

DER BETRIEBSWIRT

EUROPLATZ FRANKFURT

Künstliche Intelligenz hat Tücken

Algorithmen sind eine Macht, doch wer sich blind auf sie verlässt, kann Scheinmustern zum Opfer fallen.

Von Thomas Hutzschenreuter

Künstliche Intelligenz (KI) ist in aller Munde. Es herrscht eine regelrechte Goldgräberstimmung rund um datenbasierte Algorithmen. Die Möglichkeiten scheinen nahezu unbegrenzt, und so verdrängt sie nicht, dass gefragt wird, ob sich nicht auch unternehmerische Entscheidungen automatisieren lassen. Eigentümer und Führungskräfte von Unternehmen stellen sich dabei insbesondere drei Fragen: In welchen Bereichen können unternehmerische Entscheidungen durch Algorithmen ersetzt werden? Welche Bereiche lassen sich mithilfe von Algorithmen nicht automatisieren, wo schaden sie gar? Und wie wandelt sich die Rolle des unternehmerischen Entscheiders im KI-Zeitalter?

Ein Algorithmus ist ein Vorhersagemechanismus. Er basiert auf Korrelationen, die in vorliegenden alten Daten ausfindig gemacht werden. Wenn ich zum Beispiel als Kunde nach einem bestimmten Produkt suche, sagt der Algorithmus dem Verkäufer vorher, für welche anderen Produkte ich mich noch interessiere. Basis dieser Vorhersage ist, für welche anderen Produkte sich bisherige Kunden des Verkäufers interessiert haben, die ebenfalls nach dem von mir gesuchten Produkt suchten. Aus diesen Daten wird ein Muster gebildet, das auf meine Suche angewendet wird. Das Muster kann dabei beliebig durch den Einbezug weiterer Daten, etwa zu meiner Person oder der Situation meiner Suche, verfeinert werden. Unabhängig vom Ausmaß der einbezogenen Daten bleibt die Basis der Vorhersage immer eine Korrelation. Was ihr fehlt, ist Kausalität, also ein Verursachungsprinzip. Ein Algorithmus sagt nur vorher, dass ich mich für bestimmte Produkte interessiere, nicht aber, warum.

Die Güte der Vorhersage hängt vom Wahrheitsgehalt der alten und neuen Daten ab sowie davon, ob die Korrelation auch für die neuen Daten wirklich besteht. Das extrahierte Muster ist kein gesichertes Wissen, sondern eine Annahme, die zutreffen kann oder eben nicht. Trifft sie nicht zu, handelt es sich um ein Scheinmuster. Kauft ein Kunde etwa ein Buch über Rosenzucht, wird ihm Werbung für das Thema zugestellt, obwohl er keinen Garten besitzt und das Buch ein Geschenk für einen Freund war. Der Kauf war also nur mit der Rosenzucht assoziiert, nicht aber kausal von ihr abhängig. Ein solches Scheinmuster hatte tödliche Folgen für einen Tesla-Fahrer, dessen autonom fahrendes Auto in einen Laster raste. Der Tesla-Algorithmus interpretierte die weiße Seitenwand des Lasters gemäß dem Scheinmuster „Weiße Fläche bedeutet Himmel“ tatsächlich als Himmel.

Algorithmen sind für Unternehmen dann profitabel anwendbar, wenn es nicht von Bedeutung ist, dass man die Kausalität nicht kennt. Dies ist der Fall, wenn es sich um oft wiederkehrende Anwendungen mit stabilen Zusammen-



Illustration Peter von Tresckow

hängen handelt. Ein Algorithmus ist viel besser als ein menschlicher Entscheider in der Lage, etwa den besten Platz für ein Objekt in einem Zentralhochlager mit Tausenden Einzelprodukten zu finden. Weitere typische erfolgreiche Anwendungsgebiete für Algorithmen sind der Einkauf von Verbrauchsgütern, die Wartung von Maschinenteilen und die Planung von Warenströmen, jedoch auch nur unter stabilen Bedingungen, wie die Chipkrise derzeit eindrucksvoll zeigt. Entfällt die Stabilität der Bedingungen, hat die algorithmische Steuerung fatale Folgen.

Völlig anders ist mit unternehmerischen Entscheidungen umzugehen, die selten getroffen werden müssen und für die sich die jeweilige Situation einzigartig darstellt. Beispiele hierfür sind der Bau einer neuen Fabrik, der Kauf eines Unternehmens im Ausland oder der Einstieg in ein neues Geschäftsfeld. Für solche Entscheidungen fehlt es an einer für den Algorithmeinsatz geeigneten Datenbasis, da wirklich wichtige Daten anderer Unternehmen geschützt sind. Viel schwerer wiegt jedoch, dass diese Entscheidungen auf unternehmerischer Imagination basieren. Die Erzielung von Gewinnen jenseits der Norm setzt Vorteile gegenüber Wettbewerbern voraus. Solche Vorteile sind jedoch nur erreichbar und zu verteidigen, wenn sich ein Unternehmen von seinen Wettbewerbern unterscheidet. Insofern kommt es bei einzigartigen unternehmerischen Entschei-

dungen gerade auf den Bruch in Mustern und das Überraschende an, das sich der Antizipation durch andere möglichst entzieht. Unternehmerisch zu sein heißt ja gerade, etwas zu sehen, was andere (noch) nicht sehen. Es wäre somit sogar schädlich, sich hier auf einen musterforschenden Algorithmus zu verlassen. Während Smartphoneanbieter noch auf möglichst viele Funktionen setzen, erkannte Apple-Gründer Steve Jobs in der Nutzerfreundlichkeit das entscheidende Merkmal. Und Biontech veranschrieb sich der Entwicklung von Medikamenten auf mRNA-Basis schon zu einem Zeitpunkt, als dieser Forschungsrichtung noch wenig zugehört wurde.

Während sich Algorithmen unter den Bedingungen der Wiederholung und Stabilität sinnvoll einsetzen lassen, scheitern sie für seltene Entscheidungen, deren Situation einzigartig ist. Genau diese Entscheidungen sind es aber, die ein Unternehmen erst konstituieren und grundlegend entwickeln. Unternehmerische Entscheidungssituationen sind somit nicht vollständig durch Algorithmen und Analytik lösbar. Stattdessen kommt es gerade bei den richtungweisenden Entscheidungen, wozu übrigens auch Investitionen in Algorithmen gehören, auf den menschlichen unternehmerischen Entscheider an.

Die unternehmerischen Entscheider bringen ein, was nicht in den Daten zu sehen ist. Denn in unternehmerische Entscheidungen gehen je nach Entschei-

dungssituation Wissen, Prognosen und Imaginationen ein. Algorithmen sind Werkzeuge, die Prognosen automatisieren. Sie können menschliche Arbeit dort ersetzen, wo gut gesichertes Wissen vorliegt sowie eine hohe Wiederholungsrate und Stabilität gegeben sind. Sie können transparent machen, wenn ein Entscheider von ihrer Empfehlung abweichen würde, und so ermöglichen, dass sich die unternehmerischen Entscheider explizit mit solchen Abweichungen auseinandersetzen, etwa für die Personalauswahl.

Was Algorithmen jedoch nicht liefern, sind Imaginationen und Visionen. Sie kennen weder Emotionen noch Sorgen, kein Hoffen und kein Vertrauen. Genau dies sind aber zentrale Ressourcen für richtungsweisende Entscheidungen und damit das exklusive Feld unternehmerischer Entscheider. Deren Rolle wird sich im Zeitalter der KI ähnlich wandeln wie physische Berufe im Zuge der Produktionsautomatisierung. Sich wiederholende Entscheidungen, die ohne Imaginationen und Visionen auskommen, werden automatisiert. Für unternehmerische Entscheidungen, in denen es auf individuelle Urteilskraft ankommt, braucht es auch weiterhin einen menschlichen Entscheider. KI ist der (neue) Besen, doch der unternehmerische menschliche Entscheider bleibt der Meister.

Thomas Hutzschenreuter ist Inhaber des Lehrstuhls für Strategic and International Management an der TU München.

Hohe Boni können den Wandel im Betrieb blockieren

Eine Umfrage zeigt, wie Unternehmen variable Vergütungen nutzen / Von Patrick Kampkötter und Dirk Sliwka

Aktuell sorgen Berichte für Diskussionen, dass die Deutsche Bank und andere internationale Finanzunternehmen ihre Bonuspools signifikant erhöhen wollen. Wie immer wird dies nicht nur von der Öffentlichkeit kritisch begleitet, auch die Europäische Zentralbank hat jüngst eine Mäßigung für Bonuszahlungen gefordert. Aber wie entwickelt sich die Ausgestaltung von Bonusssystemen eigentlich über Branchen hinweg in Deutschland – also nicht nur in der Bankenszene?

Über viele Jahre haben Ökonomen variable Vergütungen als zentrales Instrument zur Steigerung der Leistung von Beschäftigten angesehen, insbesondere zur Belohnung individueller Leistung. Zwar gab es immer auch Kritik an der Nutzung von Bonuszahlungen zur Motivation von Beschäftigten. Jedoch zeigte sich empirisch gerade in angelsächsischen Ländern über lange Zeit ein stetig steigender Anteil der Jobs, in denen variable Vergütung genutzt wird.

Seit 2012 befragen wir als Teil eines Forschungsteams in einer repräsentativen Längsschnittbefragung (LPP) alle zwei Jahre Betriebe der Privatwirtschaft mit mehr als 50 Beschäftigten über die Nutzung verschiedenster Personalinstrumente. Zu Beginn der Befragung im Jahr 2012 nutzte mit 58 Prozent die Mehrheit der Betriebe variable Vergütungen und

ein erheblicher Teil davon (59 Prozent) nicht nur für Führungskräfte, sondern auch für Beschäftigte ohne Führungsverantwortung.

Bei der Betrachtung der Längsschnittdaten fällt eine Entwicklung auf: Seit 2014 ist der Anteil der Betriebe, die variable Vergütungssysteme nutzen, stetig gesunken. Im Jahr 2020 betrug der Anteil der variabel vergütenden Betriebe nur noch 47 Prozent. Die Daten geben auch Aufschluss über die Struktur der variablen Vergütung.

Typischerweise basieren Bonuszahlungen in Unternehmen auf drei Komponenten: der individuellen Leistung der Person, dem Erfolg eines Teams und dem Erfolg des Unternehmens insgesamt. Für Führungskräfte ist hierbei der Unternehmenserfolg am wichtigsten. Nahezu die Hälfte ihrer Bonuszahlungen beruht auf diesem. Individuelle Leistungsbewertungen haben ein geringeres Gewicht – und dieses hat von 34 Prozent in 2012 auf 29 Prozent in 2020 weiter abgenommen. Bei Beschäftigten ohne Führungsverantwortung spielt traditionell die individuelle Leistung eine größere Rolle. Aber auch hier ist deren relatives Gewicht im gleichen Zeitraum von 50 Prozent auf 44 Prozent gesunken.

Die Gründe für diese beiden zentralen Trends, also den Rückgang der Nutzungs-

häufigkeit variabler Vergütungen und des Gewichts der individuellen Leistung, sind vielfältig. Zum einen haben gerade in Großunternehmen kritische Diskussionen über die Nützlichkeit von Bonuszahlungen zugenommen. Prominente Unternehmen wie Bosch oder SAP haben öffentlichkeitswirksam individuelle Bonuszahlungen zurückgeführt oder sogar abgeschafft. Ein wichtiges Argument gerade gegen individuelle Bonuszahlungen ist, dass sie manchmal zu einem starren Festhalten an vergangenen Zielen führen können, wenn diese die Grundlage der variablen Vergütung sind. Der Wandel zu agileren Strukturen in Unternehmen, die schnellere Anpassungen des Handelns ermöglichen, erschwert es, Kennzahlen festzulegen, an denen die Leistung gemessen wird.

Auch hier zeigen die Daten unserer jährlichen Umfrage interessante Muster: Während 2012 noch 60 Prozent der Betriebe schriftlich fixierte Zielvereinbarungen nutzten, lag dieser Anteil in 2020 nur noch bei 51 Prozent. Lange Zeit haben Vergütungsberater und Managementforscher empfohlen, Zielvereinbarungen als Grundlage variabler Vergütungen heranzuziehen. In der Tat gaben 2018 noch 55 Prozent der solche Zielvereinbarungen nutzenden Unternehmen an, dass sie diese auch formelbasiert zur

Berechnung variabler Vergütung heranzuziehen. Dieser Anteil lag aber schon zwei Jahre später nur noch bei 30 Prozent.

Es besteht jedoch eine Gefahr bei der Betrachtung von Trends: Sie liegt in der Versuchung, aus dem Trend abzuleiten, was gerade „best practice“ ist, und dies zu imitieren. Es ist häufig keine kluge Idee, das eigene Vergütungssystem nur deswegen zu ändern, weil viele andere Unternehmen eine bestimmte Änderung vollzogen haben. Es ist vielmehr wichtig herauszufinden, welches Vergütungssystem im eigenen Unternehmen funktioniert. Aktuelle Studien, welche die Wirkung spezifischer Vergütungsinstrumente gezielt in Unternehmen untersuchen, zeigen, dass es stark vom Geschäftsmodell des Unternehmens und den betrachteten Tätigkeiten abhängt, welche Form der Vergütung die Leistung der Beschäftigten am besten fördert. Die Betrachtung von Trends ist dennoch wichtig, um Denkanstöße zu erhalten, wachsam mögliche Veränderungen im eigenen Umfeld zu verfolgen und existierende Systeme zu hinterfragen.

Patrick Kampkötter ist Inhaber des Lehrstuhls für Managerial Accounting an der Eberhard Karls Universität Tübingen.

Dirk Sliwka ist Inhaber des Lehrstuhls für Personalwirtschaftslehre an der Universität zu Köln.

Hört auf Nixon!

Von Jörg Krämer

Die hohe Inflation beunruhigt die Menschen. Die ersten Ökonomen fordern, dass der Staat den Unternehmen Obergrenzen für Preiserhöhungen vorschreiben soll. Solche Preiskontrollen würden massiv in die Vertragsfreiheit eingreifen, das Preissystem als Lenkungsinstrument einer Marktwirtschaft aushebeln und die Notenbank aus ihrer Verantwortung für eine niedrige Inflation entlassen. Aber jenseits solcher ordnungspolitischen Argumente zeigen die Erfahrungen aus den USA der frühen Siebzigerjahre, dass Preiskontrollen die Inflation am Ende sogar verstärken.

Der damals amtierende Präsident Richard Nixon hatte während des Zweiten Weltkriegs in einer Bundesbehörde für Preiskontrollen gearbeitet und war sich der Problematik dieser Eingriffe bewusst. Laut mittlerweile veröffentlichten Tonbandaufnahmen aus dem Weißen Haus sagte Nixon im Februar 1971 zu seinen Mitarbeitern: „Sie haben nicht einmal am Ende des Zweiten Weltkriegs funktioniert. Sie werden niemals in Friedenszeiten funktionieren.“ Kurze Zeit später änderte er jedoch seine Meinung, um seine Chancen bei der anstehenden Präsidentenwahl zu erhöhen.

Im August 1971 ließ Nixon Löhne, Preise und Mieten für 90 Tage einfrieren. Danach durften große Unternehmen ihre Preise höchstens um 2,5 Prozent anheben, Lohnerhöhungen waren auf 5,5 Prozent begrenzt. Kommissionen überprüften die Einhaltung der Vorgaben. Von Januar 1973 bis April 1974 dauerten die Preis- und Lohnkontrollen an, waren aber deutlich lockerer als zuvor.



Die Ökonomen der Federal Reserve Bank von Minneapolis haben 1978 die Wirkung der Preis- und Lohnkontrollen untersucht. Die Studie belegt das Versagen dieser Politik. Während der ersten beiden Phasen mit strengen Kontrollen (bis Januar 1973) senkten Preiskontrollen die Inflation schätzungsweise um zwei Prozentpunkte. Darauf hatte Nixon mit Blick auf die Präsidentenwahl im November 1972 spekuliert.

Aber in den zwei Jahren nach der Lockerung der Kontrollen fiel die Inflation nach den Schätzungen der Ökonomen deutlich höher aus, als es ohne die Eingriffe zu erwarten gewesen wäre. Die Absatze der Unternehmen waren nämlich während der Phase der strengen Kontrollen gezwungenermaßen deutlich schwächer gestiegen als ihre Lohnkosten. Auf den Rückgang ihrer Gewinne reagierten die Unternehmen wie im Lehrbuch mit einer Senkung ihrer Produktion. Als die unverändert starke Nachfrage auf das geschrumpfte Angebot stieß, zog die Inflation wieder an. Alles in allem haben die Preiskontrollen die Inflation erhöht und nicht gesenkt – so wie es Nixon im kleinen Kreis vorhergesagt hatte.

Die hohe US-Inflation begann erst Anfang der Achtzigerjahre zu sinken, nachdem Notenbank-Präsident Paul Volcker mit Rückendeckung des neu gewählten Präsidenten Ronald Reagan die lockere Geldpolitik beendete. In einer Marktwirtschaft sorgen nicht staatliche Preiskontrollen, sondern nur eine stabilitätsorientierte Geldpolitik für eine dauerhaft niedrige Inflation.

Der Autor ist Chefvolkswirt der Commerzbank.

WIRTSCHAFTSBÜCHER

Chefsache Cyberresilienz

Zwei Bücher zum Stärken der Abwehr

Cybersicherheit ist zu einer der größten Herausforderungen für die vernetzte Welt geworden. Erst jüngst rief das Bundesamt für Sicherheit und Informationstechnik (BSI) „Warnstufe Rot“ aus. Es reift die Erkenntnis, dass Cyberresilienz, Datenschutz und Sicherung der IT-Infrastruktur längst nicht mehr nur als technische Spezialthemen für Datenschutzbeauftragte und IT-Leiter betrachtet werden dürfen. Für Unternehmen resultieren aus den Hackerangriffen zwei Gefahren: teure Betriebsunterbrechungen und erhebliche Haftungsrisiken für das Führungspersonal. Für Unternehmen ist es ein Gebot der Sorgfaltspflicht, alles dafür zu tun, die Cyberresilienz technisch und organisatorisch zu stärken und dabei stets rechtskonform zu handeln. Die vorliegenden beiden praxisorientierten Schriften sind aus einem Verlag ermöglichen den Zugang zu dem komplexen Thema, das aus technischer und auch juristischer Sicht ein Minenfeld darstellt.

Das von der Bilanzexpertin Carola Rinker herausgegebene Sammelwerk wird etwas vollmundig als Praxisleitfaden für optimiertes IT-Risikomanagement angekündigt. Es ist bei näherer Betrachtung eher ein interessantes Lesebuch mit fünf recht ausführlichen Beiträgen von spezialisierten Wirtschaftsberatern zu bisher in der Fachliteratur eher wenig behandelten Facetten des Themenkomplexes. Man darf den Autoren attestieren, dass sie tief in die Thematik eingestiegen sind. Bedauerlich ist jedoch, dass sich dabei Redundanzen und auch Ausflüge in theoretische Grundlagen und langatmige Begriffsdefinitionen eingeschlichen haben. Eine Straffung durch Herausgeberin und Lektorat hätten dem Buch gutgetan. Dem Leser sei daher eine Lektüre nach dem Prinzip des Rosinenpickens empfohlen, denn Rosinen gibt es tatsächlich zu entdecken.

Der erste Beitrag ist eine lehrbuchhafte Darstellung des Aufbaus eines IT-Risikomanagementsystems in der Praxis und der dabei anstehenden Arbeitspakete. Der zweite Beitrag widmet sich der Identifikation, Bewertung und Beurteilung von Cyber-Risiken und geht auch auf die für Kapitalgesellschaften dringend gebotene Berichterstattung über Cyber-Risiken ein. Der dritte Beitrag behandelt Cyber-Risiken, die sich durch die immer weiter voranschreitende unternehmensübergreifende Vernetzung ergeben. Der vierte Beitrag geht kenntnisreich auf die Entwicklung und Auswahl von Sicherheitskontrollen ein und bewertet die in diesem Zusammenhang relevanten Auditberichte, Zertifikate und Testate, die hilfreich sind, aber natürlich keinen ultimativen Schutz gegen Cyberattacken bieten können. Der Autor gibt zudem einen interessanten Ausblick auf rechtliche Entwicklungen in der Cyber-sicherheit. Der fünfte leider zu deskriptive Beitrag, der von der Herausgeberin verfasst wurde, enthält eine statistische

Auswertung der Darstellung der Cyber-Risiken in den Geschäftsberichten deutscher börsennotierter Unternehmen. Es wird deutlich, dass hier weiterer Handlungsbedarf besteht. Man hätte gerne noch mehr darüber erfahren, was aus der Sicht der Autorin eine gute Berichterstattung ausmacht.

Das nunmehr in der zweiten Auflage erschienene umfangreiche Handbuch Datenschutz und IT-Sicherheit, an dem unter der Ägide von Uwe Schläger und Jan-Christoph Thode zahlreiche Experten mitgewirkt haben, verbindet die juristischen und die technischen Aspekte des Datenschutzes und der IT-Sicherheit miteinander. Die steigende Zahl von Cyberfällen und der lasche Umgang mit sensiblen (personenbezogenen) Daten haben den Gesetzgeber auf den Plan gerufen. So wurden seit dem Inkrafttreten der EU-Datenschutz-Grundverordnung (DSGVO) im Jahr 2018 die regulatorischen Daumenschrauben immer mehr angezogen. Dies zeigt sich an deutlich erhöhten Bußgeldern, die von Datenschutz-Aufsichtsbehörden schon mehrfach verhängt wurden. Mit der DSGVO und dem neuen Bundesdatenschutzgesetz wurde der Datenschutz auf völlig neue Grundlagen gestellt. Im ersten Teil der umfangreichen Schrift geht es vor allem um die gesetzeskonforme Sorgfalt beim Umgang mit personenbezogenen Mitarbeiter- und Kundendaten. Im zweiten Teil werden die rechtlichen Grundlagen der IT-Sicherheit und technisch-organisatorische Maßnahmen, die im Kampf gegen Sicherheitsvorfälle wichtig sind, behandelt. Die überarbeitete und erweiterte zweite Auflage des Handbuchs hat die Entwicklungen der letzten drei Jahre gut eingearbeitet. So werden sowohl neue Gerichtsurteile zum Datenschutz als auch Ansätze der IT-Sicherheit behandelt, die sich herauskristallisiert und bewährt haben. Letztere verdienen im aktuellen Bedrohungsumfeld besondere Beachtung. Insgesamt liegt ein wertvolles Nachschlagewerk für die Praxis vor, das klarmacht: Cyberresilienz ist heute Chefsache! Warnungen hat es genug gegeben.

Die Lektüre der beiden verwandten Schriften weist zwar nicht den Königsweg zur Immunität gegen Angriffe aus dem Netz, sie zeigt jedoch Ansatzpunkte für den Aufbau einer gestärkten Defensive auf. Hierzu bedarf es einer konzertierten Aktion von Unternehmensleitung, IT-Experten, Juristen, Abschlussprüfern und vor allem auch der Mitarbeiter. ROBERT FIETEN

Carola Rinker (Hrsg.): Cyber Security in der RisikoBerichterstattung. Praxisleitfaden für optimiertes IT-Risikomanagement. Erich Schmidt Verlag, Berlin 2021, 224 Seiten, 40 Euro.

Uwe Schläger, Jan-Christoph Thode (Hrsg.): Handbuch Datenschutz und IT-Sicherheit. 2., neu bearbeitete und erweiterte Auflage. Erich Schmidt Verlag, Berlin 2022, 732 Seiten, 98 Euro.