BEST OF 2023

2023

BEST OF 2023

MANAGEMENT & STRATEGIE

„Die Kluft zwischen den USA und der EU im Bereich KI ist übertrieben“ 3
Wie das IT-Sicherheitskennzeichen die IoT-Security stärken kann 10
KI-Projekte sind selten allein zu schaffen 14
Digitale Ethik mithilfe von KI-Werkzeugen realisieren 19
Model Drift – Hintergründe und Empfehlungen 25
Was die Datenschützer zur Haftung bei KI sagen 31
Warum im Top-Management nichts mehr ohne Daten-Know-how geht 36
Synthetische Daten – wann lohnt sich der Einsatz? 41
Resultate beschleunigen mit KI 46
Design-Recycling mit Künstlicher Intelligenz 50
Keine KI ohne zielführende Datenarchitektur 54
5 Tipps, um ein Unternehmen KI-ready zu machen 58

TECHNOLOGIE & ZUKUNFT

Die Macht der Künstlichen Intelligenz im Kundenservice 62
„KI kann eine noch größere Chance darstellen als der Internet-Boom in den 90ern“ 66
Wie sich Algorithmen für Maschinelles Lernen schützen lassen 73
KI-Potenziale für Life Science erkennen und nutzen 77
Wie sich Künstliche Intelligenz inzwischen prüfen lässt 81
Stream-Processing mit Apache Flink 85
Wie Low-Code der IoT-Security helfen kann 89
ML-Modelle einfach trainieren mit StreamSets Transformer 93
Daten abfragen und Dashboards erstellen mit Redash 97
Das leistet KI in der Produktion und der Pharmazie 101
Scikit-learn – KI, Statistik, Mathematik, Analyse oder Data Mining mit Python 108
Der Status quo bei KI in der Cybersicherheit 113

Interview mit Jessica Newman, Zentrum für langfristige Cybersicherheit an der UC Berkeley

„Die Kluft zwischen den USA und der EU im Bereich KI ist übertrieben"

29.11.2021 | Von Ekaterina Venkina

Eine „Bill of Rights" für die KI-gestützte Welt, regulatorische Herausforderungen und soziotechnische Risiken: Im Interview wirft Jessica Newman vom Zentrum für langfristige Cybersicherheit an der UC Berkeley einen Blick auf die jüngsten KI-Entwicklungen in den Vereinigten Staaten und Europa.

Jessica Newman, Programmleiterin für die KI-Sicherheitsinitiative (AISI) beim Zentrum für langfristige Cybersicherheit (CLTC) der UC Berkeley, im Gespräch mit BigData-Insider.

***BigData-Insider:* Frau Newman, Sie schreiben, dass es sowohl „übertrieben als auch kontraproduktiv" sei, sich auf die regulatorische „Kluft" zwischen der EU und den USA bei der Entwicklung von KI-Standards zu konzentrieren. Warum sind Sie der Meinung, dass diese Unterschiede unverhältnismäßig stark hervorgehoben werden?**

Newman: In der Öffentlichkeit ist die Auffassung weit verbreitet, dass die EU der technologische Wächter der Welt ist und die USA den digitalen Wilden Westen darstellen. Doch wenn es um KI geht, scheint die Realität etwas differenzierter zu sein. Das EU-Gesetz zur Künstlichen Intelligenz (Artificial Intelligence Act,

AIA) verbietet eine kleine Anzahl von KI-Anwendungen, die unannehmbare Risiken darstellen, und führt Verpflichtungen für Systeme mit hohem Risiko ein. Der Großteil der KI-Nutzung bleibt jedoch ungeregelt, und es werden lediglich freiwillige Leitlinien vorgeschlagen, um einen verantwortungsvollen Einsatz zu fördern. Ich denke also nicht, dass es sich um einen extremen Regulierungsvorschlag handelt.

Gleichzeitig gibt es in den Vereinigten Staaten bereits Gesetze, die einen Teil der Regulierung leisten, die der AIA zu ermöglichen versucht. Viele Städte hierzulande haben die biometrische Echtzeitüberwachung durch die Strafverfolgungsbehörden bereits verboten. Auch die Federal Trade Commission hat angedeutet, dass KI-Produkte unter ihre Verbraucherschutzgesetze fallen werden. Die EU hat strengere Datenschutzgesetze, aber die Unterschiede zwischen Washington und Brüssel sind weniger grundlegend, wenn es um KI-Technologien geht.

Außerdem gibt es zahlreiche Signale für ein gemeinsames Interesse an transatlantischer Zusammenarbeit in diesem Bereich. Die OECD-Grundsätze für Künstliche Intelligenz wurden sowohl von den USA als auch von Deutschland sowie von Dutzenden anderer gleichgesinnter Länder gebilligt. Beide Länder sind Mitglieder der Globalen Partnerschaft zur Künstlichen Intelligenz (Global Partnership on Artificial Intelligence, GPAI). Die jüngsten Beratungen des EU-US-Handels- und Technologierats (Trade and Technology Council, TTC) sind eine wirklich gute Gelegenheit für die Verbündeten, bei kritischen Technologien zusammenzuarbeiten. Sowohl die USA als auch die EU erkennen an, dass KI-Technologien die Sicherheit und die Grundrechte der Menschen verletzen können, und sind sich einig, dass es dringend notwendig ist, diese gefährlichen und schädlichen Folgen durch Kooperation zu verhindern. Ziel ist es, Hochrisikofälle zu beseitigen und proaktiv gemeinsame KI-Standards festzulegen.

Eric Lander, der das Büro für Wissenschafts- und Technologie-Politik (Office of Science and Technology Policy, OSTP) im Weißen Haus leitet, und Alondra Nelson, OSTP-Vize-Chefin für Wissenschafts- und Gesellschaftspolitik, veröffentlichten kürzlich einen Beitrag in WIRED. Darin weisen sie darauf hin, dass das Weiße Haus eine „Bill of Rights für eine KI-gestützte Welt“ vorbereitet. Welche Folgen könnte dies für die amerikanische KI-Strategie haben?

Newman: Es ist ein gutes und wichtiges Zeichen, das einen Wandel in der KI-Politik der USA signalisiert. Es bedeutet nicht nur, dass wir KI-Risiken eindämmen werden, sondern auch, dass wir die Rechte und Werte der Amerikaner in den Mittelpunkt stellen werden, um sicherzustellen, dass unsere neuen Technologien die Art von Gesellschaft unterstützen, von der wir alle ein Teil sein wollen. Das bedeutet, dass es inakzeptabel ist, KI-Systeme zu haben, die Menschen massiv schaden werden. Wir müssen das Konzept kodifizieren, dass mächtige Technologien auch den Respekt für unsere demokratischen Werte voraussetzen. Derzeit befindet sich die „Bill of Rights" in der Phase der öffentlichen Besprechungen, aber es wurde bereits angedeutet, dass sie sich auf die Anforderungen an die staatliche Auftragsvergabe auswirken oder zu neuen Gesetzen und Vorschriften führen könnte.

Sehen Sie eine Bereitschaft des Silicon Valley, die von Washington vorgeschlagenen „Bill" zu unterstützen?

Newman: Ich habe den Eindruck, dass die Unternehmen im Valley zurzeit generell mehr Orientierung und Regulierung fordern. Die jüngsten Enthüllungen im Zusammenhang mit den Facebook Papers haben deutlich gemacht, dass die derzeitigen Rechenschaftsmechanismen für die großen Tech-Giganten nicht ausreichen.

Die „AI Bill of Rights" ist nur für die USA gedacht, aber wir sprechen hier über Unternehmen, die länderübergreifend tätig sind ...

Newman: Bis zu einem gewissen Grad können sogar länderbezogene Gesetze beeinflussen, wie diese Unternehmen auf der globalen Bühne agieren. Dies ist zum Beispiel bei der Datenschutz-Grundverordnung der EU und dem kalifornischen Verbraucherschutzgesetz (California Consumer Privacy Act, CCPA) der Fall. Aber es geht nicht nur um den Schaden für den Einzelnen, sondern auch um die Folgen für Gemeinschaften und Gesellschaften, um die potenziellen Risiken sozialer Unruhen. Es könnte auch noch um die Auswirkungen von Social Credit Scoring auf gesellschaftlicher Ebene und den Zustand der Demokratien gehen. Ich denke, dass die Arbeit, die das Nationale Institut für Standards und Technologie (National Institute of Standards and Technology, NIST) derzeit leistet, um den Rahmen für das KI-Risikomanagement zu entwickeln, von großer Bedeutung

sein wird. Es wird eine gemeinsame Sprache und eine Reihe von Praktiken bieten, mit denen Unternehmen arbeiten können, um eine robustere Reihe von KI-Praktiken mit Gemeinsamkeiten zwischen ihnen zu entwickeln. Und ich weiß, dass auch die EU den Fortgang dieser Arbeit genau verfolgt.

Olaf Groth, Professor für globale Strategie, spricht von der Magna Charta für die globale KI-Wirtschaft, einer kollektiv entwickelten KI-Charta der Rechte. Glauben Sie, dass so etwas möglich ist?

Newman: Ich mag diese Idee. Ich verstehe sie so, dass es um ein globales Dokument geht, das die Freiheit der Menschen und ihre Kontrolle über undurchsichtige maschinelle Entscheidungen bekräftigt. Es könnte sicherlich von einem der verschiedenen internationalen Foren aufgegriffen werden. Ich würde mir wünschen, dass sie mehr Anklang findet, denn wir brauchen sinnvolle globale Rahmenwerke dieser Art.

Welche Foren sind Ihrer Meinung nach derzeit die erfolgreichsten Austauschplattformen für die EU und die USA zum Thema KI?

Newman: Die GPAI leistet hervorragende Arbeit auf dem Gebiet der KI-Forschung. Die Normen, die derzeit entwickelt werden, und die Art und Weise, wie sie gestaltet werden, werden den Verlauf der technologischen Entwicklungen und deren Auswirkungen auf der ganzen Welt verändern. Die Zusammenarbeit zwischen der EU und den USA könnte also eine starke Voraussetzung bieten, um die Aushöhlung der Menschenrechte durch die Verbreitung von KI-Technologien zu verhindern.

Auch bei der ersten Sitzung des TTC in Pittsburgh wurden eine Reihe von Verpflichtungen eingegangen, mit denen die USA und die EU meiner Meinung nach zuallererst beginnen sollten. Hervorgehoben wurden Mechanismen für den Informationsaustausch und die Koordinierung internationaler Standards. Es wurde erörtert, wie Überwachung, Desinformation und soziale Manipulation mit KI-Technologien bekämpft werden können. Wie konvergente Kontrollansätze für sensible duale Technologien entwickelt werden können. Dies ist ein Bereich, der sehr bedeutsam sein kann. Ich denke, dass ein breites und vielfältiges Engagement der Interessengruppen für den langfristigen Erfolg des TTC im Allgemeinen entscheidend ist.

Was sind die größten Bedrohungen im Zusammenhang mit KI-Entwicklungen? Sind es Risiken für kritische Infrastrukturen, für die soziale Ordnung oder für demokratische Institutionen durch Verzerrungen, die durch Algorithmen verursacht werden können?

Newman: Am sinnvollsten ist es, die mit der KI verbundenen Gefahren als soziotechnische Risiken zu betrachten. Ein Aspekt davon ist die Art und Weise, wie KI-Systeme trainiert werden und wie es zu Verzerrungen kommt. Gleichzeitig sind es aber auch Menschen, die diese Datensätze kuratieren und entscheiden, was gebaut werden soll. Wenn wir nur die technische Dimension betrachten, übersehen wir gleich zu Beginn alle sozialen Einflüsse. Und dann ist da natürlich noch die Frage der Auswirkungen, der Impact-Faktor. Wir müssen darüber nachdenken, welche Länder und Gemeinschaften davon betroffen sind.

Verfügen wir derzeit über ausreichende Überwachungsmechanismen, um Kontrolle auszuüben?

Newman: Die OECD-Beobachtungsstelle für KI-Politik (OECD AI Policy Observatory, OECD.AI) verfolgt die verschiedenen Entwicklungen im Bereich der KI-Technologien und die Reaktionen der diversen Interessengruppen darauf. Die Partnership on AI hat die Artificial Intelligence Incident Database entwickelt. Damit wird versucht zu verfolgen, wann KI-Systeme Unfälle haben, Fehler machen oder versehentlich jemandem Schaden zufügen. Soweit ich weiß, sind derzeit unabhängige Forscher für diese Datenbank verantwortlich. Damit sie erweitert werden könnte, brauchen wir Anreize für Unternehmen, transparenter zu sein.

Das US-Verteidigungsministerium (U.S. Department of Defence, DoD) ist, wie einige Experten betonen, ein starker Befürworter des „Zentaurenmodells“; wie groß ist also die Gefahr einer raschen Militarisierung des KI-Bereichs in den USA?

Newman: Das gemeinsame Zentrum für Künstliche Intelligenz (Joint Artificial Intelligence Centre, JAIC) hat ein starkes Programm, um verantwortungsvolle KI-Praktiken im US-Verteidigungsministerium einzuführen. Ein Pilotprojekt zur verantwortungsvollen KI-Beschaffung ist derzeit im Gange. Damit soll sichergestellt werden, dass ein Rahmen vorhanden ist, um zu bewerten, welche Daten in die Entwicklung von KI-Technologien einfließen und wie sie von dem DoD erworben werden. Darüber

hinaus hat das Ministerium eine Reihe von ethischen Grundsätzen für KI angenommen, nachdem über ein Jahr lang eine öffentliche Konsultation dazu stattgefunden hat. Ich habe auch mit Interesse zur Kenntnis genommen, dass die NATO kürzlich eine KI-Strategie veröffentlicht hat. Ich denke, dies ist ein weiteres Indiz dafür, dass die USA und andere Militärmächte verstanden haben, dass wir nicht so schnell vorgehen können, dass wir den Einsatz unsicherer Technologien riskieren.

Wo sehen Sie die größten Schwachstellen bei der Entwicklung ethischer Standards für KI, und wie können diese überwunden werden?

Newman: Zum jetzigen Zeitpunkt kann ich zwei zentrale Herausforderungen nennen. Die erste besteht darin, KI-Entwickler dazu zu bringen, sich an Standards zu halten, und die zweite Herausforderung ist die Repräsentation, also die Einbeziehung verschiedener Akteure. Entscheidungen über die KI-Ethik müssen von Menschen getroffen werden, die über ein breites Spektrum an Fachwissen verfügen und alle Bevölkerungsgruppen vertreten, auf die sich diese Entscheidungen auswirken werden. Insbesondere müssen wir den globalen Süden stärker einbeziehen, als dies bisher der Fall war.

In welchen Bereichen könnte die deutsch-amerikanische KI-Zusammenarbeit zu Synergieeffekten führen? Die Biden-Administration sprach Anfang dieses Jahres über das Konzept, „Techno-Demokratien" zu vereinen? Ist das möglich? Oder ist das ein Wettlauf, bei dem jeder für sich ist?

Newman: Ich habe den Eindruck, dass es in Deutschland hervorragende KI-Forscher, Institute und wirklich einflussreiche und spannende Plattformen für die Ausarbeitung von KI-Richtlinien gibt. Der Bericht der Datenethikkommission, der das Risikoprofil für KI in Form einer Pyramide erstellt hat, war sehr einflussreich.

Es besteht ein gemeinsames Verständnis dafür, dass die Werte, die wir in die KI-Systeme einbringen, dann auf die ganze Welt übertragen werden. Es gibt also ein echtes Interesse daran, mit gleichgesinnten Demokratien zusammenzuarbeiten, um sicherzustellen, dass KI-Systeme die universellen Menschenrechte und demokratischen Grundsätze achten. Natürlich stehen auch nationale Interessen auf dem Spiel. Und natürlich garantieren die aktuellen Entwicklungen nicht, dass alle Nationen gleichermaßen

unterstützt werden. Es müssen Anstrengungen unternommen werden, um mit den Ländern zusammenzuarbeiten, die Regionen außerhalb der EU haben, um sicherzustellen, dass ganze Teile der Welt nicht zurückgelassen werden.

Glauben Sie, dass die Entwicklungen im Bereich der Künstlichen Intelligenz, die wir derzeit erleben, weit über die technologische Seite hinausgehen? Dass wir uns mitten in einer globalen Umgestaltung befinden?

Newman: Ich bin tatsächlich der Meinung, dass wir uns in einer kognitiven Revolution befinden. Ich glaube, dass wir in bestimmten Branchen bereits ein gewisses Maß an Kontrolle darüber verlieren, wie Algorithmen Menschen und Gesellschaften beeinflussen. Wir sehen das in den sozialen Medien und im Finanzwesen, wo es darum geht, eine sinnvolle menschliche Kontrolle aufrechtzuerhalten und menschliche Werte zu schützen, während die Interaktion zwischen Mensch und KI zunimmt. Technologie sollte für uns arbeiten und menschliche Interessen und Werte fördern.

In seinem Buch „Rule of the Robots: How Artificial Intelligence will transform everything“ beschreibt Martin Ford zwei mögliche Szenarien, wie unsere Zukunft mit KI aussehen könnte. Das eine nennt er das „Star-Trek“-Szenario: Die Menschen sind hoch gebildet, gehen Herausforderungen nach, die sie als lohnend empfinden, und werden für ihre intrinsische Menschlichkeit geschätzt. Das zweite ist viel düsterer und eine Anspielung auf „The Matrix“. Die reale Welt wird zu ungleich, und die Bevölkerung beschließt, in alternative Realitäten zu fliehen. Wie lautet Ihre Prognose?

Newman: Ich denke, wir nähern uns jetzt dem düsteren Szenario, in dem Ungleichheiten und Ungerechtigkeiten innerhalb der Länder und in der Welt erheblich zunehmen. Ich glaube, dass wir hier wirklich eingreifen müssen, um diese zukünftigen Entwicklungen in Richtung des ersten Szenarios zu verschieben, in dem die Menschen in der Lage sind, sich an lohnenden Aktivitäten zu beteiligen und ein sinnvolles Leben zu führen.

Mehr Transparenz in der IoT-Sicherheit

Wie das IT-Sicherheitskennzeichen die IoT-Security stärken kann

17.01.2022 | VON DIPL.-PHYS. OLIVER SCHONSCHEK

Hersteller und Anbieter können ihre IT-Produkte mit dem freiwilligen IT-Sicherheitskennzeichen des BSI auszeichnen. Eine technische Prüfung ist damit allerdings nicht verbunden, wie Kritiker betonen. Trotzdem kann das IT-Sicherheitskennzeichen viel bewirken, gerade im Internet of Things (IoT). Das Sicherheitsbewusstsein und die Transparenz im Markt können profitieren.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wird ein freiwilliges IT-Sicherheitskennzeichen einführen. Damit sollen Verbraucherinnen und Verbraucher die Möglichkeit erhalten, sich leichter über vom Hersteller zugesicherte Sicherheitsfunktionen von vernetzten, internetfähigen Produkten und Diensten zu informieren. (Symbolbild)

Mit dem IT-Sicherheitsgesetz 2.0 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Auftrag erhalten, ein freiwilliges IT-Sicherheitskennzeichen einzuführen. Damit sollen Verbraucherinnen und Verbraucher die Möglichkeit erhalten, sich leichter über vom Hersteller zugesicherte Sicherheitsfunktionen von vernetzten, internetfähigen Produkten und Diensten zu informieren.

Das IT-Sicherheitskennzeichen soll in Zukunft zum Beispiel auf den Verpackungen von Produkten aufgebracht sein. Das Etikett des IT-Sicherheitskennzeichens enthält dann einen Link und einen QR-Code, den Verbraucherinnen und Verbraucher scannen

können. Darüber gelangen sie auf eine Webseite des BSI mit aktuellen Sicherheitsinformationen zum Produkt, wie dieses Beispiel zeigt.

Offensichtlich steigt so die Transparenz, und das ist auch dringend notwendig: Während mehr und mehr Alltagsgegenstände mit dem Internet und mit anderen smarten Dingen vernetzt werden, ist es für Verbraucherinnen und Verbraucher immer schwieriger zu beurteilen, welche Geräte und Dienste welche Sicherheitseigenschaften besitzen, so das BSI.

Security by Design als Wettbewerbsvorteil

„Je häufiger das IT-Sicherheitskennzeichen genutzt wird, desto einfacher, schneller und breiter können wir wichtige Sicherheitsinformationen einzelner Geräte zu den Menschen bringen", so Arne Schönbohm, Präsident des BSI. „Unsere Informationen können dabei helfen, Sicherheitslücken in digitalen Alltagsgeräten schnell und zuverlässig zu schließen. Das IT-Sicherheitskennzeichen ist ein sichtbares Symbol für eine wichtige Botschaft: Informationssicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung!"

Die Idee dahinter ist, dass es für Hersteller und Anbieter immer interessanter wird, möglichst schon zu Beginn für Sicherheit zu sorgen und Schwachstellen so schnell wie möglich zu schließen. So erklärt das BSI: Herstellern bietet das IT-Sicherheitskennzeichen die Möglichkeit, über dieses zu kennzeichnen, dass ihre Produkte einschlägige IT-Sicherheitsstandards erfüllen. Dies kann ein Anreiz sein, bereits während der Entwicklungsphase neuer Produkte und Dienste wichtige Sicherheitsanforderungen zu berücksichtigen. Hersteller können damit das steigende Informationsbedürfnis der Verbraucherinnen und Verbraucher erfüllen und ihr Produkt am Markt hervorheben, da IT-Sicherheit bei der Kaufentscheidung eine Rolle spielt.

Keine Prüfung, aber Marktüberwachung

Zu Beginn muss der Antragsteller insbesondere eine Zusicherung darüber abgeben, dass er die zugrundeliegenden Anforderungen für sein Produkt oder seine Dienstleistung geprüft hat und diese erfüllt. Ist der Nachweis plausibel, erfolgt die Erteilung des IT-Sicherheitskennzeichens seitens BSI.

Das Fehlen einer Tiefenprüfung durch das BSI wurde bereits mehrfach kritisiert von Verbraucherschützern, Verbänden und Wirtschaftsvertretern.

Auch wenn es die Vorabprüfung nicht gibt, so ist doch eine Aufsicht vorgesehen: Nach der Erteilung des IT-Sicherheitskennzeichens überprüft die durch das IT SiG 2.0 ermöglichte BSI-Marktaufsicht am Standort Freital anlasslos (z. B. durch Stichproben) die Einhaltung der Anforderungen bei einzelnen Produkten. Bei Bekanntwerden von Schwachstellen in Produkten mit Sicherheitskennzeichen prüft das BSI die Informationen, setzt sich mit dem Hersteller in Verbindung und stellt entsprechende Informationen für die Verbraucherinnen und Verbraucher auf der zum Kennzeichen gehörigen Internetseite zur Verfügung.

Folgen für die Sicherheit, gerade im IoT

Bislang können Anträge für IT-Sicherheitskennzeichen in den Kategorien Breitbandrouter und E-Mail-Dienste gestellt werden. Das BSI plant zeitnah, das IT-Sicherheitskennzeichen für weitere Kategorien zu öffnen. Man erwartet, dass dies dann auch Bereiche wie Smart Home umfassen wird.

Das IT-Sicherheitskennzeichen ist zwar freiwillig und auch kein Zertifikat oder Gütesiegel, das nach einer unabhängigen Prüfung verliehen wird. Trotzdem kann es einiges für die Sicherheit erreichen, gerade bei IoT, da es dort zum einen bisher eher schlecht um die Sicherheit vieler Geräte bestellt ist, die Anwenderinnen und Anwender sich der Risiken nicht bewusst sind und die Absicherung im IoT durchaus komplex ist.

Zudem kann eine steigende Transparenz für die Sicherheit bei Verbraucherprodukten im IoT auch der IoT-Sicherheit in Unternehmen helfen, nicht nur, weil auch private IoT-Geräte zum betrieblichen Risiko werden können. Man denke nur an Home-Office in Verbindung mit Smart-Home-Produkten.

Es ist aber auch generell zu erwarten, dass eine Zunahme an Transparenz die Erwartungen der Nutzer an IoT-Sicherheit erhöht, dass sich Anwenderinnen und Anwender zunehmend für die Sicherheitseigenschaften von IoT-Lösungen interessieren, privat wie beruflich, und dass die Hersteller erkennen, dass der Markt zunehmend nach Sicherheitsinformationen verlangt.

Wenn aber mehr Transparenz in der IoT-Sicherheit entsteht, bildet sich auch ein Druck auf die Umsetzung von Sicherheitsmaßnahmen, denn welcher Anbieter oder Hersteller will schon mit Schwachstellen in der Öffentlichkeit „glänzen“.

Der Bedarf an Sicherheitsinformationen und deren Bedeutung auf dem Markt können schließlich den Weg ebnen für wirkliche IoT-Sicherheitssiegel, auf Basis von vorherigen, unabhängigen

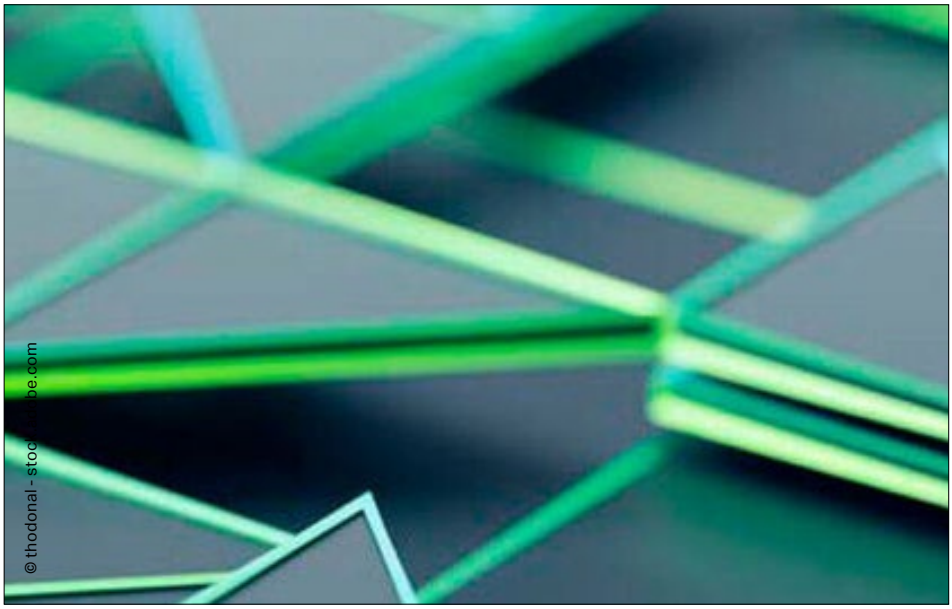
Tiefenprüfungen. Wie in anderen IT-Bereichen werden Zertifizierungen auch im IoT an Bedeutung gewinnen. Das IT-Sicherheitskennzeichen kann dabei durchaus als ein Wegbereiter gesehen werden.

Make or Buy

KI-Projekte sind selten allein zu schaffen

14.02.2022 | VON LIC.RER.PUBL. ARIANE RÜDIGER

Bei Projekten rund um Machine Learning (ML) und Künstlicher Intelligenz (KI) stellt sich die Frage, wie viel Unternehmen selbst entwickeln wollen und wo sie externe Hilfe zuziehen. Die Entscheidung darüber ist vielschichtig. Eine strukturierte Herangehensweise kann helfen.



Blockchains haben klare Vorteile gegenüber Datenbanken. Sie gelten als unveränderlich, weitgehend fälschungsresistent und beinahe unvernichtbar.

KI-Projekte unterscheiden sich von anderen Softwarevorhaben in verschiedenen Bereichen und so auch die nötigen Make-or-Buy-Entscheidungen. Ein Papier der Initiative for Applied Artificial Intelligence, entstanden an dem Entrepreneur-Zweig der TU München, UnternehmerTUM, befasst sich mit Inhalten und Struktur solcher Entscheidungsprozesse.

Die Autoren empfehlen, Projekte zunächst nach strategischem Wert und „unfairem Vorteil“ zu klassifizieren. Letzteres sind unternehmensspezifische Skills und Daten, die andere nicht haben. Projekte, die beide Konditionen erfüllen, sollten unbedingt selbst gemacht werden, Projekte, die keine der beiden Bedingungen erfüllen, möglicherweise eingestellt werden.

Die beiden übrigen Fälle – also entweder hoher strategischer Wert, aber fehlende Skills respektive Daten oder aber Skills und

Daten vorhanden, strategischer Wert unsicher – erfordern weitergehende Erwägungen.

Drei Herangehensweisen

Grundsätzlich sind drei Herangehensweisen an Make-or-Buy denkbar: Die komplette Eigenentwicklung einschließlich Inhouse-Training des ML-Modells ist sehr aufwendig. Hybride Projekte verwenden vortrainierte ML-Modelle oder weitergehende Module, wie sie etwa AWS oder Google anbieten und kombinieren sie mit eigenen Entwicklungsanstrengungen. Schließlich ist auch der externe Einkauf kompletter KI-Applikationen möglich. Hier stellt sich allerdings die Integrationsfrage.

In KI-Projekten sind vier verschiedene Ebenen zu berücksichtigen, die jeweils eigene Make-or-Buy-Entscheidungen erfordern: Die Infrastrukturebene umfasst Systeme und Prozesse für Entwicklung, Training, Bereitstellung und Wartung von KI-Applikationen. Die Daten-Ebene beschreibt die vorhandenen oder benötigten Daten und deren möglichen Quellen einschließlich Zukauf oder synthetischer Generierung.

Die Ebene der ML-Fähigkeiten umfasst die grundlegenden Funktionen von KI/ML-Produkten, nämlich künstliches Sehen, Hören, Sprachverstehen und Bewegen sowie die Fähigkeit zur Entdeckung (z. B. von Zusammenhängen), Suchen und Planen, Prognostizieren und Neues erschaffen. Je nach Projekt werden von ihnen nur einige benötigt. Falls das Unternehmen sie nicht selbst hat, muss dafür ein Lieferant gefunden werden.

Die oberste Ebene bildet die konkrete Applikation, mag sie nun für die Anwender sichtbar sein oder nicht. Applikationen basieren auf den Ressourcen der drei unteren Ebenen.

Sechs Faktoren

Ob gekauft oder selbst entwickelt wird, wird bei jeder einzelnen Make-or-Buy-Entscheidung von sechs Faktoren beeinflusst:

Wie groß sind der Wettbewerbs- und der strategische Vorteil des Projekts (Effizienzgewinne, Kostensenkungen, neue Funktionen ...)?

Wie wichtig ist die Kontrolle des ML-Modells (z. B. Lock-in-Risiken, regulatorische Anforderungen)?

Wie viel kann das Unternehmen aus dem Projekt zum eigenen Nutzen lernen?

Werden in dem Projekt Ressourcen (Daten oder Fähigkeiten) eingesetzt, die das eigene Unternehmen signifikant von Wettbewerbern unterscheiden?

Wie leistungsfähig sind langfristig und in Bezug auf die eigenen Projektziele die ins Auge gefassten Lösungen externer Lieferanten?

Welche Kosten entstehen bei den verschiedenen Erbringungsvarianten?

In jeder Phase des Produktlebenszyklus müssen diese Entscheidungen von Neuem getroffen werden, allerdings sind sie je nach Phase von unterschiedlicher Relevanz. So kann die Ideenfindung am ehesten in kompletter Eigenregie durchgeführt werden – allerdings sollte man durchaus im Auge behalten, ob es vielleicht bereits ein fertiges ML-Produkt für den angestrebten Zweck gibt. Dies gilt auch für den PoC, denn ein bereits vorhandenes Tool kann hier ein wichtiges Zeichen für grundsätzliche Machbarkeit sein. Außerdem sollte man mögliche Lerneffekte mit in die Überlegungen einbeziehen. Sie können mangelnden Praxisnutzen teils kompensieren.

Dem Einsatz näher sind die Erstellung eines Minimalprodukts (Minimum Viable Produkt, MVP) und schließlich die Skalierung des Produkts. In der MVP-Phase kann eine am Markt erhältliche Lösungsalternative die Entscheidung erleichtern. Für die Skalierung ist die Make-or-Buy-Frage am wichtigsten. Dabei müssen vor allem die langfristigen Kosten möglicher Alternativen berücksichtigt werden.

Wie man bei der Skalierung vorgeht, um eine Make-or-Buy-Entscheidung zu treffen, hängt davon ab, wie strategisch wertvoll ein Projekt ist. Projekte mit geringem strategischen Wert sollten möglichst irgendwie an strategisch bedeutende Projekte angebunden werden, statt Ressourcen dort zu investieren.

Ist ein Projekt ausreichend hoch bewertet, sollte man entscheiden, ob das Unternehmen das ML-Modell selbst besitzen sollte, etwa, um wichtiges Wissen im Haus zu behalten. Wird das bejaht, hängt der Grad der eigenen Entwicklungsanstrengungen vor allem vom Vorhandensein eigener Daten- und Fähigkeitsressourcen sowie den Kosten ab. Je nachdem kommen eine komplette Eigenentwicklung, eine hybride Entwicklung oder aber auch die Nutzung einer externen Anwendung in Betracht, wenn sonst die Kostennachteile zu groß werden.

Partner auch bei Eigenerstellung

Auch bei Eigenerstellung braucht man meist Partner, zum Beispiel interne, mit denen man sich vorhandene KI-Ressourcen teilt. Sogar externe Entwickler (Freelancer) oder Forschungsinstitutionen werden in solche Projekte öfter einbezogen. Bei Externen ist auf die Sicherung des geistigen Eigentums zu achten. Akademische Forschung arbeitet häufig noch weit entfernt von der Praxisreife. Hier müssen besonders klare Vereinbarungen darüber getroffen werden, wem welche Ergebnisse am Ende zustehen.

Wer Hybrid- oder externe Erstellung vorzieht, arbeitet meist mit anderen Arten von Partnern zusammen. Beispielsweise mit Cloud-Providern, die KI-Tools oder -Prozessketten bereithalten. Fragen des Dateneigentums und der Integration von Lösungen in die eigene Infrastruktur können dabei Probleme aufwerfen.

Weitere wichtige Partner sind Start-ups, die eventuell auch als strategische Ressource übernommen werden können, größere Lösungsprovider und Integratoren sowie Lieferanten von Software, die sich in die eigenen Produkte einbetten lässt.

Alle Lieferanten sollten sorgfältig qualifiziert werden. Dabei kommt es in der PoC- und MVP-Phase vor allem auf die Beherrschung und Qualitätssicherung von Werkzeugen, ausreichende Versicherungen und Dokumentation an. In der Skalierungsphase sind darüber hinaus ausreichende Hardwareressourcen, Wartungsprozesse und -werkzeuge, Zertifikate, ein sicherer Umgang mit den Daten sowie eine geordnete Übergabe- und Trainingsphase bei der Auswahl zu berücksichtigen.

Benchmarks sind nur eingeschränkt aussagefähig

Benchmarks zur Bewertung basieren meist auf der Verarbeitung generischer Daten und sind daher nur eingeschränkt aussagefähig. Bei externen Lösungen ist unter Umständen ihr Entwicklungspotenzial etwa in Gestalt einer klaren Roadmap wichtiger als die aktuelle Leistung. Schließlich sollte man einen Vendor-Lock-in-vermeiden, beispielsweise, indem man das verwendete Modell mit eigenen Daten trainiert oder die Übertragbarkeit des Modells sicherstellt. Wird das alles berücksichtigt, können durchaus lang andauernde und tiefgehende Partnerschaften zwischen KI-Anwendern und KI-Lieferanten entstehen.

Am Ende der Partnersuche steht meist ein Vertrag. Er sollte in der Regel fünf Themen umfassen: die Datenbeschaffung, die Parameter einer Machbarkeitsstudie, eine Rentabilitätsberechnung, die

gewünschte Qualität und den gewünschten Umfang des Projekts und schließlich seine Integration in die übrige IT-Umgebung.

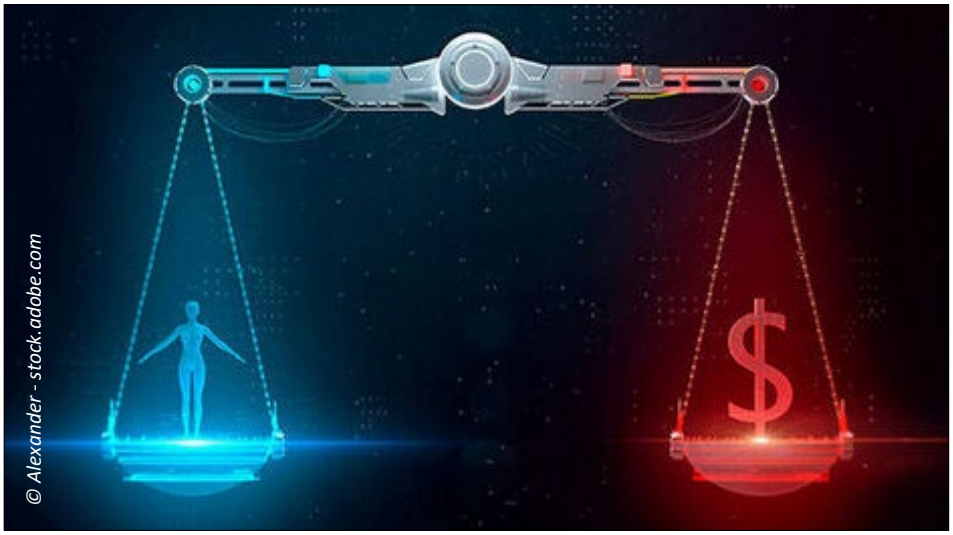
Außerdem sollten geeignete Leistungsmaßstäbe für das abgeschlossene Entwicklungsprojekt definiert und festgelegt werden, mit welchen Methoden diese zu messen sind. Weiter ist zu regeln, wer auf die Trainingsdaten Zugriff bekommt oder wie man den generierten Wert verteilt. Dazu gehört auch das Recht, unter bestimmten Bedingungen geistige Eigentumsrechte an Modellen und Daten herauszukaufen. Schließlich sollten die Aspekte Datenschutz und Risikoverteilung sowie Risikoprävention im Vertrag geregelt sein.

Künstliche Intelligenz und Ethik

Digitale Ethik mithilfe von KI-Werkzeugen realisieren

14.03.2022 VON MICHAEL MATZER

KI-Modelle, die Entscheidungen unterstützen oder gar automatisch ausführen, müssen nach ethischen Prinzipien fungieren. Doch beim Trainieren der Modelle tritt immer wieder einseitige, unfaire Voreingenommenheit auf. Während also KI-basierte Entscheidungen Erfolg haben werden, sind Werkzeuge nötig, die für die Fairness, Transparenz und Erklärbarkeit der KI-Modelle sorgen. Der Artificial-Intelligence-Act der EU soll künftig den rechtlichen Rahmen dafür bereitstellen.



Die EU will dafür sorgen, dass zumindest grundlegende Standards für die Qualität und Anwendung von KI-Algorithmen eingehalten werden.

Im September 2020 führte ein Data Scientist ein Experiment mit dem Twitter-Algorithmus aus, der die Anzeige größerer Bilder steuerte. Twitter fokussiert stets auf den relevantesten Teil eines Bildes. In einem Foto, das einen Demonstranten mit einem Plakat zeigt, auf dem ein Slogan steht, wird Twitter in der Vorschau voraussichtlich auf den Slogan fokussieren.

Das Experiment ging anders vor, denn Twitter wurde vor eine Wahl gestellt. Es sollte zwischen einem prominenten weißen US-Politiker und dem prominentesten schwarzen Politiker, nämlich Barack Obama, wählen. Die Bezeichnung „der relevanteste Politiker“ war nicht durch die Krawattenfarbe festgelegt, sondern durch die Hautfarbe. Twitter musste eingestehen, dass das Unternehmen beim Testen des Algorithmus nicht genügend auf mög-

liche Voreingenommenheiten (bias) geachtet hatte. Das fing bereits in der Datenmenge an, die für das Training des KI-Modells verwendet worden war: viel mehr weiße als schwarze Männer, von Frauen ganz zu schweigen.

Apropos: Auch bei der Gleichbehandlung der Geschlechter neigte ein Google-Algorithmus dazu, einfach Stereotypen zu übersetzen, falls das grammatische bzw. natürliche Geschlecht sowohl männlich als auch weiblich sein konnte. In der türkischen Sprache etwa wird grammatisch gar nicht nach weiblich oder männlich unterschieden. Beide Versionen wären also korrekte Übersetzungen. Doch Google zeigte auch hier seine Voreingenommenheit: Ein „doctor" war – vor der Änderung des Algorithmus – stets männlich.

Diese Befunde sind alles andere als trivial, sondern werden die künftige IT-Nutzung vieler Endkunden, Organisationen, Politiker und Unternehmen beeinflussen. Die Gesamtheit dieser Phänomene nennt Michael O'Connell, Chief Analytics Officer beim Softwarehersteller Tibco „Digitale KI-Ethik". Er ist dieser Entwicklung gegenüber positiv eingestellt: „Politische Themen wie die Regulierung sozialer Plattformen hinsichtlich Falschmeldungen, Hassbotschaften und die Rekrutierung von Terroristen, werden üblicherweise durch eine ethische Brille betrachtet und führen zu Forderungen nach einer verantwortungsvollen, fairen, transparenten und haftbaren KI." Parlamente beraten über solche Maßnahmen ebenso wie über Autonomes Fahren und medizinische Implantate, die KI-gesteuert sind.

O'Connell kommt zu der Prognose: „Wir werden 2022 mehr KI-Start-ups sehen, die auf ethische KI und Tools fokussiert sein werden. Damit werden sich KI-Anwendungen regulieren lassen, indem sie Industriestandards wie die der Robotics Industry Association (RIA) und des IEEE folgen." Während so mancher der Meinung sei, dass dies die Innovationsfähigkeit einschränken werde, so erwartet O'Connell „eher einen gegenteiligen Effekt: Ethische KI wird in dem Maße zu besseren Datenerkenntnissen führen, wie Unternehmen dafür sorgen müssen, dass alle von Daten gespeiste Algorithmen, ohne diskriminierende Verzerrungen in den Ergebnissen, vertrauenswürdig und sauber sind."

Die europäische Gesetzgebung will dafür sorgen, dass zumindest die grundlegenden Standards für die Qualität und Anwendung von KI-Algorithmen eingehalten werden. Die EU-Kommission definiert im Entwurf des Artificial Intelligence Act vom April 2021 in erster Linie, welche Gefahren durch „legale" KI von den An-

wendern abgewendet werden sollen. Es gibt vier Kategorien von Gefahren: verbotene Anwendungen, Hochrisiko-Anwendungen, Anwendungen mit bestimmten Merkmalen und sonstige Anwendungen. Die größte Gefahr gilt dem Leben, der Unversehrtheit und der Gesundheit von EU-Bürgern. Der Entwurf, der vom EU-Parlament debattiert werden muss, sieht bei Verstößen gravierende Rechtsfolgen vor, wie sie schon in der DSGVO zu sehen sind.

Verschiedene Institute und Organisationen haben den AI Act Entwurf bereits analysiert und kommentiert. Während sie die Absicht begrüßen, finden sie doch Lücken und Unzulänglichkeiten. Das Future of Life Institute sieht das Risiko, dass Einschränkungen, die nur auf individueller Ebene unterdrückt werden, auf gesamtgesellschaftlicher Ebene dennoch verheerende Auswirkungen haben können, so etwa dann, wenn es um demokratische Wahlverfahren geht.
Das „Leverhulme Centre for the Future of Intelligence“ und „Centre for the Study of Existential Risk“, zwei Institute der Universität Cambridge, empfehlen eine erhöhte Flexibilität der Regulierung. Und Access Now Europe, eine Organisation, die bedrohte digitale Rechte von Usern verteidigt und erweitert, sagt gar das Versagen des vorgelegten Gesetzes vor, wenn es um die Grundrechte der Bürger geht. Diese Grundrechte würden bei biometrischen Anwendungen wie Gefühlserkennung und KI-gestützten Lügendetektoren berührt. Transparenz bei deren Einsatz reiche nicht, sondern es müssten Verbote her.

IBM AI Fairness 360

In einem IBM-Werkzeug namens „AI Fairness 360“ hat IBM Research eine umfassende Bibliothek zum Aufzeigen und Herausrechnen von „Bias“ bereitgestellt, also von einer potentiellen Voreingenommenheit in datenbasierten Entscheidungssystemen. Diese Open-Source-Bibliothek kann von jedem Entwickler verwendet und erweitert werden.
Im nächsten Schritt müssen die Designer fragen, wie sie ihre Black Box „öffnen“ und erklären können. Nach IBM-Angaben kommen hier diverse Programme und Services als auch Verfahren zum Einsatz. Dazu kann auch Watson OpenScale gehören, ein Monitoring-Werkzeug, mit dem sich KI-Lösungen nicht nur in Bezug auf ihre Zuverlässigkeit, sondern hinsichtlich ihrer Unvoreingenommenheit überwachen und generell nachvollziehen lassen. Hier wird KI erklärbar gemacht und die Black Box des KI-Modells verschwindet.

Zu guter Letzt wird die fertige Lösung zusammen mit dem Kunden beurteilt. Löst sie überhaupt das gegebene Problem? Ist sie vertrauenswürdig und ihre Ergebnisse nachvollziehbar? In der anschließenden Projektphase versuchen die Entwickler, die Fehlerrate eines KI-Modells zu senken. Sie eliminieren unerwünschte Einflussfaktoren auf das Modell und versuchen, gegebene Vorhersagen noch besser erklärbar zu machen.

SAS

Die Analytics-Plattform SAS Viya unterstützt Advanced Analytics mit Frameworks wie PD (Partial Dependence), LIME (Local Interpretable Model-Agnostic Explanations) und ICE (Individual Conditional Expectation). Diese Features sollen die Transparenz für Unternehmen herstellen, die KI-gestützte Applikationen einführen wollen. In der Viya-Version 3.4 sollen die drei genannten Frameworks die Erklärbarkeit der KI-Blackbox erleichtern. In einem Blogbeitrag erklärt ein SAS-Manager den theoretischen Hintergrund für die Thematik.

Amazon SageMaker Clarify

Mit dem Feature Clarify in seinem ML-Service Amazon SageMaker bietet Amazon Web Services (AWS) mehrere Methoden, um im Machine Learning Voreingenommenheit und Einseitigkeit in den Trainingsdaten festzustellen und zu beseitigen. Clarify ist mit der Entwicklungsumgebung SageMaker Studio integriert. Auch Amazon SageMaker Data Wrangler, Amazon SageMaker Experiments und Amazon SageMaker Model Monitor lassen sich ankoppeln.

„Data Scientists können damit Verzerrungen vor und nach dem Training des Modells entdecken und etwaige Voreingenommenheit begrenzen, sowie Vorhersagen besser erklären“, erklärt Constantin Gonzalez, Principal Solutions Architect bei AWS. Mithilfe einer Reihe statistischer Metriken können sie das Ausmaß des Bias messen und bestimmen. Das ist besonders wichtig, wenn so manchem Betrachter die „kleinen Unterschiede“ unerheblich scheinen sollten. Anschließend kann der Data Scientist erklären, wie bestimmte Werte zum vorhergesagten Ergebnis beitragen werden, und zwar sowohl im Gesamtmodell als auch für einzelne Vorhersagen. Gonzalez ergänzt: „Weil sich damit über den gesamten ML-Workflow hinweg Bias-Effekte erkennen lassen, können die Entwickler letztlich mehr Transparenz und Fairness in ihre ML-Modelle einbauen.“

Ein Aspekt, der unterschätzt wird, wird von Amazon SageMaker Model Monitor aufgedeckt, und zwar das Phänomen, dass im Laufe der Zeit der Bias und die Gewichtung der Faktoren „wandern". Diese – zunächst nur unmerkliche – Drift lässt sich schwer feststellen, kann sich aber Jahre später in ihren Auswirkungen umso negativer bemerkbar machen. „Auch wenn Ihre ursprünglichen Daten oder Ihr Modell nicht verzerrt waren, können Veränderungen in der Welt zu Abweichungen in einem bereits trainierten Modell führen", erläutert Gonzalez weiter. „So könnte beispielsweise eine wesentliche Änderung der demografischen Merkmale von Hauskäufern dazu führen, dass ein Modell zur Beantragung eines Hauskredits verzerrt wird, wenn bestimmte Gruppen in den ursprünglichen Trainingsdaten nicht vorhanden oder nicht genau repräsentiert waren." Ähnliches könnte bei Prä-Covid- und Covid-Daten auftreten.

In einem englischsprachigen Blog demonstriert AWS, wie sich die verschiedenen Tools nutzen lassen, um Verzerrungen aufzuspüren und die Transparenz des KI-Modells zu erhöhen.

Anwender

„Bundesliga Match Facts, powered by AWS", bietet Bundesliga-Fans auf der ganzen Welt ein besseres Fan-Erlebnis bei Fußballspielen. „Mit diesen live aus den offiziellen Daten der Bundesliga-Spiele ermittelten Statistiken erhalten Zuschauer detaillierte Einblicke in das Spielgeschehen", erklärt Gonzalez. Mit Amazon SageMaker Clarify kann die Bundesliga nun interaktiv erklären, was einige der wichtigsten, zugrunde liegenden Komponenten sind, die das ML-Modell dazu veranlasst haben, beispielsweise einen bestimmten „xGoals"-Wert vorherzusagen. Die Kenntnis der jeweiligen Merkmalszuordnungen und der erklärenden Ergebnisse hilft den Verantwortlichen bei der Modellfehlersuche und erhöht das Vertrauen in ML-Algorithmen, was zu qualitativ hochwertigeren Prognosen führt.

Die Varo Bank ist eine digitale Bank mit Sitz in den USA. Sie nutzt KI/ML, um schnelle, risikobasierte Entscheidungen zu treffen und ihren Kunden innovative Produkte und Dienstleistungen anzubieten. „Varo", sagt Sachin Shetty, Head of Data Science, Varo Money, „setzt sich stark für die Erklärbarkeit und Transparenz unserer ML-Modelle ein, und wir sind gespannt auf die Ergebnisse von Amazon Sagemaker Clarify, um diese Bemühungen voranzutreiben." In den USA sind beispielsweise die beiden Gesetze „Equal Credit Opportunity Act" (ECOA) und der „Fairness in Housing Act" zu beachten.

Bei der Betrugserkennung spielen KI-Algorithmen bereits eine wichtige Rolle. Für digitale Banken ist Betrugserkennung umso bedeutsamer. „Zopa ist eine in Großbritannien ansässige digitale Bank und ein Peer-to-Peer-Kreditgeber“, erklärt Jiahang Zhong, Head of Data Science. „Bei unseren ML-Anwendungen, wie etwa unserer Anwendung zur Betrugserkennung, ist es für uns wichtig zu verstehen, wie jeder Faktor zur Entscheidung des Modells beiträgt. Der Einblick in die Logik des Modells schafft Vertrauen bei unseren internen und externen Stakeholdern. Außerdem hilft es unserem operativen Team, schneller zu reagieren und unseren Kunden einen besseren Service zu bieten. Mit Amazon SageMaker Clarify können wir jetzt schneller und nahtloser Modellerklärungen erstellen.“

Kommentar von Christian Schreiner, Eoda

Model Drift – Hintergründe und Empfehlungen

18.03.2022 VON CHRISTIAN SCHREINER

Digitalisierte Unternehmen stehen oft vor bestimmten Herausforderungen: Dienste, wie Absatzprognosen, Nutzerverhalten, Automatisierungen oder andere Vorhersagen, die vorher zuverlässig funktionierten, werden mit der Zeit immer ungenauer oder unzuverlässiger.

Der Autor: Christian Schreiner ist Marketing Manager bei Eoda

Die „Schuld“ ist dabei nicht bei den Entwicklern der Modelle zu suchen, sondern liegt in der Natur der Sache: Die Daten, die Ziele der Modelle und wir Menschen verändern uns. Dieses Phänomen wird „Model Drift“ genannt und äußert sich auf unterschiedliche Weise. Die Folgen sind z. B. erhöhte Kosten durch falsche Schlussfolgerungen bei Kampagnenplanungen oder durch Ausfälle von automatisierten Diensten. Eine mögliche „Lösung“ mag in verschiedenen Workarounds gefunden werden – oder aber darin, den Umstand zähneknirschend zu akzeptieren.

Aber selbst ein funktionierender Workaround ist auf Dauer teurer als die eigentliche Behebung des Problems. Solche Workarounds sind nämlich oft umständlich, mit höherem Arbeitsaufwand verbunden oder nur symptomatisch erfolgreich. Daher ist es sinn-

voll, Ursachen und Auswirkungen zu identifizieren, bevor es zu kritischen Problemen kommt.

Model Drifts – warum man sich damit auseinandersetzen sollte

Es gibt verschiedene Arten von Drifts, die sich in der Ursache und den Auswirkungen unterscheiden. Drei davon werden wir näher beleuchten und auch, welche Maßnahmen sich empfehlen. Die folgenden Beispiele sollen einen kurzen Überblick geben, wie sich Drifts äußern können und wodurch sie bedingt werden. Der Verständlichkeit wegen werden sie nicht in aller Detailtiefe dargestellt.

Concept Drift

Bei einem Concept Drift verändern sich die statistischen Eigenschaften der Ziele. Das kann durch eine plötzliche Änderung der Gesamtsituation erfolgen, aber auch z. B. durch die Einführung neuer Technologien und/oder Trends, wie Modegeschmack oder gesellschaftlicher Art. Beispiele:

Online-Marketing – Ist meine Werbung für die Zielgruppe relevant?

In einem Social-Media-Netzwerk wird eine bestimmte Zielgruppe innerhalb der Nutzer definiert. Nehmen wir an, dass u. a. die Online-Zeit innerhalb des Netzwerks ein Kriterium für das Engagement der Nutzer widerspiegelt. Je länger die Nutzer sich auf der Plattform bewegen, desto wahrscheinlicher ist es, dass sie die gewünschte Werbeeinblendung sehen. Waren zu Beginn des Social-Media-Netzwerkes vermehrt die jüngere Generation, z. B. 14 bis 20 Jahre, in der Nutzerpopulation vertreten, wurden diesen entsprechende Mode-Anzeigen ausgespielt. Altert nun die Population, z. B. durch Abwanderung oder im Laufe der Zeit, werden älteren Nutzern weiterhin die entsprechenden Anzeigen ausgespielt – wobei diese für diese Zielgruppe nicht relevant sind.

Data Drift

Hierbei ändern sich die Eigenschaften bzw. die Verteilung der unabhängigen Variablen innerhalb der Datenpopulation. Das kann auch durch o. g. Trends erfolgen, ist aber oft durch eine

grundlegende Änderung zu erklären, z. B. bei der Einführung neuer Variablen. Beispiel:

Retail – Funktionieren die Aktionsgeschäfte?

Ein einfaches Beispiel ist das Kaufverhalten vor und während der aktuellen Corona-Pandemie. Deutlich wird der Concept Drift beim sprunghaften Anstieg des Absatzes für Nudeln und Toilettenpapier im 2. Quartal 2020 – eine Entwicklung, die weder die Experten noch entsprechende Modelle vorhersagen konnten.

Vorsicht: Nutzt man Daten extremer Situationen zum Training von Modellen, kann dies ebenfalls zu Drifts führen. Beim o. g. Beispiel könnte eine direkte Korrelation beider Produkte im 2. Quartal als mögliches Aktionsgeschäft identifiziert werden.

Drifts aufgrund vorgelagerter Datenänderungen

Ursachen betreffen hier Änderungen in der Infrastruktur und/oder der Datenpipelines. Neue Technologien, aber auch Optimierung können dazu führen, dass Modelle nicht mehr ordnungsgemäß funktionieren. Das kann darin liegen, dass bestimmte Messwerte wegfallen, weil z. B. Sensoren nicht mehr verbaut sind oder bestimmte Datenquellen nicht mehr einbezogen werden. Die Grenze zwischen Concept und Data Drift verläuft in diesem Fall fließend.

Umsetzen eines Drift-Aware-Systems

Zum Entgegenwirken von Drifts braucht es ein System zur Erkennung dieser. Es kombiniert idealerweise verschiedene Methoden zur Identifikation und bietet eine Möglichkeit der Einflussnahme auf die entsprechenden Modelle.

Monitoring

Dauerhaftes oder periodisches Beobachten der Genauigkeit der Modellergebnisse ist der erste Schritt. Je schneller Abweichungen erkannt werden, desto schneller können sie behoben werden. Oft reicht eine bloße Visualisierung in einem Dashboard aus, um die Ursache zu identifizieren. Dazu vergleicht man aktuelle Modellergebnisse mit denen von Test- oder initialen Trainingsdaten. So

lassen sich erste Anhaltspunkte finden, welche Art von Drift(s) und welche Ursachen vorliegen könnten: In welcher Form äußert sich der Drift? Gibt es plötzliche, graduelle oder wiederkehrende Änderungen?

Nicht alle Business-Intelligence-Lösungen bieten standardmäßig entsprechende Dashboards. Daher wird oft, neben Lösungen zur Modellausführung, zu zusätzlichen Lösungen gegriffen, um diese umzusetzen. Diese haben meist ihre eigenen Anforderungen, wodurch der Gesamtwartungsaufwand des Systems erhöht wird.

Daher findet aktuell der Schritt zur Integration solcher Lösungen im BI-Umfeld statt. Noch sinnvoller sind jedoch moderne Plattformen, wie YUNA, die neben BI-Funktionen auch zentrale Funktionen zur Modellentwicklung, -ausführung und -steuerung bieten und die Möglichkeiten solche Dashboards bereitzustellen.

In YUNA kann ein solches Monitoring-Dashboard, neben einer reinen Visualisierung, zusätzlich mit einem „DataLabeling"-Widget genutzt werden, welches Visualisierungen direkt kommentieren bzw. das Ergebnis zu kategorisieren lässt. Diese Informationen werden dann an Data Scientists automatisch weiterleitet. So können End User mit ihrer Erfahrung, auch ohne Data-Science-Hintergrund, den Ergebnissen direkt das Label „tatsächlicher Drift" oder bspw. „einmalige Anomalie" zuordnen und so Nachbesserungen anstoßen. Anschließend wird das Modell durch die Data Scientists entsprechend angepasst.

Das Modell anpassen

Je nach Ursache des Model Drifts wird ein neues Modell entwickelt oder es müssen evtl. neue Daten miteinbezogen sowie die genutzten Daten und das Modell modifiziert werden (Retraining & Resampling). Dabei empfiehlt es sich Folgendes zu beachten und abzuschätzen:

1. Anpassung der Datenpipeline

ETL-Pipelines müssen angepasst oder erweitert werden, um evtl. neue Datenquellen zu nutzen oder die aktuellen Daten entsprechend vorzubereiten.

2. Entwicklung eines neuen Modells

Abhängig von der Komplexität des Modells oder der vorhandenen Strukturen, ist ein neuer Ansatz ein probates Mittel. Hierbei kann ein Data Labeling notwendig sein. Dieser Prozess ist

zeitaufwendig und kann vereinfacht werden: Mit dem zuvor angesprochenen Widget können ebenfalls End User beim eigentlichen Data Labeling unterstützen.

3. Retraining & Resampling bestehender Modelle

Modell wird mit einem neuen Trainingsdatensatz oder der Aktualisierung bzw. Neugewichtung der initialen Daten erneut trainiert. Danach werden die neuen Ergebnisse mit der Realität verglichen.

4. Teilweise Nutzung des Modells – Zusammenarbeit zwischen Modell und Mensch

Wenn das Modell in einem Teilbereich nicht verlässlichen funktioniert, können End User zur Genauigkeit beitragen, z. B. durch eine manuelle Eingabe. Hier braucht es Lösungen wie YUNA, die eben jene Eingabe erlauben. Die Eingabe wird dann genutzt, um Modelle durch Active Learning zu optimieren.

Vorsicht: Auch wenn das aktualisierte Modell erwartungsgemäß funktioniert, können Model Drifts erneut auftreten. Daher empfiehlt es sich die o.g. Schritte entweder

- **Regelmäßig** oder
- **Anhand festgesetzter Grenzwerte**

durchzuführen.

Feintuning

Um die Genauigkeit zu erhöhen und mögliche Ursachen schneller zu identifizieren, kann es hilfreich sein, bestimmte Modellparameter anzupassen:

- Konsequente Nutzung von Zeitstempeln! So lässt sich der Zeitpunkt, an dem das Modell und die Realität auseinanderdriften, leichter identifizieren – das verkürzt die Suche nach der Ursache.
- Wenn Modelle in Teilbereichen besser funktionieren, kann der Vorhersagezeitraum geändert werden, z. B. von monatlich auf wöchentlich.
- Warten, weil die neue Datenbasis noch nicht ausreicht, um verlässliche Ergebnisse zu liefern.

Idealerweise lassen sich alle notwendigen Schritte in einer Lösung umsetzen. Auf diese Weise verringern sich nicht nur die

Fehleranfälligkeit und Wartungskosten, sondern auch die Reaktionszeit an sich.

Fazit

- Nichts tun ist immer mit höheren Kosten verbunden.
- Die Genauigkeit von Modellen kann mit der Zeit, als natürlicher Prozess, erneut nachlassen.
- Die Ursachen können vielfältig sein.
- Mittels Monitoring und Retraining lassen sich Model Drifts beheben.
- Es lohnt sich Softwarelösungen zu nutzen, die mit einem vollumfänglichen Funktionsumfang Dashboarding, BI-Funktionen, Visualisierung und Modellverwaltung unterstützen.

Künstliche Intelligenz und Compliance

Was die Datenschützer zur Haftung bei KI sagen

02.05.2022 | VON DIPL.-PHYS. OLIVER SCHONSCHEK

Trifft eine KI eine falsche Entscheidung, kann schon heute ein Schadensfall eintreten. In Zukunft ist die Frage, wer dann in der Haftung ist, noch weitaus wichtiger. Auch der Datenschutz hat sich mit der Frage nach der Haftung bei KI befasst. So hat sich dazu kürzlich der Europäische Datenschutzausschuss (EDSA) zu Wort gemeldet, mit spannenden Aussagen.

Der Europäische Datenschutzausschuss (EDSA) befasst sich auch mit Fragen der Haftung bei KI.

Unternehmen setzen eine große Hoffnung auf KI, wie zum Beispiel eine Umfrage des Digitalverbands Bitkom zeigt. So erwarten 44 Prozent schnellere und präzisere Problemanalysen durch KI, 35 Prozent beschleunigte Prozesse und 30 Prozent einen geringeren Ressourcenverbrauch, wovon auch die Umwelt profitieren würde. Auch mit Blick auf die Beschäftigten bietet KI viele Vorteile. 39 Prozent rechnen mit der Vermeidung menschlicher Fehler im Arbeitsalltag, 31 Prozent erhoffen sich durch KI-Systeme Expertenwissen, das sonst nicht vorhanden wäre, und 28 Prozent gehen davon aus, dass sich Mitarbeiter dank KI-Unterstützung auf wichtigere Aufgaben konzentrieren können.

Schon heute ist die Verwendung von KI vielschichtig und durchaus in sensiblen, kritischen Bereichen zu finden: Am häufigsten verwenden jene Unternehmen, die bereits KI nutzen, die entspre-

chenden Technologien für personalisierte Werbung (71 Prozent). 64 Prozent nutzen KI zur Verbesserung interner Abläufe in der Produktion und Instandhaltung, 63 Prozent im Kundendienst, etwa bei der automatisierten Beantwortung von Anfragen. Rund jedes zweite Unternehmen setzt KI bei der Analyse des Kundenverhaltens im Vertrieb (53 Prozent) oder bereichsübergreifend bei Texten wie Berichten oder Übersetzungen (50 Prozent) ein. In der Buchhaltung nutzen 44 Prozent KI, etwa für automatisierte Buchungen, 43 Prozent setzen auf KI zur Managementunterstützung, etwa bei der Entwicklung von Strategien. KI-basierte Tools haben 39 Prozent in ihrer IT-Abteilung eingeführt, 35 Prozent in der Logistik, etwa für bessere Routenplanungen.

Es gibt einen Grund, hier nochmals die Hoffnungen für KI und den bisherigen Einsatzbereich von KI aufzuführen: KI kann zu Fehlern führen und zu Schäden, wirtschaftlicher Art, in Zukunft wohl auch für Leib und Leben von Menschen, wenn man zum Beispiel an autonome Fahrzeuge denkt.

Die Frage nach der Haftung

Wenn ein Schadensfall eintritt, stellt sich schnell die Frage, wer für den Schadensersatz zuständig ist, wer in der Haftung ist. Das gilt auch für Schäden im Bereich Datenschutz, da KI-Lösungen sehr häufig mit personenbezogenen Daten umgehen und diese nutzen und nutzen werden.

Die Datenschutz-Grundverordnung (DSGVO) sagt hierzu: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter. Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

Die DSGVO erklärt zudem: Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

Hier werden mehrere Problempunkte sichtbar: Nutzt ein Unternehmen (Verantwortlicher) oder Dienstleister (Auftragsverarbeiter) eine KI-Lösung, kann der Schaden durch die KI verursacht sein. Schadensersatz nach DSGVO leisten müssten aber im Fall des Falles das Unternehmen oder aber der Dienstleister, nicht der Hersteller der KI. Hier wird erneut das Problem sichtbar, dass die DSGVO die Rolle des Herstellers nicht kennt.

Ein weiterer Punkt: Wie soll das Unternehmen oder der Dienstleister nachweisen, dass die KI den Schaden verursacht hat? Meist ist die Transparenz zur und das Wissen über die KI doch recht eingeschränkt.

Nun haben sich die Datenschutzaufsichtsbehörden, vertreten durch den Europäischen Datenschutzausschuss (EDSA), dazu zu Wort gemeldet.

Datenschützer wenden sich an EU-Kommission

Der EDSA hat sich an den zuständigen EU-Kommissar gewendet, um auf die Fragen hinzuweisen, die sich zur Haftung bei KI-Nutzung stellen. Es lohnt sich, die Hinweise und Änderungswünsche für eine Haftung bei KI-Einsatz genau anzusehen, da sich darin viele spannende Punkte befinden, die in der Diskussion zur KI-Haftung nicht vergessen werden sollten.

So hält es der EDSA für relevant, die Haftungsregelung für Anbieter von KI-Systemen zu stärken und sicherzustellen, dass Auftragsverarbeiter und Verantwortliche sich vertrauensvoll auf die KI-Systeme verlassen können.

Zudem wird darauf hingewiesen, dass der Haftungsrahmen für KI-Systeme, die als Sicherheitsmaßnahmen für die Verarbeitung personenbezogener Daten verwendet werden, im Zusammenspiel mit bestehenden Vorschriften wie der DSGVO gesehen werden müsse. Vor allem, wenn es um die Zuweisung von Verantwortlichkeiten geht. Um diesbezüglich Klarheit zu schaffen, ist der EDSA der Ansicht, dass die Rolle und Verantwortlichkeit des Anbieters der KI genau definiert werden muss.

Aufgrund der Natur von KI könnte die Zuweisung der Verantwortung gegenüber einer Partei besonders schwierig sein, insbesondere dann, wenn die Beweislast beim Einzelnen liegt, da letzterer sich dessen möglicherweise nicht bewusst ist, dass KI verwendet wird.

In den meisten Fällen würden die notwendigen Informationen fehlen, um die schädliche Wirkung der KI zu beweisen. Daher müsse die Erklärbarkeit des Systems sichergestellt sein. Zu diesem Zweck betont der EDSA die positiven Auswirkungen der Einbeziehung systematischer menschlicher Überwachung von KI und der Transparenz für den Endverbraucher.

Haftung bei Attacken auf KI

Auch hinsichtlich möglicher Angriffe auf KI gibt es für die Datenschützer Regelungsbedarf:

Einschränkungen und Risiken beim Einsatz von KI-Systemen aufgrund verschiedener Arten von Angriffen, zum Beispiel Cyber-Attacken, sollten auch in den Verantwortlichkeits- und Haftungsregelungen berücksichtigt werden, so der EDSA.

Anbieter von KI-Systemen sollten dafür verantwortlich sein, Benutzern Minderungstools für bekannte und neue Typen von Angriffen bereitzustellen, und die KI-Anbieter sollten für die Einbettung von Security by Design während des gesamten Lebenszyklus der KI verantwortlich sein. Der EDSA ist der Auffassung, dass diese Maßnahmen verbindlich sein sollten, insbesondere wenn das KI-System als Sicherheitsmaßnahme für die Verarbeitung personenbezogener Daten verwendet wird.

Außerdem sollte das KI-System von einer gründlichen und zugänglichen Dokumentation begleitet werden, um die Ursache eines Systemausfalls zu verstehen, insbesondere wenn dies zu einer Datenschutzverletzung geführt hat, und um den Ausfall rechtzeitig stoppen zu können.

Die Rolle der Daten

Es sei von wesentlicher Bedeutung, dass in der bevorstehenden Rechtsordnung zur KI-Haftung der vorläufigen Bewertung der Qualität der Daten, die von maschinellen Lernalgorithmen verwendet werden, um ihre Entscheidungen zu treffen, eine vorrangige Rolle zukommt, so die Datenschützer.

Messbarkeit des Fairnessgrades und die Kausalität von algorithmischen Entscheidungen im Allgemeinen sollten eine Säule der neuen Haftungsregeln sein, um ein vertrauenswürdiges technologisches Umfeld zu schaffen und die negativen Auswirkungen zu begrenzen, die sich aus dem Auftreten von Fehlentscheidungen ergeben.

Wichtig sei es ebenfalls, die KI-Haftung eigenständig zu regeln und nicht nur innerhalb des AI Acts.

Der Grund: Die danach auferlegten Verpflichtungen gelten nur für eingeschränkte Kategorien von KI-Systemen mit hohem Risiko, wobei absehbar ist, dass einige KI-Systeme, die nicht in diese Kategorien aufgenommen wurden, ebenfalls zu Haftungsfällen führen könnten.

Es zeigt sich: Die Datenschützer haben viele zentrale Punkte der KI-Haftung angesprochen, die es zu regeln gilt, nicht nur im Sinne des Datenschutzes, sondern auch für den Verbraucherschutz und zur Klärung der KI-Compliance.

Kommentar von Harald Trautsch, Dolphin Technologies

Warum im Top-Management nichts mehr ohne Daten-Know-how geht

03.06.2022 / VON HARALD TRAUTSCH

Bauchgefühl und Instinkt waren gestern, was heute zählt, ist Big Data: Daten sind die neue harte Währung der Zukunft, die über Erfolg im Business entscheidet – und an denen sich so manche Unternehmenslenker die Zähne ausbeißen werden. Warum aber sollten nicht nur CIOs/CTOs und CEOs ihre Daten im Griff haben, sondern auch CFOs, COOs, CMOs und HR-Chefs? Und warum geht es bei Big Data vor allem darum geht, die richtigen Fragen zu stellen? Eine Kurz-Analyse.

Der Autor: Harald Trautsch ist CEO und Gründer von Dolphin Technologies und Absolvent des Global Executive MBA der WU Executive Academy.

Der neue Goldrausch sind die Daten, denn kaum ein Business wird künftig ohne Digitalisierung überleben. Und wo Digitalisierung ist, da gibt es auch digitale Daten. Wie man sie richtig nutzt und jene identifiziert, die wirklich den Vorsprung bedeuten – darüber ist das Know-how in vielen Unternehmen noch immer recht überschaubar gesät.

Interdisziplinäres Daten-Know-how als roter Faden im Unternehmen

Längst sind es nicht mehr „nur“ die Datenexperten und Data Scientists in den IT-Abteilungen, auch und gerade die Top-Führungskräfte müssen einordnen können, wie Daten gewonnen und ausgewertet werden, und wann welche Datenerhebungen überhaupt Sinn machen. Data Science ist ein gutes Instrument, um wissenstechnische Breite zu schaffen und nicht nur im eigenen Scheuklappen-Silo zu bleiben. Daten zu sammeln und auswerten zu können, reicht aber nicht. Denn: Datenauswertungen sind nur so gut wie die Fragen, die gestellt werden. Deshalb erhalten verschiedene Menschen auch unterschiedliche Informationen aus den erhobenen Datensets, weil sie eben andere Fragen stellen.
Kurzum, jede Führungskraft und jeder Entscheider in einem Unternehmen – vor allem aber as Top-Management – benötigt ein umfangreiches Datenverständnis – mit unterschiedlichen Implikationen und Schwerpunkten:

Chief Executive Officer (CEO): Datenwissen als Entscheidungshilfe

Bei Data Science sei die Erwartungshaltung an der Unternehmensspitze oft groß: Hier geht es darum, wie ich Algorithmen und Künstliche Intelligenz anwenden kann, um das Maximum aus den Daten herauszuholen. Manchmal sind gar nicht genug Daten vorhanden, um Analysen zu machen. Oft müssten Unternehmen die Daten systematischer und vollständiger erheben, um überhaupt ihre Fragen beantworten zu können. Oder es werden zu viele unnütze Daten gesammelt, die für das Business keinen Wert haben. CEOs sollten sich das berühmte Bauchgefühl und den Entrepreneurial Spirit für Dinge aufheben, zu denen Datenerhebungen nicht möglich sind. In allen anderen Situationen brauchen sie die richtigen Informationen aus vorhandenen Datenquellen, um gute Entscheidungen zu treffen. Die richtigen Kennzahlen und KPIs können mit entsprechender Analyse und Auswertung unternehmerische Entscheidungen deutlich verbessern.

Chief Information Officer (CIO)/Chief Technology Officer (CTO): Datensicherheit erhöhen

Dieser Rolle ist ausgeprägtes Wissen um Big Data, Datenerhebungen und -analysen immanent. Der CIO/CTO sitzt an der Quelle und kann entscheidend dazu beitragen, dass Daten aus

verschiedenen Systemen sinnvoll zusammengeführt werden. Entscheidungen über Architektur und Struktur der Services setzen sich ebenfalls aus unternehmensinternen Daten, Informationen Dritter und der grundlegenden Strategie in Bezug auf den Umgang mit Daten zusammen, wobei das Feld der Data Governance eine fast noch größere Rolle als Data Science selbst spielt: Der CIO/CTO muss für ein gelebtes Grundverständnis zum Thema Datensicherheit im gesamten Unternehmen sorgen – und das über alle Ebenen hinweg.

Chief Finance Officer (CFO): Finanzplanung verbessern

Der CFO wiederum ist dafür verantwortlich, die richtigen Finanzdaten erheben und auswerten zu lassen. Er schaut sehr stark retrospektiv auf seine Daten – auf Umsätze, Kosten und Erträge. Sein Fokus sollte aber viel mehr sein: Wie kann ich mit den Erkenntnissen über die bisher gewonnenen Daten in die strategische Finanzplanung gehen? Dazu gehört auch, die Daten genauer zu prüfen und zu hinterfragen: Bei jeder Entscheidung, in jedem Businessplan geht es darum, die dahinterliegenden Daten zu verstehen. Warum sollten wir X Millionen Euro in das Projekt B investieren? Sind die Informationen und die dahinterliegenden Daten überhaupt valide?

Vielen Unternehmen ist auch der monetäre Wert von Daten nicht bewusst. Daten können Kosten verursachen oder zum hohen finanziellen Risiko werden – wenn etwa sensitive Kundendaten in die falschen Hände geraten, oder wenn die schlechte Datenqualität in Analyseprozessen falsche Ergebnisse produziert.

Chief Operation Officer (COO): Prozesse optimieren

Gerade, wenn es um operational Tasks geht, sind Daten unverzichtbar. Der COO darf hier durchaus ein bisschen Kreativität an den Tag legen, um sich zu überlegen, was man aus Daten herausholen kann. Deshalb ist es auch so wichtig, dass er in die Data Governance eingebunden ist. Data Science ist per Definition immer ein interdisziplinäres Feld. Das sollte sich idealerweise auch in der Praxis widerspiegeln: Während das technische Know-how eher beim CTO angesiedelt ist, liegt das Prozess- und Strukturwissen beim COO. Auch für den COO sind Kenntnisse in Data Governance daher von zentraler Bedeutung. Man muss als COO Prozess- und Produktionsdaten verstehen, um Entscheidungen treffen und Abläufe und KPIs, beispielsweise im Quality Manage-

ment, der Unternehmensstrategie anpassen zu können. Bessere Qualität bedeutet beispielsweise nicht notwendigerweise eine geringere, sondern eine optimale Fehlerquote. Nur so kann man sichergehen, nicht am Markt vorbeizuproduzieren und durch höhere Preise Marktanteile zu verlieren.

Chief Marketing Officer (CMO): Teure Kampagnen verhindern

Gerade im Marketing gibt es sehr viel Potenzial, wenn es darum geht, wertvolle Daten zu nutzen, um die eigenen Zielgruppen besser zu erreichen. Hier kann man Daten zum Pricing, zu Seasonality-Effekten und Customer-Journey-Analysen nutzen, um das Kundenverhalten besser zu verstehen, die richtigen Kunden anzuziehen und sie langfristig zu halten. Für Marketingkampagnen helfen Algorithmen und Methoden wie etwa das Clustering, um die Zielgruppenerreichung zu verfeinern und sie via Kundensegmentierung individueller anzusprechen. Wer im Marketing auf die falschen Daten achtet oder sie falsch interpretiert, kann viel Geld verlieren. Einer meiner Kunden wollte beispielsweise mit einer digitalen Werbekampagne neue Kunden für eine Smartphone App gewinnen. Seine Agentur achtete ausschließlich auf die Downloadzahlen und nicht auf Registrierungen oder tatsächliche Käufe. Das Ergebnis war, dass die Kampagne immer mehr auf die falsche Zielgruppe optimiert wurde und sich der Geschäftserfolg erst einstellte, als man die richtigen Metrics aus Erfolgsindikatoren identifiziert hatte.

Chief People Officer (CPO)/ Chief Human Resources Officer (CHRO): Daten sind kein Allheilmittel

Im Recruiting und Human Resources Management werden viele sensible personenbezogene Daten erhoben und gespeichert. Hier ist Datensicherheit wieder ein Thema. Darüber hinaus sollten sich gerade Recruiter nicht zu sehr auf Algorithmen und daraus ermittelte Daten verlassen. Standardisierte Auswahlverfahren sind von Menschen gemacht und nur vermeintlich objektiv. Sie laufen Gefahr, gewisse Biases fortzuführen. Bei einer Vorauswahl der CVs kann das dazu führen, dass der Algorithmus bunte interessante Lebensläufe, die von den Vorgaben abweichen, ausselektiert. Über Machine Learning können auch Biases gelernt werden. Dann gibt es keine Verantwortlichen für die Entscheidung – weil ja ein Algorithmus entschieden hat. Man muss

daher bei allen Benefits der Künstlichen Intelligenz transparent festhalten, wer die Verantwortung für die Letztentscheidungen trägt. Gerade bei der Umsetzung von HR-Maßnahmen werden wertvolle Daten gewonnen, etwa bei Mitarbeiterbefragungen, beim 360-Grad-Feedback. Auch hier muss man die Ergebnisse aber genauer hinterfragen: Wenn ich weiß, dass X Prozent der Mitarbeiter unzufrieden im Job sind, heißt das noch lange nicht, dass sie ihn wechseln wollen. Oft würden geringfügige Änderungen der Rahmenbedingungen ausreichen, um die Zufriedenheit zu steigern. Auch hier gilt es wieder, die richtigen Fragen zu stellen, um brauchbare Antworten zu erhalten.

Kommentar von Alys Woodward, Gartner

Synthetische Daten – wann lohnt sich der Einsatz?

06.07.2022 VON ALYS WOODWARD

Synthetische Daten sind eine wichtige Ressource, um Machine-Learning-Modelle zu trainieren, Systeme zu testen und Prototypen zu erstellen. Im Trend liegen Plattformen für synthetische Daten für tabellarische Daten und Bilddaten. Gartner empfiehlt Anbietern, eine Differenzierung für bestimmte Datentypen und Anwendungsfälle zu treffen.

(Bild: Gartner)

Die Autorin: Alys Woodward ist Senior Research Director bei Gartner

Synthetische Daten sind eine Klasse von Daten, die künstlich erzeugt werden. Sie stammen nicht aus direkten Beobachtungen aus der realen Welt. Daten können mit verschiedenen Methoden erzeugt werden, beispielsweise durch statistisch strenge Stichproben aus realen Daten, semantische Ansätze oder durch ein Generative Adversarial Network. Hinzu kommen Simulationsszenarien, in denen Modelle und Prozesse interagieren, um völlig neue Datensätze von Ereignissen zu erzeugen. Es gibt verschiedene Arten von synthetischen Daten. Darunter fallen tabellarische oder relationale Daten, textbasierte oder bild- sowie videobasierte Informationen. Letztere werden oft als Bilddaten bezeichnet, da es sich bei Videos um eine Reihe von Bildern handelt.

Schätzungen von Gartner zufolge werden sich bis 2030 synthetische Daten in Unternehmen durchsetzen. Sie werden mehr als 95 Prozent der für das Training von KI-Modellen (Künstliche Intelli-

genz) verwendeten Daten ausmachen. Synthetische strukturierte Daten, die zum Trainieren von KI-Modellen verwendet werden, wachsen mindestens dreimal so schnell wie echte strukturierte Daten. Synthetische Daten verbessern Ergebnisse, wenn echte Daten teuer, unausgewogen, nicht verfügbar oder aufgrund von Datenschutzbestimmungen nicht verwendbar sind.

Wo sie zum Einsatz kommen

Echte Daten sind fast immer die beste Quelle für Erkenntnisse. Diese sind jedoch oft teuer, unausgewogen, nicht verfügbar oder aufgrund von Datenschutzbestimmungen unbrauchbar. Um diese Probleme zu lösen, können synthetische Daten erstellt werden, die in der Regel auf den ursprünglichen realen Daten basieren, manchmal in Kombination mit anderen Techniken wie dem differentiellen Datenschutz. Werden synthetische Daten mit realen Daten kombiniert, entsteht ein verbesserter Datensatz, der die Schwächen der realen Daten ausgleicht.

Manchmal werden Daten als „erweitert“ (augmented) bezeichnet. Bei strukturierten Daten lassen sich die Daten auf Zeilenebene erweitern, indem fehlende Felder hinzugefügt werden, zum Beispiel um demografische Informationen aus der Wohnadresse und dem Bildungsgrad abzuleiten. Bei erweiterten Daten handelt es sich manchmal um einen erweiterten Bilddatensatz, dem zusätzliche Randfälle hinzugefügt wurden. Da reale Daten immer in Verbindung mit synthetischen Daten verwendet werden, gelten erweiterte Daten als eine besondere Art von synthetischen Daten, da sie nicht rein „real“ sind.

Wenn Synthetische Daten und Künstliche Intelligenz sich treffen

Synthetische Daten werden derzeit hauptsächlich zum Training von ML-Modellen (Machine Learning) für strukturierte und unstrukturierte Daten, zum Testen von Systemen und zum Erstellen von Produktdemos und Prototypen verwendet. Die Breite ihrer Anwendbarkeit macht sie zu einem entscheidenden Beschleuniger für Künstliche Intelligenz: Sie ermöglichen KI dort, wo Datenmangel KI unbrauchbar macht – etwa aufgrund von Verzerrungen oder der Unfähigkeit, seltene oder noch nie dagewesene Szenarien zu erkennen. Synthetische Daten werden die Einführung von KI und letztlich digitale Geschäftsmodelle beschleunigen.

Synthetische Daten für das Training von ML-Modellen stellen sicher, Modelle so zu trainieren, dass sie ein breites Spektrum an Situationen oder Grenzfällen erkennen. So kann das Modell besser an seinen spezifischen Zweck angepasst werden. Auch lassen sich ML-Lösungen realisieren, die nicht möglich wären, wenn sie nur auf realen Daten beruhen. Die Verringerung des Unterschieds zwischen den Daten, auf die das Modell trainiert wurde, und den Daten, auf die das Modell in der realen Welt stößt, verringert die „Domänenlücke“ in der ML-Terminologie.

Synthetische Daten für Testsysteme sind in einer Struktur erstellbar, die identisch mit den nicht erhältlichen Produktionsdaten ist. Sie können mit einer breiteren Palette möglicher Ereignisse oder Pfade durch das System angereichert werden und ihr Volumen ist für Volumentests erhöhbar.

Synthetische Daten sind für Hackathons, Produktdemonstrationen und internes Prototyping verwendbar, um einen Datensatz mit den richtigen statistischen Attributen zu replizieren. Beispiele sind hier ein synthetischer Datensatz für einen Hackathon, um Wege zur Bekämpfung von Finanzbetrug zu finden. Möglich ist auch ein Demonstrationssystem eines Technologieprodukts für ein Verkaufsgespräch mit einem Kunden, der die Bedarfsplanung im Einzelhandel verbessern will. Oder es entsteht ein internes Prototypsystem, um CFOs Kreditinformationen anzuzeigen, ohne Zeit für den Zugriff auf Produktionsdaten zu benötigen – bei gleichzeitiger Sicherstellung der Glaubwürdigkeit der Angaben.

Solche Daten müssen die richtigen statistischen Verteilungen aufweisen und auch für den Betrachter richtig aussehen. Zum Beispiel müssen die richtigen Postleitzahlen den Städten zugeordnet werden, anstatt sie zufällig zu erstellen. Weisen die Daten sichtbare Fehler auf, besteht die Gefahr, dass Geschäftsanwender und potenzielle Kunden ihnen nicht trauen. Allzweck-Datensätze von Anbietern sind in Verkaufsgesprächen weniger effektiv als Datensätze, die auf die Bedürfnisse des potenziellen Kunden zugeschnitten sind. Für Proofs of Concept können Anbieter eine simulierte Version des Datensatzes des Kunden erstellen.

Da es sich bei synthetischen Daten häufig um eine erweiterte oder abgeglichene Version eines realen Datensatzes handelt, werden synthetische Datensätze meist für einen ganz bestimmten Bedarf erstellt. So kann beispielsweise ein Datensatz, der nach demografischen Gesichtspunkten erstellt und abgeglichen wurde, um ein ML-Modell für die Personalbeschaffung zu trainieren,

nicht für die Analyse des Profils dieser Bevölkerung verwendet werden, da die demografischen Merkmale der Bevölkerung für das Training des Modells optimiert wurden und nicht der Realität entsprechen.

Budgetplanungen und Anbieterprüfung

Es gibt viele reine Anbieter von Plattformen für synthetische Daten, die sich ausschließlich auf die Erzeugung synthetischer Daten konzentrieren. Hinzu kommen angrenzende Bereiche, in denen Anbieter breiter angelegter Plattformen signifikante Funktionen für synthetische Daten als Teil ihres Angebots umfassen. Zu diesen Segmenten gehören Softwaretestplattformen, 3D-Simulationsplattformen, Computer-Vision-Plattformen, DataOps-Plattformen, Data-Science- und ML-Systeme sowie datenschutzfreundliche Berechnungsplattformen. Da synthetische Daten nur die Wertschöpfung ermöglichen, anstatt selbst einen Wert zu schaffen, wird die Konkurrenz zu reinen Plattformen für synthetische Daten durch die synthetischen Datenfunktionen innerhalb breiterer Plattformen weiterhin ein Merkmal dieses Marktes sein.

Wo Unternehmen bereits Geld ausgeben, um echte Daten zu generieren und zu kommentieren, können synthetische Daten die Kosten deutlich senken und gleichzeitig die Qualität steigern. Die Bildseite synthetischer Daten ist derzeit weitaus lukrativer als die Tabellendatenseite, da der ROI klar und einfach zu bewerten ist. Unternehmen, die Bild- und Videodaten benötigen, um ML für autonome Fahrzeuge, intelligente Türklingeln und Drohnen zu trainieren, verfügen über beträchtliche Budgets und sind bereit, diese bei Bedarf manuell zu erstellen. Synthetische Daten bringen deutliche Verbesserungen bei den Kosten, der Zeit bis zur Wertschöpfung und der Qualität der Datenbeschriftung, und darin wie Anbieter das vorhandene Budget nutzen können.

ROI und geschäftliche Vorteile für tabellarische synthetische Daten sind weniger eindeutig an bestimmte Budget-Limits gebunden. Sie beziehen sich eher auf die Effizienz und darauf, dass Aktionen etwas schneller und besser erledigt werden als auf spezifische gemessene Verbesserungen. Diese Faktoren in Kombination mit dem mangelnden Verständnis für synthetische Daten machen sie weniger überzeugend. Auch wird es schwieriger, innerhalb des Unternehmens Projekte zu starten.

Fazit

Letztendlich werden synthetische Daten Teil des KI/ML-Toolkits werden und die Modellentwicklung, das Training und die Governance beschleunigen sowie verbessern. Dafür müssen Unternehmen die Verwendung synthetischer Daten in Bezug auf Anwendungen und Grenzen verstehen. Es ist wichtig Partnerschaften auszuweiten, damit synthetische Daten für mehr Unternehmen und mehr geschäftliche Anwendungsfälle verfügbar sind.

Bio- und Life-Science

Resultate beschleunigen mit KI

15.08.2022 VON DIPL. BETRIEBSWIRT OTTO GEISSLER

Das Sprachverständnis der Künstliche Intelligenz (KI) kann biomedizinische Inhalte klassifizieren und extrahieren, um dadurch verwertbare Erkenntnisse zu erzielen. Beispielsweise bei der Entdeckung von Arzneimitteln, Gestaltung klinischer Studien oder der Verfolgung unerwünschter Wirkungen im Prozess der Arzneimittelsicherheit.

Unternehmen der Bio- und Life-Science-Branche können sich einen Wettbewerbsvorteil verschaffen, indem sie Daten mit KI zugänglicher und besser nutzbar machen.

Informationen zu extrahieren, sind jedoch aber nicht in der Lage, Texte zu lesen oder Sprache zu verstehen. Infolgedessen entgehen ihnen wichtige Informationen, die nicht perfekt mit der Zielsetzung der Suche übereinstimmen.

Dies gilt insbesondere für wissenschaftliche Inhalte, bei denen ein und derselbe Begriff unterschiedliche Konzepte bezeichnen kann oder unterschiedliche Begriffe auf dasselbe Konzept verweisen können. KI-Technologien wie maschinelles Lernen (ML) und natürliches Sprachverständnis (NLU) sind dazu befähigt, das Ökosystem der modernen Medizin wesentlich zu optimieren.

Evidenzbasierte Ermittlung von Wissen

Der Prozess der Arzneimittelforschung, eine Schlüsselanwendung der evidenzbasierten Wissensermittlung, nimmt immens viel Zeit, Aufwand und Ressourcen in Anspruch. Selbst wenn ein Zielmolekül die verschiedenen Phasen des Prozesses durchläuft – von der Hypothesenbildung bis hin zu klinischen Versuchen

– gibt es keine Garantie, dass daraus ein marktfähiges Arzneimittel entsteht.
Um den Prozess der Arzneimittelentdeckung zu beschleunigen, setzen die Pharmaunternehmen heute auf KI-gestützte Technologien. Beispielsweise unterstützt eine KI-Lösung von expert.ai die Forscher bei der Identifizierung von Schlüsseldaten aus einem riesigen Datenvolumen wissenschaftlicher Literatur als auch bei der Skalierung von Prozessen der Investigation von Arzneimitteln.

Die patentierte KI-Technologie von expert.ai ermöglicht eine genaue Identifizierung und Verknüpfung biomedizinischer Informationen wie Krankheiten, Medikamente, Behandlungen, Symptome, Gene, Proteine und andere Datenelemente aus einem riesigen Fundus. Das geschieht dank KI allerdings in einer Geschwindigkeit, die sonstige Verfahren oder menschliche Fähigkeiten bei weitem übersteigen.

Für den Aufbau einer geeigneten Logik entwickelte expert.ai einen Wissensgraphen, der auf Daten aus den Bereichen Bio- und Life-Science spezialisiert ist. Der Wissensgraph erlaubt die Standardisierung und Verknüpfung von Daten wie beispielsweise die Gruppierung von Krankheiten in Krankheitsfamilien oder die Identifizierung von Wirkmechanismen und Medikamentenklassen. Dabei erzielt die Tiefe und Breite des Wissensgraphen eine große Präzision, Abdeckung und Granularität bei der Kategorisierung von Dokumenten, der Extraktion aussagekräftiger Daten sowie der Verknüpfung von Informationen wissenschaftlicher Inhalte oder medizinischer Notizen in jedem Therapiebereich.

Entwurf klinischer Studien

Die Entwicklung von Arzneimitteln ist traditionell ein langer und vor allem kostspieliger Prozess. Im Durchschnitt dauert es in etwa 10 bis 15 Jahre, um ein neues Medikament auf den Markt zu bringen. Ungefähr die Hälfte dieser Zeit sowie deren Investitionen werden in den klinischen Studienphasen der Arzneimittelentwicklung verbraucht. Der Aufbau einer klinischen Landschaft für die Arzneimittelentwicklung erfordert die Erfassung, Auswertung und Verknüpfung von klinischen Studien auf der ganzen Welt. Ferner müssen die Schlüsseldaten aus halbstrukturierten bis unstrukturierten Daten extrahiert und für eine benutzerfreundliche Darstellung bzw. fundierte Entscheidungsfindung aufbereitet werden.

Klinische Studien gestatten es, das volle Potenzial der KI während des gesamten Lebenszyklus der Arzneimittelentwicklung zu nutzen, beginnend mit dem Design und der Planung, der Identifizierung von Prüfärzten und Standorten, der Rekrutierung von Patienten und der Überwachung unerwünschter Ereignisse. Zum Beispiel wertet expert.ai dazu Daten von mehr als 700.000 klinischen Studien weltweit aus. Dazu gehören unter anderem Register für klinische Studien wie clinicaltrials.gov, EUDRA, EU-PAS, Register aus Japan und Australien. Die KI-Plattform des Unternehmens kümmert sich um das Mapping, die Deduplizierung und die Verknüpfung von Daten in verschiedenen Registern, um den Forschern die Nutzung der Daten zu erleichtern.

Durch den Einsatz modernster NLU- und ML-Technologien in Kombination mit Standard- und benutzerdefinierten Taxonomien kann expert.ai wichtige Begrifflichkeiten verstehen und verknüpfen, sodass Wissenschaftler die Daten identifizieren und gezielt auswählen können, die ihnen am ehesten dabei helfen, die Planung und Entwicklung ihrer klinischen Studien zu beschleunigen.

Hilfe bei der Patientenrekrutierung

Eines der wichtigsten Kriterien für die Planung und den Erfolg klinischer Studien ist die Patientenrekrutierung. Solche Informationen werden unter den Zulassungskriterien der Studie beschrieben, die in einem unstrukturierten Datenfeld detailliert aufgeführt sind.

In den Einschlusskriterien sind die wichtigsten Merkmale zur Erfüllung der anvisierten Patientenpopulation vermerkt. In den Ausschlusskriterien werden die zusätzlichen Hauptmerkmale aufgeführt, die die Studie beeinträchtigen oder das Risiko für ein ungünstiges Ergebnis oder unerwünschte Ereignisse erhöhen könnten. So ist beispielsweise das Vorhandensein von Komorbiditäten zu vermeiden, damit ein Patient für eine Rekrutierung in klinischen Studien infrage kommt.

Die Expert.ai-Technologie sorgt dafür, dass diese unstrukturierten Daten in strukturierte Informationen umgewandelt und Schlüsselattribute für ein Patientenprofil erstellt werden. Die Patientenprofile lassen sich dann als Screening-Tool verwenden, um Patientenpopulationen aus realen Daten wie elektronischen Gesundheitsakten (EHR) zu identifizieren. Darüber hinaus wird die Analyse von einer einzelnen Studie auf eine Reihe zusam-

menhängender Studien ausgeweitet, sodass diese Informationen für die Gestaltung von Kohorten für neue Studien verwendet werden können.

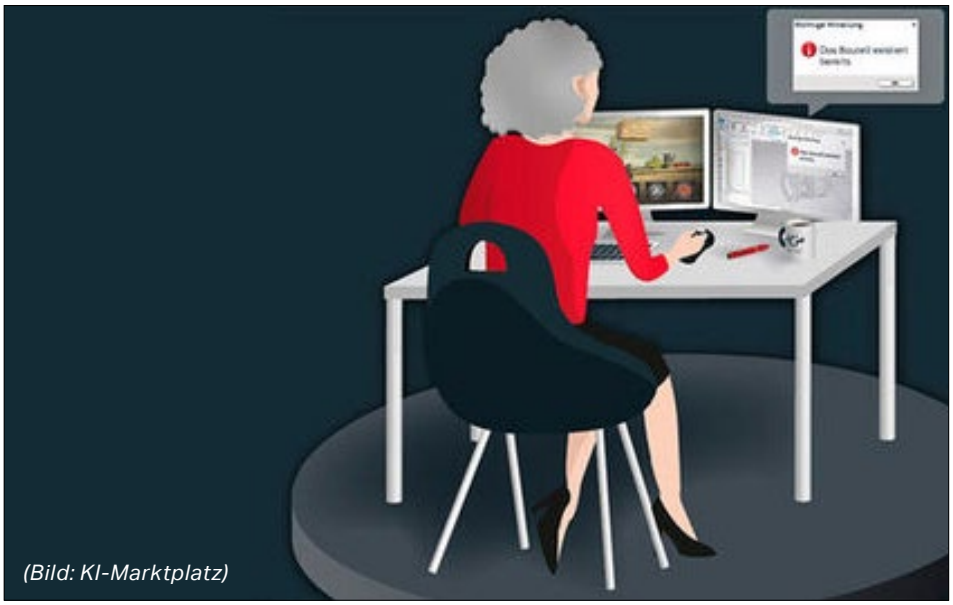
Die Expert.ai-Technologie erleichtert auch die retrospektive Analyse für das Design neuer Studien, indem sie Datenpunkte wie die Änderung der Rekrutierungszahlen und die Zeit, die für den Wechsel von einem Rekrutierungsstatus zum anderen während der Dauer der klinischen Studie benötigt wird, verfolgt.

Use Case des BMWK-Förderprojekts „KI-Marktplatz“

Design-Recycling mit Künstlicher Intelligenz

15.09.2022 Von Dr. Inessa Seifert

Die Wiederverwendung von zuvor bereits entwickelten Bauteilen kann den Entwicklungs-, Produktions- und Lageraufwand in der industriellen Fertigung stark minimieren. Ein Use Case des BMWK-Förderprojekts „KI-Marktplatz“ setzt deshalb auf Künstliche Intelligenz, um gleiche oder ähnliche Bauteile zu identifizieren.



Die Wiederverwendung von Bauteilen in verschiedenen Maschinen mithilfe von KI kann die Herstellungs-, Entwicklungs- und Lagerkosten signifikant reduzieren und individuelle Kundenanforderungen ermöglichen.

„Du kannst jede Farbe haben, die du willst, solange sie schwarz ist“, sagte einst Henry Ford als das Modell T, das erste massenweise gefertigte Auto der Welt, 1908 erstmalig vom Fließband rollte. Die Herstellung in mehreren Farben und Formen war zum damaligen Zeitpunkt weder wirtschaftlich noch organisatorisch möglich. Fast 115 Jahre später hat sich die Produktion exponentiell entwickelt. Egal in welcher Branche, Kundinnen und Kunden wünschen sich heutzutage eine immer größere Produktauswahl in allen erdenklichen Farben, Formen und Designs. Im Zeitalter der Massenindividualisierung können auch Kleinstzahlen von Produkten zu ähnlich wirtschaftlichen Bedingungen hergestellt werden, wie einst das Ford Modell T.

Vor dieser Herausforderung steht auch der Landmaschinenhersteller CLAAS aus dem nordrhein-westfälischen Harsewinkel. Der 1913 gegründete Konzern ist ein europaweit führender Hersteller von Mähdreschern und produziert auch Mähwerke, Schwader, Heuwender und vieles mehr. Wie auch andere Branchen sieht sich das Unternehmen mit steigender Produktkomplexität und -variantenzahl konfrontiert. Dabei wurde eine potenzielle Lösung bereits identifiziert: Die Wiederverwendung von Bauteilen in verschiedenen Maschinen kann die Herstellungs-, Entwicklungs- und Lagerkosten signifikant reduzieren und individuelle Kundenanforderungen ermöglichen. Die Suche nach identischen oder ähnlichen Teilen kann sich dabei jedoch schwierig gestalten. In vielen Fällen können Standardbauteile nicht einfach wiederverwendet werden. Dazu kommt, dass die Stammdaten der Bauteile oft nur unvollständig gepflegt sind und damit keine ausreichende Grundlage existiert, um gezielt nach passenden Teilen zu suchen.

Digitales Ökosystem für KI-gestützte Produktenwicklung

Künstliche Intelligenz (KI) kann die Suche nach geeigneten Bauteilen erleichtern. Wie das genau funktioniert, zeigt das Förderprojekt KI-Marktplatz, das im Rahmen des KI-Innovationswettbewerbs des Bundesministeriums für Wirtschaft und Klimaschutz gefördert wird. Mit dem Wettbewerb werden ausgewählte Leuchtturmprojekte unterstützt, weiterentwickelt und im Idealfall zur Marktreife geführt. Der Landmaschinenhersteller CLAAS ist einer von mehreren Konsortialpartner des KI-Marktplatzes.

Um eine Lösung für das Problem der Gleich- und Ähnlichteile zu erarbeiten, erprobt CLAAS im Rahmen des Förderprojekts einen Ansatz, bei dem entsprechende KI-Lösungen in Computer Aided Design-Software (CAD) integriert werden. CAD ermöglicht es Nutzerinnen und Nutzern, bequem Produkte, Bauteile oder Gebäude über digitale Interfaces zu gestalten. Durch die Integration von KI-Algorithmen soll im Rahmen der Software-Anwendung ein intelligentes Gleichteilmanagement entstehen und prototypisch umgesetzt werden. In diesem Zuge werden die über die CAD-Software entworfenen digitalen Modelle nach ihrer Geometrie und Funktion klassifiziert. Wenn Stammdaten fehlen, sollen die KI-Anwendungen nicht nur dazu in der Lage sein, diese zu ergänzen, sondern den Datensatz auch um weitere übergreifende Informationen (Metadaten) zu erweitern.

Auf Basis dieser vervollständigten Datensätze ist es nun möglich, KI-Verfahren wie das Case Based Reasoning (CBR) zu verwen-

den, um identische Bauteile hinsichtlich Geometrie und Funktionalität in der Datenbank zu identifizieren. Die CBR-Verfahren erlauben es Usern zudem, Feedback zu den Bauteilen einfließen zu lassen und dadurch das Wissen über deren Wiederverwendung, Anpassung oder Ablehnung im Produktionsprozess noch weiter zu ergänzen. In weiteren Schritten könnten diese Informationen dazu verwendet werden, um z. B. die Qualität und Leistungsfähigkeit von Bauteilen und Werkzeugen zu verbessern.

Smartes Bauteilmanagement

Zunächst aber will CLAAS das KI-gestützte Bauteilmanagement nutzen, um mittelfristig die Bauteilanzahl in ihrer Bestandsdatenbank zu reduzieren und beherrschbar zu halten. Wenn ein neues Bauteil über CAD entworfen wird, sollen die KI-Lösungen bereits während der Konstruktion identische oder ähnliche Bauteile identifizieren. Statt der neu entworfenen Teile können auch Teile vorgeschlagen werden, die wiederverwendet werden können. Der Konstruktionsaufwand wird auf diese Weise signifikant verringert, Ressourcen geschont und Lagerkapazitäten eingespart. Auf lange Sicht entsteht so auch die Grundlage für individuelle und deutlich effizientere Kundenanfertigungen. Die Produktion neuer Entwürfe kann so aus bereits bestehenden Bauteilen automatisiert errechnet wird.

Das smarte Bauteilmanagement ist nur einer der vielversprechenden Use Cases, die im Rahmen des KI-Marktplatzes umgesetzt werden sollen. Im Rahmen des digitalen Ökosystems entstehen auch KI-Lösungen, die über Produktions-, Maschinen- und Sensordaten möglichst effiziente Maschinenbelegung errechnen, die Wartung und Reparatur von Geldautomaten optimieren oder defekte KFZ-Bauteile frühzeitig identifizieren. Der KI-Marktplatz leistet damit einen essenziellen Beitrag, um die Zukunftstechnologie Künstliche Intelligenz in vielen wirtschaftlich relevanten Bereichen voranzubringen.

Der KI-Marktplatz ist ein Projekt im Bereich der fertigenden Industrie, bei dem ein bundesweit einzigartiges digitales Ökosystem entstehen soll, das Unternehmen per KI bei der Produktentwicklung unterstützt. Auf der Plattform können KI-Anbieter, -Anwender sowie Expertinnen und Experten unter datenschutzrechtlich sicheren Bedingungen KI-Lösungen entwickeln und austauschen. Unternehmen und Akteure rund um die Produktentstehung erhalten über den Marktplatz Zugriff auf Beratungsdienstleistungen und KI-Bausteine. Damit potenzielle Projekt-

partner sich unkompliziert finden können, arbeitet die Plattform mit einem intelligenten Matching-System. Zudem können über entsprechende digitale Stores KI-Lösungen nach dem Baukastenprinzip oder Trainingsdaten zur KI-Entwicklung zusammengestellt und bezogen werden.

Künstliche Intelligenz

Keine KI ohne zielführende Datenarchitektur

26.09.2022 VON DIPL. BETRIEBSWIRT OTTO GEISSLER

Datenmissmanagement ist der entscheidende kritische Faktor, der den zukünftigen KI-Erfolg eines Unternehmens ernsthaft gefährden kann. Das ist ein Ergebnis des globalen Forschungsberichts von MIT Technology Review Insights. Welche Schritte müssen CIOs für KI-Implementierungen jetzt ergreifen?

(Bild: Databricks)

Robin Sutara, Field CTO bei Databricks: „Meiner Meinung nach ist einer der wichtigsten Faktoren für die erfolgreiche Skalierung von KI der Aufbau einer soliden Datenkultur."

In vielen Unternehmen verharren die Technologien der Künstlichen Intelligenz (KI) noch in der Einführungsphase. Um KI-Ziele zu unterstützen, gaben die Befragten der MIT-Studie an, dass für sie die Geschwindigkeit der Datenverarbeitung ganz oben auf ihrer Liste steht. Daher sind sogenannte „KI-Leader" aus KI-gesteuerten Unternehmen der Ansicht, dass sie das Tempo der Datenverarbeitung erhöhen müssen (55 Prozent).

Zu den größten Herausforderungen wird von den Befragten jedoch das Thema Datenmanagement gezählt. 72 Prozent gaben an, dass Datenprobleme das Erreichen ihrer KI-Ziele bis 2025 eher gefährden als andere Faktoren. „Das wichtigste und von den Befragten am häufigsten genannte Problem für den Erfolg von KI ist die Tatsache, dass viele Unternehmen nicht wissen,

wie sie mit ihrem gesamten Datenbestand umgehen oder wie sie deren Qualität messen sollen“, stellt Robin Sutara, Field CTO bei Databricks, heraus.

Fokussierte KI-Ziele erreichen

Unternehmen müssen hierzu vier verschiedene Stacks aufbauen, um alle ihre Daten-Workloads zu bewältigen: Business Analytics, Data Engineering, Streaming und Machine Learning (ML). „Alle vier dieser Stacks erfordern sehr unterschiedliche Technologien und leider sind sie nicht immer gut in Einklang zu bringen“, erklärt Sutara. „Das Ergebnis sind meist viele Datenkopien, kein einheitliches Sicherheits- und Governance-Modell, geschlossene Systeme und wenig produktive Datenteams.“ Danach folgen in der Reihenfolge ihrer Wichtigkeit vier dringende Erfordernisse:

1. Die Sicherstellung ausreichender Daten für die KI-Modelle.
2. Die Verbesserung der Überwachung der Datenabfolge in diesen Modellen.
3. Die Verbesserung des Zugangs des Unternehmens zu externen Daten und deren Integration.
4. Die Ermöglichung einer stärkeren Zusammenarbeit bei Entwicklungsdaten und KI-Modellen.

Hindernisse für die Einführung von KI

„Um die Skalierbarkeit von KI zu gewährleisten, muss vor allem eine Datenkultur geschaffen werden, in der Menschen, Fähigkeiten und Technologie zusammenkommen“, betont Sutara. So werden bis 2025 von den europäischen Befragten Investitionen in die Entwicklung von „Talenten“ und deren Fähigkeiten (38 Prozent) und in die Datenqualität (32 Prozent) als die beiden wichtigsten Prioritäten für die Skalierung von KI und ML gefordert.

Andere Hindernisse wie die Grenzen bestehender Daten und KI-Technologien und der Mangel an KI-qualifizierten Fachkräften spielen ebenfalls eine große Rolle. Zu den größten Hindernissen für die Einführung von KI und ML (Machine Learning), die von den europäischen Befragten in der Umfrage genannt wurden, zählen ebenfalls starre Organisationsstrukturen (34 Prozent), starre Prozesse (33 Prozent) und Einschränkungen der vorhandenen Daten und KI-Technologien (33 Prozent).

„Meiner Meinung nach ist einer der wichtigsten Faktoren für die erfolgreiche Skalierung von KI der Aufbau einer soliden Datenkultur“, sagt Sutara. „Lassen Sie mich daher näher erläutern, was wir damit meinen. Eine gute Datenkultur lässt sich durch folgende drei Maßnahmen erreichen: Menschen, Prozesse und

Technologie. Um eine Datenkultur voranzutreiben, muss jede Person im Unternehmen zur richtigen Zeit den richtigen Zugang zu den richtigen Daten haben."
Aus der Prozessperspektive erfordert dies eine Überprüfung der internen Prozesse und Governance-Modelle sowie die Schaffung von Rahmenbedingungen, die eine konsequente Anwendung von Grundsätzen ermöglichen, bei denen Daten eine zentrale Rolle bei der Umsetzung der Prozesse spielen. Dabei müssen auch Möglichkeiten zur Iteration und Verbesserung auf der Grundlage von Mitarbeiter-Feedback und neuen Daten, die im Rahmen dieser Prozesse erstellt und gesammelt werden, gegeben sein. „Bei der technologischen Säule des Aufbaus einer Datenkultur geht es vor allem darum, eine einfache, offene und zukunftssichere Plattform zu schaffen, die es jedem im Unternehmen ermöglicht, Daten zu nutzen", so Sutara. „Hier hilft die ‚Macht' des Lakehouse."

Aufbau einer zielführenden Datenkultur

Eine praktische Lösung ist die Einführung einer Lakehouse-Architektur. „Das heißt, die Unternehmen sind nicht mehr an die Beschränkungen und die Komplexität von Legacy-Architekturen gebunden", so Sutara. „Eine solche Architektur bietet flexible, leistungsstarke Analysen, Data Science und ML, indem sie die Leistung, Zuverlässigkeit und Governance von Data Warehouses mit der Skalierbarkeit, den niedrigeren Kosten und der Workload-Flexibilität des Data Lakes kombiniert." Beispielsweise vereinheitlicht und skaliert die Lakehouse-Plattform von Databricks Daten, Analysen und KI-Funktionen auf folgende Weise:

- Multi-Cloud: Databricks ist eine einheitliche Datenplattform für alle drei großen öffentlichen Clouds (AWS, Azure, Google Cloud). Das heißt, ein einziges Tool für Data Engineering, Data Science, ML und Analytik.
- Offen: Die Architektur ist offen, um durch die Verwendung offener Standards und Datenzugriffe sowie die Nutzung von Innovationen aus der Open-Source-Community Lock-Ins zu vermeiden.
- Hohe Leistung zu niedrigen Kosten: Databricks Delta Lake ändert die Größe der Datenpartitionen dynamisch, um die beste Kombination aus Kosten und Leistung zu erzielen. Mit Databricks SQL können Kunden eine Multi-Cloud-Lakehouse-Architektur betreiben, die bis zu 12-mal preiswerter und leistungsfähiger ist als herkömmliche Cloud-Data-Warehouses.

- Skalierbar und kollaborativ: Die Plattform für Data Science und maschinelles Lernen ermöglicht es Entwicklern und Data Scientists, ihre Daten zu erforschen, Modelle zu erstellen und zu produzieren und ihre Analysen im großen Umfang zu teilen. Mit einem automatisierten vollständigen ML-Lebenszyklus lässt sich die Zeit vom Experimentieren mit ML-Modellen bis hin zu robusten Produktionsimplementierungen deutlich verkürzen.

„Das Aufbrechen von Datensilos mit einer offenen Lakehouse-Architektur ist der erste Schritt, um die „Macht“ der Daten in einem Unternehmen wirklich zu erschließen“, unterstreicht Sutara. „Auf diese Weise können sich Führungskräfte auf Menschen, Prozesse und den Geschäftswert konzentrieren.“

Kommentar von Christian Schlögel, Körber

5 Tipps, um ein Unternehmen KI-ready zu machen

28.10.2022 VON CHRISTIAN SCHLÖGEL

Künstliche Intelligenz (KI) ist die Schlüsseltechnologie, die diese Dekade prägen wird wie keine andere. Sie wird große Auswirkungen haben auf Unternehmen, das öffentliche Leben und die ganze Gesellschaft und als Treiber der vierten industriellen Revolution fungieren.

(Bild: Körber)

Der Autor: Christian Schlögel ist Vorstand und Chief Digital Officer bei Körber

Künstliche Intelligenz macht rasante Fortschritte. Der Unterschied zu klassischen Softwaresystemen ist, dass KI-Systeme autonom dazulernen können und sich über die Zeit verbessern. Dies geschieht durch Einbeziehung neuer Daten oder neuer Erkenntnisse und zwar ohne, dass eine Veränderung des Systems notwendig ist. Aus diesem Grund ist es wichtig, von Anfang an auf hohe Datenqualität zu achten und darauf, dass die Daten sämtliche notwendigen Teilbereiche umfassen und nicht „biased“ sind.

Noch zu selten nutzen Industrieunternehmen das Potenzial von KI, um sichtbaren Mehrwert zu schaffen. Dabei ist der Einsatz von KI in anderen Bereichen längst etabliert. Von Chatbots bis zu medizinischen Diagnosen mit höherer Genauigkeit als von den besten Experten – KI ist keine Zukunftsmusik mehr und kann sich insbesondere für mittelständische Firmen sehr lohnen. Doch was muss ich beachten, wenn ich mein Unternehmen auf

diese so wichtige und wertvolle Technologie vorbereiten will? An welchen Stellschrauben muss ich drehen, um mein Unternehmen KI-ready zu machen?

Fangen wir mit Machine Learning an. Sie ist die heute am häufigsten genutzte KI-Technologie. Mittels Machine Learning können Aktivitäten implementiert werden, deren Ergebnisse besser und exakter sind als die eines Menschen. Machine Learning wird oft als erste Grundlage genutzt, um Prozesse und unternehmerische Abläufe zu optimieren. Die Verarbeitung großer Datenmengen oder das Gruppieren und Segmentieren von Daten gehören zu den wichtigsten Grundlagen für datenbasierte Optimierung. Dies kann mithilfe von Machine Learning automatisiert und optimiert werden, sowohl bei der Neuentwicklung, aber auch bei der Optimierung bestehender Systeme.

Eine KI kann beispielsweise Objekte erkennen, Sprache verstehen, vor allem aber Entwicklungen vorhersagen. Gerade Letztgenanntes bringt zahlreiche Anwendungsmöglichkeiten für die Industrie 4.0 mit sich. Maschinen mit Sensoren auszustatten, ist eine einfache Sache. Den gesamten Maschinenpark miteinander kommunizieren zu lassen und KI als Ratgeber für Maschinenführer in die eigene Fabrik einzuführen, ist hingegen eine viel komplexere Aufgabe. Gerade hier kann Machine Learning seine Fähigkeiten voll ausspielen.

Aber wie steigt man am besten ein? Diese fünf Schritte sollte man beachten:

1. Das KI-Projekt ist mehr als nur ein weiteres Softwareprojekt

Bei der Implementierung von KI in Unternehmen handelt es sich um mehr als die Integration eines zusätzlichen Software- oder Projektmanagement-Tools. Das Projekt sollte als Change-Management gesehen werden. Die Arbeitsweise von Unternehmen ändert sich durch den Einsatz von KI über kurz oder lang drastisch. Das gilt es, schon vor den ersten handfesten Plänen zu berücksichtigen.

2. KI- und Datenstrategie definieren

KI hat das Potenzial, ein Unternehmen in vielen Bereichen grundlegend zu verändern. Daher ist es wichtig, die technischen und ökonomischen Aspekte von KI zu verstehen und eine klare und auf Ihr Unternehmen abgestimmte KI-Strategie zu definieren. Folgende kommunikative und strategische Schritte sind dabei unbedingt ratsam:

- Klare Ziele definieren, die man mit KI erreichen möchten.
- Einbinden dieser Ziele in die Gesamtstrategie des Unternehmens.
- Konkrete Zwischenziele für die ersten zwölf Monate fixieren.
- Etablieren von C-Level- und Management-Trainings zur KI- und Datenstrategie, um alle Entscheider auf den gleichen Stand zu bringen.

3. Den Reifegrad und die Qualität der Daten analysieren

Eine Bestandsanalyse ist essenziell: Wie ist der Status quo meines Daten-Clusters? Wie steht es um die datengetriebene Denkweise in meiner Organisation? Genauer betrachten sollte ich auch meine existierende Daten-Wertschöpfungskette, um herauszufinden, wo das größte Potenzial für den Einsatz von KI liegt.

4. Data-Opportunity-Projekt starten und ein MVP bauen

Den Startpunkt für ein KI-Projekt findet man am besten, wenn man sich die aktuellen innerbetrieblichen Herausforderungen bewusst macht und sich fragt, wo KI einen Mehrwert stiften kann. Ein Data Opportunity Workshop kann dafür ein guter Einstieg sein und kann extern begleitet werden. Dafür gibt es Beratungsexperten wie zum Beispiel DAIN Studios, die Experten für Data Strategy und KI sind. Es gilt dabei festzustellen, welche Daten bereits vorhanden sind und was zusätzlich für die Realisierung des Anwendungsfalls benötigt wird.

Den Anwendungsfall sollte man nach ökonomischen Gesichtspunkten auswählen. Es lohnt sich, den Markt danach zu scannen, ob es bereits eine Lösung für den Anwendungsfall gibt, die sich adaptieren lässt. Für die industrielle Fertigung haben sich aus Körbers-Venture-Building-Ansatz zum Beispiel FactoryPal und InspectifAI etabliert. Falls keine Lösung am Markt vorhanden ist, sollte im nächsten Schritt mit externer Hilfe ein Minimum Viable Product (MVP) entwickelt werden, also ein Prototyp, der den Minimalanforderungen gerecht wird. Die meisten Produktideen funktionieren allerdings nicht sofort und müssen in Iterationsschritten angepasst werden. Deshalb ist es sehr wichtig, ganz dem Lean-Prinzip folgend, in einem sehr frühen Stadium des Entwicklungsprozesses Erkenntnisse über das Produkt und mögliche Kunden zu gewinnen.

5. KI-Kultur durch Aufklärung und Beteiligung schaffen

Es gilt, einen C-Level-Sponsor zu finden und die Kommunikation nicht zu unterschätzen. Damit Mitarbeiter KI-Projekte annehmen, müssen sie diese zunächst verstehen. Daher sollten Mitarbeiter aus möglichst vielen unterschiedlichen Abteilungen in die Arbeit mit der neuen Technologie direkt miteinbezogen werden.

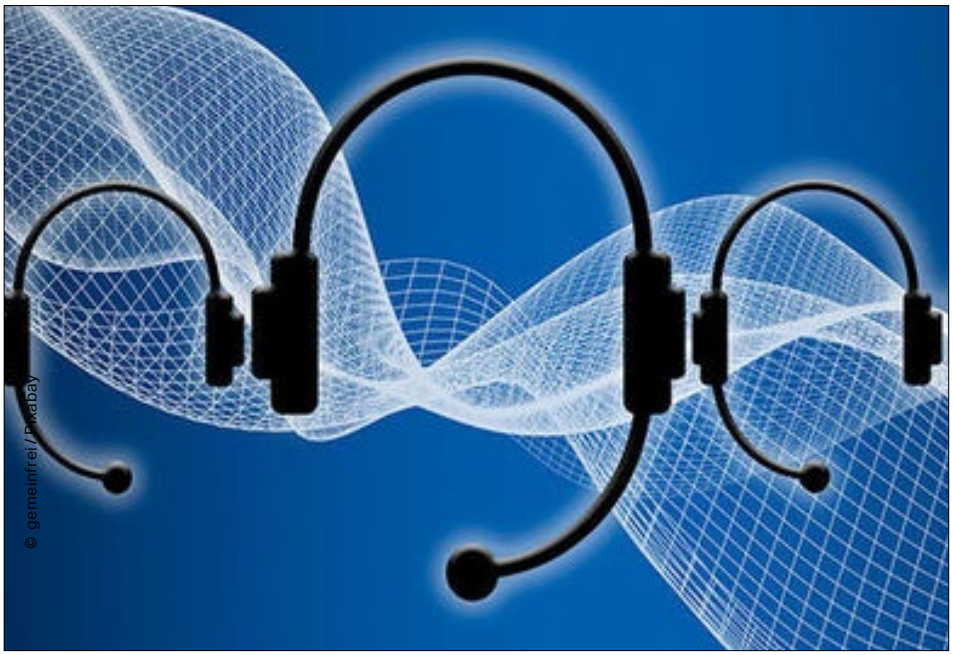
Die Implementierung von KI ist, wie bereits erwähnt, kein rein technisches Vorhaben, sondern auch ein strategisches Projekt. Nur wenn sich alle Mitarbeiter mit der Arbeit mit Daten identifizieren und ein grundlegendes Verständnis für den daraus entstehenden Mehrwert haben, funktioniert die neue Art der Zusammenarbeit. Deshalb ist es wichtig, Ziele und Nutzen von KI-Projekten an die verschiedenen Teams zu kommunizieren und in die gemeinsame Diskussion zu gehen. Für das Etablieren einer KI-Kultur müssen nicht alle Mitarbeiter ein tiefes Verständnis für große Datenmengen oder KI als solche haben. Es genügt, wenn diese wissen, woher Daten kommen, wofür man sie nutzt und wie sich der Datenworkflow künftig gestaltet. Bei Körber etwa binden wir neben hochqualifizierten Data Scientists auch Entscheider und Mitarbeiter aus verschiedensten Unternehmensbereichen in KI-Projekte ein. So versuchen wir, alle mitzunehmen auf unserer KI-Reise und es entstehen bessere Produkte. Meine Vision dabei: eine ganzheitliche Kultur der künstlichen Intelligenz im Konzern zu etablieren.

Potenziale im Beziehungs-Management

Die Macht der Künstlichen Intelligenz im Kundenservice

20.12.2021 | VON DIPL. BETRIEBSWIRT OTTO GEISSLER

KI-basierte Lösungen tragen dazu bei, Kosten zu senken, die Mitarbeiterbindung und -loyalität zu verbessern, den Umsatz zu steigern und vor allem Kundenerlebnisse in verschiedener Hinsicht zu verbessern – bei richtiger Anwendung! Was müssen Unternehmen jetzt beachten?



KI kann das Verhalten und die Vorlieben von Kunden verstehen und antizipieren.

Umfragen zufolge findet ein Großteil der deutschen Konsumenten Interaktionen mit Chatbots frustrierend. Ein genau abgestimmter Einsatz von Künstlicher Intelligenz (KI) könnte ihre Meinung sicherlich verändern. Wenn man bedenkt, dass mithilfe dieser Technologie nicht nur das Verhalten der Kunden und deren Einstellungen besser erfasst werden kann, sondern auch die Unternehmen viel proaktiver und gezielter auf Kundenanforderungen reagieren und beispielsweise Chatbots wesentlich besser programmieren könnten.

Auf diese Weise wäre es möglich, Kunden im Umgang mit Chatbots überzeugend das Gefühl zu vermitteln, dass sie als Individuen behandelt und ihre persönlichen Bedürfnisse richtig verstanden werden. Was wiederum eine ideale Voraussetzung bietet, relevante Lösungen zu unterbreiten. Das heißt, es kommt vor allem

darauf an, KI auch wirklich zielführend einzusetzen. Denn ein Chatbot kann nur so gut sein, wie die Daten und Informationen es erlauben, mit denen er programmiert wurde.

KI macht Big Data transparenter

Seit Jahrzehnten bemühen sich die Unternehmen darum, möglichst viele Daten über ihre Kunden zu sammeln, um fundierte Entscheidungen im Marketing und Kundenservice zu treffen. KI kann riesige Datenmengen, insbesondere Daten aus einer CRM-Plattform, analysieren und in leicht zugängliche Reports verdichten. Dies macht es für Unternehmen einfacher, auf wichtige Details ihrer Zielgruppe zuzugreifen, sie zu verstehen und zu nutzen. Diese Daten gelten im Allgemeinen als zuverlässiger verglichen mit denen von Menschen gesammelten, verarbeiteten und analysierten Informationen.

Obwohl die KI-Technologie noch nicht alle Aufgaben eines menschlichen Kundendienstmitarbeiters erfüllen kann, handelt es sich bei vielen Verbraucheranfragen um sehr einfache Anfragen, die von den aktuellen KI-Lösungen ohne menschliches Zutun gut bearbeitet werden können. Auf diese Weise wird die KI den Menschen unterstützen und mit ihm zusammenarbeiten, die stupiden und langweiligen Jobs beseitigen und es ihnen ermöglichen, sich auf jene Kunden zu konzentrieren, die „eingehendere Hilfe“ benötigen.

KI-Anwendungsfall „Augmented Messaging“

Ziel ist es, die negativen Kundenerlebnisse im Umgang mit Bots zu vermeiden. Dies wird nicht mit den sogenannten allgemeinen Bots funktionieren, sondern mit AI-Augmented Messaging, das für routinemäßige und einfache Aufgaben eingesetzt werden kann. Angeboten wird eine solche Technologie unter anderem von LivePerson.

Damit lassen sich einfache Fragen direkt von einem Bot bearbeiten. Sobald die Konversation zu kompliziert wird, besteht die Möglichkeit, dass der Bot das Gespräch an einen Agent weiter gibt – und umgekehrt. Dies birgt den Vorteil, dass menschliche Agenten ihre Zeit damit verbringen, das zu tun, was derzeit nur menschliche Agenten bewältigen können, und minimiert die Zeit, die sie für Aufgaben aufwenden müssen, die Bots ebenfalls bearbeiten können.

KI-Anwendungsfall „E-Mail-Anfragen“

Nicht selten kann es sehr zeitaufwendig sein, jede E-Mail von einem Mitarbeiter zu lesen, um den Bedarf des Kunden zu erfassen und zu erkennen, wie das Unternehmen damit umgehen soll. KI ist dazu in der Lage, den Prozess zu beschleunigen. DigitalGenius bietet beispielsweise eine KI-gestützte Technologie an, die E-Mails scannt und markiert, um sie an den geeigneten Ansprechpartner weiterzuleiten.

Das System stellt dann den zuständigen Service-Agenten auch Makros und Clips aus den besten Antworten der Vergangenheit zur Verfügung, damit in kurzer Zeit eine Antwort erfolgen kann. Die Technologie ermöglicht es dem Anwender, die Zahl der auf eine Antwort wartenden Kundenanfragen um die Hälfte zu reduzieren und versetzt Service-Center in die Lage, Kunden innerhalb von 24 Stunden eine Antwort zu senden. DigitalGenius konstatiert, dass mehr als 80 Prozent aller eingehenden Anfragen von dem KI-System markiert und sortiert werden können.

KI-Anwendungsfall „verbesserte Kundentelefonate“

Auf rein technischer Ebene ist es für ein System schwieriger mit Sprache umzugehen als mit Texten eines Chat. Hintergrundgeräusche, ungewöhnliche Sprachmuster, Akzente und schlechte Aussprache erschweren es einer KI, Stimmen in Text zu übersetzen. Umfragen ergaben, dass Kunden bei einfacheren Anfragen Chats oder Anrufe in gleicher Häufigkeit nutzen, um Antworten zu erhalten. Für beispielsweise komplexere Finanzfragen bevorzugen Kunden ihre Fragen am Telefon zu stellen.

Das Start-up Cogito hat dafür ein Echtzeit-Konversationsanalyse-Tool entwickelt, das auf Erkenntnissen aus Verhaltenswissenschaften und des Deep Learning basiert. Das KI-System von Cogito analysiert Gespräche sowohl hinsichtlich des Inhalts als auch des Tons. Dies geschieht, indem es sogar unter anderem Nachahmungen, Lautstärkeänderungen, Tonhöhenänderungen erkennen kann, um Echtzeiteinblicke in die Gefühle der Kunden zu liefern. Gleichzeitig werden diese Daten mit allen bisherigen Telefonaten verglichen. Zudem bietet das KI-System den Kundendienstmitarbeitern Vorschläge zur Optimierung der Interaktion und zur Bewertung der Performances – natürlich in Echtzeit.

In einem Praxistest bei einer Versicherungsgesellschaft mit 200 Agenten führte die KI-Lösung zu einer knapp 30-prozentigen Verbesserung der Net Promoter Scores (Kennzahl zur Kundenzufriedenheit), einer 6-prozentigen Verbesserung der Problemlösung sowie weniger Anrufern, die mit einem Agenten sprechen wollten. Cogito konstatiert ferner, dass das KI-System Rückrufe um 10 Prozent reduziert.

Ausblicke in die Zukunft

Rund ein Drittel der Großunternehmen nutzen bereits KI-Technologien im Bereich Kundenservice. Damit gehört der Kundenservice nach der IT-Branche zum zweithäufigsten Einsatzbereich von KI durch Unternehmen. Neben den Anwendungen in Call Centern wird die Technologie zukünftig auch zu wesentlichen Entlastungen insbesondere von Kassierern, Hostessen und Verkäufern in lokalen Geschäften beitragen.

Aktuell verwenden Unternehmen KI-Systeme, um Menschen zu ersetzen und die Interaktionen mit Kunden auf niedriger Ebene zu optimieren oder die Performance der Agenten zu verbessern. Wenn sich Serviceleistungen nun deutlich veredeln lassen, dann erwarten die Kunden aber auch deutlich mehr davon. Dank der Technologie erwarten insbesondere junge Verbraucher, dass Servicemitarbeiter ihre Kontakt- und Produktinformationen bereits kennen, wenn sie von ihnen kontaktiert werden.

Interview mit Thomas Neubert, Intel

„KI kann eine noch größere Chance darstellen als der Internet-Boom in den 90ern“

10.01.2022 | VON EKATERINA VENKINA

Thomas Neubert lebt seit 30 Jahren im Silicon Valley. Bei Intel in Santa Clara ist er für den Übergang zu neuen Technologien in Zusammenarbeit mit externen Start-ups zuständig. Er ist Mitbegründer und amtierender Vorsitzender der German American Business Association, die 2003 in Kalifornien gegründet wurde. Ein Gespräch über den KI-„Megashift“ und seine Bedeutung für das Business-Ökosystem in Deutschland.

Thomas Neubert, Senior Director Strategic Business Incubation & Innovation bei Intel und Gründer der Plattform Transatlantic AI eXchange, im Gespräch mit BigData-Insider

BigData-Insider: Herr Neubert, auf Ihrem LinkedIn-Profil werden Sie als „Evangelist für Transatlantic AI eXchange“ bezeichnet. Ist Künstliche Intelligenz (KI) eine Art Religion für Sie?

Neubert: (lacht) Nein, das ist sie nicht. Es ist witzig. Meine Frau hat mich genau das Gleiche gefragt, als ich meine Visitenkarte drucken ließ. Intel hat 16 vertikale Anwendungsbereiche skizziert, in denen KI Verbesserungen bringen und viele Prozesse effizienter, billiger, schneller und präziser machen wird. Sie wird sich auf die eine oder andere Weise auf fast jeden einzelnen Aspekt unseres Lebens auswirken. Meiner Meinung nach geht es bei der KI also eher um horizonta-

le Skalierung. Deshalb ist dies eine ebenso große oder sogar noch größere Chance, als es das Internet Ende der 90er-Jahre war. Die Entwicklung selbst mag nicht so drastisch sein, aber sie wird die Welt verändern.

Kate Crawford, Autorin von „Atlas of AI", sagt, Künstliche Intelligenz sei „weder künstlich noch intelligent." Sie wird aus natürlichen Materialien geschaffen und Menschen führen die Aufgaben aus, die KI autonom erscheinen lassen, so die Microsoft-Forscherin.

Neubert: Ich würde dieser Aussage nur teilweise zustimmen. Künstliche Intelligenz braucht ein Front-End-Tool oder eine Reihe von Daten, die Menschen gesammelt haben, sie braucht also menschlichen Input. Das ist richtig. Aber es muss klar sein, dass Deep Learning und Künstliche Intelligenz Unterkategorien des maschinellen Lernens sind, nicht umgekehrt. Für mich besteht die Einzigartigkeit der KI darin, dass Daten in die Maschine zurückgeleitet werden können und sie aus ihren Fehlern lernt, um besser, schneller und genauer zu werden. Mit anderen Worten: Sie kann sich selbst korrigieren.

Eine relativ homogene Gruppe von Fachleuten in einer wohlhabenden Branche ist derzeit für große technologische Durchbrüche in der KI verantwortlich. Das mag provokant klingen, aber haben wir es hier nicht mit einer Art Elfenbeinturmdenken zu tun?

Neubert: Stellen Sie sich die berühmte Glockenkurve der Entwicklung vor. Bei der Künstlichen Intelligenz befinden wir uns noch in der „Early-Adopter"-Phase. Die USA haben die Führung ergriffen, weil ihre visionären IT-Konzerne Deep-Tech-Firmen aufgekauft haben. China geht sehr aggressiv vor und tut auch viel mehr als alle anderen. Die Kluft besteht also zwischen diesen beiden großen Ländern mit ihren riesigen, führenden High-Tech-Unternehmen und dem Rest der Welt. Die für die Entwicklung von KI-Anwendungen erforderlichen Tools sind immer noch sehr umständlich. Um sie zu benutzen, ist ein gewisses Maß an Ausbildung erforderlich. Im Moment geht es also darum, wer die besten Grundlagen für KI auf globaler Ebene entwickelt. In dieser Hinsicht arbeiten alle Länder auf die eine oder andere Weise daran.

In Deutschland entstehen derzeit viele KI-Campus. Sind diese Entwicklungen vergleichbar mit dem, was wir einst im Valley gesehen haben?

Neubert: Wir haben in Deutschland einige Kernstädte mit etablierten technischen Universitäten: Berlin, Hamburg, München. Ich würde auch Karlsruhe, Aachen und Tübingen erwähnen, die ebenfalls auf den Zug der KI-Entwicklung aufspringen. In Saarbrücken gibt es das Deutsche Forschungszentrum für Künstliche Intelligenz (DFKI). Diese KI-Campus entwickeln sich nun in Zusammenarbeit mit diesen Universitäten und Einrichtungen. Sie könnten sogar noch einen Schritt weiter gehen und private Investitionen annehmen. So wie es im Silicon Valley geschieht. Wachstumsbeschleunigungs- und Inkubatorprogramme müssen sehr früh ansetzen, damit es eine direkte Verbindung zu den Lehrplänen der Universitäten gibt und die Studierenden direkt an den Start-ups beteiligt sind. Das ist in Deutschland noch nicht so üblich. Das ist eine kulturelle Sache, ein strukturelles Phänomen. Es bricht gerade aus und das ist ein positives Zeichen. Hand in Hand mit diesen Forschungszentren muss die Industrie gehen: Hersteller von Autos und medizinischen Geräten, Anbieter von Biotechnologien für das Gesundheitswesen. Sie werden eng mit diesen Zentren zusammenarbeiten müssen, um die nächste Generation von KI-Produkten zu entwickeln. Es geht darum, Prototypen für Anwendungsfälle zu schaffen, die die Industrie dann übernehmen, anpassen und auf den Markt bringen wird.

Vor einem Jahr haben Sie die Transatlantic AI eXchange Platform ins Leben gerufen. Wie kann sie zu diesen Entwicklungen beitragen?

Neubert: Es handelt sich im Moment um einen Online-Raum für Webinare und Workshops. Sie bringt Multiplikatoren aus Industrie, Forschung und Regierung zusammen. Ziel ist es, Trends und „Moonshot"-KI-Anwendungsfälle vorzustellen. Bis Dezember 2021 haben wir acht Veranstaltungen durchgeführt. Für 2022 sind zwölf weitere geplant. Wir wollen den transatlantischen KI-Austausch vorantreiben. Gleichzeitig hoffen wir, von den Europäern zu lernen, wie die USA ihre KI-Bemühungen besser auf die spezifischen Bedürfnisse der EU ausrichten können.

Ist das deutsche Business-Ökosystem bereit für den Vormarsch der KI?

Neubert: Ich denke, Deutschland hat das erkannt: Es muss wettbewerbsfähig bleiben und darf den vierten industriellen Megas-

hift in 20 Jahren nicht verpassen. Ist die Start-up-Szene dafür bereit? Hat die junge Generation die Offenheit für Unternehmertum? Die Antwort ist ein klares „Ja." Ob das gesamte Ökosystem bereit wäre? Nein, denn es gibt große Unternehmen. In diesen ist das mittlere Management, die derzeitige Generation von Führungskräften, das Problem. Wir müssen diese beiden Welten zusammenbringen. Wir brauchen mehr Agilität und die richtige Denkweise. Unternehmer müssen die Möglichkeit haben, zu scheitern und es erneut zu versuchen. Das ist das Schöne am Silicon Valley. Große Konzerne in Deutschland haben das Geld und das Potenzial, KI so schnell wie möglich einzusetzen, um ihr bestehendes Geschäftsmodell zu verbessern oder neue Bereiche zu erschließen. Einige von ihnen investieren bereits kräftig in ihre KI-Abteilungen. Sie stellen externe Spezialisten ein, KI-Experten von Universitäten. Der nächste Schritt wird sein, dass sie ihr internes Fachwissen aufbauen und dann selbst zur treibenden Kraft werden.

Welche Auswirkungen werden die Europäische Datenschutzverordnung und die Regelungen zur Datensichtbarkeit auf die Branche haben?

Neubert: Lassen wir die Bundesregierung in Berlin und Brüssel die Regulierungsarbeit machen, denn das wird noch lange dauern. Inzwischen kann Deutschland bei der Entwicklung der Technologien aufholen. Wenn amerikanische oder chinesische Unternehmen ihre auf ihren KI-Algorithmen basierenden Dienstleistungen in Europa verkaufen wollen, müssen sie die europäischen Vorschriften einhalten und die gleichen Standards anerkennen und etablieren, um ihre Produkte auch weiterhin europäischen Kunden anbieten zu können. Ich bin absolut dafür. KI-Technologien sind zu sensibel. Sie können zu viele Leben beeinflussen, indem falsche Entscheidungen getroffen werden. Wir müssen einen Schritt zurücktreten, über die Gefahr sprechen, sie angehen und dann weitermachen. Wir brauchen auch Transparenz bei KI-Modellen und -Grafiken, damit die Leute wirklich verstehen, was in KI-Algorithmen vor sich geht. Warum werden bestimmte Entscheidungen getroffen? Denn wenn wir das nicht wissen, kann das sehr negative Auswirkungen haben.

Könnte es sein, dass, wenn Europa die komplexen Vorschriften einführt, die Technologie bereits einen Schritt voraus ist? Dass die Diskrepanz bei den Geschwindigkeiten zu groß sein wird?

Neubert: Ja, das ist in der Tat ein gewisses Risiko. Die Heraus-

forderung besteht in zweierlei Hinsicht. Erstens müssen die europäischen Regulierungsbehörden effektiver, reaktionsschneller und effizienter werden. Das ist einfach eine Tatsache des Lebens. Wenn sie das nicht erkennen, haben wir ein Problem. Die ersten rechtlichen Grundlagen müssen so schnell wie möglich geschaffen werden. Dies ist der Grundrahmen, der sich mit den sensiblen Aspekten der Künstlichen Intelligenz befassen wird. Zweitens muss die Überarbeitung dieser Grundlage mit den neuen Entwicklungszyklen Schritt halten. Dies wird wahrscheinlich eine Dauerschleife sein. Die Innovation ist der Regulierung meist ein bis zwei Schritte voraus, was völlig normal ist.

Haben Sie als Vorsitzender der German American Business Association neue Impulse von der Biden-Administration gespürt?

Neubert: Es ist natürlich ein drastischer Unterschied zur vorherigen Administration. Auch in Berlin haben wir eine neue Regierung. Ich denke, ihre Einstellung zur Künstlichen Intelligenz ist der der Biden-Administration sehr ähnlich. Ich hoffe also, dass es eine sehr synergetische Beziehung sein wird. Auf politischer Ebene stehen wir erst am Anfang der Neudefinition und des Wiederaufbaus dieser vertrauensvollen Beziehung. In praktischer Hinsicht haben beide Länder erkannt, dass sie einander wirklich brauchen. Die USA sind bei der Entwicklung von KI und der Integration von KI in vertikale Anwendungen weit voraus. Deutschland versucht, so gut es geht, aufzuholen. Ich sehe das nicht als echten Wettbewerb. Gleichzeitig haben die USA erkannt, dass Europa wahrscheinlich einer der größten Märkte für den Verkauf ihrer KI-Produkte ist – abgesehen von China mit all seinen Schwierigkeiten. Es besteht also ein gemeinsames Interesse daran, sich gegenseitig zu helfen.

Sie leben seit 30 Jahren im Silicon Valley. Wird es sich wegen der KI-Durchbrüche neu erfinden müssen?

Neubert: Als ich ins Valley kam, gab es hier noch keine Handys und keine Videokonferenzen. Ich habe den Hype um das Internet miterlebt. Dann kam die Schattenseite zum Vorschein, und die Blase platzte. Es war bitter, es war hart, aber wir sind viel stärker daraus hervorgegangen als zuvor. Dann kam die Finanzkrise. Und auch das war schlimm. Das Valley hat sich von einem Halbleiter- und Hardware-Zentrum zu einem Internet- und dann zu einem Software-Standort gewandelt.

Jetzt stehen wir buchstäblich am Anfang der Phase, in der sich alles – nun ja, nicht alles, aber vieles – um Künstliche Intelligenz und deren Implementierung drehen wird. Wird es ähnlich sein wie in den verrückten Zeiten, als das Internet entwickelt wurde? Nein, ganz und gar nicht. Denn alle haben daraus gelernt. Und es ist auch nicht von vornherein etwas völlig Neues, denn KI ist eher eine Steigerung. Außerdem wird es überall auf der Welt ähnliche Entwicklungen geben. Die Technologie wird sich extrem schnell demokratisieren. Die Infrastruktur, Software, öffentliche Cloud-Dienste und erschwingliche Hardware sind bereits da. Die KI-Phase auf globaler Ebene wird also viel schneller kommen und weniger schmerzhaft sein als die Internet-Phase.

Wenn Sie jetzt die Möglichkeit hätten, als Start-up-Gründer eine KI-basierte Anwendung zu entwickeln, welche wäre es dann?

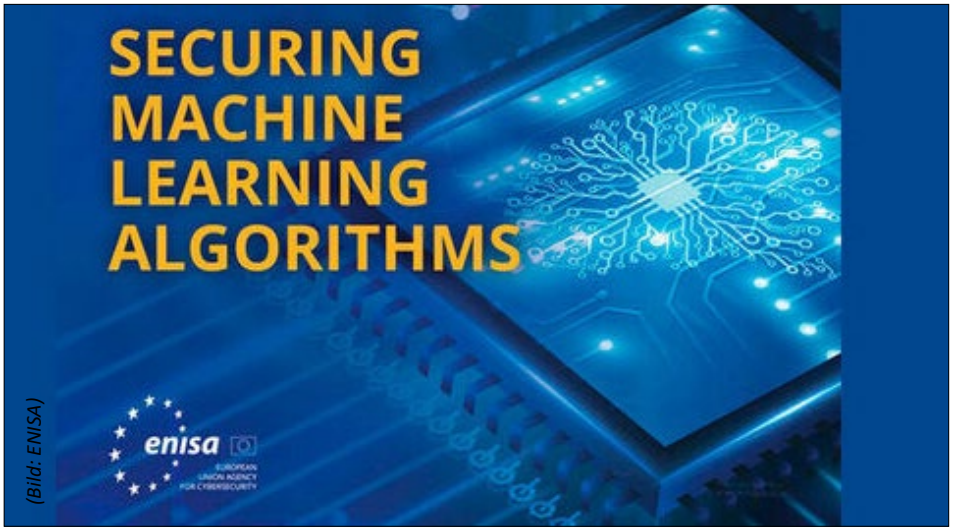
Neubert: Nun, wenn ich schlau wäre, würde ich es Ihnen nicht verraten (lacht). Aber Spaß beiseite, eine zündende Idee habe ich leider noch nicht. Oder ich bin noch nicht auf das richtige Start-up gestoßen. Mein größter Wunsch wäre es, die Welt mithilfe von Künstlicher Intelligenz positiv zu verändern, und zwar im Bereich der digitalen Bildung. Wenn also jemand ein Start-up oder eine Idee im Kopf hat, die mich anspornen könnte ...

Mehr Sicherheit bei Künstlicher Intelligenz

Wie sich Algorithmen für Maschinelles Lernen schützen lassen

07.02.2022 | VON DIPL.-PHYS. OLIVER SCHONSCHEK

Künstliche Intelligenz (KI) spielt nicht nur auf Seiten der IT-Sicherheit eine zunehmend wichtige Rolle. KI ist auch ein mögliches Angriffsziel und Angriffswerkzeug. IT-Sicherheitsbehörden wie die EU-Agentur für Cybersicherheit geben deshalb Hinweise, wie sich die Algorithmen für Maschinelles Lernen besser gegen Missbrauch und Manipulation schützen lassen.



(Bild: ENISA)

Die EU-Agentur für Cybersicherheit ENISA hat Hinweise für die Absicherung von Algorithmen für Maschinelles Lernen veröffentlicht.

Damit der KI-Einsatz im eigenen Unternehmen vorangebracht werden kann, fordern 54 Prozent der Befragten Hilfe bei der rechtlichen und ethischen Beurteilung des KI-Einsatzes, so eine Umfrage des Digitalverbandes Bitkom.

Grundsätzlich sehen die Unternehmen eine breite Palette von Vorteilen von KI. So erwarten 44 Prozent schnellere und präzisere Problemanalysen durch KI, 39 Prozent rechnen mit der Vermeidung menschlicher Fehler im Arbeitsalltag, 21 Prozent erwarten die Verbesserung von bestehenden Produkten und Dienstleistungen, 17 Prozent rechnen sogar mit völlig neuen Angeboten dank KI.

Realität werden können die Erwartungen an KI aber nur dann, wenn ethische Fragen geklärt werden können, der Datenschutz bei einer KI-Lösung stimmt und die Sicherheit bei der KI gewährleistet ist. Doch wie soll Sicherheit bei KI aussehen?

Sicherheitsbehörden warnen vor KI-Risiken

Vor dem Sicherheitskonzept steht immer eine Risikoanalyse. Zudem gilt: Neue Technologien sollten nicht eingesetzt werden, ohne sich der möglichen Risiken bewusst zu sein. So erklärt die EU-Agentur für Cybersicherheit ENISA zu KI: Die Vorteile dieser aufkommenden Technologie sind erheblich, aber auch die Bedenken wie potenzielle, neue Möglichkeiten der Manipulation und Angriffsmethoden.

Der Exekutivdirektor der EU-Agentur für Cybersicherheit, Juhan Lepassaar, sagte dazu: „Cybersicherheit ist eine der Grundlagen vertrauenswürdiger Lösungen für Künstliche Intelligenz. Ein gemeinsames Verständnis von KI-Cybersicherheitsbedrohungen wird der Schlüssel für die weit verbreitete Einführung und Akzeptanz von KI-Systemen und -Anwendungen in Europa sein."

Unternehmen erhalten aber auch Sicherheitshinweise

Die IT-Sicherheitsbehörde ENISA beschränkt sich aber nicht auf die Risikohinweise, auch konkrete Empfehlungen zur Absicherung von KI kommen von dort. ENISA möchte Antworten finden und geben auf Fragen wie: Wie wird maschinelles Lernen cybersicher? Wie verhindert man Cyberangriffe auf maschinelles Lernen? Wie wird Sicherheit möglich, ohne die Leistung der KI zu beeinträchtigen?

Grundsätzlich gilt: KI-Sicherheit ist in weiten Teilen verbunden mit Datensicherheit, denn Algorithmen des maschinellen Lernens werden verwendet, um Maschinen die Möglichkeit zu geben, aus Daten zu lernen, um Aufgaben zu lösen, ohne dass sie explizit dafür programmiert werden. Allerdings benötigen solche Algorithmen zum Lernen extrem große Datenmengen. Und weil sie dies tun, können sie auch spezifischen Cyber-Bedrohungen wie Datenmanipulation und Datenausspähung ausgesetzt sein, wie ENISA betont.

Es gibt kein Patentrezept für KI-Sicherheit, aber Sicherheitstipps

Wenn es um die Absicherung der Algorithmen für das Maschinelle Lernen (ML) geht, trifft die Security auf einen sehr komplexen Bereich und auf vielfältige Anwendungsszenarien. Deshalb macht ENISA zuerst einmal deutlich:

- Es gibt keine Wunderwaffe zur Abwehr von ML-spezifischen Angriffen.
- Einige Sicherheitskontrollen können von Angreifern umgangen werden. Allerdings können Schutzmaßnahmen die Messlatte immer noch höher legen für Angreifer.
- Sicherheitskontrollen führen oft zu einem Kompromiss zwischen Sicherheit und Leistung.
- Der Kontext der Anwendung muss berücksichtigt werden, um die Risiken richtig

Auf dieser Basis bietet ENISA eine Übersicht über mögliche Sicherheitskontrollen, die jeweils auf den konkreten Schutzbedarf und das aktuelle Risiko der KI-Anwendung angepasst werden müssen, darunter auch diese technischen:

Beurteilen Sie das Expositionsniveau des verwendeten Modells: Einige Modelldesigns werden häufiger verwendet oder geteilt als andere (z. B. Open Source-Sharing). Diese Aspekte müssen bei der Risikoanalyse berücksichtigt werden: Modelle, die direkt aus dem Internet entnommen wurden, sollte man nicht ungeprüft wiederverwenden. Man sollte nur Modelle verwenden, bei denen die Bedrohungen klar identifiziert sind und deren Sicherheit kontrolliert wird.

Überprüfen Sie die Schwachstellen der verwendeten Komponenten, damit diese über ein angemessenes Sicherheitsniveau verfügen: Während des Lebenszyklus eines ML-Algorithmus werden mehrere Komponenten (wie Software, Programmierbibliotheken oder andere Modelle) verwendet, um das Projekt abzuschließen. Um sicherzustellen, dass diese Komponenten ein angemessenes Sicherheitsniveau bieten, müssen Sicherheitsüberprüfungen durchgeführt werden. Zum Beispiel: Wenn eine Open-Source-Bibliothek verwendet werden soll, sollten Code-Reviews oder eine Überprüfung auf bekannte Schwachstellen durchgeführt werden.

Es sollte eine Risikoanalyse der Gesamtanwendung durchgeführt werden, um die Besonderheiten des Kontexts zu berücksichtigen, einschließlich Motivation des Angreifers, Sensibilität der verarbeiteten Daten (z. B. medizinische oder personenbezogene Daten), das Anwendungshosting (z. B. durch Dienste von Drittanbietern, Cloud- oder On-Premises-Umgebungen), die Modellarchitektur (z. B. deren Darstellung, Lernmethoden) und der ML-Anwendungslebenszyklus (z. B. Modellfreigabe).

Die Daten müssen überprüft werden, um sicherzustellen, dass sie dem Modell entsprechen und die Aufnahme schädlicher Daten begrenzt wird: Bewerten Sie das Vertrauensniveau der Quellen, um zu überprüfen, ob es im Kontext der Anwendung angemessen ist. Schützen Sie die Integrität entlang der gesamten Datenlieferkette. Bei gelabelten Daten stellt sich die Frage, ob dem Aussteller des Labels vertraut wird.

Definieren und überwachen Sie Indikatoren für das ordnungsgemäße Funktionieren des Modells: Definieren Sie Dashboards zur Integration von Sicherheitsindikatoren (wie ungewöhnliche Änderungen im Modellverhalten), um das ordnungsgemäße Funktionieren des Modells im Hinblick auf den Business Case zu verfolgen, insbesondere um eine schnelle Identifizierung von Anomalien zu ermöglichen.

Stellen Sie sicher, dass für Testumgebungen angemessener Schutz bereitgestellt wird: Testumgebungen müssen auch entsprechend der Sensibilität der darin enthaltenen Informationen gesichert werden.

ML-Projekte müssen den üblichen Prozess zur Integration von Sicherheit in Projekte einhalten, einschließlich der folgenden: Risikoanalyse der gesamten Anwendung, Überprüfung der Integration von Cybersicherheits-Best Practices in Bezug auf die Architektur, sichere Entwicklung.

Prüfen Sie, ob die KI-Anwendung in bestehende betriebliche Sicherheitsprozesse integriert wird: Überwachung und Reaktion, Patch-Management, Zugriffsmanagement, Cyber-Resilienz.

Prüfen Sie die Erstellung einer adäquaten Dokumentation (z. B. technische Architektur, Härtung, Verwertung, Konfigurations- und Installationsunterlagen).

Denken Sie an Sicherheitschecks vor Produktionsstart (z. B. Sicherheitsaudit, Pen-Tests).

Es zeigt sich: Man muss Security nicht neu erfinden, um KI besser zu schützen, vieles ist einem Unternehmen bereits bekannt und anderweitig erprobt, aber Security muss auf die Besonderheiten von KI angepasst werden, immer passend zur jeweiligen KI-Anwendung.

Best Practices

KI-Potenziale für Life Science erkennen und nutzen

28.02.2022 VON DIPL. BETRIEBSWIRT OTTO GEISSLER

Life-Science-Unternehmen werden in den nächsten Jahren verstärkt mit Technologien der Künstlichen Intelligenz (KI) in ihren Arbeitsabläufen experimentieren. Dafür sind verschiedene Use Cases für Teilbereiche wie der Forschung, Entwicklung von Medikamenten und der Vermarktung bereits angedacht oder schon im Einsatz.

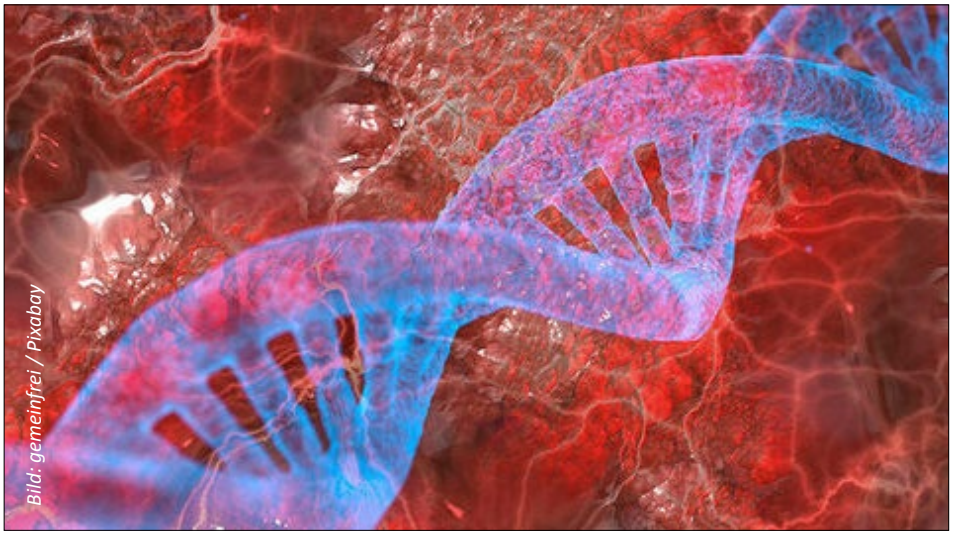


Bild: gemeinfrei / Pixabay

Die KI eröffnet der Life-Sciences-Branche bahnbrechende Möglichkeiten. Jedoch fehlen häufig die notwendigen Fachleute.

Die Künstliche Intelligenz (KI) ist in der Lage, große Mengen an Daten auszuwerten und unterstützt Forscher dabei, wiederkehrende Muster zu erkennen und deutlich schneller präzise Schlussfolgerungen zu ziehen. Gegenwärtig konzentriert sich die Verwendung der KI-Technologien in dem Bereich der Biowissenschaften meist auf Experimente und Pilotprojekte.

Use Case 1: Pipettier-Roboter automatisiert Prozesse

Die flexible Architektur des Pipettier-Roboters „Andrew+“ mit Cloud-basierter proprietärer Software OneLab soll dank einer Machine-Vision-Lösung den Übergang von mühsamen manuellen Pipettier-Vorgängen zu fehlerfreien, voll robotisierten Laborabläufen ermöglichen. Bei Machine-Vision handelt es sich um eine KI-Technologie, mit der bildgebende automatische Inspektionen und Analysen für Prozesssteuerungen und Roboterführungen bereitgestellt werden können. Ein Plus: Für den Anwender

sind keine Kenntnisse in Programmierung, Laborrobotik oder Automatisierungstechnik erforderlich.
Auf diese Weise lassen sich in der Molekularbiologie, Immunologie, Zellbiologie, Mikroskopie und anderen Forschungslabors der Biowissenschaften Flüssigkeiten mit größerer Genauigkeit und konsistenter Wiederholbarkeit für Experimente handhaben und messen. Wobei der Pipettier-Roboter Andrew+ nicht nur den Liquid-Handling-Prozess automatisiert, sondern dem Anwender auch die vollständige Kontrolle über den Arbeitsablauf durch die OneLab-Softwareplattform gibt. Das heißt, Reproduzierbarkeit und vollständige Rückverfolgbarkeit der Probenvorbereitung durch eine intuitive Browser-basierte Softwareumgebung.

Zusätzlich erlaubt OneLab es dem Anwender, eigene Pipettier-Protokolle in wenigen Minuten grafisch zu entwerfen und sie weltweit in jedem Labor auszuführen. Laufende Experimente können sogar über Fernüberwachung begleitet werden. Mit dem Andrew+ Pipettier-Roboter und seinem integrierten Portfolio aus Hardware und intuitiver Software wird es Pharmaunternehmen letztlich ermöglicht, ihre F&E-Prozesse deutlich zu beschleunigen.

Use Case 2: KI-gestützte Suchmaschine zu Antikörpern

Die BenchSci-Plattform wurde zu dem Zweck entwickelt, um sowohl die Wissenschaft als auch Pharmaunternehmen dabei zu unterstützen, ihre Forschungen durch den Einsatz von Modellen für Maschinelles Lernen (ML) zu beschleunigen. Die Plattform hilft Wissenschaftlern dabei, ihr Experimentdesign zu optimieren und somit die Produktivität zu verbessern. Diese maschinellen Lernmodelle sind dazu in der Lage, wichtige Erkenntnisse aus wissenschaftlichen Daten sowie den internen Datenbanken von Pharmaorganisationen zu extrahieren. Ferner können sie die biomedizinische Bedeutung extrahierter Daten analysieren und Beziehungen zwischen den einzelnen biologischen Einheiten herstellen.

Der Anwender kann die Plattform nutzen, indem er eine Suchanfrage in die Suchleiste eingibt und nach Protein-, Gen- oder Klon-IDs sucht. Die Anwendung zeigt dann allgemeine Hyperlinks an, die zu Informationen über Antikörper führen, die sich als wirksam erwiesen haben. Laut BenchSci wurde das der Software zugrundeliegende maschinelle Lernmodell auf 5,1 Millionen Antikörperprodukten, mehr als die Millionen von Herstellern gelieferten Daten und 45.000 Daten von Drittanbietern trainiert.

Wobei die Datenbank jeden Monat mit Informationen aus neuen Veröffentlichungen sowie über neue Produkte aktualisiert wird.

Use Case 3: Software zur Krebsfrüherkennung

Das Biotechnologie- und Pharmaunternehmen Grail entwickelte eine Software zur Krebsfrüherkennung im Blutkreislauf, die medizinische Forschungszentren bei der Durchführung von Studien unterstützen kann. Dadurch sollen die Überlebensraten bei Krebs erhöht und die Krebssterblichkeit sowie das Krebsleiden mithilfe des maschinellen Lernens verringert werden. Das der Software zugrundeliegende maschinelle Lernmodell wurde auf klinischen Daten bzw. Sequenzierungsdaten von Krebspatienten wie beispielsweise zellfreien Nukleinsäuren, die von Tumoren ins Blut abgegeben werden, trainiert.

Die Software soll daher in der Lage sein, die Existenz von Krebszellen im Frühstadium vorherzusagen. Dafür ist es geboten, dass der Anwender zuvor Daten über die körperlichen Krebssymptome in die Software hochlädt. Zusätzlich organisiert Grail selbst verschiedene klinische Studien. Eine dieser Studien, die Circulating Cell-free Genome Atlas (CCGA)-Studie, zielt darauf ab, genomische Krebssignale im Blut von Menschen mit Krebs zu entdecken und sie mit krebsfreien Studienteilnehmern zu vergleichen.

Use Case 4: Vermarktung von Arzneimitteln

Die Decision Support Engine von Aktana unterstützt Vertriebs- und Marketingmitarbeiter von Pharmaunternehmen dabei, mithilfe von Maschinellem Lernen relevante Informationen und Handlungsvorschläge für die Kontaktaufnahme mit Zielpersonen im Gesundheitswesen und den Gesundheitsorganisationen zu liefern. Wobei das maschinelle Lernmodell, das der Software zugrunde liegt, auf Daten des Kundenbeziehungsmanagements (CRM) trainiert wurde.

Die Algorithmen sind in der Lage, segmentierte Arztgruppen mit ähnlichen Merkmalen zu erstellen. Dies hilft den Marketingteams bei der Personalisierung ihrer Botschaften und Kommunikationskanäle. Solche segmentierte Arztgruppen könnten beispielsweise jene sein, die ihre Kommunikation lieber per E-Mail oder Telefon pflegen, die gleichen Spezialisierungen aufweisen oder auch dazu tendieren, neue Behandlungen für ihre Patienten in Betracht zu ziehen.

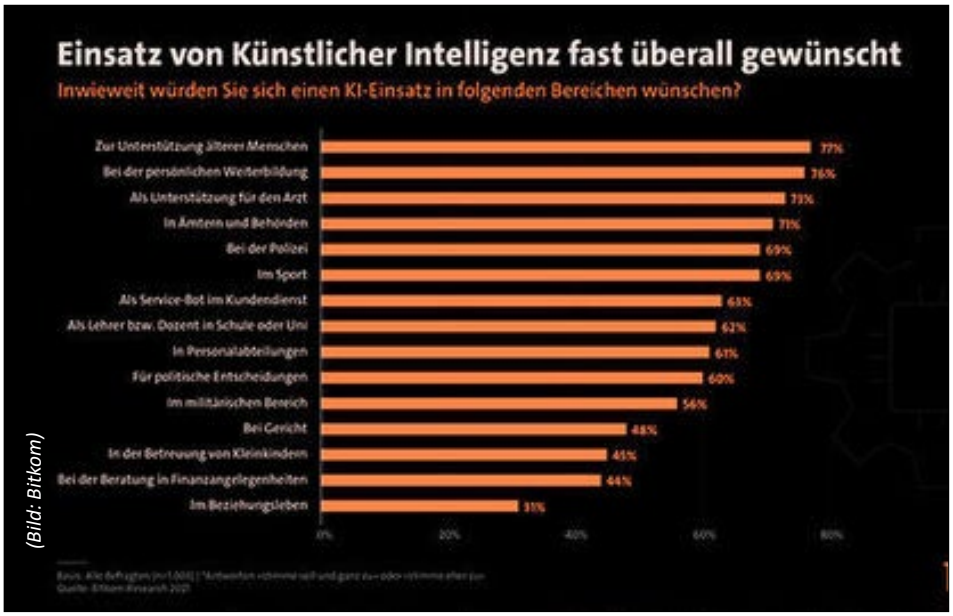
Das System erteilt den Vertriebsmitarbeitern des Kundenunternehmens dann eine Reihe von Empfehlungen, wie und wann sie auf der Grundlage des bevorzugten Kanals, der geografischen Nähe, der Verfügbarkeit und der Anrufhistorie mit ihren Zielpersonen idealerweise kommunizieren sollten.

Auditierung von KI

Wie sich Künstliche Intelligenz inzwischen prüfen lässt

28.03.2022 VON DIPL.-PHYS. OLIVER SCHONSCHEK

Fast drei Viertel der Bevölkerung in Deutschland sieht Künstliche Intelligenz als Chance. Voraussetzung ist aber das Vertrauen in die KI-basierte Lösung. Deshalb sind Auditierung und Zertifizierung von Datenschutz, Ethik und anderer Compliance-Vorgaben bei KI sehr wichtig. Inzwischen gibt es dafür auch zunehmend Frameworks und Prüfwerkzeuge. Wir geben einen Überblick.



(Bild: Bitkom)

In fast allen Lebensbereichen wünscht sich eine Mehrheit den Einsatz von Anwendungen, die auf KI basieren, so der Digitalverband Bitkom. Viele Anwendungsbereiche sind dabei sensibel, sodass die Frage nach Datenschutz, Ethik und Compliance bei KI mehr als gerechtfertigt erscheint.

Mögliche Anwendungsbereiche für Künstliche Intelligenz (KI) sind mehr als vielfältig. Wie eine Bitkom-Umfrage ergab, sehen Bundesbürgerinnen und Bundesbürger KI-basierte Lösungen zum Beispiel als Unterstützung für den Arzt (73 Prozent), um die bestmögliche Diagnose und Therapie zu finden. Jeweils 7 von 10 befürworten eine KI-Nutzung in Ämtern und Behörden (71 Prozent), etwa um Anträge schneller bearbeiten zu können, oder bei der Polizei (69 Prozent), zum Beispiel um mit Videokameras Gefahrensituationen automatisch erkennen oder Orte mit hoher Verbrechenswahrscheinlichkeit identifizieren zu können.

Diese Beispiele machen sehr deutlich, dass die Nutzung von KI durchaus in sensiblen Bereichen erfolgt und zunehmend statt-

finden wird. Auch aus diesem Grund hatte die EU-Kommission bereits Vorschriften und Maßnahmen für Vertrauen im Bereich der Künstlichen Intelligenz vorgeschlagen.

Margrethe Vestager, die für das Ressort „Ein Europa für das digitale Zeitalter" zuständige Exekutiv-Vizepräsidentin, erklärte dazu: „Bei Künstlicher Intelligenz ist Vertrauen ein Muss und kein Beiwerk." Vestager erläuterte auch die Vorteile: „Mit der Schaffung der Standards können wir weltweit den Weg für ethische Technik ebnen und dafür sorgen, dass die EU hierbei wettbewerbsfähig bleibt. Unsere Vorschriften werden zukunftssicher und innovationsfreundlich sein und nur dort eingreifen, wo dies unbedingt notwendig ist, nämlich wenn die Sicherheit und die Grundrechte der EU-Bürger auf dem Spiel stehen."

Die KI-Verordnung der EU soll demnach sicherstellen, dass die Europäerinnen und Europäer dem vertrauen können, was die KI zu bieten hat. Verhältnismäßige und flexible Vorschriften sollen den spezifischen Risiken, die von KI-Systemen ausgehen, gerecht werden und die weltweit höchsten Standards setzen.

Doch wie kann man als Unternehmen eine KI-basierte Lösung auf Vertrauenswürdigkeit prüfen? Wie lassen sich Transparenz, Ethik, Datenschutz und weitere Compliance-Vorgaben für KI auditieren?

Normierung und Standardisierung bei KI

Bevor Audits und eine Prüfung der KI-Compliance sinnvoll sind, müssen die Normen und Standards festgelegt sein, deren Umsetzung und Einhaltung überprüft werden sollen. Wir erinnern uns: Das Deutsche Institut für Normung (DIN) und die Deutsche Kommission für Elektrotechnik (DKE) haben gemeinsam mit den Federführern der KI-Strategie der Bundesregierung sowie Fachleuten aus Wirtschaft, Wissenschaft, betroffenen Behörden und Zivilgesellschaft eine Normungsroadmap erarbeitet. Erste Ergebnisse, um über Normen und Standards den Weg zu verlässlichen sowie vertrauensvollen KI-Systemen und Anwendungen zu ebnen, wurden bereits vorgestellt.

Deutschland ist dabei das erste Land weltweit, das den derzeitigen Bestand und Bedarf an Normen und Standards für KI derart umfassend analysiert hat, wie zum Beispiel der Verband der Internetwirtschaft eco betont.

KI-Lösungen prüfen und zertifizieren

Unter anderem die Fraunhofer-Gesellschaft untersucht mit mehreren Instituten Compliance-Fragen zur KI, darunter die Frage, wie vertrauenswürdige KI konkret umgesetzt werden kann.

Dabei kann Fraunhofer IAIS bereits mehrere Projekte vorweisen, in denen KI-basierte Lösungen untersucht und bewertet werden:

- ScrutinAI soll das Vorgehen der KI sichtbar machen (Visual Analytics)
- CARLA-Simulator untersucht KI-Sicherheit für das Autonome Fahren (Simulation-Based Testing)
- Mit Whitebox-Zwillingen und der regelbasierten Schwachstellenanalyse sollen Blackbox-Modelle und ihre Entscheidungen transparent, nachvollziehbar gemacht werden und potenzielle Schwachstellen behoben werden

Im Rahmen einer strategischen Kooperation entwickeln Expertinnen und Experten des BSI (Bundesamt für Sicherheit in der Informationstechnik) und des Fraunhofer IAIS Prüfverfahren für KI-Systeme. Ziel der Kooperation ist es, technische Produkt- und Prozessprüfungen von KI-Systemen in der Wirtschaft zu etablieren und die Entwicklung einer KI-Zertifizierung „made in Germany“ voranzubringen.

Es gibt auch bereits einen KI-Prüfkatalog des Fraunhofer IAIS. Der Prüfkatalog adressiert zwei Zielgruppen gleichermaßen: „Mit dem KI-Prüfkatalog haben wir jetzt ein praxistaugliches Dokument, das von unabhängigen Prüforganisationen als Grundlage für zukünftige Produktprüfungen genutzt werden kann. Gleichzeitig stellt er Unternehmen das Handwerkszeug zur Verfügung, mit dem sie bereits im Entwicklungsprozess ihre Systeme selbst evaluieren und verbessern können und sich so auf zukünftige regulatorische Anforderungen vorbereiten können“, sagte dazu Prof. Dr. Stefan Wrobel, Institutsleiter Fraunhofer IAIS und Mitglied in der von der Bundesregierung gegründeten Koordinierungsgruppe KI-Normung und Konformität.

Prüfungskataloge und Prüfungsdienste sind bereits verfügbar

Weitere Beispiele für KI-Kriterienkataloge wie auch KI-Prüfservices sind ebenfalls auf dem Markt verfügbar:

- Der Kriterien-Katalog AIC4 (Artificial Intelligence Cloud Ser-

vice Compliance Criteria Catalogue) spezifiziert Mindestanforderungen an die sichere Verwendung von Methoden des maschinellen Lernens in Cloud-Diensten. Er ist als Erweiterung des Kriterien-Kataloges C5 (Cloud Computing Compliance Criteria Catalogue) des BSI konzipiert.

- Das Institut der Wirtschaftsprüfer in Deutschland e. V. hat den Entwurf eines IDW Prüfungsstandards: Prüfung von KI-Systemen (IDW EPS 861) (02.2022) veröffentlicht.
- Das Konsortialprojekt „ExamAI – KI Testing & Auditing“ untersucht anhand von zwei konkreten Anwendungsbereichen (Mensch-Maschine-Kooperation in der Industrieproduktion sowie KI-Systeme im Personal- und Talentmanagement), wie sinnvolle Kontroll- und Testverfahren für KI-Systeme aussehen können. Dabei hat das Projektteam bereits ein „Integratives Framework für KI-Audits“ veröffentlicht.
- Consileon hat ein Audit von KI-Systemen im Finanzsektor vorgestellt.
- Tetrai bietet als Dienstleistung KI Audits, ein „red flag“ KI Audit und ein „extensive“ KI Audit.

Es zeigt sich: An Bemühungen zur Standardisierung, Normung und Zertifizierung von KI mangelt es nicht. Zudem gibt es bereits Prüfungskataloge und Audit-Services für KI. Damit wird die Suche und Auswahl von KI, die bestimmten Compliance-Vorgaben nachkommt, deutlich einfacher. Zudem wird die Grundlage für Werkzeuge gelegt, mit denen Unternehmen zunehmend eigenständig KI-Prüfungen vornehmen können.

Datenanalyse, nicht nur fürs IoT

Stream-Processing mit Apache Flink

16.05.2022 | VON THOMAS JOOS

Für eine effektive, schnelle und unmittelbarer Verarbeitung von Daten zur Analyse ist Data Streaming eine enorm wichtige und interessante Vorgehensweise. Apache Flink ist ein Open Source Tool, das diese Möglichkeiten bietet.

(Bild: Flink.Apache.org)

Apache Flink ist ein quelloffenes Stream Processing Framework, das leistungsstarke Stream- und Batch-Processing-Funktionen bietet.

Apache Flink ist ein Tool für das Data Streaming/Stream Processing von großen Datenmengen. Das quelloffene Stream Processing Framework bietet leistungsstarke Stream- und Batch-Processing-Funktionen.

Der Quellcode des Projektes steht auch auf GitHub zur Verfügung. Viele Anwendungen im Bereich der Datenanalyse erhalten mittlerweile ihre Daten in Echtzeit von einer großen Anzahl an Quellen. Im IoT-Bereich ist zum Beispiel das Streaming von Daten eher die Regel als die Ausnahme. Damit die Anwendungen, die diese Daten verarbeiten sollen, auch mit den richtigen Daten versorgt werden, sind Tools wie Apache Flink kaum mehr wegzudenken.

Data Streaming reduziert die Notwendigkeit zur teuren Datenspeicherung

Muss eine Anwendung große Datenmengen aus verschiedenen Quellen analysieren, erfolgt häufig zunächst eine Speicherung

der Daten in einer Datenbank. Aus dieser Datenbank heraus wird das Analyse-Programm mit den notwendigen Daten versorgt. Dadurch leidet natürlich die Leistung und gleichzeitig erhöhen sich die notwendigen Investitionen für die Analyse, da Massenspeicher in Form von Datenbanken natürlich teuer ist und entsprechender Speicherplatz notwendig ist.

Beim Einsatz von Data Streams oder Stream Processing ist keine Datenspeicherung und vorherige Aufbereitung der Daten notwendig. Durch Tools wie Apache Flink werden die eingehenden Daten in Echtzeit verarbeitet. Alle zu analysierenden Daten werden bereits beim Erstellen analysiert, ohne zuvor erst kompliziert und teuer gespeichert werden zu müssen. Tools wie Apache Flink helfen dabei, Datenströme zu empfangen und weiterzusenden. Dabei finden Analysen statt und die Lösung sorgt dafür, dass die Daten für das Analyseprogramm effizient und fehlertolerant zur Verfügung stehen. Die wichtigsten Features von Apache Flink sind:

- APIs in Java und Scala
- Eine Laufzeitumgebung, die gleichzeitig einen sehr hohen Durchsatz und eine geringe Ereignislatenz unterstützt
- Unterstützung für Ereigniszeit und Out-of-Order-Verarbeitung in der DataStream-API, basierend auf dem Dataflow-Modell
- Verschiedene Zeitsemantiken (Ereigniszeit, Verarbeitungszeit)
- Fehlertoleranz mit Verarbeitungsgarantie
- Natürliches back-pressure in Streaming-Programmen
- Bibliotheken für Graphverarbeitung (Batch), maschinelles Lernen (Batch) und komplexe Ereignisverarbeitung (Streaming)
- Integrierte Unterstützung für iterative Programme (BSP) in der DataSet-API (Batch)
- Benutzerdefinierte Speicherverwaltung für Umschalten zwischen In-Memory- und Out-of-Core-Datenverarbeitungsalgorithmen
- Kompatibilitätsschichten für Apache Hadoop MapReduce
- Integration mit YARN, HDFS, HBase und anderen Komponenten des Apache-Hadoop-Ökosystems

Hoher Durchsatz und niedrige Latenz sind wichtig

Bei der Analyse der Daten spielt der Datendurchsatz eine wichtige Rolle. Dieser muss mit der Menge an Daten zurechtkommen,

die zum Beispiel von den IoT-Sensoren versendet werden. Gleichzeitig muss die Latenz niedrig sind, damit diese Daten auch effektiv und schnell verarbeitet werden können.

Normalerweise arbeiten Anwendungen wie Apache Flink nie alleine. Solche Anwendungen erhalten Daten von Quellen, verarbeiten diese Daten, und senden diese anschließend an weitere Anwendungen. Das heißt, dass Flink nicht nur schnell Daten empfangen und verarbeiten muss, sondern die Daten auch in der Geschwindigkeit weitersenden kann, dass die Ziel-Anwendung die vorbereiteten Daten effektiv nutzen kann. Dazu kann Apache Flink die analysierten Daten und die Streams in Dateisystemen ablegen. Zum Einsatz kommen hier unter anderem HDFS oder S3. Auch das Speichern in herkömmlichen Datenbanken ist möglich, zum Beispiel Apache Cassandra oder ElasticSearch.

Apache Flink ermöglicht eine sehr schnelle Verarbeitung von großen Datenmengen und ist in diesem Bereich auch in der Lage Berechnungen zustandsorientiert durchzuführen. Dabei ist das Tool auch genau in der Verarbeitung. Diese Kombination aus Leistungsfähigkeit, Geschwindigkeit und Genauigkeit macht Apache Flink ideal für den Einsatz in Umgebungen, in denen unbegrenzte Datenströme schnell und zuverlässig analysiert werden sollen. Ein Streaming-Beispiel sieht zum Beispielfolgendermaßen aus:

```
case class WordWithCount(word: String, count: Long)
val text = env.socketTextStream(host, port, '\n')
val windowCounts = text.flatMap { w => w.split("\\s") }
.map { w => WordWithCount(w, 1) }
.keyBy("word")
.window(TumblingProcessingTimeWindow.of(Time.
seconds(5)))
.sum("count")
windowCounts.print()
```

Apache Flink ist stark skalierbar

Gleichzeitig ist Apache auch stark skalierbar und kann die auf einer großen Anzahl von Clusterknoten eingehenden Daten verarbeiten. Das ermöglicht wiederum eine Zusammenarbeit mit anderen Verarbeitungslösungen wie Hadoop, YARN oder Apache Mesos. Beim Betrieb in einem Cluster kann mit Flink sichergestellt werden, dass die Analyse mit hoher Verfügbarkeit stattfin-

den kann.

Weitere Stärken sind die einfache Integration in bestehende Systeme. Dabei hilft auch die REST API, die Anwendungen steuern kann. Dazu kommen weitere APIs mit denen sich auch andere Frameworks und eine Vielzahl an Anwendungen anbinden lassen. Dazu kommen nahezu alle bekannten Operationen zum Verarbeiten von Daten. Diese Flexibilität ermöglicht es zum Beispiel den Zustand jedes eingehenden Ereignisses zu speichern und Timer zu hinterlegen. Zum Zeitpunkt des Auslösens des Timers kann Flink den Zustand des Ereignisses aufrufen und mit anderen Ereignissen für Berechnungen korrelieren.

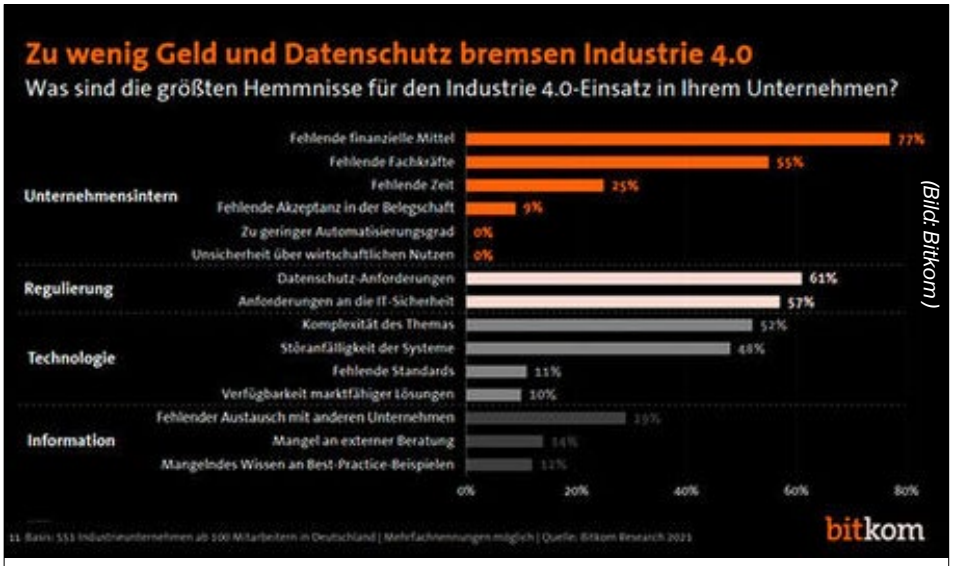
Zusätzlich bietet Apache Flink auch eine API für den Zugriff auf Tabellen und eine SQL-Unterstützung für Abfragen. Diese Abfragen können auch auf die Quellen ausgeführt werden. Dadurch lassen sich Daten aus einer begrenzten Anzahl an Daten auslesen, aber auch aus kompletten Datenströmen. Weitere APIs ermöglichen auch die Verarbeitung komplexerer Daten und Muster in Ereignissen.

Mehr Sicherheit bei IoT-Apps

Wie Low-Code der IoT-Security helfen kann

30.05.2022 / VON DIPL.-PHYS. OLIVER SCHONSCHEK

Sicherheitslücken bei IoT-Anwendungen sind leider keine Seltenheit. Um die IoT-Sicherheit zu erhöhen, werden mehr Fachkräfte für die IoT-Entwicklung benötigt. Alternativ können Low-Code-Plattformen die App-Entwicklung erleichtern und für Security by Design in den IoT-Apps sorgen. Dazu müssen aber die Low-Code-Lösungen selbst Sicherheitsanforderungen erfüllen.



Die Unternehmen erleben aktuell eine Vielzahl von Hemmnissen, die den Einsatz von Industrie-4.0-Anwendungen erschweren, so eine Bitkom-Umfrage. So würden 77 Prozent gerne mehr investieren und klagen über fehlende finanzielle Mittel. 61 Prozent fühlen sich durch Datenschutz-Anforderungen behindert, 57 Prozent von Anforderungen an die IT-Sicherheit.

Die Hemmnisse für den Einsatz von Industrie-4.0-Anwendungen haben sich in den vergangenen Jahren praktisch nicht verändert, so der Digitalverband Bitkom. Die größten Herausforderungen sind fehlende finanzielle Mittel (77 Prozent), Anforderungen an den Datenschutz (61 Prozent) und an die IT-Sicherheit (57 Prozent) sowie der Fachkräftemangel (55 Prozent).

„95 Prozent der deutschen Industrieunternehmen sehen Industrie 4.0 als Chance für das eigene Geschäft. Die Entwicklung und der Einsatz solcher Lösungen sind daher ein Muss für eine erfolgreiche Digitalisierung des Standorts Deutschland“, so Bitkom-Hauptgeschäftsführer Dr. Bernhard Rohleder.

Doch die IT-Sicherheitsanforderungen bei Industrie 4.0 und

IIoT (Industrial IoT) sind komplex, die personellen Ressourcen für Entwicklung und Security bekanntlich knapp. Damit die Sicherheit bei den IoT-Apps trotzdem verbessert werden kann, sind neue Ansätze gefragt.

Low-Code hilft bei der Entwicklung von Apps

Laut dem Analystenhaus Gartner werden in Zukunft Fachleute außerhalb der IT den Großteil der Technologieprodukte und -dienstleistungen entwickeln. Bis 2024 soll dies bereits bei 80 Prozent der Technologieprodukte und -services der Fall sein.
Rajesh Kandaswamy, Distinguished Research Vice President bei Gartner, erklärt auch, wie dies möglich werden soll: „Das Wachstum digitaler Daten, der Low-Code-Entwicklungstools und der durch Künstliche Intelligenz (KI) unterstützten Entwicklung gehören zu den vielen Faktoren, die eine Demokratisierung der Technologieentwicklung über IT-Experten hinaus ermöglichen."
Ähnlich sieht dies das Marktforschungshaus GlobalData: Die Notwendigkeit der digitalen Transformation hat demnach die Nachfrage nach Anwendungsentwicklung in vielen Branchen beschleunigt. Es besteht jedoch eine starke Abhängigkeit von IT-Experten oder -Plattformen, um der steigenden Nachfrage nach der Erstellung neuer Anwendungen gerecht zu werden. Laut GlobalData werden es Low-Code-No-Code-Plattformen (LCNC) sein, die es Nicht-IT-Experten ermöglichen, die Anwendungsentwicklung schneller voranzutreiben.
Kiran Raj, Principal Disruptive Tech Analyst bei GlobalData, kommentiert: „LCNC-Technologien können die Lücken schließen, indem sie Silos zwischen Unternehmensleitern und der IT aufbrechen und es Nicht-Entwicklern, oft als Citizen Developers bezeichnet, ermöglichen, schnell neue Anwendungen für verschiedene Branchen zu entwickeln, einschließlich Finanzen, Dienstleistungen, Gesundheitswesen, Fertigung, Einzelhandel und Technologie."

IoT-Apps sind wichtiger Anwendungsfall von Low-Code

Die Siemens-Tochter Mendix hat die Ergebnisse der internationalen Studie „State of Low-Code 2021" zum Status Quo der Low-Code-Technologie in der Arbeitswelt veröffentlicht: Modellbasierte, visuelle Softwareentwicklung über Low-Code involviert mehr Mitarbeiterinnen und Mitarbeiter in die Digitalisierung und wird heute vielseitig in unterschiedlichen Branchen eingesetzt. Die wichtigsten Einsatzgebiete sind laut den deutschen Befragten Anwendungen für komplexe, individuelle Unternehmenssoft-

ware (37 %), industrielle IoT-Apps (35 %), für automatisierte, existierende Arbeitsprozesse (35 %), für Data Modeling und Visualisierung (34 %) sowie für automatisierte Anwendungen der Robotic Process Automation (31 %).

„Mit Low-Code lassen sich IoT-Apps deutlich schneller und effizienter entwickeln als mit traditionellen Methoden“, erläutert Tino Fliege, Solution Architect bei OutSystems. „Denn im Low-Code-Kosmos erfolgt die Erstellung von Anwendungen nicht Codezeile für Codezeile, sondern mithilfe visueller Modellierung: Vorgefertigte Funktionsbausteine lassen sich auf einer grafischen Oberfläche per Drag-and-drop zusammenstellen, sodass das Rad nicht jedes Mal neu erfunden werden muss, sondern Entwickler auf bestehende Standardfunktionen zurückgreifen können.“

Tino Fliege ergänzt: „Durch umfangreiche Konfigurationsoptionen sowie die Möglichkeit, beliebig eigenen Code zu ergänzen, lassen sich die entwickelten IoT-Shop-Floor-Apps dennoch passgenau auf die individuellen Anforderungen des jeweiligen Szenarios zuschneiden. Die konkrete Anbindung zu den genutzten IoT-Geräten bzw. zu IoT-Plattformen wie PTC Thingworx, AWS IoT oder Azure IoT erfolgt über Standard-Schnittstellen, welche zum Beispiel die OutSystems-Low-Code Plattform zur Verfügung stellt. Auf diese Weise lassen sich die übertragenen IoT-Daten der Maschinen oder Sensoren für beliebige Szenarien nutzen, beispielsweise um sie aufzubereiten und zu visualisieren oder um auf Events zu reagieren, etwa indem eine Notabschaltung ausgelöst wird.“

IoT-Sicherheit hängt dann auch von Low-Code-Sicherheit ab

Eine Low-Code-Plattform kann dabei nicht nur die Entwicklung unabhängiger von den knappen Entwickler-Ressourcen machen, da die Fachabteilungen selbst die IoT-Apps erstellen können. Dank Low-Code-Lösung können die IoT-Apps auch mit den notwendigen Sicherheitsfunktionen ausgestattet werden, ganz im Sinne von Security by Design.

Voraussetzung ist dabei, dass die Low-Code-Plattform selbst die Sicherheit verinnerlicht. Das zeigen zum Beispiel IoT-Apps im Automotive-Bereich, denn hier verarbeiten Hersteller und Zulieferer nicht selten hochsensible Daten, wie detaillierte Produktinformationen und vertrauliche Prototypen. Dass deren Applikationen einem standardisierten Schutzniveau gerecht werden,

belegt der auf der ISO-Norm 27001 basierende Prüfstandard TISAX des Verbands der Automobilindustrie VDA.

TISAX (Trusted Information Security Assessment Exchange) wurde 2017 vom Verband der Automobilindustrie VDA entwickelt und wird seither von der ENX Association betrieben. Es handelt sich um ein Prüfmodell für ein einheitliches Informationssicherheitsniveau in der gesamten Wertschöpfungs- und Lieferkette. Vom Hersteller über Zulieferer bis hin zu Dienstleistern stellt es einen standardisierten Fragenkatalog bereit und ermöglicht damit die branchenweite Anerkennung der Prüfergebnisse.

Nach TISAX ist zum Beispiel „Sentry" von OutSystems zertifiziert worden. Anwender der Plattform für moderne Applikationsentwicklung können sich damit darauf verlassen, dass mit der entsprechenden Lösung verarbeitete Daten sicher und umfassend geschützt sind, so OutSystems.

„In einer derart sensiblen Branche wie der Automotive-Industrie hat Sicherheit oberste Priorität, sowohl physisch als auch digital", erklärt José Casinha, Chief Information Security Officer bei OutSystems. „Für die deutsche Industrie stellt die Automobilfertigung eine der Kernbranchen dar – und damit auch für unsere Aktivitäten am DACH-Markt. Unser Ziel besteht darin, Kunden in diesem Bereich umfassend zu unterstützen und mit der TISAX-Zertifizierung haben wir weiter in dieses Ziel investiert."

Es zeigt sich, dass über sichere Low-Code-Lösungen auch mehr Sicherheit in IoT-Apps kommen kann, trotz Fachkräftemangel in Security und Programmierung. Somit lassen sich bestimmte Hemmnisse bei Industrie 4.0 durchaus beseitigen.

Modernes ETL aus verschiedenen Datenquellen

ML-Modelle einfach trainieren mit StreamSets Transformer

20.06.2022 Von Thomas Joos

Mit StreamSets Transformer kann modernes ETL auch mit Apache Spark zum Einsatz kommen. Sinnvolles Einsatzgebiet ist zum Beispiel das Trainieren von ML-Modellen oder das Sammeln von Daten aus verschiedenen Cloud-Plattformen.

StreamSets Transformer hat den Vorteil, dass Anwender zunächst nichts programmieren müssen, sondern die Verbindungen und Konfigurationen in einer Weboberfläche konfigurieren können.

Tools wie Hadoop und Spark können riesige Datenmengen in kürzester Zeit verarbeiten. Die Herausforderung besteht darin, diesen Big Data Tools auch Daten in der Geschwindigkeit und Menge zur Verfügung zu stellen, sodass eine effektive Verarbeitung möglich ist. StreamSets Transformer ermöglicht es, verschiedene Datenquellen, zum Beispiel rund um das maschinelle Lernen, zu integrieren und zu automatisieren. Dadurch können Datenpipelines erstellt werden, mit denen sich aus verschiedenen Quellen riesige Datenmengen verarbeiten lassen.

Zusammen mit Apache Spark ist es dadurch möglich, Trainingsdatensätze zu kombinieren, zu verbinden und auch anzureichern. Die Datenvorbereitung kann dadurch komplett automatisiert werden. Parallel dazu kann auch Scala und PySpark-Code

als Teil der Datenpipeline zum Einsatz kommen. StreamSets Transformer steht unter einer Apache-2.0-Lizenz zur Verfügung.

Der Vorteil der Umgebung ist, dass Anwender zunächst nichts programmieren müssen, sondern die Verbindungen und Konfigurationen, die für StreamSets Transformer notwendig sind, in der Weboberfläche konfigurieren können. Diese bietet auch Drag-&-drop. In der Oberfläche können darüber hinaus auch mehrere Pipelines und Verbindungen parallel zum Einsatz kommen. Der Anbieter stellt auch eine kostenlose Version zur Verfügung.

Konnektoren zu AWS, Azure, GCP, Snowflakes, Databricks und auch SAP HANA

Wenn Daten auf verschiedene Quellen und Cloud-Plattformen verteilt sind, spielt die Konsolidierung und die Angleichung für Unternehmen eine wichtige Rolle. Diese Daten müssen dann wiederum auf Plattformen, auf denen sie verarbeitet werden sollen, leistungsstark zur Verfügung stehen. StreamSets Transformer hat als Datenpipeline-Engine die Aufgabe ETL-, ELT- und Data-Transformation-Pipelines zu erstellen. Diese können wiederum nativ mit Snowflake oder Apache Spark zum Einsatz kommen.

Um Daten zu streamen, sind Connectoren zur Quell-Plattform notwendig. Hier bietet StreamSets Transformer Verbindungen zu den wichtigsten Clouddiensten wie AWS, Azure, GCP, Databricks und auch Snowflakes. Streamsets bietet aber auch zahlreiche andere Konnektoren. Alle Optionen sind auf der Webseite des Projektes zu finden.

Zu den möglichen Verbindungen gehören auch Hive, Hadoop, MapR, Kafka, MongoDB, Oracle, MySQL, PostgreSQL, Salesforce, SAP HANA und Microsoft SQL Server. Sogar Windows-Ereignisanzeigen lassen sich auslesen und streamen. StreamSets unterstützt damit mehr als 40 Speicher- und Datenbankquellen sowie Kafka Streams und MapR Streams. Microsoft Azure SQL Data Lake und mehr als 30 andere Datenbanken, Speicher- und Streaming-Plattformen lassen sich über das Dashboard anbinden.

Komponenten von StreamSets Transformer verstehen

Basis von StreamSets Transformer sind „Environments“ und „Deployments“. Eine „Environment“ legt fest, wo die StreamSets-Engines eingesetzt werden sollen. Sie stellt die für den Betrieb der Engines die erforderlichen Ressourcen dar. Im Dashboard von

Streamsets können dazu auch mehrere „Environments“ erstellt werden. Alle Aufgaben dazu lassen sich skripten oder in der grafischen Oberfläche konfigurieren.

Ein „Deployment“ ist eine Gruppe von identischen Engine-Instanzen, die in einer „Environment“ eingesetzt werden. Ein Deployment definiert den Typ, die Version und die Konfiguration der StreamSets-Engine, die verwendet werden soll. Auch hier ist es möglich mehrere Deployments in einer Environment zu betreiben und damit eine flexible Struktur aus einer Kombination von verschiedenen Environments und Deployments aufzubauen.

Eine Data Collector Engine führt Daten-Ingestion-Pipelines aus, die datensatzbasierte Datentransformationen im Streaming-, CDC- oder Batch-Modus durchführen. Um eine Data Collector Engine einzurichten, ist ein Deployment in einer Environment notwendig.

Eine Transformer-Engine führt Datenverarbeitungspipelines auf Apache Spark aus, die mengenbasierte Transformationen wie Joins, Aggregate und Sortierungen für die gesamte Datenmenge durchführen. Um eine Transformer-Engine einzurichten ist ein Deployment in einer Environment notwendig.

Erste Schritte mit StreamSets Transformer auf der Cloud-Plattform

Auf der Webseite ist es auch möglich kostenlos über die Cloud mit der Plattform zu arbeiten. Dazu gibt es verschiedene Tutorials, mit denen sich die Möglichkeiten der Plattform mit Beispieldaten schnell und kostenlos testen lassen. Die Einrichtung dauert nur wenige Minuten und es sind keine lokalen Installationen notwendig.

Beim Einsatz der Cloud-Plattform besteht der Vorteil, dass sehr schnell eine kostenlose Version von StreamSets Transformer zur Verfügung steht. In der Oberfläche sind verschiedene Anleitungen, Hilfen und Dokumentationen zu finden, um eine erste Umgebung aufzubauen. Wer erweiterten Support und mehr Funktionen benötigt, kann auf die erweiterten Editionen Professional oder Enterprise wechseln.

- Die Plattform besteht vor allem aus fünf Komponenten, die sich in der Weboberfläche anpassen lassen:
- Control Hub ist das Dashboard zum Erstellen, Bereitstellen und Betreiben von Datenströmen.

- Data Collector ist ein Open Source Tool für die Entwicklung von Streaming-Daten-Pipelines mit einer grafischen Benutzeroberfläche und einer Befehlszeilenschnittstelle.
- Data Collector Edge ist ein Datenerfassungs- und Analysetool für IoT- und Cybersicherheits-Edge-Systeme, das über einen Agenten ausgeführt wird.
- Data Protector erkennt und sichert Daten, während sie eine Pipeline durchlaufen, um die Einhaltung von GDPR/DSGVO, HIPAA und anderen Gesetzvorgaben zu unterstützen.
- DataFlow Performance Manager fügt historische Vergleiche und Daten-SLAs für Verfügbarkeit, Genauigkeit und Sicherheit hinzu.

StreamSets wird mit mehr als 50 vorinstallierten Transformationsprozessoren geliefert, die der Benutzer per Drag-and-Drop auf einen grafischen Arbeitsbereich ziehen kann. Die Prozessoren können Daten aus verschiedenen Quellen anbinden, entfernen, konvertieren, parsen und aggregieren. Entwickler können ihre eigenen benutzerdefinierten Prozessoren in Java, Java Expression Language (EL), JavaScript, Jython, Groovy und Scala schreiben.

Fazit

Wer einen Datenstream aus verschiedenen Quellen zu Apache Spark oder Snowflake aufbauen will, erhält mit StreamSets Transformer eine ideale Plattform dazu, die auch noch leicht zu bedienen ist. Die kostenlose Version ist vor allem für Testzwecke interessant und bietet bereits alle Möglichkeiten, die StreamSets Transformer kennt. Es lohnt sich einen Blick auf die Plattform zu werfen, da sie faktisch ohne Aufwand in wenigen Minuten einsatzbereit ist.

Datenvisualisierungen

Daten abfragen und Dashboards erstellen mit Redash

22.08.2022 VON THOMAS JOOS

Mit Redash können verschiedene Datenquellen angebunden und über Dashboards visualisiert werden. Es können parallel auch mehrere Datenquellen zusammengefasst werden. Der Betrieb der Lösung ist auch mit Docker möglich.

(Bild: © Andrey Popov - stock.adobe.com)

Mit Redash lassen sich Daten aus verschiedenen Datenquellen auslesen, um sie dann zu visualisieren.

Redash hilft dabei, Daten aus verschiedenen Datenquellen auszulesen und anschließend zu visualisieren. Die Einrichtung des Systems ist mit Docker relativ einfach möglich. Mit Redash können auch umfangreichere Datenmengen abgerufen und visualisiert werden. Daher unterstützen auch AWS und Microsoft Azure Redash in verschiedenen Bereichen zur Visualisierung der in der Cloud gespeicherten Dateien.

Um zum Beispiel Daten aus dem Azure Data Explorer mit Redash zu visualisieren, kann die Verbindung zwischen den Systemen im Azure-Portal konfiguriert werden. Wie das geht, zeigt Microsoft auf der Seite „Visualisieren von Daten aus Azure Data Explorer in Redash“. Auch in der Google Cloud kann Redash bereitgestellt werden. Die verschiedenen Datenquellen, die Redash unterstützt sind auf der GitHub-Seite des Projektes aufgelistet.

Nach der Einrichtung von Dashboard kann die Lösung als Zentrale für die Visualisierung von Daten aus verschiedenen Quellen

genutzt werden. Hier ist es auch möglich, mit einer Benutzersteuerung und auch über Gruppen verschiedene Benutzer im System einzubinden.

Redash installieren und testen

Der schnellste Weg, um Redash zu installieren, ist über Docker. Die Einrichtung dazu beschreiben die Entwickler auf der Webseite „Docker Based Developer Installation Guide“. Das Docker-Image für Redash steht über den Befehl docker pull redash/redash zur Verfügung. Die Verwaltung von Redash erfolgt über eine Weboberfläche. Diese zeigt nach der Installation die verschiedenen Möglichkeiten an, um Daten mit Redash zu visualisieren.

Neue Datenquellen an Redash über die Weboberfläche anbinden

Mit der Weboberfläche ist es möglich, schnell und einfach nach dem Anklicken von „Connect a Data Source“ über den Menüpunkt „Data Sources“ die verschiedenen Quellen anzubinden. Wir zeigen nachfolgend, in welcher Reihenfolge die Anbindung von Datenquellen zur Visualisierung erfolgen sollte.

Auf der Seite „Data Sources“ können mit „New Data Source“ zusätzliche Quellen angebunden werden. Nach dem Aufrufen dieser Option zeigt Redash die zahlreichen Datenquellen an, die sich anbinden lassen. Zunächst wird die jeweilige Datenquelle ausgewählt.

Anschließend werden im Fenster die spezifischen Verbindungsdaten zur Datenquelle konfiguriert. Auf diesem Weg lassen sich zum Beispiel auch Datenbanken auf Basis von MySQL, MongoDB oder PostgreSQL anbinden. Auch komplette Data Lakes können mit Redash verbunden werden. Wichtig ist, dass der verwendete Port in den Firewalls zwischen den Systemen freigeschaltet wird. Generell ist es auch sinnvoll, dass Redash ein eigenes Benutzerkonto für die Datenquelle bekommt. Das Benutzerkonto kann bei der Anbindung der Datenquelle genutzt werden. Mit „Test Connection“ lässt sich die Anbindung an die jeweilige Datenbank testen, mit „Save“ wird die Datenquelle in Redash hinterlegt. Auf diesem Weg können nahezu beliebige, verschiedene Datenquellen an Redash angebunden werden.

Abfragen auf angebundenen Datenquellen ausführen

Sobald eine Datenquelle an Redash angebunden ist, können aus Redash heraus Abfragen erstellt werden. Dazu wird der Menü-

punkt „Create\New Query“ verwendet. Mit dem Redash-Icon in der Menüleiste kann zur Startseite der Redash-Weboberfläche gewechselt werden. Hier steht auch noch der Menüpunkt „Create your first Query“ zur Verfügung, wenn noch keine Abfragen erstellt wurden.
Beim Erstellen einer neuen Abfrage ist es sinnvoll durch Anklicken von „New Query“ oben links der Abfrage einen neuen Namen zu geben, der klarmacht, welche Daten die Abfrage erhalten soll. Mit dem Icon „Format Query“ passt die Oberfläche die geschriebene Abfrage an die Formatierung von Redash an, sodass diese übersichtlicher wird. Geschrieben werden die Abfragen in der jeweiligen Syntax der angebundenen Datenquelle. Mit „Execute“ kann die Abfrage auf die Datenquelle direkt in Redash zunächst getestet werden. Wenn die Abfrage korrekt ist, kann sie mit „Save“ gespeichert werden.
Anschließend können im Fenster über eine neue Abfrage Daten abgerufen werden. Funktioniert die Abfrage, kann in Redash ein Zeitintervall festgelegt werden, in dem das Tool die Daten immer wieder aus der Datenquelle abruft. Abfragen stehen erst dann im System zur Verfügung, wenn über „Publish“ die Abfrage im System hinterlegt wird.

Visualisierungen und Dashboards mit Redash erstellen

Nach dem Anbinden von Datenquellen und dem Erstellen von Abfragen, mit denen Daten aus dem System ausgelesen werden können, ist es mit „New Visualization“ innerhalb der Abfrage möglich, die abgerufenen Daten zu visualisieren. Dadurch können aus den angebundenen Datenquellen in kurzer Zeit aktuelle Daten abgerufen und anschließend auch gleich visualisiert werden.
Welche Visualisierung zum Einsatz kommen sollen, hängt von den Anforderungen ab. Hier lassen sich in der Weboberfläche zahlreiche Einstellungen vornehmen, die Redash im Fenster auch gleich anzeigt. Sind die Daten erst einmal in Redash verfügbar, können verschiedene Arten von Visualisierungen erstellt werden. Eine Visualisierung ist erst dann verfügbar, wenn sie gespeichert wird.
Visualisierungen werden wiederum mit Dashboards veröffentlicht. Sobald eine Visualisierung zur Verfügung steht, kann mit „New Dashboard“ ein neues Dashboard erstellt werden. Der Menüpunkt steht auch wieder auf der Hauptseite von Redash zur Verfügung. Ein Dashboard kann aus Textbausteinen und aus Widgets bestehen. Über die Widgets können wiederum die vor-

handenen Abfragen und Visualisierungen ausgewählt werden, die anschließend im Dashboard zur Verfügung stehen. Es ist an dieser Stelle auch möglich, mehrere Widgets und damit auch mehrere Visualisierungen in einem Dashboard zu veröffentlichen. Diese Visualisierungen nutzen wiederum die Abfragen auf die jeweilig verknüpfte Datenquelle im Hintergrund. Wenn die Oberfläche so angepasst ist, wie gewünscht, kann auch das Dashboard mit „Publish“ veröffentlicht werden. Anschließend kann das Dashboard auch geteilt werden. Dazu erstellt Redash einen Link, den die berechtigten Anwender aufrufen können. Der beste Weg für das gemeinsame Arbeiten an Dashboards ist aber das Einladen weiterer Benutzer zu Redash, sodass diese das Dashboard direkt über die Webseite der Redash-Lösung aufrufen können.

Künstliche Intelligenz

Das leistet KI in der Produktion und der Pharmazie

05.09.2022 VON MICHAEL MATZER

Künstliche Intelligenz (KI) gewinnt eine immer größere Bedeutung und wird im Jahr 2030 einen Wirtschaftswert von 13 bis 15 Billionen US-Dollar erreichen, sagt McKinsey voraus. Doch es gibt viele Hürden auf dem Weg zu erfolgreichen KI-Projekten zu überwinden, v. a. in Europa und Deutschland. Ein Roundtable von Experten und Praktikern hat sich über Erfahrungen und Ansichten über diese wichtige Entwicklung in der Technologie ausgetauscht. **Künstliche Intelligenz (KI) gewinnt eine immer größere Bedeutung und wird im Jahr 2030 einen Wirtschaftswert von 13 bis 15 Billionen US-Dollar erreichen, sagt McKinsey voraus. Doch es gibt viele Hürden auf dem Weg zu erfolgreichen KI-Projekten zu überwinden, v. a. in Europa und Deutschland. Ein Roundtable von Experten und Praktikern hat sich über Erfahrungen und Ansichten über diese wichtige Entwicklung in der Technologie ausgetauscht.**

(Bild: InspectifAI)

Die optische Kontrolle pharmazeutischer Produkte überwacht das gesamte „Fließband" auf Unregelmäßigkeiten, etwa bei der Befüllung von kleinen Behältern (blau).

Niko Mohr, Partner bei der Unternehmensberatung McKinsey, sagt für den KI-Markt einen Wirtschaftswert von 13 bis 15 Billionen US-Dollar voraus. „Bei den Anwendungsfeldern von KI sind Produktion, Fertigung und Supply Chain mit etwa 25 bis 30 Prozent des Economic Values vertreten. Das ist substanziell. Zugleich sind alle Technologien vorhanden strategisch durchzustarten . Doch die Projekte liegen hinter den Erwartungen zurück.

Sein Befund basiert, neben praktischen Erfahrungen mit Kunden, auf einer Umfrage von McKinsey zum globalen Einsatz von KI-Technologien, dem McKinsey Global Survey on AI 2021. Dieser fand heraus, dass der Einsatz von KI stetig wächst und die Vorteile weiterhin signifikant geblieben sind. Während der COVID-19-Pandemie zeigten sich die Vorteile vor allem auf der Kosteneinsparungsseite, weniger in der Expansion. Während der geschäftliche Einsatz von KI selbstverständlich wird, werden auch die Tools und Anwendungen verfeinert, die den größten Nutzen aus KI erzielen.

Laut des McKinsey-Reports verwenden Unternehmen, die führend bei der Anwendung von KI sind, nicht nur die Grund-, sondern auch die fortschrittlichen KI-Praktiken, wozu beispielsweise MLOps gehört. Zudem zeichnen sie sich dadurch aus, dass ihre Investition in KI-Technologien (wie Machine Learning) effizienter verwendet wird. Erfolgskritisch ist laut den Autoren des Reports die Nutzung der Vorteile von Cloud-Technologie sowie der Einsatz von Methoden, die die mit KI verbundenen Risiken begrenzen. Die Ergebnisse der Untersuchung legen nahe, dass Unternehmen zu wenig in diesen Bereich investieren.

„Es fehlt an Courage und Konsequenz, mit der ‚wir' diese Themen angehen", sagte Niko Mohr. „Mehr und mehr Unternehmen setzen sich mit dieser Thematik auseinander. Körber ist mit seinem Geschäftsfeld Digital ein bestes Beispiel dafür, indem es die Herausforderungen angenommen und sich extrem weiterentwickelt hat." Körber Digital hat drei Tochterunternehmen gegründet – mehr dazu unten. „Führend sind diejenigen, die sich mit den Potenzialen von KI im Branchenvergleich früh auseinandersetzen. Diese Frontrunner können die Nachzügler substanziell outperformen und hinter sich lassen." Die führenden Wirtschaftsnationen machen Mohr zufolge rund 60 Prozent des bisher erreichten Value Pools aus: Japan, Westeuropa und USA. Auf China entfallen etwa 22 Prozent und auf die Entwicklungsländer etwa 16 Prozent. „Bis 2030 wird sich dieses Verhältnis weiter Richtung China und der Entwicklungsländer verschieben, die deutlich an Bedeutung gewinnen werden, während die führenden Nationen etwas verlieren."

Die Möglichkeit, mit großen Datenmengen Analysen durchzuführen, sei in Europa bedeutend schwieriger als in anderen Re-

gionen der Welt, berichtet Mohr. „Die großen Automobilhersteller machen ihre Tests mit autonomen Fahrzeugen deshalb in den USA und China. Nur mit dem entsprechend großen Datenvolumen lassen sich Algorithmen trainieren und deutliche Schritte nach vorne machen." Mohr resümiert: „Europa und Deutschland entwickeln sich im Vergleich zu den USA und China deutlich langsamer."

Körber & Co.

Körber ist ein internationaler Technologiekonzern mit rund 12.000 Mitarbeitern und mehr als 100 Standorten weltweit. In den Geschäftsfeldern Digital, Pharma, Supply Chain, Tissue und Tabak bietet das Unternehmen Produkte, Lösungen und Services. Im Geschäftsfeld Digital bietet und entwickelt Körber „digitale Produkte, Dienstleistungen und Lösungen mit Experten, Wissenschaft und Partnern aus verschiedenen Branchen der Logistik, Pharma-, Tissue- und Tabakindustrie, um die globale Fertigung zu transformieren. Darüber hinaus zielen wir auf den Aufbau von Technologieunternehmen für eine durch künstliche Intelligenz getriebene Produktionseffizienz."

Daniel Szabo sprach als CEO des Geschäftsfelds Digital, Christian Schlögel als Chief Digital Officer (CDO) des Körber-Konzerns. Schlögel sieht die große Bedeutung von KI, „aber wir sind noch ganz am Beginn." Immerhin gebe es jetzt vier Technologien, die den Aufschwung von KI ermöglichen: „Cloud Computing, Sensorik, Big Data, IoT, und alles zu einem günstigen Preis." KI sei wie ein Baukasten von Technologien: Wissensmanagement, Reasoning (Schlüsse ziehen), Fragestellungen für Vorhersagen und das Berechnen von Szenarien. Wichtig sei die Mensch-Maschine-Schnittstelle (HMI): „Interaktion, Wahrnehmung und Verstehen durch Computer" sei von zentraler Bedeutung.

Noch viele Altlasten

Für Produktionsunternehmen, die ganz am Anfang ihrer Digitalisierungs-Journey stehen, bedeuten diese Bedingungen eigentlich beste Startmöglichkeiten. Doch Daniel Szabo von Körber Digital konstatiert, dass es noch viele Brownfield-Systeme gebe, die Schritte vor Digitalisierung und Industrie 4.0 zu bewältigen hätten. „Die Herausforderung besteht nun darin, Probleme zu identifizieren, die durch das Nutzen von digitaler Technologie

gelöst werden können und dadurch ausreichend großen Mehrwert stiften. Der Grund ist simpel: In der ersten Digitalisierungswelle wurde viel in Datensammeln gesteckt, aber kaum etwas damit erreicht. Daher will heute kaum noch jemand signifikante Beträge investieren, wenn kein Mehrwert zu sehen ist.“ Seine gute Nachricht: „Es gibt noch ganz viele Potenziale. Es kommt darauf an, User-zentrierte Lösungen zu entwickeln, die einen messbaren Mehrwert schaffen, das heißt, für Kunden und andere Stakeholder-Gruppen.“ Mohr warnt jedoch, Industrie 4.0 nicht mit KI zu verwechseln.

Kein Datenmangel

Schlögel entgegnet Mohrs Perspektive auf die Herausforderungen des Datenmangels: „Wir müssen unseren Datenschutz nicht auflösen, aber wir können Daten anonymisieren. Es ist wichtig, den Wert von Daten zu erkennen und Datenzugriff als einen Wettbewerbsvorteil zu bewerten. Alles andere würde Fußfesseln bedeuten. Es gilt, smartere Lösungen zu finden: Wie können wir Software-Unternehmen die Möglichkeit geben, auf solche Daten zuzugreifen, ohne den gläsernen Mitarbeiter oder Bürger zu erzeugen?“ Szabo gibt Schlögel recht: „Es gibt Privacy-Enhancing-Computation-Technologien wie Maskieren, Anonymisieren und Pseudonymisieren, die es ermöglichen, Daten zur Verfügung zu stellen, um Algorithmen zu trainieren, ohne den Wettbewerbsvorteil freizugeben.“

Niko Mohr rät, „vorausblickend in Technologien zu investieren, die auch künftig im KI-Umfeld Relevanz besitzen: Dazu gehört Data-centric AI, beispielsweise Simulation, Operations Management inklusive OEE (Overall Equipment Effectiveness) , Predictive Maintenance, Human Productivity und Inventory Optimization.“ Mit Energieffizienz ließe sich der Green Deal der EU unterstützen, ergänzt Schlögel und verweist auf einen Anwendungsfall in zwei Körber-Tochterunternehmen namens FactoryPal und InspectifAI: „Mit FactoryPal können wir den OEE um 30 Prozent erhöhen inklusive der Optimierung von Parametern wie beispielsweise den Energieverbrauch. Bei InspectifAI können wir die Fehlauswurfrate in der pharmazeutischen Produktion mittels KI-gestützten visuellen Qualitätskontrollen um 85 Prozent senken.“

FactoryPal: KI in der Qualitätskontrolle

FactoryPal ist ein 2020 gegründetes Körber-Start-up im Bereich Industrial IoT aus Berlin. „Das Team bietet eine Software-as-a-Service-Lösung an, mit der die Fertigung in Fabriken weltweit effizienter gestaltet werden kann“, berichtet FactoryPal-CTO Andreas Schilling. „Die auf KI basierende Technologie analysiert Maschinendaten, verbindet Produktionslinien miteinander und optimiert so Arbeitsprozesse.“

FactoryPal richte sich initial an produzierende Unternehmen auf dem europäischen Markt. „Die Lösung wird für Kunden in der Tissue-Industrie eingesetzt und soll perspektivisch auf andere Bereiche der Fertigungsindustrie und internationale Märkte ausgeweitet werden.

InspectifAI: KI in der Pharmazie

Während FactoryPal mithilfe von KI für mehr Effizienz in der Fertigung sorgt, konzentriert sich das 2021 gegründete Körber-Venture InspectifAI auf den pharmazeutischen Markt. „Ziel ist es, die optische Inspektionskontrolle von pharmazeutischen Produkten wie z. B. Impfstoffdosen zu revolutionieren“, erläutert InspectifAI-CTO Moritz Strube. „Mittels KI-Unterstützung sollen die Inspektionsentscheidungen von heutigen Inspektionsmaschinen optimiert werden, sodass die sehr hohe Rate fälschlicherweise aussortierter Produkte, sogenannter False Ejects, auf ein Minimum reduziert wird.“

Der Use Case verspricht, einen hohen Mehrwert zu erzielen. „Gerade Hersteller pharmazeutischer Produkte müssen in deren Produktion größte Sorgfalt walten lassen. Ein beschädigtes oder verunreinigtes Produkt im Handel bedeutet schwerwiegende Folgen für Patient und Produktionsunternehmen bis hin zur Schließung des Produktionsstandortes. Zu Recht gestalten sich die Inspektionskontrollen daher als besonders wichtig und genau. Diese Vorsicht und Sorgfalt führt im Extremfall dazu, dass beinahe jedes dritte Produkt von der Inspektionsmaschine fälschlicherweise aussortiert wird. Das nachträgliche, händische Prüfen der aussortierten Produkte durch Mitarbeiter ist zeit- und kostenintensiv. Hier setzt InspectifAI an.

Seit 2021 entwickelt Körber Digital eine Softwarelösung, die direkt aus der Erfahrung von Inspektionsspezialisten lernt und dieses Wissen mittels trainierter Deep-Learning-Modelle einer Inspektionsmaschine zugänglich macht. Dadurch wird die Ent-

scheidungstreue und -sicherheit der Inspektionsmaschine deutlich erhöht. Vereinfacht gesagt, trifft die Software InspectifAI eine bessere Entscheidung als bisherige Bildverarbeitungsmethoden, sodass es nichtmehr zum fälschlichen Auswurf der Produkte kommt. Was einfach klingt, kann den Arbeitsaufwand für Unternehmen und damit auch Kosten drastisch senken.

„Je nach pharmazeutischem Produkt und vorherrschenden Produktionsvarianzen kann die False-Eject-Rate zwischen 50 und 99 Prozent reduziert werden", erläutert Moritz Strube. „Mit unserer Lösung beschränken wir uns nicht auf Inspektionsmaschinen aus dem Hause Körber, sondern fokussieren alle Maschinen, die vollautomatische visuelle Inspektionsaufgaben in der Pharmaproduktion erfüllen. Mit unserem Ansatz, durch KI den visuellen Inspektionsprozess zu verbessern, stiften wir einen großen Mehrwert für alle Hersteller pharmazeutischer Produkte. Eine genaue und zuverlässige Kontrolle ohne ständige Rückläufer, unabhängig von der einzelnen Inspektionsmaschine, bedeutet eine erhebliche Effizienzsteigerung der Kontrollen."

Personalmangel

Für Daniel Szabo fehlt es vor allem an geeignetem Personal, um den KI-Markt in Deutschland und Europa zu fördern. „Die Kompetenz ist da, ebenso die Talente in Deutschland, aber auf der Entscheiderebene fehlt noch das Verständnis, um einerseits den Mut zu haben, Lösungen voranzubringen, andererseits zu investieren, um die richtigen Leute an Bord zu holen, die sich damit auskennen, und ihnen dann auch den notwendigen Freiraum zu geben, um Wert-Pools zu erkennen und freizusetzen."

Szabo über Kritik an den Vorständen und Aufsichtsräten: „Die Entscheider haben die Sorge, Wettbewerbsvorteile abzugeben. Daten haben irgendwie einen Mehrwert, aber das Datensammeln und -speichern erzeugt keinen Mehrwert. Man muss etwas damit machen und darüber eine Verhaltensänderung herbeiführen, damit sich etwas ändert. Nur dann kann ich einen Wert wirklich zutage fördern."

Guter Rat

Szabo empfiehlt: „Suche dir einen Partner, mit dem du das Projekt zusammen machen kannst. Sei bereit, gemeinsam im Ökosystem zu arbeiten und nicht alles als proprietäre eigene Lösung zu bauen. Für die meisten mittelgroßen Spieler wird keine Chance vorhanden sein, dort mitzuspielen." Körber hat in DAIN Stu-

dios investiert, ein deutsch-finnisches Unternehmen für Unternehmensberatung im KI-Umfeld.

Ein guter Start

„Die Resonanz und das Interesse der Pharmaunternehmen ist beeindruckend“, zeigt sich InspetifAI-CTO Moritz Strube erfreut. „Bereits heute befinden wir uns in konkreten Projekten mit Vertretern aus unterschiedlichen Kundensegmenten, von Top-10-Pharmaunternehmen bis hin zu Vertragsherstellern.“

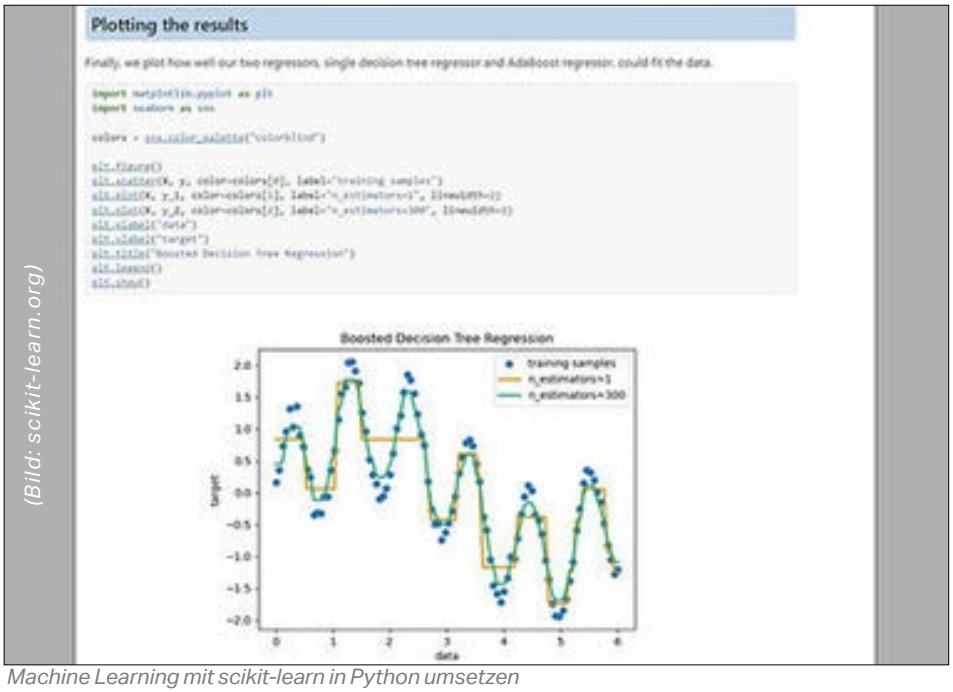
Das liege unter anderem daran, dass die InspectifAI-Vision nicht bei der Optimierung der Einzelanlage ende. „Wenn es gelingt, das erlernte Wissen mittels KI-Modellen im Inspektionsmaschinennetzwerk des Pharmaherstellers zu transferieren, ergeben sich enorme Skalen- und Netzwerkeffekte. Kostenersparnisse, Qualitätsgewinne sowie Produkt- und Patientensicherheit potenzieren sich im selben Maße.“

Data Science und Machine Learning

Scikit-learn – KI, Statistik, Mathematik, Analyse oder Data Mining mit Python

10.10.2022 VON THOMAS JOOS

Wer sich mit Künstlicher Intelligenz (KI) und Machine Learning (ML) oder auch mit Programmen im Bereich Statistik, Mathematik, Analyse oder Data Mining beschäftigt, sollte sich die Möglichkeiten der Python-Library scikit-learn anschauen. Der Beitrag gibt einen Überblick.



Machine Learning mit scikit-learn in Python umsetzen

Bei scikit-learn handelt es sich um eine freie Software-Bibliothek für Python. Die Library scikit-learn leitet sich von SciPy Toolkit ab und baut auf der Programmiersprache Python auf. Im Fokus der Bibliothek stehen Möglichkeiten zur Programmierung von Anwendungen im Bereich von Machine Learning und anderen Bereichen. Scikit-learn kann auch Pakete wie NumPy, SciPy, oder Matplotlib einsetzen.

Scitcit-learn in eine aktuelle Python-Umgebung integrieren

Die Integration in einer 64-Bit-Installation von Python 3 ist sehr einfach über einen der Befehle „pip install -U scikit-learn“, „pip

install scikit-learn“ oder „conda install scikit-learn“ möglich. Die Installation lässt sich danach mit den folgenden Befehlen überprüfen:

```
python -m pip show scikit-learn
python -m pip freeze
python -c "import sklearn; sklearn.show_versions()"
```

Für die Einarbeitung finden sich im Internet auch zahlreiche Beispieldaten für das das Machine Learning.

Schlanke API, gute Dokumentation und Einheitlichkeit der Komponenten

Die Bibliothek bietet eine einheitliche und schlanke API, inklusive einer umfassenden Dokumentation. Das ist für das Schreiben von Programmen zum Thema mathematische, wissenschaftliche oder statistische Anwendungen mit Python ein wichtiger Faktor. Auch für das Data Mining und zur Datenanalyse kann scikit-learn genutzt werden, genauso wie für Anwendungen, die sich mit den Themen KI und ML beschäftigt.

Ein Vorteil dieser Einheitlichkeit ist, dass Entwickler und Analysten, sobald sie die grundlegende Verwendung und Syntax von scikit-learn für einen Modelltyp verstanden haben, sehr einfach zu einem neuen Modell oder Algorithmus wechseln können. Dadurch lassen sich mit scikit-learn entwickelte Komponenten auch in größere Programme einbinden. Die Library kann parallel zu PyTorch genutzt werden. PyTorch ist ein Machine Learning-Framework auf Basis von Open Source.

Bots, Sprachassistenten und andere KI/ML-Lösungen entwickeln

Scikit-learn steht unter der BSD-Lizenz kostenlos zur Verfügung. Die Library kommt auch zum Entwickeln von Bots oder für das Entwickeln von Apps für Sprachassistenten und anderer Lösungen zum Einsatz. Wenn Künstliche Intelligenz und Machine-Learning-Programme mit Python entwickelt werden sollen, ist es sinnvoll, sich die Möglichkeiten von scikit-learn genauer anzuschauen. Scikit-learn kann darüber hinaus von Computerprogrammen erstellte Nachrichten im Internet von

menschlich erstellten Texten unterscheiden, da auch hier KI-Komponenten zum Einsatz kommen.

Die Entwickler von scikit-learn stellen auch verschiedene Tutorials bereit. Die Library kann auch gemeinsam mit Pandas oder TensorFlow zum Einsatz kommen. Das Open Source Framework TensorFlow wird von zahlreichen anderen KI-Programmen und -Tools genutzt. Mit den Bibliotheken können ML-Modelle entwickelt und trainiert werden. Scikit-Learn teilt dazu seine Teilbibliotheken auf:

- Classification
- Regression
- Clustering
- Dimensionality Reduction
- Model Selection
- Preprocessing

Das Importieren der Teilbibliotheken erfolgt zum Beispiel mit:

```
import sklearn.cluster as cl
# Neuronales Netz zur Klassifikation
from sklearn.neural_network import MLPClassifier
# Neuronales Netz zur Regression
from sklearn.neural_network import MLPRegressor
```

Um einen Überblick zu den verfügbaren Modellen zu erhalten, kann der folgende Code zum Einsatz kommen:

```
from sklearn import tree
```

Wichtig ist dabei, das Modell zu initialisieren. Danach lässt sich es trainieren (fit). Im Anschluss können zum Beispiel sich Prädiktionen (predict) und die Genauigkeit (score) ausgegeben werden. Mit scikit-learn ist es möglich eine Vielzahl von Modellarten und Anwendungen umzusetzen. Der komplette Datenvorverarbeitungs- und Trainingsprozess kann zum Beispiel auch in Pipelines zusammengefasst werden.

Integration von Python-Komponenten in andere Anwendungen

Anwendungen, die mit scikit-learn geschrieben werden, lassen sich auch in andere Programme integrieren. Dadurch können Programme KI-Funktionen erhalten, die mit scikit-learn entwickelt wurden. Im Bereich von ML arbeitet scikit-learn auch mit Funktionen von Cloud-Lösungen aus dem Bereich KI/ML zusammen, zum Beispiel auch mit Azure Databricks. Die Microsoft-Cloud-Lösung vereint verschiedene Big Data Use Cases auf einer einzigen Plattform. Auch das maschinelle Lernen und Data Science lassen sich einbinden.

Azure Databricks enthält viele maschinelle Lernbibliotheken, unterstützt aber auch die einfache Interaktion mit vielen anderen gängigen maschinellen Lernframeworks wie XGBoost, scikit-learn, TensorFlow, Keras und Horovod. Mit Azure Machine Learning können Modelle auf Basis von scikit-learn auch im großen Stil trainiert werden. Beispiele dafür beschreibt Microsoft in der Dokumentation zu Azure Machine Learning.

Der Markt für automatisiertes Machine Learning ist hart umkämpft. Angebote gibt es unter anderem. von DataRobot, Google (AutoML Tables), H2O (Driverless AI), IBM (AutoAI), Microsoft (Azure Automated ML) und als Open-Source-Bibliotheken wie Auto-Weka, Auto-sklearn oder TPOT. Viele dieser Systeme nutzen dafür scikit-learn als ML-Bibliothek für Python.

Daten mit scikit-learn darstellen

Beim maschinellen Lernen geht es vor allem darum, Modelle aus Daten zu erstellen. Dazu ist die Darstellung der Daten wichtig, damit diese auch richtig verarbeitet werden können. Daten in scikit-learn lassen sich zum Beispiel mit Datentabellen darstellen. Eine Tabelle ist dabei generell ein zweidimensionales Gitter, in dem die Zeilen einzelne Elemente des Datensatzes darstellen und die Spalten Mengen, die mit jedem dieser Elemente verbunden sind. Informationen lassen sich dadurch als zweidimensionales numerisches Array oder als Matrix betrachten. Hier lassen sich zum Beispiel noch NumPy-Arrays oder Pandas DataFrame nutzen und scikit-Learn-Modelle akzeptieren auch SciPy-sparse-Matrizen.

Die Stichproben in den Zeilen können sich dabei auf die einzelnen Objekte beziehen, die durch den Datensatz beschrieben werden. Die Stichprobe kann zum Beispiel eine Person, ein Dokument, ein Bild, eine Tondatei, ein Video, ein astronomisches Objekt oder etwas anderes sein, das mit einer Reihe von quanti-

tativen Messungen beschrieben werden kann. Die Merkmale in den Spalten beziehen sich wiederum auf die einzelnen Beobachtungen, die jede Stichprobe auf quantitative Weise beschreiben.

Nachbericht IT-Sicherheitsfachmesse it-sa 2022

Der Status quo bei KI in der Cybersicherheit

14.11.2022 VON DIPL.-PHYS. OLIVER SCHONSCHEK

Wenn sich die Security-Branche trifft, dann ist der Fachkräftemangel eines der führenden Themen. Hoffnungsträger ist Künstliche Intelligenz (KI). Doch was kann KI oder Machine Learning bereits in der Security übernehmen? Wie sind die Erwartungen, was in Zukunft möglich wird? Kann KI eine vollautomatische Security Realität werden lassen? Die it-sa 2022 ermöglichte hierzu Einblicke. Der Ruf nach mehr IT-Sicherheit wird immer lauter, gerade mit Blick auf die Sicherheit Kritischer Infrastrukturen, so eine Botschaft der IT-Sicherheitsfachmesse it-sa, die im Oktober 2022 in Nürnberg stattfand.

Untypische Muster in der Kommunikation innerhalb einer Unternehmens-IT führen eine sich anbahnende Gefahr vor Augen.

Doch dieses Mehr an Security ist sehr herausfordernd: IT-Security-Professionals zählen zu den derzeit gefragtesten Arbeitnehmern, Fachkräfte mit entsprechenden Kenntnissen sind rar. Mit der Unterstützung der Initiative „Deutschlands bester Hacker“ fördert zum Beispiel die it-sa die Suche nach neuen Talenten.

Neben der Talentsuche und den zunehmenden Weiterbildungsmöglichkeiten in der Security gibt es eine weitere Stoßrichtung: Die zunehmende Nutzung von KI in der Security. Was aber bietet KI in der Security Stand heute, und was kann sie in absehbarer Zukunft leisten? Ist sie in der Lage, die Security-Fachkräfte nicht

nur zu unterstützen und zu entlasten, sondern auch fehlendes Personal in der Cybersicherheit zu ersetzen?

Kann IT-Sicherheit komplett automatisiert werden?

Spricht man mit Security-Expertinnen und -Experten zum Beispiel auf der Security-Fachmesse it-sa, hat keiner Sorge, einmal den eigenen Job zu verlieren und durch eine KI-Lösung ersetzt zu werden. Die meisten IT-Sicherheitsfachkräfte sehen in KI, sofern man davon so spricht, eine Unterstützung. Dabei ist es weniger die „Intelligenz" in Security-Lösungen als vielmehr die Möglichkeit, Abläufe in der Security zu automatisieren.

Machine Learning ermöglicht die Suche nach auffälligen Mustern, nach Anomalien in den verschiedensten Daten der Security, im Netzwerkverkehr, in den Protokollen der Anwendungsaktivitäten oder bei Zugriffsversuchen auf Daten, um nur einige Beispiele zu nennen.

In bestimmten Bereichen können entsprechende Regeln aufgestellt werden, nach denen Maschinen dann auf Basis erkannter Vorfälle auch Reaktionen einleiten, als Auto-Response der Security. Welche Aktivitäten automatisch ablaufen dürfen und wo der Mensch nochmals überprüft, hängt von der genauen Situation ab.

So könnte man durchaus einen einzelnen Nutzer von seinem E-Mail-Konto automatisch trennen, wenn das Risiko für böswillige Aktionen gesehen wird und dafür viele andere Nutzerkonten verschont bleiben. Ob man allerdings eine große Zahl scheinbar verseuchter Endpoints automatisiert „kaltstellt", da sind die Security-Expertinnen und -Experten eher skeptisch.

Gefragt sind Teams aus Security-Fachkraft, Maschine und Kunde

Bei einem möglichen Security-Vorfall kann eine Maschine eine Anomalie entdecken, je nach Regel dann selbst aktiv werden oder es der Security-Fachkraft melden. Die Security-Analystinnen und -Analysten prüfen die Warnung und reagieren, je nach Vereinbarung direkt oder nach Rücksprache mit dem Kunden, teilweise geben sie auch eine Warnung mit Handlungsempfehlungen an den Kunden weiter, der dann selbst aktiv wird.

Security ist in dieser Vorstellung also Teamwork, wobei das Team aus Security-Fachkraft, Maschine und Kunde besteht. Vollautomatische Security ist dies in aller Regel nicht, sodass der Fach-

kräftemangel zwar gemindert wird durch die Automatisierung, aber nicht behoben werden kann.

Was aber kann die KI oder Machine Learning bisher konkret leisten, wie kann die Security bislang unterstützt werden, und wo kann die Automatisierung noch viel weiter gehen als heute üblich? Das zeigen Beispiele und Gespräche von der it-sa 2022.

Ein Security-Experte wie Sebastian Ganschow, Director Cybersecurity Solutions at NTT Ltd. in Deutschland, sieht die aktuelle Lage von KI in der Security zum Beispiel so: „Ein automatisches Security Operations Center ohne jeden menschlichen Analysten und ohne jede menschliche Analystin wird es meines Erachtens nicht geben. Vieles, was in der Security als KI bezeichnet wird, sind eigentlich eher Expertensysteme und Machine Learning. Die Nutzung von KI im eigentlichen Sinne ist in anderen Branchen bereits fortgeschrittener. Was uns Menschen gegenüber KI auszeichnet, ist zum Beispiel etwas wie Bauchgefühl. Hier wird Deep Learning den Maschinen in Zukunft auch noch einiges ermöglichen."

Beispiele für Machine Learning / KI in der Security

Anomaly Shield von Airlock dient der Erkennung von Bots mit Machine Learning: Airlock Anomaly Shield lernt während der Inbetriebnahme, wie sich die echten Benutzer einer Anwendung verhalten. Für das Unsupervised Learning werden die Rohdaten aufbereitet und aggregiert, um die Präzision und Trefferquote zu optimieren. Die in der Trainingsphase gelernten Machine-Learning-Modelle bilden die Charakteristika der Businessanwendung ab. Im Betrieb werden alle aktiven Sitzungen permanent mit dem gelernten Verhalten verglichen. Wenn die Abweichung zu groß ist, wird die Sitzung als Ausreißer gekennzeichnet. Ob eine Anomalie nur protokolliert wird, oder ob die Sitzung terminiert und die IP-Adresse blockiert wird, lässt sich für jede Anwendung getrennt steuern.

Sailpoint: KI hilft bei Prüfung und Schärfung der Rollen und Privilegien: Empfehlungen auf Basis von Künstlicher Intelligenz helfen dabei, Entscheidungen zur Gewährung von Benutzerzugriffen zu treffen. Der Self-Service und das automatisierte Policy-Management von IdentityNow ermöglichen zudem mit KI-Unterstützung, den Zugriff nur gemäß der von einem Unternehmen erstellten Policies zu gewähren, erklärt der Anbieter.

SentinelOne: KI bei XDR (Extended Detection and Response):

Endpoint Protection (EPP) und Endpoint Detection and Response (EDR) von SentinelOne kombinieren Automatisierung mit KI und ML, um moderne Angriffe in Echtzeit, mit Maschinengeschwindigkeit und ohne zusätzlichen Eingriff zu erkennen und zu beheben. Dies bedeutet, dass Unternehmen ihre Ressourcen auf die Bewältigung betriebsspezifischer Aufgaben konzentrieren können, so der Anbieter. In diesen Bereichen arbeitet die Security dann sehr „selbstständig".

ForeNova: Detection and Response-Dienste und Analyse des Netzwerkverkehrs: NovaCommand soll für kleine und mittelständische Unternehmen das Erkennen von Angriffen aufgrund von anomalem Netzwerkverkehr handhabbar machen. Die Technologie verzeichnet automatisch und KI-gestützt Anomalien im ein- und ausgehenden sowie im internen Netzwerkverkehr und damit mögliche Angriffe. Die nicht-intrusive Network Detection and Response analysiert die Daten auf den Mirror-Ports nicht intrusiv, sodass sie keine Leistungseinbußen verursacht, so der Anbieter. Die Spiegelung des Datenverkehrs ermöglicht auch eine rückwirkende Analyse von Sicherheitsereignissen.

Fortra, früher HelpSystems: Unterstützung der Managed Security Services mit Machine Learning: Fortra bietet Unternehmen umfangreiche Security-Lösungen aus einer Hand, darunter Lösungen wie Alert Logic, Digital Guardian, Cobalt Strike, Tripwire, Digital Defense, Terranova Security, Clearswift, Agari, PhishLabs, Core Security, GoAnywhere, Boldon James und Titus. In Zukunft werden viele Funktionen der nun zu Fortra gehörenden Lösungen über eine zentrale Plattform verfügbar sein. Die Services zu den einzelnen Lösungen werden aber weiterhin durch einzelne Spezialteams erbracht, ebenso wird es keine zentrale KI-Engine geben, sondern KI-Unterstützung bei den verschiedenen Lösungen.

Vectra AI: KI-gestützte Bedrohungserkennung und -reaktion: Vectra legt den Fokus auf die Analyse von Angriffssignalen. Im Gegensatz zu anderen Ansätzen, die sich auf die Erkennung von Anomalien konzentrieren und von Menschen feinjustiert und gewartet werden müssen, deckt die Angriffssignalintelligenz von Vectra die gesamte Geschichte eines Angriffs auf, indem sie kontinuierlich nach bekannten Angreifertaktiken, -techniken und -verfahren (Tactics, Techniques, and Procedures, TTPs) sucht, so der Anbieter. Der Signal-Intelligence-Ansatz von Vectra AI reduziert demnach die SIEM-Kosten sowie die Notwendigkeit, Erkennungsregeln zu erstellen.

FRAGEN AN BOB BOTEZATU, DIRECTOR THREAT RESEARCH & REPORTING BEI BITDEFENDER

Welche Bedeutung hat KI inzwischen?

Bob Botezatu: Künstliche Intelligenz ist zu einem festen Bestandteil unseres Lebens geworden. KI wird in zahlreichen Szenarien eingesetzt, von der Identifizierung von Objekten auf Bildern bis zur Unterstützung der Cybersicherheit, und gilt als Allheilmittel für alles.

Doch während die Anwendungen des maschinellen Lernens meist für ihre positiven Auswirkungen bekannt sind, werden einige Implementierungen für das genaue Gegenteil verwendet – Nutzerverfolgung, Massenüberwachung und Identitätsnachahmung (Deepfakes).

Wie wird KI bisher zum Schutz eingesetzt?

Bob Botezatu: Bei Bitdefender arbeiten wir seit 2009 an Algorithmen für maschinelles Lernen. Diese entwickeln und trainieren wir ständig, um neue und unbekannte Bedrohungen zu identifizieren. Künstliche Intelligenz und maschinelles Lernen sind unerlässlich, um eine Bedrohungslandschaft zu bekämpfen, die größer und raffinierter ist als je zuvor.

Machine-Learning-Algorithmen verkürzen die Erkennungszeit für moderne Bedrohungen erheblich, da sie große Datenmengen schneller analysieren können, als ein Mensch es je könnte. Wenn sie darauf trainiert sind, verschiedene Arten von Malware-Verhalten genau zu erkennen, können diese Algorithmen eine hohe Erkennungsrate haben, selbst bei neuen oder unbekannten Mustern.

2019 führte Bitdefender eine Kindersicherungstechnologie ein, die mithilfe patentierter KI-Algorithmen Online-Konversationen auf potenzielles Mobbing, Anfragen für Treffen mit Fremden und die Offenlegung persönlicher Informationen wie persönliche Adressen oder Kreditkartendaten überprüft.

Zur Gegenseite: Wie kann KI von Cyberkriminellen eingesetzt werden?

Bob Botezatu: Einer der wichtigsten Anwendungsszenarien von Künstlicher Intelligenz in der Cyberkriminalität steht im Zusammenhang mit Social Engineering und der Nachahmung von Personen. Durch die Erstellung gefälschter Bilder, Audio- und sogar

Videoinhalte erhöhen Cyberkriminelle nun ihre Chancen, ihre Zielpersonen für teure Betrügereien zu gewinnen.

Deepfakes helfen Bedrohungsakteuren inzwischen auch dabei, gefälschte Nachrichten und Desinformationen über soziale Medien zu verbreiten, um wichtige Ereignisse zu beeinflussen.

Auf welche KI-Gefahren muss man sich vorbereiten?

Bob Botezatu: Viele der heute verfügbaren KI-Anwendungen sind für cyberkriminelle Aktivitäten etwas zu teuer oder nicht effektiv genug. Da Computer aber immer günstiger und leistungsfähiger werden, wird das Training von fortgeschrittenen KI-Modellen zukünftig viel einfacher werden. Der Schutz vor fortgeschrittenen Deepfake-Angriffen wird neue Technologien und neue Verteidigungsschichten erfordern.

IMPRESSUM
Vogel IT-Medien GmbH
Max-Josef-Metzger-Straße 21
86157 Augsburg
Tel.: +49 (0) 821-2177-0
Fax: +49 (0) 821-2177-150
Email: zentrale@vogel-it.de
Internet: www.vogel-it.de

Handelsregister Augsburg
HRB 1 19 43
Umsatzsteueridentifikationsnummer:
DE 127502716

Geschäftsführer: Werner Nieberle

Inhaltlich Verantwortliche gemäß § 55 Absatz 2 RStV:
Nico Litzel, Florian Karlstetter, Ulrike Ostler, Stephan Augsten, Andreas Donner, Peter Schmitz, Dr. Jürgen Ehneß (Anschrift siehe Verlag)

Vogel IT-Medien
Die **Vogel IT-Medien GmbH**, Augsburg, ist eine 100prozentige Tochtergesellschaft der **Vogel Communications Group**, Würzburg. Seit 1991 gibt der Verlag Fachmedien für Entscheider heraus, die mit der Produktion, der Beschaffung oder dem Einsatz von Informationstechnologie beruflich befasst sind. Dabei bietet er neben Print- und Online-Medien auch ein breites Veranstaltungsportfolio an. Die wichtigsten Angebote des Verlages sind: **IT-BUSINESS, eGovernment, BigData-Insider, CloudComputing-Insider, DataCenter-Insider, Dev-Insider, IP-Insider, Security-Insider, Storage-Insider.**

Vogel Communications Group
Das Fachmedienhaus **Vogel Communications Group** ist einer der führenden deutschen Fachinformationsanbieter mit rund 100 Fachzeitschriften und 60 Webseiten sowie zahlreichen internationalen Aktivitäten. Hauptsitz ist Würzburg. Die Print- und Online-Medien bedienen vor allem die Branchen Industrie, Automobil, Informationstechnologie und Recht/Wirtschaft/Steuern.