Künstliche Intelligenz im Anti Financial Crime

Automatisch prüfen, schneller reagieren

Manchen Branchen liegt das Digitale im Blut. Während ingenieurslastige Industrien das Erheben von Daten erst aufwändig lernen müssten, bewegen Banken hingegen seit jeher Zahlungs- und damit Informationsströme. Ob einst auf Papier und Magnetbändern, dann auf Servern im Keller oder jetzt in der Cloud: Das Sammeln von Daten und das Gewinnen von Erkenntnissen ist ureigenes Bankengeschäft.

01 | Die Wertschöpfungskette einer Bank

Quelle: adesso SE.

Beste Voraussetzungen also, um von den Möglichkeiten der Künstlichen Intelligenz im Transaction Banking zu profitieren. Denn: Ohne Daten keine KI. Es bedarf Daten in ausreichender Menge, damit KI-Anwendungen ihre Stärke ausspielen. Dazu gehört das Erkennen von Mustern, Anomalien oder anderen Auffälligkeiten. Menschliche Experten kommen aufgrund der Datenmenge, der Komplexität der Zusammenhänge oder der Geschwindigkeit von Veränderungen hierbei an ihre Grenzen. KI-Anwendungen sind gerade für komplexe Sachverhalte und große Datenmengen bestens geeignet.

Ein weiterer Vorteil ist das hohe Tempo – bedingt durch die zur Verfügung stehende Rechenleistung –, in dem die Systeme arbeiten können. Gerade im Banking mit seinen Prozessen im Millisekundentakt ist Schnelligkeit ein entscheidender Vorteil.

Von der Produktentwicklung bis hin zum Kundenmanagement – potenzielle Einsatzgebiete für KI-Lösungen gibt es quer durch die Wertschöpfungskette einer Bank. Datengetriebene Anwendungen ermöglichen schnellere Prozesse, genauere Kundenansprachen und geringere Kosten. Sie sind Werkzeuge, die etablierte Banken im Wettbewerb mit BigTechs und FinTechs unterstützen. Vor diesem Hintergrund ist es für die Verantwortlichen von hoher Relevanz, sich mit den Möglichkeiten und Potenzialen von KI-Anwendungen auseinanderzusetzen.

Die folgenden Ausführungen greifen ein Beispiel aus dem Bereich Risikomanagement /-steuerung auf. Hier lassen sich KI-Anwendungsfälle entwickeln, die Banken zügig umsetzen können – ein schneller Return on Investment ist somit gewährleistet. » 1

Neue Betrugsmuster überlisten Systeme

Lange juristische Auseinandersetzungen, Strafen in Millionenhöhe und nachhaltige Imageschäden: Wenn die Prüfprozesse und -mechanismen einer Bank rund um Geldwäsche, Sanktionen oder Embargo versagen, können die Folgen drastisch sein. Dies ist kein Einzelfall. Der Blick in die Fachmedien zeigt, dass neue Betrugsmuster die schwer anpassbaren Systeme wieder und wieder überlisten. Gleichzeitig werden diese Themen immer bedeutsamer: Einerseits setzen die politisch Verantwortlichen Sanktionen gegen Personen, Institutionen oder Staaten häufig als Mittel ein. Andererseits arbeiten Kriminelle mit neuesten technologischen Möglichkeiten und State-of-the-Art-Verfahren, um ihre illegalen Machenschaften zu verschleiern.

Entsprechend aufwändig ist das Prüfen und Bewerten von Zahlungen. Die Surveillance-Prozesse einer Bank dienen dazu, Transaktionen zu erkennen, die gegen bestehende Vorgaben verstoßen. Erschwert wird die Aufgabe durch die Masse an Transaktionen: Größere Banken haben es tagtäglich mit Millionen Buchungen zu tun, in denen sie die kritischen identifizieren müssen. Immer noch spielt das manuelle Prüfen dabei eine große Rolle.

Die typischen Prozesse in einer Bank rund um Surveillance sehen folgendermaßen aus: Jede Transaktion wird auf Basis verschiedener Echtzeitprüfungen – sogenannter Controls – auf Verstöße gegen Embargo-, Sanktions- oder Geldwäschevorgaben geprüft. Dazu vergleichen die Systeme die Zahlungsinformationen mit Listen illegaler Empfänger. Ziel der Bank ist eine hohe Erkennungsquote von Verstößen – und das mit geringem Aufwand und ohne Verzögerung von Überweisungsprozessen.

Im ersten Schritt prüft ein sogenanntes Anti-Financial-Crime-Screening-System die eingehenden Transaktionen. Hier kommt häufig ein proprietäres System mit einfachen Regelwerken und Texterkennungsverfahren zum Einsatz. Die Prüfung erfolgt zweistufig: Liegen keine Auffälligkeiten vor, wird die Transaktion prozessiert. Bei zurückgewiesenen (rejected) Transaktionen kommt der Mensch ins Spiel. Sogenannte True Positives werden nicht ausgeführt. Hier bestätigt sich der Verdacht durch die menschliche Prüfung.

Anders bei den False Positives: Sie sind Fehlalarme. Hier erzeugen die sensiblen Filter des Systems einen unbegründeten Verdachtsfall, der – in der Regel nach einer Vier-Augen-Prüfung

– dann doch prozessiert werden kann. Die Gründe für die teuren False Positives sind vielfältig: beispielsweise fehlerhafte Informationen in den Transaktionen oder keine eindeutige Zuordenbarkeit von Feldern.

Um einen Eindruck der Dimensionen des Themas zu vermitteln: Rund zwei Prozent aller SEPA-Buchungen bei einer weltweit tätigen großen deutschen Bank können nicht automatisiert geprüft werden. Mit Blick auf US-amerikanische Überweisungen und das dort gebräuchliche veraltete Zahlungsverkehrsformat steigt diese Quote auf circa fünf Prozent. Entsprechend groß ist der Aufwand, den die manuelle Bearbeitung verursacht.

KI erkennt über 70 Prozent aller False Positives

Zwischen der bisherigen Prüfmaschine und der manuellen Nachprüfung ist der Einsatz einer KI-Lösung sinnvoll. Die Idee ist, dass eine trainierte Anwendung die Fehlalarme erkennt und automatisiert freigibt. Der Einsatz in einer Großbank zeigt, dass ein KI-System als zwischengeschaltete Anwendung über 70 Prozent aller False Positives erkennt. Entsprechend sinkt die Zahl der Vorgänge, mit denen die Mitarbeiter sich beschäftigen müssen. Das KI-System lernt im Laufe der Zeit dazu, dies verspricht eine weitere Effizienzverbesserung.

Unter der Motorhaube der beschriebenen KI-Anwendung arbeitet ein Kafka-basiertes System, das die Daten in Echtzeit an sogenannte Consumer weiterleitet. Diese Consumer enthalten die KI-Logik: Zunächst erfolgt die Entity-Recognition über neuronale Netze, danach die Prüfung gegen bestehende Sanktions- und Embargolisten.

Die Fehlertoleranz des Systems erreicht das Projektteam durch den Einsatz sogenannter String-Metrik-Verfahren (String-Ähnlichkeits-Metrik oder String-Distanz-Funktion). Diese KI-Technologien erlauben den Aufbau eines – im Vergleich zur bisherigen Prüfmaschine – flexibleren und fehlertoleranteren Regelwerks. So erkennt die Anwendung Tippfehler mit einer deutlich höheren Wahrscheinlichkeit und kann deren Konsequenzen besser einschätzen.

Um den Aufwand für die Einführung des KI-Prüfsystems gering zu halten, ist der Einsatz vorkonfigurierter Modelle sinnvoll. Große Anbieter wie Google bieten Lösungen mit vorbereiteten Sprachmodellen an. Die Aufgabe des Projektteams ist es, das System auf den entsprechenden Bankenkontext zu trainieren (sogenanntes Transferlernen). Dazu nutzt es die in den Prüfprozessen gesammelten Daten.

KI in die Banken bringen

Der bereits erläuterte KI-Einsatz in den Surveillance-Prozessen einer Bank ist der erste Schritt zur weitreichenden Automatisierung der Prüfung von Transaktionen. Das Reduzieren der False-Positive-Quote um über 70 Prozent beweist – ganz im Sinne eines Minimum Viable Products (MVP) –, dass das KI-System zu besseren Ergebnissen kommt als der bisherige regelbasierte Ansatz. Die Überlegung liegt nahe, das System nicht erst nachgeschaltet einzusetzen, sondern die ganze Prüfung KI-gestützt aufzusetzen. In dieser Ausbaustufe würde der ganze Prozess von der KI profitieren: Das System lernt in seiner Gesamtheit, der Betrieb ist kostengünstiger.

Der zweite Schritt ist der Aufbau eines KI-basierten Prüfsystems, das die Bank zunächst parallel zum bisherigen betreibt. Dies erlaubt das Trainieren, Anpassen und Härten der Anwendung im Echtbetrieb. Sobald die KI-Lösung die definierten Prüfkriterien erfüllt, integrieren die Experten die Anwendung in die bestehenden Bankprozesse und –systeme – und schalten das Altsystem ab. Abläufe werden beschleunigt, die Qualität der Ergebnisse wird verbessert.

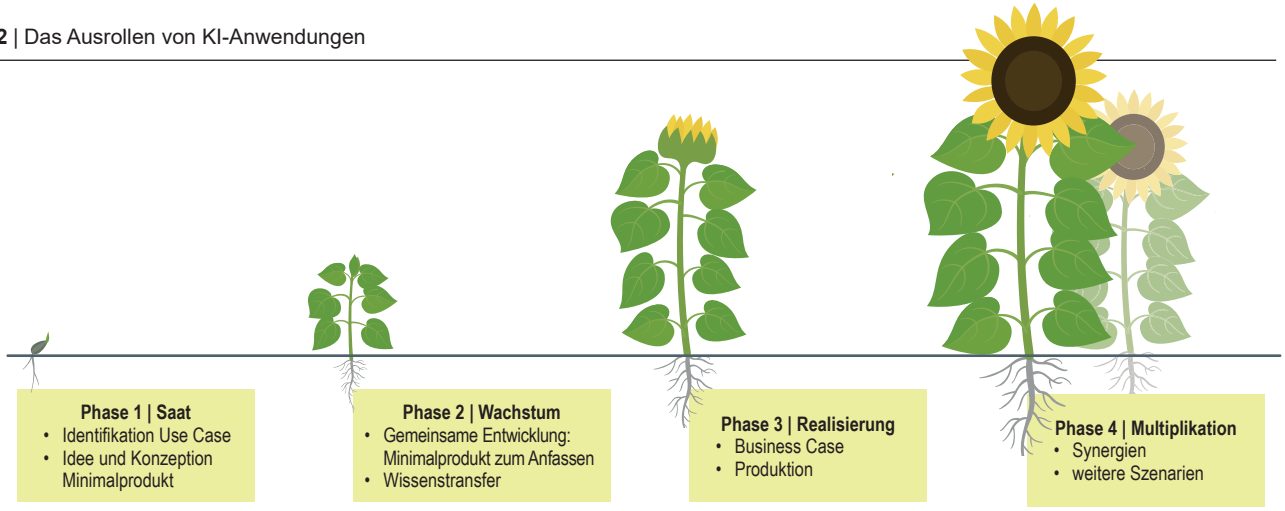
Im nächsten Schritt setzen die Verantwortlichen KI für die verbleibenden Prüfprozesse ein – beispielsweise in den Bereichen Geldwäsche oder Know Your Customer (KYC). » 2

Dieses Vorgehen empfiehlt sich generell für das Ausrollen von KI-Anwendungen in Banken: Am Anfang stehen das Identifizieren eines Use Case und das Entwickeln einer Idee, um einen Anwendungsfall mit KI zu lösen. Auf dieser Basis konzipieren und bauen die Experten ein Minimum Viable Product. Stellt dieses seine Tragfähigkeit für den Echtbetrieb unter Beweis, rollen die Entscheider die Anwendung für ähnliche Business Cases weiter aus. Der Ansatz reduziert die Risiken von Fehlschlägen: Was nicht funktioniert, erkennen die Beteiligten frühzeitig. Gleichzeitig wird dafür gesorgt, dass die Verantwortlichen erste KI-Erfolge schnell einfahren können.

Anti Financial Crime gemeinsam bekämpfen

Zurück zum Anwendungsfall rund um Geldwäsche, Sanktionen oder Embargo. Das Potenzial dieser Idee bietet nicht nur einzelnen Bank Möglichkeiten. Geldinstituten eröffnen sich neue Chancen, wenn sie bei der KI-gestützten Überwachung von Transaktionen zusammenarbeiten. Ein Forschungsprojekt des Bundesministeriums für Bildung und Forschung (BMBF) geht in diese Richtung. Unter dem etwas sperrigen Titel „Künstliche Intelligenz für sichere Web-Infrastrukturen mit digitalem Identitätsmanagement“ arbeiten hier Experten

02 | Das Ausrollen von KI-Anwendungen



Quelle: adesso SE.

an einem KI-gestützten Sicherheitsmanagement für komplexe Web-Infrastrukturen. Dieser Ansatz lässt sich für den beschriebenen Anwendungsfall nutzen.

Banken sind in diesem Geflecht von Transaktionen als Empfänger und Sender auf vielfältige Art miteinander verbunden. Jede Bank prüft ihre Transaktionen mit ihren Methoden und verbessert Schritt für Schritt die eigenen Verfahren. Hätte eine Bank die Informationen über alle Prozesse, stünden ihr mehr Daten zur Verfügung. Mögliche Geldwäschefälle oder neue Betrugsmuster ließen sich schneller erkennen und effektiver bekämpfen. Doch das Teilen derart geschäftskritischer Daten ist für eine einzelne Bank aus vielerlei Gründen unmöglich.

KI-Technologien eröffnen einen Weg, bei dem alle Beteiligten von den Erkenntnissen profitieren, ohne Daten preiszugeben. In jedem Geldhaus arbeitet ein bankspezifisches Modell mit den eigenen Daten. Während des Einsatzes lernen die Modelle und verbessern die Qualität ihrer Aussagen. Diesen Lernfortschritt – und nur diesen – speist jedes Finanzinstitut in ein gemeinsames Metamodell ein. Die ursprünglichen Datensätze werden nicht geteilt.

Das Metamodell integriert die einzelnen Erkenntnisse zu einem Gesamtbild, das dann wieder zurückfließt in die einzelnen Modelle. Diese Idee des förderierten Modells erlaubt es jedem beteiligten Unternehmen, ohne gemeinsame Daten gemeinsam zu lernen.

Fazit

Im Risikomanagement und der Risikosteuerung einer Bank stecken zahlreiche Anknüpfungspunkte für den Einsatz von KI-Anwendungen. Im Anti-Financial-Crime-Umfeld können Verantwortliche schnell erste Anwendungsfälle realisieren. Die Erfahrungen, die sie auf diese Weise gewinnen, sind die Grundlage für das breitere Ausrollen von KI-Anwendungen – ein Ausrollen, das auch in der bankenübergreifenden Zusammenarbeit funktioniert. Jetzt schaffen die Entscheider die Grundlagen, um langfristig vom KI-Einsatz zu profitieren.

Autor

Udo Müller ist Diplom-Betriebswirt (BA) und bei der adesso SE als Senior Business Developer für Analytics und Künstliche Intelligenz im Bereich Banking verantwortlich.