WHITE PAPER

PRAXISORIENTIERTE EINBLICKE ZUM UMGANG MIT RISIKEN BEIM EINSATZ KÜNSTLICHER INTELLIGENZ

Erkenntnisse aus der Umsetzung von Maßnahmen, die den sicheren und gesetzeskonformen Einsatz von Künstlicher Intelligenz fördern.

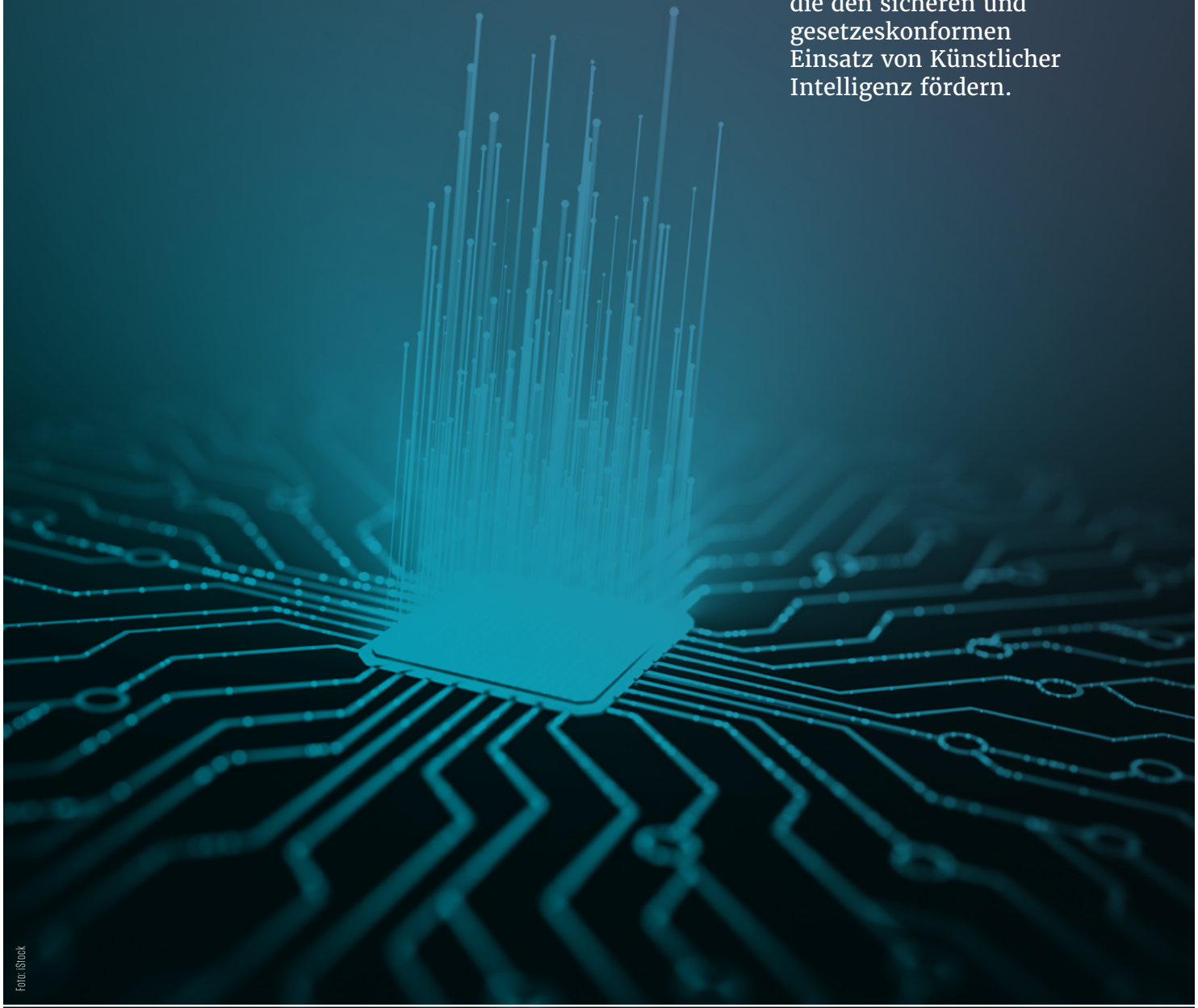

Foto: iStock

protiviti®
Global Business Consulting

WHITE PAPER

PRAXISORIENTIERTE EINBLICKE ZUM

UMGANG MIT RISIKEN BEIM EINSATZ KÜNSTLICHER INTELLIGENZ

Foto: iStock

INHALTSVERZEICHNIS

3 ZUSAMMENFASSUNG

3 EINLEITUNG

KI ist so bedeutend wie nie zuvor

Ohne besondere Sorgfalt sind KI-Projekte zum Scheitern verurteilt

4 ABWARTEN WIRD BESTRAFT

KI-Einsatz bedeutet auch Kontrollverlust

Auf das Beste hoffen, auf das Schlimmste vorbereitet sein

Finanzielle Schäden drohen

5 HANDLUNGSEMPFEHLUNGEN

Gemeinsames KI-Verständnis und KI-Bewusstsein schaffen

Kontrolliertes Wachstum

Risikobewertung

Dedizierte Überwachungskonzepte

Prüfungsvorbereitung

KI-Governance etablieren

8 FAZIT UND AUSBLICK

ZUSAMMENFASSUNG

In diesem White Paper berichtet Protiviti über aktuelle Ansätze und Erfahrungen im Risikomanagement für Systeme, die auf Künstlicher Intelligenz (KI) basieren. Insbesondere werden die Herausforderungen beleuchtet, mit denen unsere Kunden beim produktiven Einsatz von KI konfrontiert waren, und wie wir sie dabei unterstützen konnten, diese zu meistern. Der Schwerpunkt dieses Papers liegt auf der Risikominderung und der Antizipation kommender regulatorischer Implikationen, die im Vorschlag der Europäischen Kommission für ein Gesetz zur Künstlichen Intelligenz (EU AI Act)[1] festgelegt sind. Es bietet praxisorientierte Einblicke, die sich an Managementfunktionen, KI-Teams, Risiko- und Compliance-Funktionen sowie an Prüfer*innen von KI-Systemen richten. Wir konnten feststellen, dass je früher Unternehmen die Risiken von KI mit einem strukturierten Ansatz erkennen und abmildern, desto weniger Nacharbeiten und zusätzliche Kosten entstehen und desto besser kann das Potenzial von KI genutzt werden.

»Traditionelle IT-Risikomanagement-Mechanismen lassen wesentliche Aspekte aus, die für das KI-Risikomanagement wichtig sind«

SEBASTIAN MAYER, DIRECTOR

EINLEITUNG

Künstliche Intelligenz ist eine Schlüsseltechnologie und ein leistungsfähiges Werkzeug, das Unternehmen in fast allen Branchen dabei hilft, ihre Digitalisierung weiter voranzutreiben, innovative Produkte oder Dienstleistungen zu entwickeln und ihre Wettbewerbsfähigkeit zu stärken. Obwohl bereits viele Unternehmen KI als Buzzword verwenden, beispielsweise um ihr innovatives Image oder ihre Produkte zu bewerben, herrscht immer noch eine große Kontroverse darüber, wie KI einheitlich definiert werden kann. Einerseits zeigen uns die fortlaufenden Diskussionen, dass das Feld der KI aus vielen verschiedenen Technologien, Techniken und Konzepten besteht, die sich nur schwer in einer einzigen Definition zusammenfassen lassen, und dass es in diesem Bereich rasante Entwicklungen gibt, die die Grenzen der KI stetig erweitern. Andererseits gilt es, den Begriff der KI zu entmystifizieren – insbesondere für KI-Nutzer*innen –, um klarzumachen, dass es sich hierbei nicht um „digitale Magie" handelt, sondern vielmehr um die ausgeklügelte Anwendung mathematischer Modelle. In diesem Paper werden wir uns auf KI in Form von Systemen beziehen, die in der Lage sind, menschliche Fähigkeiten wie logisches Denken, Lernen oder Planung zu imitieren und mit ihrer Umgebung zu interagieren.[2] Wie später aufgezeigt wird, strebt die Europäische Kommission jedoch eine deutlich umfassendere Definition von KI an, die den Regelungsbereich von KI in der EU enorm vergrößern wird.

KI ist so bedeutend wie nie zuvor

Der Begriff „KI" wurde vor mehr als 60 Jahren zum ersten Mal eingeführt.[3] Doch warum hat er dann jüngst einen solchen Aufschwung erlebt? Die beiden Hauptgründe sind: Den Unternehmen stehen mehr Daten zur Verfügung als je zuvor und der Einsatz hoher Rechenleistung ist billiger denn je. Um die Analogie eines Autos anzuwenden: Es gibt mehr

»Die bevorstehende EU-Verordnung für Künstliche Intelligenz muss ernst genommen werden, da sie die Anforderungen an die KI-Governance erheblich verändern wird«

ANDREJ GREINDL, MANAGING DIRECTOR

Treibstoff (d. h. Daten), der genutzt werden kann, und der Hochleistungsmotor (d. h. die Rechenleistung) ist sehr erschwinglich, was die Nutzung von KI stark befeuert. Daher überrascht es nicht, dass fast 70 % der Unternehmen in Deutschland KI als die wichtigste Technologie für ihre eigene Zukunft ansehen.[4]

Ohne besondere Sorgfalt sind KI-Projekte zum Scheitern verurteilt

Neben dem enormen Potenzial von KI müssen wir uns bewusst sein, dass sie einige Merkmale aufweist, die sie von traditionellen IT-Systemen unterscheidet. Der Einsatz von KI bringt auf verschiedenen Ebenen neue Herausforderungen und Risiken mit sich. Dazu gehören z. B. die hohe Empfindlichkeit ihrer Leistung in Bezug auf die Datenqualität, die neuen Rollen und Verantwortlichkeiten, die sie in bestehende Organisationsstrukturen einbringt, oder die zusätzlichen Anforderungen an die Informationssicherheit, die berücksichtigt werden müssen. Falls diese Aspekte nicht ausreichend gewürdigt werden, steht nicht nur die Leistungsfähigkeit eines KI-Systems auf der Kippe, es drohen auch weitreichende finanzielle Einbußen und Reputationsschäden. Nur diejenigen Organisationen, die ihren individuellen Handlungsbedarf antizipieren und entsprechende, auf KI zugeschnittene organisatorische und technische Maßnahmen umsetzen, werden mit KI nachhaltig erfolgreich sein.

ABWARTEN WIRD BESTRAFT

Vergleicht man den Entwicklungsprozess eines KI-Systems mit dem eines traditionellen IT-Systems, wird eines der wichtigsten Unterscheidungsmerkmale deutlich: Klassische Programmierung folgt oft einem imperativen Weg, d. h. Eingabedaten werden mit einem von Hand programmierten Regelwerk kombiniert, um eine gewünschte Ausgabe zu erzeugen. Im Gegensatz dazu schlägt KI – insbesondere in Anwendungsfällen, die auf maschinellem Lernen beruhen – den deklarativen Weg ein, bei dem Eingabedaten mit Ausgabedaten kombiniert werden, um den verbindenden Regelsatz automatisiert und weitestgehend autonom zu generieren. Dieser Ansatz ist sehr vielversprechend, da der Regelsatz „Wissen" über die Beziehung zwischen Eingabe- und Ausgabedaten enthält, aus dem ein intelligent erscheinender Algorithmus hervorgeht. Noch wichtiger ist, dass er auf zuvor unbekannte Eingabedaten angewendet werden kann, z.B. um die entsprechende Ausgabe vorherzusagen. Darüber hinaus kann KI durch Training stetig weiter lernen, indem zusätzliche Eingabe-Ausgabe-Datenkombinationen zur Verfügung gestellt werden, sodass sie in der Lage ist, selbstständig Handlungsempfehlungen abzuleiten und komplexe Probleme mit überschaubarem Aufwand zu lösen.

KI-Einsatz bedeutet auch Kontrollverlust

Doch die Nutzung von KI verlangt einen Tribut: Wir müssen ein gewisses Maß an Kontrolle aufgeben. Nur so ermöglichen wir es den Algorithmen, komplexe Aufgaben mit unglaublicher Geschwindigkeit und Präzision zu erledigen und Strukturen in Daten zu erkennen, die ein Mensch niemals entdecken würde. Wenn Organisationen sich nicht auf die besonderen Eigenschaften von KI einstellen, gehen

sie ein großes Risiko ein. Denn solange der Lernprozess einer KI nicht durch sorgfältig ausgewählte Algorithmen, einer ausreichenden Menge an Daten in hoher Qualität, geeigneter Testmechanismen und entsprechend geschultem Personal unterstützt wird, entstehen ungenaue Modelle. Diese werden zum einen den initialen Erwartungen nicht gerecht und führen zum anderen oft zu falschen Entscheidungen. Es ist wichtig, ein Bewusstsein zu entwickeln, dass intelligente Algorithmen auf eine andere Art und Weise als traditionelle IT-Systeme (beabsichtigt oder unbeabsichtigt) manipuliert werden können und entsprechende vorbeugende Maßnahmen ergriffen werden müssen. KPIs, auf die wir uns bisher zur Leistungsüberwachung von Software verlassen haben, eignen sich nicht mehr, um uns ausreichend zu informieren, ob ein KI-System wie gewünscht funktioniert. Je nach verwendetem Modell kann es sein, dass wir nicht in der Lage sind, die von der KI getroffenen Entscheidungen zu erklären, so dass Unternehmen und ihre Kunden im Unklaren darüber sind, wie diese zustande gekommen sind und ob diese z. B. ein verzerrtes Bild wiedergeben (Stichwort „Bias"). All diese Aspekte können zu erheblichen finanziellen und rufschädigenden Folgen für ein Unternehmen führen. Microsofts KI-basierter Twitter-Chatbot Tay, der gegenüber Twitter-Nutzer*innen ausfallend wurde,[5] Ubers selbstfahrende Autos, die über rote Ampeln fuhren,[6] oder Amazons KI-Rekrutierungstool, das Frauen systematisch benachteiligte,[7] sind nur einige Beispiele, die aufzeigen, dass selbst sehr erfolgreiche Technologieunternehmen Schwierigkeiten haben, bei der praktischen Anwendung von KI alles richtig zu machen.

Auf das Beste hoffen, auf das Schlimmste vorbereitet sein

Die Risiken, die mit dem Einsatz von KI verbunden sind, sorgen dafür, dass nicht nur Unternehmen, sondern auch Regulierungsbehörden nach Wegen suchen, die eine sichere und verantwortungsvolle Entwicklung und Nutzung von KI erlauben. Derzeit ist der Vorschlag der Europäischen Kommission für ein Gesetz über Künstliche Intelligenz (AIA) vielbeachtet. Von diesem wird erwartet, dass es eine ähnlich gewichtige Rolle wie die Datenschutz-Grundverordnung (DSGVO) haben wird. Entlang eines risikobasierten Ansatzes werden KI-Systeme in die Kategorien „minimales Risiko", „begrenztes Risiko" und „hohes Risiko" bis hin zu „inakzeptablem Risiko" eingestuft. Der AIA dient dem Ziel, KI-Systeme sicher, transparent, ethisch vertretbar, fair und unter menschlicher Kontrolle einzusetzen. Je nach Risikokategorie, jedoch mit besonderem Schwerpunkt auf Hochrisikosysteme, legt der AIA Verpflichtungen für Anbieter, KI-Nutzer*innen, Händler und Importeure von KI-Systemen fest, die in der EU angeboten bzw. betrieben werden. Die Verpflichtungen reichen von der Implementierung eines KI-orientierten Risikomanagementsystems, Data-Governance-Maßnahmen, der Erstellung einer technischen Dokumentation, Aufzeichnungspflichten, Transparenz- und Informationsanforderungen sowie Anforderungen an die menschliche Aufsicht bis hin zu Maßnahmen für Genauigkeit, Robustheit und Cybersecurity.

Finanzielle Schäden drohen

Darüber hinaus legt der AIA eine sehr breite Definition von KI fest.[8] Neben allgemein als KI eingeordneten Ansätzen wie Machine Learning oder Deep Learning werden nach dem aktuellen Entwurf des AIA auch Systeme, die logik- und wissensbasierte Ansätze, statistische Ansätze oder Such- und Optimierungsmethoden nutzen, als KI eingestuft. Damit wird der Anwendungsbereich des AIA enorm ausgeweitet, so dass Systeme, die unter Umständen bereits seit mehreren Jahren produktiv eingesetzt werden, aber von Unternehmen als „Nicht-KI" eingestuft wurden, sehr wahrscheinlich in den Regelungsbereich des AIA fallen werden. Dies wird umso bedeutsamer, als dass die Nichteinhaltung des AIA kostspielige Folgen haben kann. So kann allein die Bereitstellung unvollständiger Informationen bezüglich eines KI-Systems an die zuständigen Behörden zu Geldbußen von bis zu 10 Millionen Euro oder 2% des gesamten weltweiten Jahresumsatzes eines Unternehmens führen, wobei der jeweils höhere Betrag zur Anwendung kommt. Wird ein KI-System betrieben, das nach dem AIA verboten ist, können die Geldbußen bis zu 30 Millionen Euro oder 6% des gesamten weltweiten Jahresumsatzes eines Unternehmens betragen.

HANDLUNGSEMPFEHLUNGEN

Was sollten Unternehmen also heute tun, um nicht nur auf bevorstehende Vorschriften vorbereitet zu sein, sondern auch die Risiken des Einsatzes von KI-Systemen zu minimieren? Da die Anwendungsmöglichkeiten von KI so breit gefächert sind, gibt es keinen allgemeingültigen Ansatz. Dennoch gibt es bewährte Verfahren, die von den meisten

»Die Entwicklung von KI-Modellen erfordert spezielle Validierungsverfahren, um die Modellrisiken zu reduzieren«

DENIS LIPPOLT, DIRECTOR

Unternehmen übernommen werden können. Im Folgenden haben wir einige gängige und effektive Vorgehen zusammengestellt, die wir in Zusammenarbeit mit Kunden aus unterschiedlichsten Branchen validiert haben. Dabei handelt es sich nicht um eine abschließende Darstellung der empfohlenen Maßnahmen, sie dient lediglich als Orientierung und schafft einen ersten Überblick.

Gemeinsames KI-Verständnis und KI-Bewusstsein schaffen

Unternehmen sollten sich nicht von der kontinuierlichen Diskussion von Wissenschaftler*innen, Regulierungsbehörden oder der Konkurrenz einschränken lassen, was sie unter KI verstehen und was nicht. Auch wenn es wichtig ist, diese aufmerksam zu verfolgen, muss jedes Unternehmen eine eigene Definition von KI schaffen oder finden, mit der es sich wohlfühlt und die vor allem von seinen Mitarbeitenden verstanden und akzeptiert wird. Eine der größten Hürden, die es zu überwinden gilt, ist die Verbreitung des Bewusstseins, dass KI nicht einfach nur ein weiteres Add-on ist, das in einem „eigenen Silo" arbeitet. KI, ihre Techniken und ihre Ansätze sind interdisziplinär und können daher nur dann richtig eingesetzt werden, wenn die involvierten Schlüsselfunktionen in einer Organisation zusammenarbeiten. Dazu gehören unter anderem Datenwissenschaftler*innen, Dateningenieur*innen, IT-Expert*innen, Rechtsabteilungen, Risikomanager*innen, Modellvalidierer*innen, Fachbereiche, in denen KI zum Einsatz kommen soll, und nicht zuletzt die zuständige Managementfunktion. Die Grundlage für eine erfolgreiche KI-Einführung wird geschaffen, indem funktionsübergreifende Teams zusammengebracht werden, um die Herausforderungen beim KI-Einsatz gemeinsam zu bewältigen.

Kontrolliertes Wachstum

Was für traditionelle IT-Systeme gängige Best Practice ist, wird für KI oft noch nicht angewendet. Viele Unternehmen tun sich aktuell schwer, eine abschließende Antwort auf die Frage zu geben, welche und wie viele KI-Systeme sie aktuell im Einsatz haben. Häufig liegt das daran, dass einzelne Abteilungen mit KI experimentieren und nützliche Systeme „bottom-up" implementieren. Dieser Ansatz ist zwar legitim, entwickelt sich aber zu einer unkoordinierten Skalierung, wenn mehrere Abteilungen diesen Weg parallel beschreiten. Daher müssen Unternehmen proaktiv handeln und die Verantwortung dafür übernehmen, den Überblick über laufende KI-Initiativen zu behalten und zu wissen, welche KI-Systeme derzeit in der Entwicklung oder bereits in Produktion sind. Die Pflege eines kontinuierlich aktualisierten zentralen KI-Inventars ist hierfür von entscheidender Bedeutung und kann oft durch den Einsatz bestehender IT-Inventarisierungstools umgesetzt werden. Generell ist das Management und die Minderung von KI-Risiken am effizientesten, wenn sie auf die bewährten Säulen bestehender IT-Governance aufgebaut ist und diese sinnvoll um KI-spezifische Aspekte anreichert.

Risikobewertung

Jeder KI-Anwendungsfall sollte einer Risikobewertung unterzogen werden, noch bevor die erste Zeile Code geschrieben wird. Da die Risiken beim Einsatz von KI nicht nur im System selbst liegen, sondern auch durch die zugrundeliegenden Daten verursacht werden können oder der Interaktion mit dem Umfeld (z. B. mit anderen IT-Systemen oder Menschen), muss eine breite Palette potenzieller Risikoquellen abgedeckt werden. Um die Innovationskraft nicht zu hemmen, sollten Unternehmen ein standardisiertes und verpflichtendes Risikobewertungsverfahren ent-

wickeln, das KI-Entwickler*innen und Projektmanager*innen einen effizienten Ansatz zur Identifizierung der für ihren KI-Anwendungsfall spezifischen Risiken bietet. Abhängig von den entsprechenden Risiken sollte ein Katalog mit den wichtigsten Maßnahmen zur Risikominderung erstellt und den Teams zur Verfügung gestellt werden. Falls das Risiko einer KI-Implementierung nicht mit dem „Risikoappetit" einer Organisation vereinbar ist, sollten einheitliche Mechanismen zur Aussetzung der Entwicklung greifen. Die Ergebnisse der Risikobewertung sind von zusätzlichem Wert, wenn sie in ein KI-Inventar zurückgespielt werden, so dass z.B. aktuell betriebene Hochrisiko-KI-Anwendungen in einer Organisation leicht identifiziert werden können. Neben einer ganzheitlichen Identifikation, Analyse, Bewertung, Priorisierung und Behandlung von Risiken auf Use-Case-Ebene sollte das Risikomanagement bis auf die Ebene der genutzten Modelle reichen. Ein möglicher Weg zur Umsetzung ist die Entwicklung von Modell-Risiko-Scorecards, die Modelle in Abhängigkeit von Schlüsselattributen kategorisieren, wie z. B. dem Grad der Datenqualität, der Reife des gewählten Ansatzes oder dem potenziellen Schaden oder Verlust im Falle einer schlechten Modellleistung.

Dedizierte Überwachungskonzepte

Wie bereits erwähnt, sind herkömmliche IT-KPIs in der Regel nicht zur Überwachung von KI-Systemen geeignet. Daher sollte jedes KI-System mit einer verantwortlichen Person verknüpft werden, die entscheidende Schwellenwerte festlegt, unter denen das System arbeiten darf. Typische Kennzahlen zur Leistungserfassung bei Modellen, die auf Machine Learning basieren, sind die Genauigkeit (engl. „Accuracy"), Konfusionsmatrizen, Präzision/Recall oder ROC- und AUC-Kurven. Nachdem ein Modell genehmigt und in den produktiven Betrieb überführt wurde, neigen einige Organisationen dazu, die Verantwortung über KI-Systeme von der Abteilung, die das KI-System ursprünglich entwickelt hat, auf die IT-Abteilung zu übertragen. In solchen Fällen ist eine geordnete Übergabe zwingend notwendig. Denn nur so stellt man sicher, dass die IT-Abteilung über die speziellen Überwachungsanforderungen informiert ist. Neben etablierten Verfahren, um beispielsweise Überwachungskennzahlen in einem zentralen Dashboard zu aggregieren, ist strukturiertes Handeln zur Behandlung von Grenzfällen bei KI unerlässlich. KI-Verantwortliche müssen in der Lage sein, die richtigen Maßnahmen zu ergreifen, falls ein KI-System den vorhergesehen Betriebsraum verlässt, um dieses z.B. sofort abzuschalten, wenn ein bestimmter KPI verletzt wird oder es mit zusätzlichen Daten neu zu trainieren, um den gewünschten Betriebszustand wieder herzustellen. Gerade die Überwachung von KI kommt bei vielen Unternehmen zu kurz, weil sie sich auf ihr bestehendes IT-Monitoring verlassen. Umso wichtiger ist der prozessuale und technische Aufbau von KI-spezifischen Überwachungsmaßnahmen, um deren korrekten Betrieb zu kontrollieren. Basierend auf dem zuvor ermittelten Risikoniveau eines Modells sollten regelmäßige Validierungszyklen vorgeschrieben werden, um die Eignung und Leistungsfähigkeit von KI-Systemen periodisch oder bei größeren Änderungen zu überprüfen.

Prüfungsvorbereitung

Der Einsatz von KI in Geschäftsprozessen, Produkten oder Dienstleistungen stößt nicht nur bei Nutzer*innenn oder Kund*innen auf Interesse, sondern auch bei internen und externen Prüfer*innen. Viele Branchen und Geschäftsbereiche sind bereits reguliert und erfordern daher die Durchführung regelmäßiger Audits durch eine unabhängige Stelle. Die „Betriebserlaubnis" eines KI-Systems hängt also stark vom Nachweis seiner Konformität mit geltenden Vorschriften oder Normen ab. Es ist die herausfordernde Aufgabe der KI-Teams, das Funktionsprinzip eines komplexen Algorithmus in ein Format zu übersetzen, das unabhängigen Prüfer*innen vorgelegt und von diesen geprüft werden kann. Insbesondere diejenigen, die an der Entwicklung und dem Betrieb eines KI-Systems beteiligt sind, müssen eng mit der Compliance- und Risikomanagementabteilung eines Unternehmens zusammenarbeiten, um sicherzustellen, dass die Erwartungen der Prüfer*innen erfüllt werden können und die internen Kontrollsysteme an die Besonderheiten der KI angepasst sind. Es ist die Pflicht der Unternehmensleitung, solche Verbindungen innerhalb ihrer Organisation zu schaffen und die Zusammenarbeit zu fördern. Andernfalls könnte die weitere Nutzung von Systemen untersagt werden oder es könnten Geldstrafen verhängt werden, die das Image der KI intern und extern dauerhaft schädigen.

KI-Governance etablieren

Wenn KI zentraler Bestandteil einer Organisation wird, öffnen sich viele Flanken für potenzielle Risiken. Dementsprechend müssen Organisationen Maßnahmen definieren, die diesen entgegenwirken. Die dezentrale Durchführung einzelner Maßnahmen ist jedoch nicht so effektiv wie ein ganzheitliches Governance-Modell, das alle Maßnahmen, Zuständigkeiten und Zusammenhänge für das (Risiko-) Management von KI strukturiert. Dabei muss das „Governance-Rad" nicht von Grund auf neu erfunden werden, sondern es können und sollten bestehende Best Practices wie Data-Governance-Prinzipien (z. B. für die kontinuierliche Bewertung der Datenqualität) oder das Three-Lines-Modell genutzt und für KI adaptiert werden. Wie die KI selbst ist auch KI-Governance interdisziplinär und nur dann effektiv, wenn sie entsprechend im Unternehmen positioniert ist und nicht in einem Silo oder als Add-on zu bestehenden Prozessen betrieben wird. Je nach Status quo einer Organisation ist es vielleicht sogar nicht notwendig, neues Personal einzustellen, sondern vorhandenes Schlüsselpersonal, das mit KI in Berührung kommt, fortzubilden. Ziel der KI-Governance ist es dabei, den sicheren, zuverlässigen, verantwortungsvollen und vertrauensvollen Einsatz von KI zu gewährleisten und dabei Innovationen nicht zu behindern, sondern zu fördern.

»KI-Systeme und deren Governance-Maßnahmen müssen schon heute hinterfragt werden, um sicherzustellen, dass sie nicht gegen die regulatorischen Vorgaben von morgen verstoßen«

KENTARO ELLERT, MANAGER

FAZIT

Für viele Organisationen ist der Zeitpunkt gekommen, das Potenzial von KI zu nutzen, aber auch die Risiken von KI zu erkennen und darauf zu reagieren. Die Modelle von morgen stützen sich auf die Daten von heute und müssen daher unmittelbar in Einklang mit künftigen Anforderungen und der Wachstumsstrategie eines Unternehmens gebracht werden. KI-Systeme, die bereits heute produktiv eingesetzt werden, werden in Kürze unter die kommenden Vorschriften für KI fallen, sodass sofortige Maßnahmen erforderlich sind, um einer nachträglichen Neuentwicklung von Modellen vorzubeugen und ein robustes Sicherheitsnetz zu spannen, dass die Risiken beim KI-Einsatz abfedert. Den Wettbewerbsvorteil, den KI bietet, in Kombination mit dem entstehenden regulatorischen Umfeld sollte die KI-Implementierung eines jeden Unternehmens auf die strategische Agenda befördern. Der nachhaltige Erfolg kann dabei nur über eine proaktive Steuerung des KI-Einsatzes erreicht werden. Wir von Protiviti unterstützen Sie dabei, KI in Ihrem Unternehmen zu etablieren und zu skalieren, unter Berücksichtigung eines effektiven Risikomanagements zur Einhaltung relevanter Vorgaben.

AUSBLICK

Bleiben Sie mit Protiviti auf dem Laufenden: In Kürze werden weitere Publikationen verfügbar sein, die Einblicke in ausgewählte Projekterfahrungen im KI-Bereich bieten.

Autoren: Kentaro Ellert & Denis Lippolt

SOURCES

[1] *Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF*

[2] *Angelehnt an die KI-Definition des Europäischen Parlaments: https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used*

[3] *A PROPOSAL FOR THE DARTMOUTH SUMMER RESEARCH PROJECT ON ARTIFICIAL INTELLIGENCE: https://web.archive.org/web/20080930164306/http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html*

[4] *https://www.bitkom.org/Presse/Presseinfor¬mation/Kuenstliche-Intelligenz-kommt-in-Unter¬nehmen-allmaehlich-voran*

[5] *IEEE Spectrum - In 2016, Microsoft's Racist Chatbot Revealed the Dangers of Online Conversation: https://spectrum.ieee.org/in-2016-microsofts-racist-chatbot-revealed-the-dangers-of-online-conversation*

[6] *The New York Times – A lawsuite against Uber highlights the rush to conquer driverless cars: https://www.nytimes.com/2017/02/24/technology/anthony-levandowski-waymo-uber-google-lawsuit.html*

[7] *REUTERS - Amazon scraps secret AI recruiting tool that showed bias against women: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G*

[8] *ANHÄNGE des Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION: https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0019.02/DOC_2&format=PDF*

KONTAKT

ANDREJ GREINDL
Managing Director
+49 69 963 768 145
andrej.greindl@protiviti.de

SEBASTIAN MAYER
Director
+49 69 963 768 120
sebastian.mayer@protiviti.de

www.protiviti.de