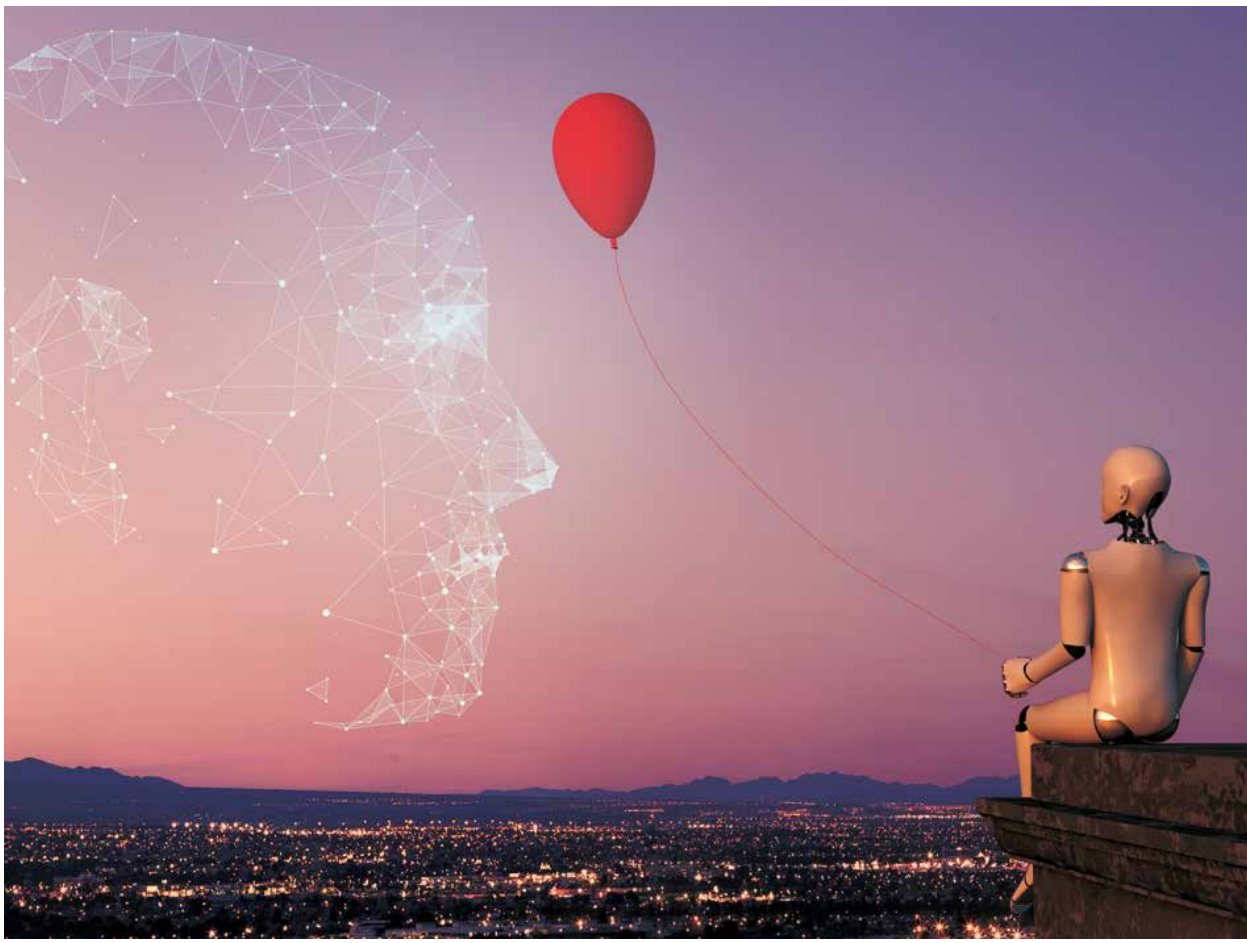
Künstliche Intelligenz (KI), oder auch Artificial Intelligence (AI), hat das Potenzial, Geschäftsmodelle grundlegend zu verändern und kommt damit einer industriellen Revolution gleich. Da sich AI mit hoher Innovationsgeschwindigkeit entwickelt, ist es entscheidend, dass sich Unternehmen schon jetzt mit dem effektiven Einsatz von „Trusted AI" auseinandersetzen, damit sie das Potenzial von AI bald schon voll ausschöpfen können.

Künstliche Intelligenz als Innovationsbeschleuniger im Unternehmen

Zuversicht und Vertrauen in Künstliche Intelligenz



pwc

www.pwc.de

Einführung
Das volle Potenzial ausschöpfen

Künstliche Intelligenz benötigt neben neuen Betriebsmodellen auch eine robuste Steuerung, um ihr volles Potenzial entfalten zu können.

Künstliche Intelligenz erweist sich als die vorherrschende Technologie der kommenden Zeit, die einen Paradigmenwechsel einleiten wird. Durch die engere Zusammenarbeit von Mensch und Maschine sowie die zunehmende Praxistauglichkeit dieser Technologie bietet AI transformatorische Möglichkeiten für Kunden, Unternehmen und Gesellschaft.

Mehr als 60 % der insgesamt 2.500 von PwC befragten Verbraucher und Entscheidungsträger glauben, dass AI Antworten auf viele der drängendsten Probleme der modernen Gesellschaft liefern kann – von der Gewinnung sauberer Energie bis hin zur Heilung schwerer Krankheiten wie Krebs.

Dabei stellt die Möglichkeit, Daten in geistiges Eigentum zu transformieren, für Unternehmen das entscheidende Kriterium dar: Mehr als 70 % der Entscheider waren der Meinung, dass AI der ausschlaggebende Geschäftsvorteil der Zukunft sein wird.

Abb. 1 Beispiele für Anwendungsfälle von AI aus unterschiedlichen Branchen

Ranking des Einflusses von AI auf Basis ihres Potenzials, Zeit zu schaffen, Qualität zu steigern und Personalisierung zu verbessern.

Rang	Branche	Anwendungsfälle mit hohem Potenzial
1	Gesundheit	• Unterstützung von Diagnosen • Früherkennung potenzieller Pandemien • verbildlichung von Diagnosen
2	Automobil	• autonome Flotten für Fahrgemeinschaften • semi-autonome Funktionen wie Fahrerassistenzsyteme • Motorüberwachung und vorausschauende, autonome Wartung
3	Finanzdienst-leistung	• personalisierte Finanzplanung • Betrugserkennung und Geldwäscheprävention • Automatisierung im Kundengeschäft
4	Transport und Logistik	• autonome LKW-Transporte und Lieferungen • Verkehrskontrolle und Staureduzierung • erhöhte Sicherheit
5	Technologie, Medien, und Tele-kommunikation	• Medienarchivierung, -suche, und -empfehlungen • Erstellung benutzerdefinierten Inhalts • Personalisierung in Marketing und Werbung
6	Einzelhandel und Kunden	• Personalisierung in Design und Produktion • Produktnachfrage prognostizieren • Inventar- und Liefermanagement
7	Energie	• intelligente Messsysteme (Smart Metering) • effizienterer Netzbetrieb und Speicherung • vorausschauende Wartung der Infrastruktur
8	Produktion	• verbesserte Überwachung und automatische Korrektur von Prozessen • Supply-Chain- und Produktionsoptimierung • On-demand-Produktion

Ungewissheit verhindert Innovationen

Die Schlüsselfrage lautet, wie sich das Potenzial von AI ausschöpfen lässt. Netflix lässt sich als Lehrbuchbeispiel dafür heranziehen, wie ein Unternehmen seine unterschiedlichen vorhandenen Daten nutzen kann, um einen produktiven Kreislauf des maschinellen Lernens zu erzeugen. Die hier erzielten Resultate haben die Art und Weise verändert, wie wir auf Medieninhalte zugreifen, und zu einem vollständigen Überdenken der Geschäftsmodelle im Unterhaltungssektor geführt. Bezogen auf die allgemeine Weltwirtschaft verläuft die Verbreitung von AI jedoch uneinheitlich. Viele Unternehmen stehen noch am Anfang ihrer Entwicklung – so untersuchen derzeit weniger als 40 % der für den *Global CEO Survey 2017* von PwC befragten Führungskräfte die Auswirkungen von AI auf künftige Qualifikationsanforderungen.

Andere Unternehmen laufen Gefahr, sich strategisch selbst zu hemmen. Dies liegt zum Teil in der Schwierigkeit begründet, aus einer schwer zu überblickenden Vielfalt von Technologien, Innovationen und Anbietern das Passende auszuwählen. Vielen fällt es zudem schwer, die Technologie- und Reputationsrisiken, die mit der Nutzung dieser weitestgehend unerprobten Technologien verbunden sind, zu bewerten und angemessen zu steuern. Zu den wichtigsten Herausforderungen gehören dabei die Prüfung, ob verwendete Daten valide sind, und die Frage, welche Sicherheitsvorkehrungen erforderlich sind, um zu gewährleisten, dass die Maschinen ihre Befehle bestimmungsgemäß ausführen. Die damit einhergehenden ethischen Aspekte reichen von der Überlegung, ob es akzeptabel ist, menschliche Entscheidungen zu beeinflussen, bis hin zur Frage, ob die Verbraucher in ausreichendem Maße über die Nutzung ihrer Daten informiert sind. Während einige Unternehmen AI vorantreiben wollen, finden sich viele andere in einer Situation, in der sie zu viele Möglichkeiten auf einmal verfolgen oder den gesamten Business Case und die damit verbundenen Risiken falsch einschätzen.

Robuste Auswertung und Ausführung

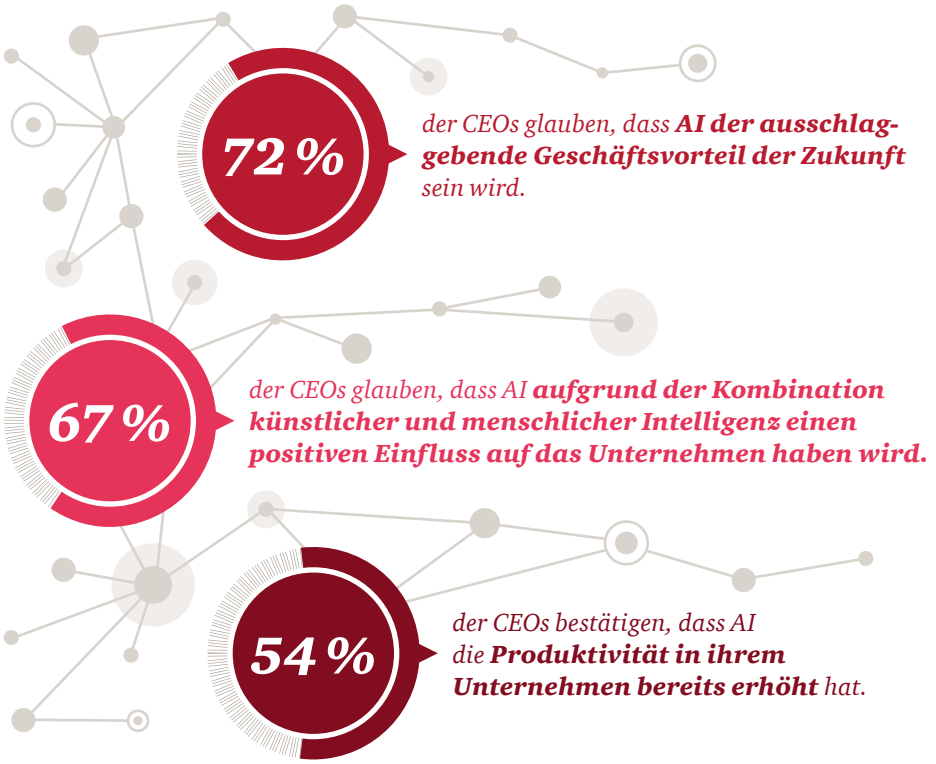
Die oben erwähnten Herausforderungen zeigen, wie notwendig ein neues Modell der strategischen Evaluierung, Steuerung und Umsetzung von AI in Unternehmen ist. Ohne ein solches werden die Unsicherheiten in Bezug auf diese Technologie dafür sorgen, dass AI entweder in vielen Unternehmen in der Testphase stecken bleibt, oder dass die Unternehmen inakzeptablen und potenziell schädlichen Risiken ausgesetzt werden.

Der Fokus muss sich deshalb auf die Bedeutung von Vertrauen und Transparenz bei der Schaffung von Trusted AI richten. Denn die Einführung von AI wird möglicherweise von vielen Interessensgruppen, innerhalb der Unternehmen wie auch bei Kunden, Aufsichtsbehörden und anderen Externen, mit Skepsis betrachtet. Es gilt daher zu planen, wie das Vertrauen aller Beteiligten in AI gestärkt werden kann. Im Wesentlichen müssen die Transparenz und das Bewusstsein dafür erhöht werden, welche Möglichkeiten AI bietet, wie AI genutzt wird, welche Leistungen sie erbringt und welche Entscheidungen durch sie getroffen oder unterstützt werden. Dies ist unserer Auffassung nach die Essenz von Trusted AI.

Obwohl aktuell noch niemand ein bestimmungsgemäßes Verhalten von komplexen, autonom agierenden Technologien garantieren kann, gibt es eine Reihe von Best Practices, einschließlich der Entwicklung und Überwachung von Kontrollen, die eine verantwortungsvolle Einführung von AI fördern und das damit verbundene Risiko minimieren.

Im vorliegenden Whitepaper untersuchen wir daher die Herausforderungen, die bei der AI-Transformation in den Unternehmen bewältigt werden müssen, und die Chancen, die sich durch AI eröffnen. Darüber hinaus werden wir Ihnen aufzeigen, wie AI effektiv umgesetzt und betrieben werden kann. Schließlich geht es darum, Innovationen zu fördern und zu beschleunigen und den Unternehmen die erforderliche Sicherheit zu geben und sie zu befähigen, die nötigen Voraussetzungen zu schaffen, um ihre AI-Vorhaben zum Erfolg zu führen.

Abb. 2 Die CEO Perspektive auf den Einfluss von AI im Hinblick auf die Business Strategie



Den Paradigmenwechsel nutzen
Wie AI die Spielregeln verändert

Die Einführung von AI hat tief greifende Auswirkungen für alle, die sich mit Unternehmensführung beschäftigen.

Das Aufkommen von AI ebnet den Weg für zahlreiche neue Betriebs- und Geschäftsmodelle. Die Fähigkeit, Datenmengen zu analysieren, die über das menschliche Verständnis hinausgehen und Auswirkungen auf jede neue Informationsmenge haben, ermöglicht es den Unternehmen, Erfahrungen zu personalisieren, Produkte und Services an individuelle Bedürfnisse anzupassen und Wachstumschancen zu identifizieren. All das geschieht mit einer zuvor unbekannten Geschwindigkeit und Präzision.

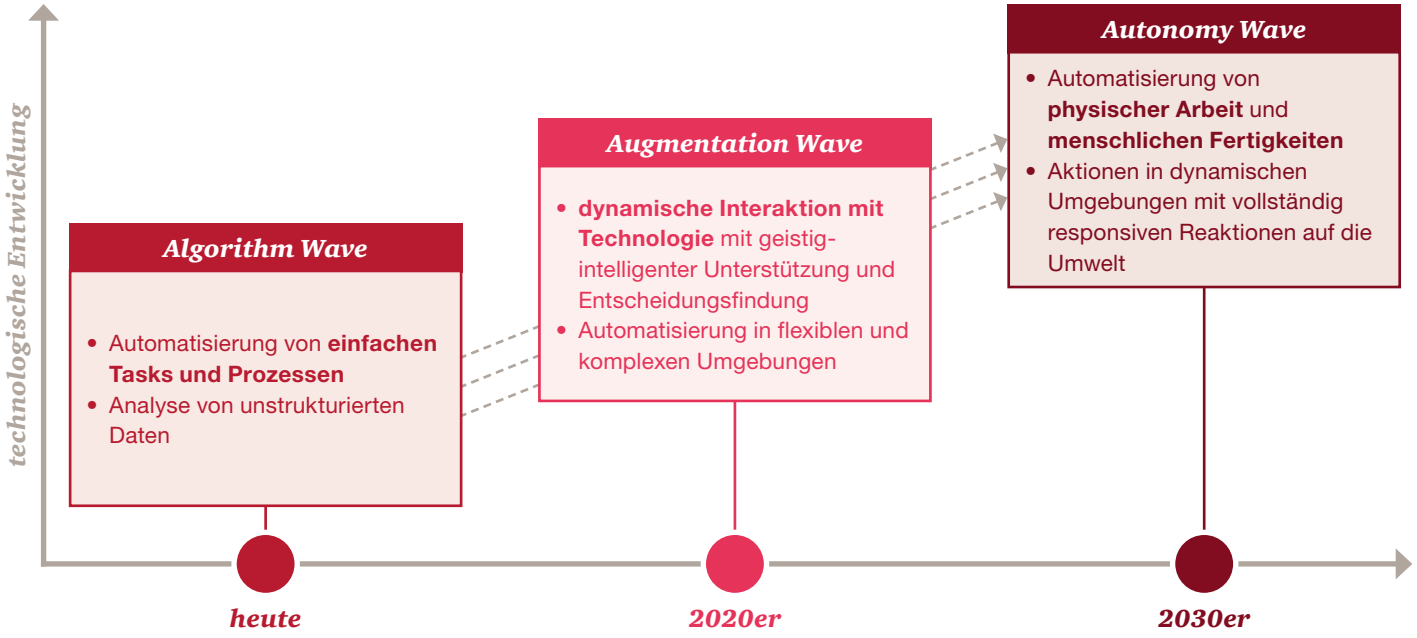
Was ist künstliche Intelligenz?

In ihrem Buch *Artificial Intelligence: A Modern Approach* definieren Stuart Russell und Peter Norvig AI als „das Entwerfen und Erstellen intelligenter Algorithmen, die Information aus der Umwelt empfangen und Maßnahmen ergreifen, die diese Umgebung beeinflussen“[1]. Der entscheidende Unterschied zwischen AI und klassischer Software zeigt sich dabei in der Fähigkeit, Maßnahmen zu ergreifen. AI ermöglicht es Maschinen, auf Signale selbsttätig zu reagieren – Signale, welche die Programmierer nicht direkt steuern und nicht vorhersehen können. Der am schnellsten wachsende Bereich von AI ist das maschinelle Lernen. Dieses beschreibt die Fähigkeit von Software, auf der Basis ihrer bisherigen Interaktion mit der Welt ihre Aktivität zu verbessern.

Das Spektrum von AI kann in drei Bereiche unterteilt werden:

- **unterstützte Intelligenz (assisted intelligence)**: heute weit verbreitet; verbessert das, was Menschen und Organisationen bereits tun
- **erweiterte Intelligenz (augmented intelligence)**: diese entsteht gerade; ermöglicht es Menschen, Dinge zu tun, die sie sonst nicht tun könnten
- **autonome Intelligenz (autonomous intelligence)**: wird für die Zukunft entwickelt; schafft Maschinen, die eigenständig agieren

Abb. 3 Die drei Wellen der aktuellen und kommenden technologischen Entwicklungen von AI



[1] Russell, S. J., Norvig, P., Canny, J. F., Malik, J. M., & Edwards, D. D. (2003). Artificial intelligence: a modern approach (Vol. 2, No. 9). Upper Saddle River: Prentice hall.

Beispiele
Wie AI sich heute schon bemerkbar macht

- **Auf dem Laufenden bleiben:** „persönliche Assistenten“ wie Alexa und Siri sowie Chatbots von beispielsweise Banking- und Mobilfunknetzbetreibern.
- **Verhalten vorhersagen:** Die Stadt Mannheim nutzt maschinelles Lernen, um verdächtiges Verhalten und gefährliche Situationen im Rahmen der Videoüberwachung frühzeitig zu erkennen und daraus Aktionen abzuleiten.
- **Medizin:** AI wird zur medizinischen Diagnostik eingesetzt. Untersuchungen von PwC zeigen, dass ein erheblicher Teil der Menschen weltweit bereit ist, bestimmte Behandlungen, Tests oder Dienstleistungen in Anspruch zu nehmen, die von einer künstlichen Intelligenz oder einem Roboter durchgeführt werden.
- **Kundenbindung:** Telekommunikations- und Medienunternehmen nutzen maschinelles Lernen für Kundenanalysen, um Kundenfluktuation vorherzusagen und Maßnahmen zur Vermeidung derselben zu empfehlen.
- **Antizipation von Nachfrage:** Einzelhändler beginnen Deep Learning zu nutzen, um Kundenaufträge eine Woche im Voraus vorherzusagen.
- **Individuelle Angebote für alle:** Die Beratung durch Roboter hat es ermöglicht, einem breiteren Kundenkreis im Finanzsektor maßgeschneiderte Investitionsoptionen anzubieten. Bis vor Kurzem wurde eine derart eingehende Anlageberatung nur Kunden mit hohem Nettovermögen angeboten.
- **Verbesserung der Qualität:** Hersteller verwenden AI, um ihre Qualitätskontrolle zu verbessern, Produktionsausfälle zu reduzieren und die Geschwindigkeit sowie den Ertrag industrieller Prozesse zu erhöhen.
- **Intelligente Prozesse:** Intelligente Prozessautomatisierung ermöglicht enorme Einsparungen in den Bereichen Finanzen, Personal und Compliance. Zur Durchführung von Routineaufgaben mit hohem Volumen wird die Automatisierung durch Roboter mit AI kombiniert.

Sich in der schieren Fülle von Algorithmen und Anwendungen zurechtzufinden, die unter den Begriff „AI“ fallen, ist zu einer gewaltigen Aufgabe geworden. Bislang lag der Schwerpunkt auf der Automatisierung bereits ausgeführter Aufgaben. Während die Beschäftigten von Routineaufgaben befreit werden und Mensch und Maschine immer enger zusammenarbeiten, beruhen die wirklichen Durchbrüche in der Entstehung völlig neuer Geschäftsmodelle auf der Basis erweiterter Intelligenz, sowie der Tatsache, dass künstliche Intelligenzen auf der Grundlage analysierter Daten begründete Entscheidungen treffen können. Die Unterhaltungsbranche ist ein prägnantes Beispiel für einen Sektor, der bereits erhebliche disruptive Veränderungen durchlaufen hat. Und das autonome Fahren ist eines von vielen Beispielen dafür, wie AI den Alltag und die Unternehmen, die damit zu tun haben, verändern wird.

Kommerziell genutzte AI hat sich in den letzten Jahren verbreitet, angetrieben von einer Kombination aus Rechenleistung, der Verfügbarkeit riesiger Datensätze sowie Fortschritten im Bereich des maschinellen Lernens, einschließlich Deep Learning. Obwohl das Maschinenlernen oft für vorhersagende Analysen sowie die Bild- und Sprachklassifizierung verwendet wird, kann es mit Elementen wie natürlicher Sprachverarbeitung, strategischer Planung und logischem Denken kombiniert werden, um leistungsstarke autonome Algorithmen bereitzustellen.

Wie verbreitet ist AI also? Ein großer Teil der Innovationen steckt noch in den Kinderschuhen und ist in Form von Proofs of Concept auf die Nutzung als Forschungs- und Entwicklungsgegenstand beschränkt. Der Fokus der Wirtschaft muss sich nun darauf richten, ein Umfeld zu schaffen, dass den erfolgreichen Transfer der Forschungsergebnisse in reale Wertschöpfung ermöglicht.

Ein neuer Ansatz

Wie die nachfolgende Tabelle zeigt, erfordert die Einführung von AI eine neue Denkweise im Hinblick auf die Bereiche Technologie, Geschäftsentwicklung und strategische Umsetzung, zusammen mit der Neugestaltung des Betriebsmodells und der Entscheidungsprozesse, die diese Bereiche untermauern. Die Veränderung betrifft nicht nur die Technologie- und Innovationsteams, sondern das ganze Unternehmen.

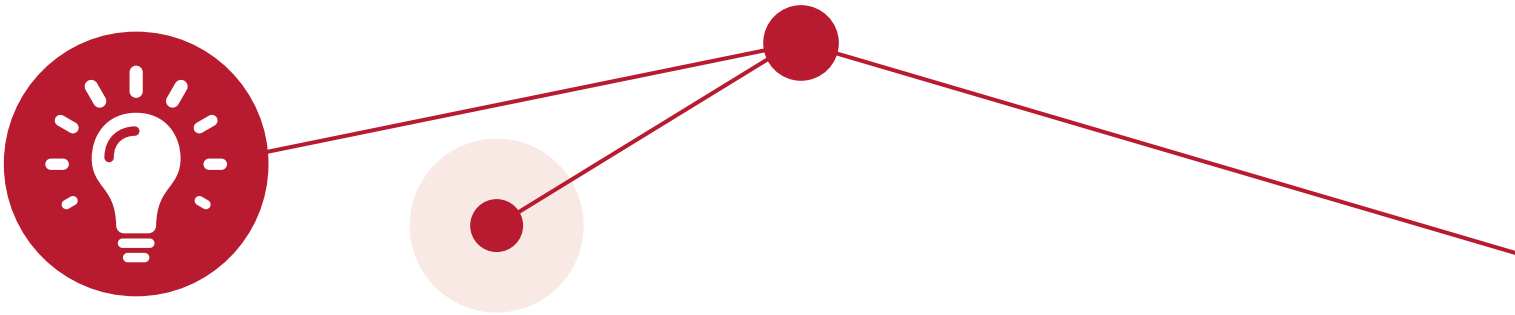
Abb. 4 Disruptiver Einfluss von AI auf die Steuerung des Unternehmens

	traditioneller Ansatz	*neuer Ansatz*
Strategie	Technologie für das Informationsmanagement	Technologie, die das Geschäft steuert
	Daten als Business Intelligence	Daten als differenzierendes geistiges Eigentum
	deterministischer Ansatz	direktionaler und adaptiver Ansatz
Design	User Experience als ein Application Layer	Benutzererfahrung als primäres Anwendungsmerkmal
	Entscheidungsfindung fest im Source Code verankert	Entscheidungsprozesse werden von Software selbstständig gelernt
	Informationsgewinnung ohne Abfragen aus einer Datenbank	gewonnene Informationen werden von Software eingeschätzt und auf Basis von Wahrscheinlichkeiten als richtige Antwort validiert
Entwicklung	lineare Technologieentwicklung	iterative Technologie- und Geschäftsmodellentwicklung
	Managementteams spezifizieren, Technologieteams setzen um	Geschäftsfachexperten in Technologieteams integriert
Betriebsmodell	feste Technologie mit punktuellen Upgrades	dynamische, adaptive Modelle; kontinuierliche testgetriebene Weiterentwicklung
	technische Risiken, beherrscht von Systemausfallzeiten und Fehlern	technische Risiken umfassen erlerntes und unerwartetes Verhalten
	klassische Cyberangriffe	kontradiktorische Angriffe

Die wichtigsten Faktoren für die AI Transformation

Digitale Wertschöpfung im Zentrum des Geschäfts- und Betriebsmodells

Der ausschlaggebende Faktor für den langfristigen Unternehmenserfolg ist die Ausschöpfung des vollen Potentials der digitalen Wertschöpfungskette. Die Wahl eines geeigneten Geschäfts- und Betriebsmodells ist entscheidend, um den erfolgreichen Weg in die Zukunft zu ebenen. Dabei wird der Einsatz von AI zu einer weitreichenden Transformation führen, die nicht nur Auswirkungen auf einzelne Unternehmen, sondern den gesamten Markt haben wird.



Strategie

1. An strategischen Zielen ausrichten

Es kommt darauf an, die AI-Innovation mit den strategischen Kernzielen und Leistungsindikatoren in Einklang zu bringen, statt eine Reihe vereinzelter Initiativen isoliert zu unterstützen. Unserer Erfahrung nach haben viele Organisationen ganz unterschiedliche Pilotprojekte gestartet. Viele versäumen es, grundsätzlich zu überlegen, wie AI ihr spezifisches Geschäft prägen kann, um zu ermitteln, welche Risiken und Chancen sich daraus ergeben.

2. Erwarten Sie keine Zauberei

AI mag zwar vieles können, sie ist und bleibt jedoch eine Technologie bzw. ein Algorithmus. Ein häufiges Problem ist der Glaube, AI werde ohne menschliches Eingreifen quasi wie von Zauberhand lernen. In Wirklichkeit müssen Sie viel Arbeit in die Beschaffung und Bereinigung von Lern- und Trainingsdaten sowie in die Schulung von Maschinen und Mitarbeitern investieren.

3. Seien Sie sich über Ihre Partner im Klaren

Wo auch immer Sie sich umsehen – es gibt Start-ups wie auch große Anbieter, die Lösungen für eine Vielzahl von Anwendungsfeldern bieten. Eine Partnerschaft mit diesen beschleunigt die Innovation, Agilität und Geschwindigkeit des Eintritts in die AI-Transformation. Dennoch ist es überaus wichtig, den konkreten eigenen Standpunkt festzulegen. Dazu gehört, dass Sie sich über die strategischen und operativen Prioritäten im Klaren sind, die Sie durch die Wahl Ihres Partners umsetzen möchten. Auch sollten Sie bedenken, dass zwar viele Anbieter ihre Lösungen verkaufen können, dieser aber nicht zwangsläufig das halten, was sie versprechen. Deren Art der Bewertung von Entwicklungsrisiken unterscheidet sich sicherlich stark von dem, was Sie selbst diesbezüglich gewohnt sind. In einer risikoreichen, schnelllebigen Anbieterlandschaft gilt die erste Überlegung der finanziellen Belastbarkeit Ihres potenziellen Partners: Wird dieses Unternehmen noch existieren, wenn Sie es brauchen? Zudem sollten Sie ermitteln, wie Sie die erforderlichen Daten beschaffen, das erforderliche Wissen für die Bereitstellung Ihrer neuen Funktionen entwickeln und wie Sie neue Plattformen in Ihre vorhandene Infrastruktur integrieren können.

4. Vertrauen in AI verankern

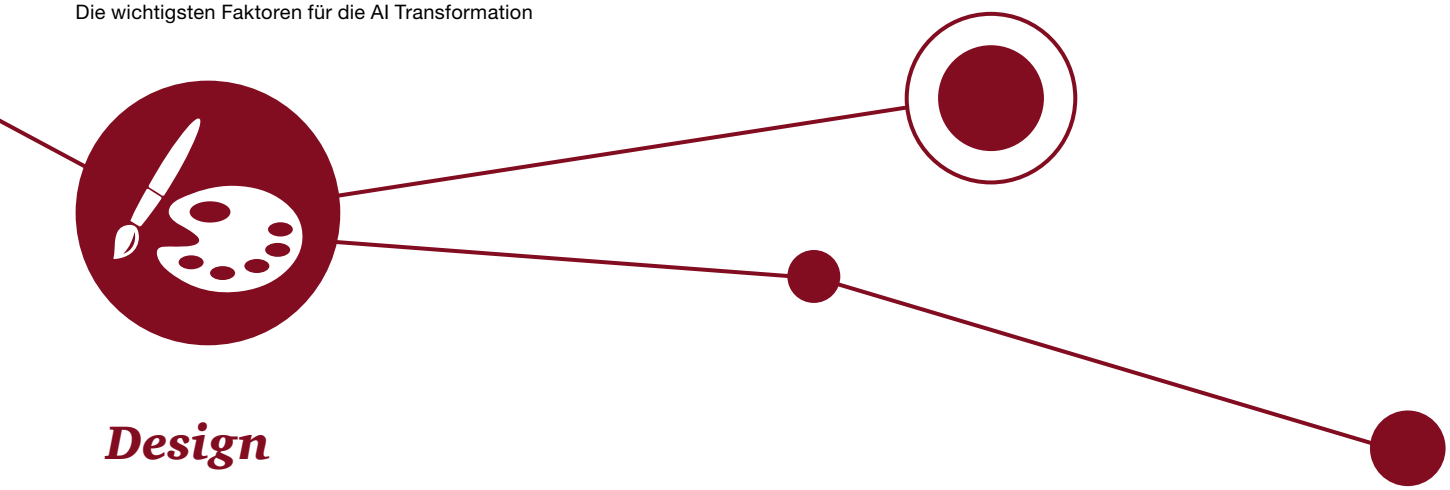
Bevor Sie AI einführen, müssen Sie unbedingt in Erfahrung bringen, was sie genau tut und wie sie es tut. Das beinhaltet, sicherzustellen, dass die Software ihren Entscheidungsprozess auf eine Weise transparent macht, die verstanden und überprüft werden kann. Insbesondere in Zusammenhang mit dem maschinellen Lernen ist es wichtig, darüber nachzudenken, wie sichergestellt werden kann, dass die Software die erwarteten Ergebnisse transparent liefert. Die Stakeholder in Unternehmen sowie die Investoren und Kunden verlangen diese Sicherheit. Die Aufsichtsbehörden erwarten sie ebenfalls. Algorithmische Transparenz ist ein Teil der Lösung, auch wenn diese möglicherweise einen Kompromiss zwischen Entscheidungstransparenz, Systemleistung und funktionalen Fähigkeiten erfordert.

5. Die Einhaltung gesetzlicher Vorschriften nachweisen

Die Aufsichtsbehörden müssen schnell sein, um mit den neuen Technologien Schritt halten zu können. Möglicherweise wird es regulatorische Einschränkungen geben, die eine Einführung von AI in stark regulierten Branchen wie dem Gesundheits- oder Finanzsektor beeinflussen. Entwicklungen wie die EU-Datenschutz-Grundverordnung verschärfen die Herausforderungen zusätzlich. Um eine Vertrauenswürdigkeit Ihrer AI zu gewährleisten, ist es wichtig, dass Sie die relevanten gesetzlichen Anforderungen erfüllen.

6. Unternehmensstruktur

Die Veränderungen innerhalb Ihrer Geschäftsmodelle als Teil Ihrer AI-Gesamtstrategie müssen sich auch in Ihrer Unternehmensstruktur widerspiegeln. Ihr Unternehmen benötigt eine dedizierte AI-Governance-Struktur, die zum Beispiel ein nominiertes Mitglied auf C-Level und einen zentralen Knotenpunkt für technisches Fachwissen umfassen kann. Um Ihr Unternehmen auf die Einführung von AI vorzubereiten, ist die Einbindung von Data Science in Ihr Unternehmen in Verbindung mit einem breiten Domänenwissen über die Geschäftsmodelle und Prozesse unerlässlich.



Design

1. Öffnen der Blackbox

AI-Anwendungen können mit Kunden kommunizieren und wichtige Geschäftsentscheidungen treffen. Vieles davon passiert jedoch quasi in einer Blackbox. Diese mangelnde Transparenz birgt unter anderem Reputations-, Finanz- und operative Risiken. Daher ist sicherzustellen, dass die Software so transparent und überprüfbar wie möglich gestaltet ist.

Die ordnungsgemäße Steuerung und der hinreichende Schutz umfassen auch die Möglichkeit, AI-Systeme zu überwachen. Dies bedeutet auch, dass fehlerhafte Komponenten schnell erkannt und korrigiert oder, falls das nicht möglich ist, das System heruntergefahren werden kann, ohne die gesamte Plattform vom Netz nehmen zu müssen. Zugehörige Prioritäten umfassen die Identifizierung von Abhängigkeiten und die Möglichkeit, Änderungen mit nur minimalen Auswirkungen auf den Geschäftsbetrieb vorzunehmen, wenn sich Vorschriften oder andere Elemente der Betriebsumgebung ändern.

2. Überzeugende Nutzererfahrungen schaffen

Viele AI-Anwendungen verwenden für die Nutzererfahrungen sehr subjektive Metriken, welche mit Intelligenz, Persönlichkeit und Vorhersagbarkeit vergleichbar sind. Auch wenn sich ein Großteil der Entwicklung auf die Analytik konzentrieren mag, hängt der Erfolg des Produkts von den emotionalen Reaktionen der Nutzer ebenso ab wie von der Erschließung neuer Möglichkeiten oder Steigerung von Effizienz. Dies bedeutet, dass ein häufiger Austausch zwischen Produkteigner und Entwicklern erforderlich ist, damit eine gute Anpassung zwischen den sich herausbildenden Erwartungen und der Funktionalität des Systems sichergestellt werden kann. Oft ist es sinnvoll, spezialisierte User-Interface-Anbieter einzubinden.

Zwar kann sich AI in bestimmten Aufgaben- oder Themengebieten besonders auszeichnen und den Menschen übertreffen, im Allgemeinen ist sie aber nicht in der Lage, Fähigkeiten oder Kenntnisse auf andere, analoge Problemfelder zu übertragen. Besonders für Menschen, die zum ersten Mal mit AI interagieren, ist dies nicht offensichtlich und kann zu Frustration und Verwirrung führen. Branding und die Gestaltung der Funktionalitäten sind daher im Zuge des Systemdesigns wichtige Überlegungen. Tun Sie dies richtig, so kann bereits eine sehr rudimentäre Software menschlich erscheinen. Tun Sie es falsch, werden Sie Ihre Nutzer verlieren.

Manche der von AI durchgeführten Analysen basieren unweigerlich auf unvollständigen oder gar falschen Informationen. Es ist daher wichtig, dass Sie die Begrenzungen der AI erkennen und Ihren Kunden kommunizieren, beispielsweise bei der Präsentation der Investitionsempfehlungen eines automatisierten Anlageberaters gegenüber Ihren Kunden.

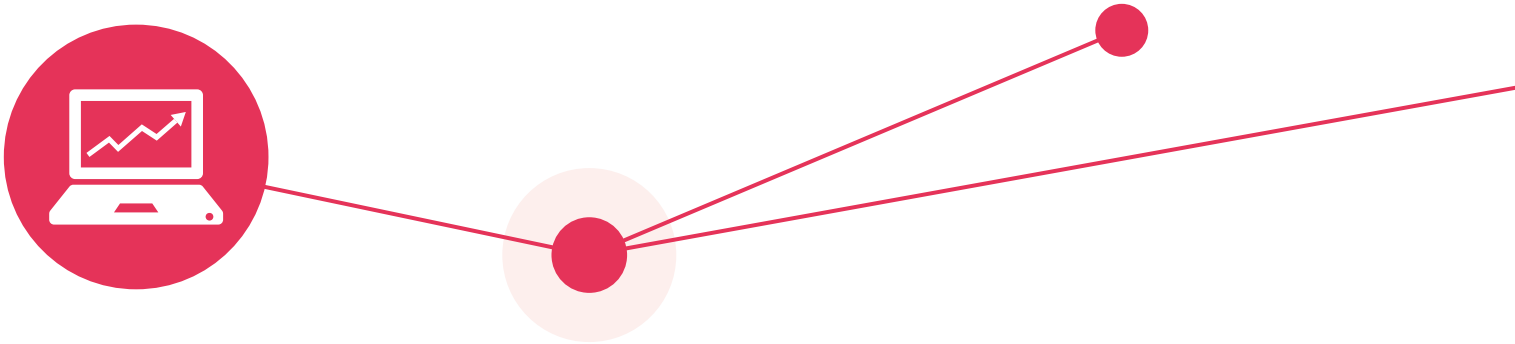
3. Einführung eines Kontrollrahmens

Die effektivsten Kontrollen werden in der Entwurfs- und Implementierungsphase erstellt und ermöglichen es Ihnen, Probleme zu erkennen, bevor sich diese bemerkbar machen, und Verbesserungspotenziale zu identifizieren.

Eine wichtige Frage ist, wer die Kontrollen entwirft und überwacht. Sowohl der Umfang der Anwendung als auch die Notwendigkeit der Überwachung von Ergebnissen erfordern das gemeinsame Engagement aller Unternehmensdisziplinen. Das Kontrolldesign verlangt erheblichen Input von den Experten aller Geschäftsbereiche. So wird für physische Anwendungen wahrscheinlich ein Input von Spezialisten aus der Sicherheitstechnik benötigt. Ein wichtiger Teil der Implementierung besteht darin, die Kontrollelemente auf mehrere Ebenen aufzuteilen (hierarchischer Ansatz).

Auf unterster Ebene kann beispielsweise eine harte Kontrollschicht eingerichtet sein, die „rote Linien“ aufzeigt und Handlungspläne für den Fall bereithält, dass diese überschritten werden. Ein Beispiel hierfür ist der maximale Transaktionswert, mit dem ein automatisierter, am Finanzmarkt tätiger Algorithmus handeln darf. Bei komplexeren Anwendungen wie bei interaktiv kommunizierenden AI-Systemen (Conversational AI) kann ein „Verhaltensregulator“ eingeführt werden, der den Kernalgorithmus abschaltet, wenn das Risiko von Fehlern wie Regelwidrigkeiten oder unangemessener Sprache zu hoch wird.

Diese Hauptkontrollen können durch Challenger-Modelle erweitert werden, die als Grundlage dafür dienen, die Eignung und Genauigkeit der AI-Techniken zu überwachen oder nach unerwünschten Befangenheiten oder Abweichungen zu suchen, während die Modelle von neuen Daten lernen. Darüber hinaus kann dieser Ansatz in die kontinuierliche Entwicklung integriert werden – mit dem Ziel, bestehende Modelle zu verbessern oder überlegene Modelle für System-Upgrades zu identifizieren.



Entwicklung

1. Programmmanagement überdenken

Werden bei derart datenabhängigen Anwendungen wie der AI traditionelle Planungs-, Design- und Entwicklungsprozesse angewendet, so sind sie von vornherein zum Scheitern verurteilt. Die traditionellen Konzepte müssen durch iterative Weiterentwicklung erneuert werden; nur so lässt sich die Komplexität der auftretenden Probleme bewältigen. Dies setzt beim Produkteigner ein hohes Maß an Engagement voraus.

2. Datenabhängigkeit kontrollieren

Die AI-Funktionalität ist aufgrund des am Modell orientierten Trainings im maschinellen Lernen stark datenabhängig und erfordert höchstwahrscheinlich einen Informationsspeicher, auch „Knowledge Base“ genannt. Dies führt häufig dazu, dass anfängliche Designspezifikationen und -erwartungen über die Grenzen dessen hinausgehen, was eine Analyse der Daten tatsächlich ermöglicht, egal wie „intelligent“ die Software ist. Eine grundlegende Voraussetzung für datenabhängige Projekte ist daher eine Erkundungsphase, in der die Datenmenge und -qualität sowie die sich hieraus ergebenden Grenzen für die resultierenden Modelle und Funktionalitäten beschrieben werden. Dies ist einer der Gründe dafür, dass AI-Implementierungen während der Entwicklungsphase einen umfassenden Designprozess durchlaufen müssen.

3. Zeit einplanen für das Trainieren und Testen

Insbesondere beim maschinellen Lernen sollte das Entwicklungsteam praxisbewährte Optimierungs- und Kreuzvalidierungsmethoden einsetzen, damit Überanpassungen und andere häufige Probleme vermieden werden können. Um ein klares Bild von Anwendungsfall und Nutzererfahrung zu gewinnen, sollten Anregungen und Beiträge auch von Stakeholdern außerhalb des eigentlichen Softwaredesignteams berücksichtigt werden, da letztere oft zu nah am Thema sind, um es noch objektiv betrachten zu können. Das Monitoring sollte Tests zur Korrektur funktionaler Schwachpunkte einschließen.

Eine Möglichkeit, Tests anzupassen und Risiken zu beschränken, besteht darin, neue AI-basierte Anwendungen zunächst im kleinen Maßstab zu testen und in einem normalen Alltagskontext Analysten und nichttechnische Benutzer eine gründliche Überprüfung vornehmen zu lassen. Experteneinschätzungen und zusätzliche kontextbezogene Informationen liefern dann eine weitere Validierung, Wirkungsabschätzung und Justierung, bevor die AI-Initiative in größerem Umfang eingeführt wird.

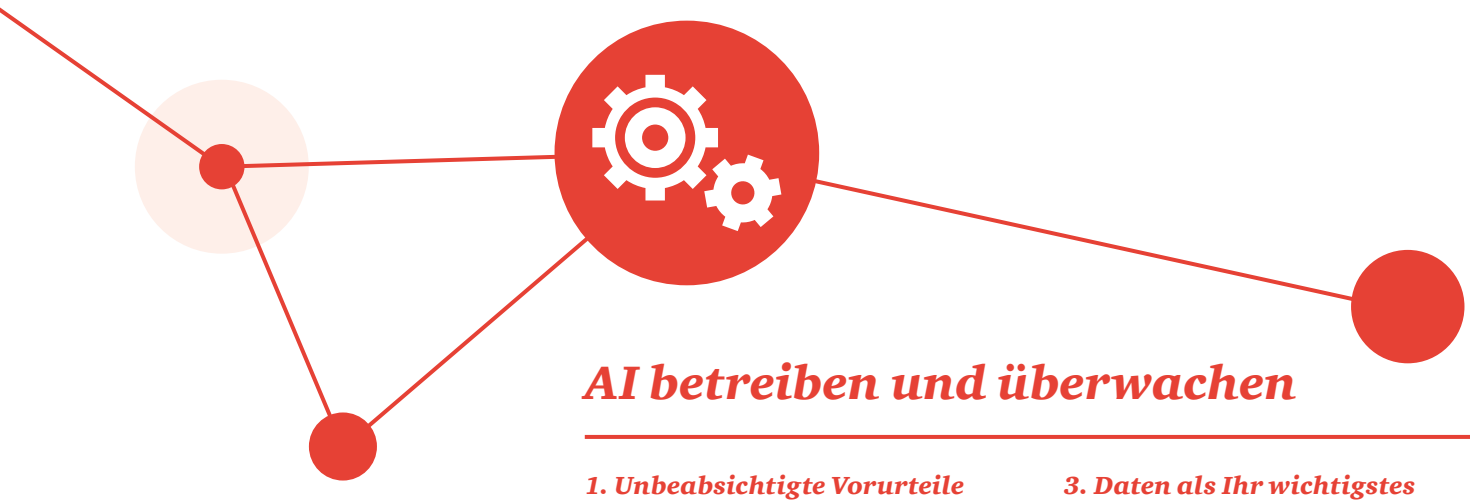
Insbesondere dann, wenn AI-Systeme direkt mit Menschen interagieren, sollte vor der Freischaltung innerhalb der Testphase eine intensive Evaluation der Nutzererfahrungen und ein stufenweiser Betatest mit nicht öffentlichen Zielgruppen stattfinden.

Letztlich kann die AI-Entwicklung mehrere Testläufe erfordern, bis man zufriedenstellende Resultate erzielt. Daher sollten Sie im Vorfeld das richtige Maß an Qualitätssicherungsmechanismen implementieren, um später rechtzeitig erkennen zu können, wann die Daten, Technologien oder Modellschulungsmethoden für den betreffenden Business Case ungenügend sind.

4. Vertrauensschwellen festlegen

Ein Gleichgewicht zwischen Automatisierung und menschlicher Validierung und Verifizierung ist maßgeblich für den Erfolg von AI. Es kann jedoch schwierig sein, die genauen Schwellenwerte und Vertrauensstufen zu definieren, ab denen menschliche Eingriffe erforderlich sind. Sind sie zu strikt, so bietet die AI nur einen begrenzten Nutzen. Sind sie zu locker, so geht man ein größeres Risiko ein als erwünscht. Eine kontinuierliche Überwachung der Leistung ist unerlässlich, um sicherzustellen, dass die Technologie innerhalb der festgelegten Parameter arbeitet.

Conversational AI agiert mit Menschen mittels subjektiver Kommunikation. Hier müssen die Vertrauensschwellen so eingerichtet sein, dass sie den sozialen Normen und Nutzererwartungen entsprechen.



AI betreiben und überwachen

1. Unbeabsichtigte Vorurteile verhindern

Da immer mehr Informationen verfügbar werden und Ihr Modell kontinuierlich reift, ist es wichtig, einer ungewollten Befangenheit gegenüber bestimmten Gruppen vorzubeugen. Um Vorurteile zu erkennen, bedarf es größtmöglicher Transparenz. Für Systeme, die aus der Interaktion mit Kunden lernen, wird eine periodische Funktionsüberwachung auf der Basis standardisierter Interaktionen empfohlen, damit unerwünschte „Trainingsdrifts“ identifiziert und verhindert werden können.

2. Vor Angriffen schützen

Modelle des maschinellen Lernens, speziell im Fall von Deep Learning, können durch böswilligen Input, der als „gegnerischer Angriff“ bezeichnet wird, negativ beeinflusst werden. Es ist möglich, durch das Identifizieren und Einspeisen von entsprechenden Datenkombinationen das Modell des maschinellen Lernens so zu manipulieren, dass das System unerwünschte Resultate produziert. Die Gefahr einer Anfälligkeit für solche Angriffe kann durch die Simulation gegnerischer Angriffe auf eigene Modelle und die Schulung dieser Modelle zur Erkennung solcher Manipulationsversuche verringert werden. Durch die Entwicklung einer spezialisierten Software bereits in der Designphase können Sie Ihre Modelle gegen Angriffe „immunisieren“.

3. Daten als Ihr wichtigstes geistiges Eigentum erkennen

Jede AI ist nur so effektiv wie die Daten, von denen sie lernt. Die Beibehaltung qualitativ hochwertiger Daten und die fortlaufende Bewertung der Wirksamkeit und Effektivität des Modells sind Schlüssel zu einer erfolgreichen AI-Plattform. Der funktionale und oft auch wirtschaftliche Vorteil der AI hängt von der Qualität und dem Umfang Ihres geistigen Eigentums ab. Die Kooperation mit einem AI-Anbieter kann unweigerlich einen Datenaustausch beinhalten, durch den Sie wertvolles geistiges Eigentum weitergeben. Es ist daher wichtig, den Wert der Daten zu verstehen, die Sie mit anderen teilen, sowie das Angebot und die Nutzung Ihrer Daten durch Dritte genau zu überwachen und zu steuern.

4. Auf systembedingte Risiken achten

Der Flash-Crash, der im Jahr 2010 die Finanzmärkte traf, zeigte, was passieren kann, wenn mehrere künstliche Intelligenzen in unbeabsichtigter Weise interagieren und dies nicht ausreichend überwacht wird. Die Sicherheitsmaßnahmen gegen Risiken sollten eine Szenario-Planung, eine Aufstellung Ihrer eigenen verwundbaren Punkte sowie Anweisungen für schnelle Reaktionen umfassen.

AI unter Kontrolle halten

Grundsätze für den effektiven Einsatz von Trusted AI

AI setzt neue Maßstäbe in der technologiegestützte Transformation. Wie kann Ihr Unternehmen sicherstellen, dass alles unter Kontrolle ist?

Welches sind die Ausgangspunkte für eine gesicherte, kontrollierte und verantwortungsvolle AI? Obwohl der Prozess im Wesentlichen offen ist, sind wir der Auffassung, dass es fünf grundlegende Anforderungen gibt, die erfüllt sein sollten, bevor Sie mit der Umsetzung Ihres Projekts beginnen.

1 Schaffen Sie Klarheit bezüglich der AI-Strategie

Auch wenn generell eine kontinuierliche Evaluierung und Anpassung nötig ist, ist es wichtig, sich vorab über die grundsätzliche Richtung im Klaren zu sein.

- Sind Sie bereit für die Veränderungen, die AI bringt?
- Sind Sie sich der gesellschaftlichen und ethischen Auswirkungen bewusst?
- Welche geschäftlichen Ergebnisse möchten Sie erzielen (z. B. Produktanpassung oder Effizienz im Backoffice)?

2 Transparenz durch Design

Die Einführung von AI wird innerhalb Ihres Unternehmens, bei Ihren Kunden und in der Gesellschaft ein emotionales Thema sein. Daher ist es wichtig zu planen, wie Sie das Vertrauen der Beteiligten in Ihre Lösung stärken können.

Es ist wichtig, den Kontrollrahmen von vornherein in Ihre Lösung zu integrieren, statt diesen erst dann zu entwerfen und anzuwenden, wenn das System entwickelt und in Betrieb ist. Der Kontrollrahmen umfasst einen Mechanismus zur Überwachung von Ergebnissen und Compliance.

3 Bauen Sie Ihre kollaborative AI-Struktur im Voraus auf

Es gibt zahlreiche Möglichkeiten, Ihr Unternehmen AI-fähig zu machen. Sie reichen vom Aufbau eines Kompetenzzentrums mit zugehörigem Vorstandsmitglied bis hin zu einer agilen Strategie zum Entwickeln und Steuern anhand ausgewählter Proofs of Concept. Unabhängig von Ihrem Ansatz ist es wichtig, die organisationsübergreifende Kommunikation, Zusammenarbeit und zentrale Koordination der AI-Initiativen sicherzustellen.

4 Bauen Sie Data Governance in die AI ein

Wenn Daten das Gold dieses Jahrhunderts sind, dann kommt es darauf an, Mechanismen zum Sourcing, Bereinigen und Kontrollieren wichtiger Dateninputs zu implementieren und sicherzustellen, dass Daten- und AI-Management integriert sind.

Integrieren Sie effektive Steuerungsmechanismen in Ihr AI-Betriebsmodell

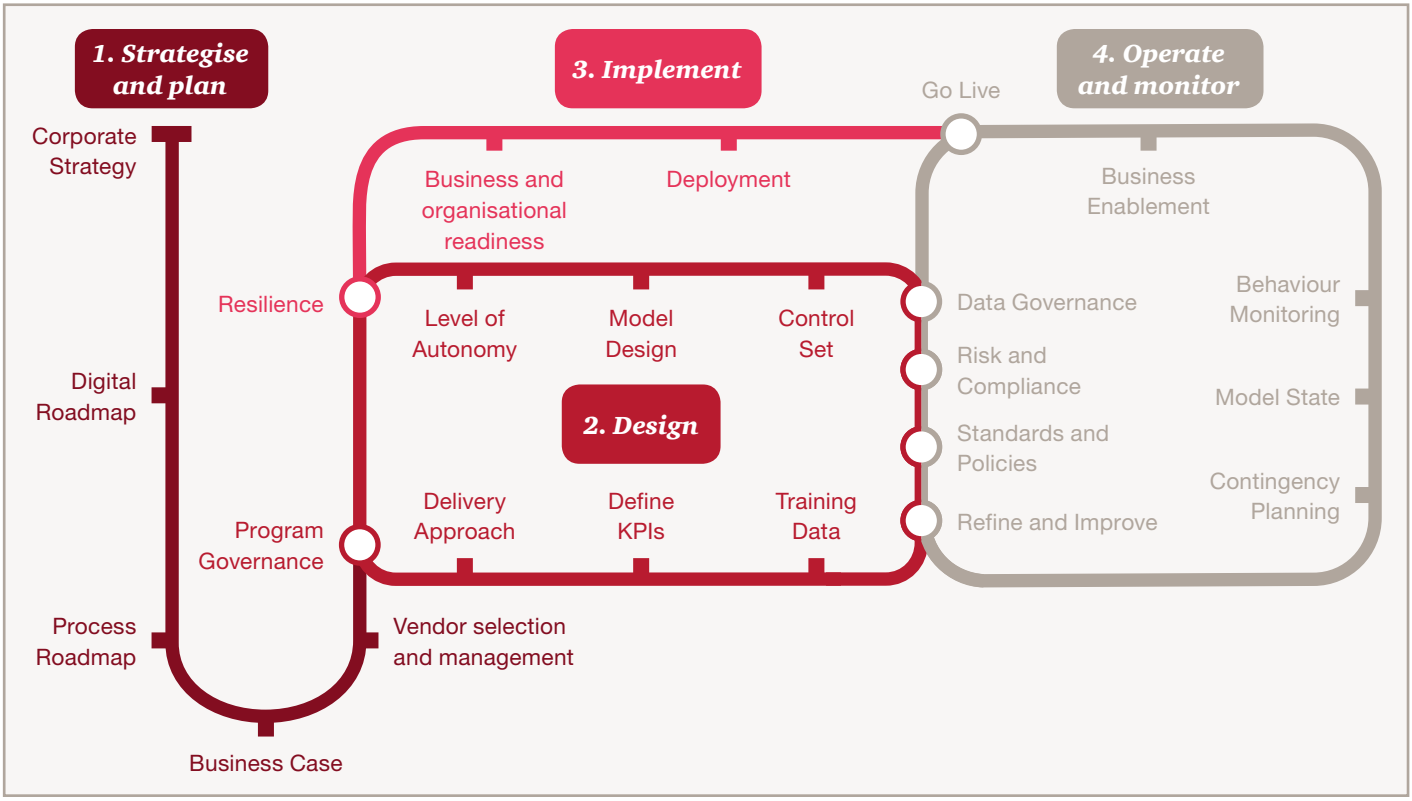
5

Die Steuerung Ihrer AI ist ein kontinuierliches Unterfangen. Sie sollten die Risiken und Möglichkeiten Ihrer AI-Plattformen kontinuierlich beobachten und bewerten, während Sie diese weiterentwickeln.

Zur Steuerung der AI gehört nicht nur die Verankerung neuer Technologien in den betrieblichen Prozessen. Erforderlich ist auch eine unternehmensweite Evaluierung mit dem Ziel, Ergebnisse zu bewerten und potenzielle Risiken sowie Chancen und Möglichkeiten zu erkennen.

In der Zusammenarbeit mit unseren Kunden soll unser „Trust in AI"-Framework (Abb. 5) Transparenz bezüglich der Durchführbarkeit des AI-Implementierungsprojekts herstellen und Vertrauen dafür schaffen, dass Kontrollen implementiert wurden, die sicherstellen, dass die Geschäftsergebnisse den Erwartungen entsprechen.

Abb. 5 PwC Trust in AI Framework



Fazit
Der Weg nach vorn

Wenn Informationen und Daten Corporate Value sind, treibt AI deren Wert auf den Zenit. Doch wie jede neue Ära muss auch sie vorausschauend, vernünftig und verantwortungsvoll vorbereitet und in ihr navigiert werden.

Unternehmen müssen sich jetzt Gedanken darüber machen, wie sie sich in einer AI-enabled Ökonomie positionieren wollen. Bestehende Wertschöpfungsketten werden sich durch AI verändern, ebenso wie neue Geschäftsmodelle und Märkte entstehen.

Es besteht eine große Chance, dass AI sich in eine positive Richtung entwickelt und Menschen dazu befähigt, mehr zu erreichen und die Probleme unserer modernen Gesellschaft zu lösen. Die Gefahr liegt darin, AI über die Grenzen einer vernünftigen Kontrolle hinaus handeln zu lassen. Ein solches Vorgehen wäre für Sie als Unternehmen nicht nur aus Gründen der Ethik und der Reputation inakzeptabel, es würde Ihr Management auch dazu veranlassen, Innovationen infrage zu stellen, zu verzögern oder vollständig zu beenden.

Wir wissen, wie wichtig die Themen Sicherheit und Kontrolle bei der Freisetzung von AI-Potenzial sind. Deshalb haben wir das „Trust in AI“-Framework entwickelt, das das Vertrauen in die effektive Bereitstellung von AI-Lösungen und deren Outputs stärken soll. Die treibende Kraft dahinter ist die Beschleunigung von Innovation und Transformation durch AI. Unser Ziel ist es, Verbraucher, Unternehmen und die Gesellschaft zu befähigen, die Chancen, die sich durch die Entwicklung von AI ergeben, zu nutzen, indem sie deren Grenzen, Schwachstellen und potenziellen Herausforderungen verstehen und mit begründeten Entscheidungen darauf reagieren.

Unser „Trust in AI“-Framework bietet einen gut nutzbaren Leitfaden, um diese Prioritäten zu bündeln und eine effektive Überwachung und Steuerung der AI-Ergebnisse zu ermöglichen. Wir sind überzeugt, dass diese Grundlagen dazu beitragen werden, innerhalb Ihres Unternehmens Innovationen zu beschleunigen und Ihre AI-Vision zu verwirklichen.

Die Grundlage jeder technologiegetriebenen Transformation ist Trust. AI treibt dies aufgrund des enormen transformatorischen Potenzials auf die Spitze.

AI ist mehr als nur eine Technologie. Die Disruption erfasst Märkte, Branchen und Unternehmen mit der Notwendigkeit, die Grundlage des effektiven Einsatzes früh zu berücksichtigen.

Ihre Ansprechpartner

Wilfried Meyer
Risk Assurance Leader
PwC Europe
Tel.: +49 511 5357-5812
Mobiltel.: +49 1707865543
wilfried.meyer@pwc.com

Hendrik Reese
Senior Manager
Artificial Intelligence und RPA
Tel.: +49 89 5790-6093
Mobiltel.: +49 151 70 42 32 01
hendrik.reese@pwc.com

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expertennetzwerks in 158 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

PwC. Mehr als 10.600 engagierte Menschen an 21 Standorten. 2,09 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

© März 2018 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft.
Alle Rechte vorbehalten.
„PwC“ bezeichnet in diesem Dokument die PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, die eine Mitgliedsgesellschaft der PricewaterhouseCoopers International Limited (PwCIL) ist. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.