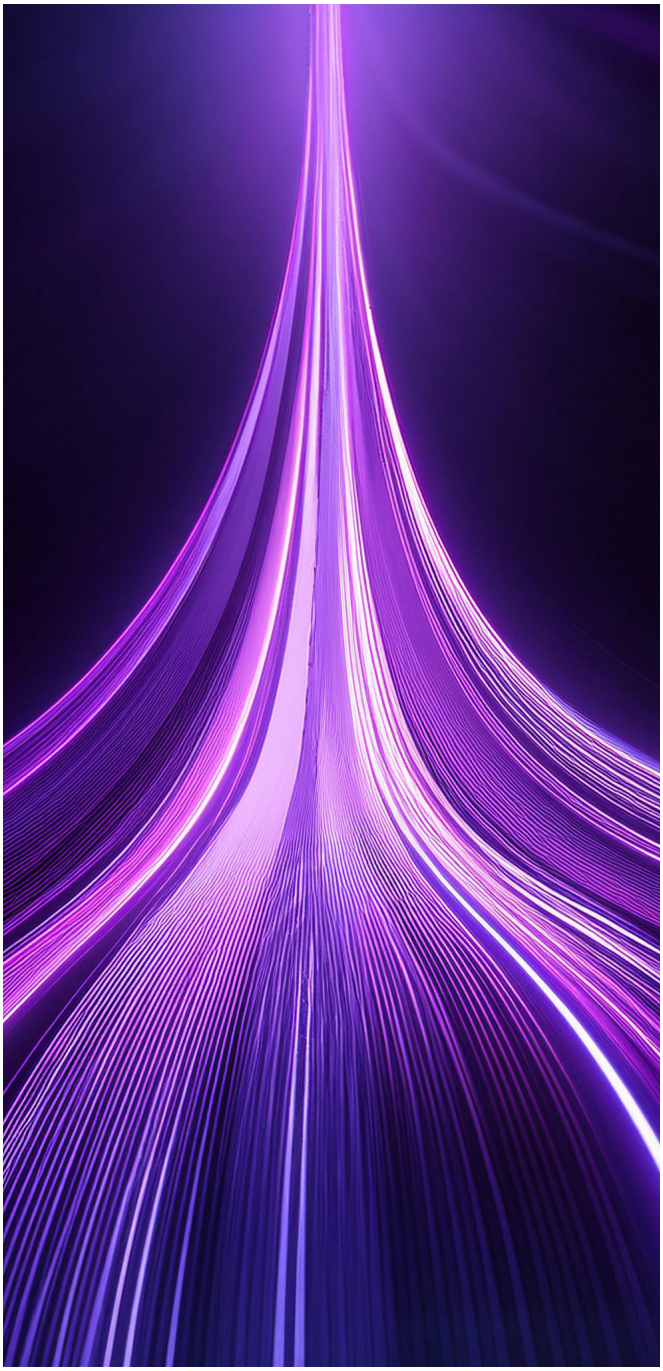
Die Technologie mag zwar im Zentrum der KI-Revolution stehen, doch letztendlich ist es der Mensch, der die Erfolgsgeschichte schreibt. KI ist kein Ersatz für menschliche Intelligenz, sondern ein Werkzeug, das menschliche Fähigkeiten erweitern und ergänzen kann. Umso wichtiger ist es, die Mitarbeitenden in den Transformationsprozess einzubinden, sie zu befähigen, KI-Systeme effektiv zu nutzen und sie von der Sinnhaftigkeit des Wandels zu überzeugen. Unternehmen, die in die Entwicklung ihrer Mitarbeiter investieren, schaffen die Basis für eine innovationsfreundliche Kultur, die die Potenziale der KI voll ausschöpfen kann. Denn trotz aller technischen Fortschritte bleibt die Fähigkeit zur kritischen Reflexion, zur kreativen Problemlösung und zum empathischen Handeln eine unverzichtbare Stärke des Menschen.

Technologische Fundamente für die Zukunft

Die technische Umsetzung einer KI-Strategie erfordert einen modularen und zukunftssicheren Ansatz. Hybride Architekturen, der Einsatz von Open-Source-Modellen und standardisierte Schnittstellen ermöglichen es Unternehmen, flexibel auf neue technologische Entwicklungen zu reagieren und eine zu starke Abhängigkeit von einzelnen Anbietern zu vermeiden. Ein besonderes Augenmerk sollte dabei auf der Implementierung robuster Sicherheitsmechanismen liegen, die sowohl klassische IT-Sicherheitsbedrohungen als auch KI-spezifische Risiken adressieren. Ein durchdachtes Security-Framework bildet somit die Basis für eine nachhaltige und verantwortungsvolle Nutzung von KI.

Ausblick in die Zukunft

Die Entwicklung von KI-Technologien wird sich auch in den kommenden Jahren mit hoher Geschwindigkeit fortsetzen. Neue Modelle, neue Anwendungen und neue Use Cases werden die Art, wie wir arbeiten und leben, grundlegend verändern. Unternehmen müssen daher agil bleiben, flexibel auf neue Trends reagieren und die Bereitschaft haben, ihre eigenen Prozesse und Strukturen immer wieder neu zu denken. Die Fähigkeit, sich schnell an neue Herausforderungen anzupassen, wird dabei zu einem entscheidenden Wettbewerbsvorteil. Dieser kontinuierliche Transformationsprozess erfordert die Etablierung von Strukturen, die sowohl Innovation als auch Sicherheit und Compliance gewährleisten. Unternehmen, die diese Herausforderungen meistern, werden die Chancen der KI-Revolution nutzen und sich eine führende Position in einer zunehmend digitalisierten Welt sichern. Der Weg ist dabei noch lang und nicht immer einfach, doch die Richtung ist klar: Die Zukunft gehört der intelligenten Zusammenarbeit zwischen Mensch und Maschine.



kiucon

Omnifact

Omnifact
ACADEMY

GW