

Presseclipping

Kunde: HAWK:AI

Publikation: Sparkassen Zeitung

Ausgabe: 31.08.2020

Seite: Online

Titel: „Geheimwaffe gegen Geldwäsche“

Page Impressions: 1.687.857

URL: <https://www.sparkassenzeitung.de/betrieb-banksteuerung/kuenstliche-intelligenz-geheimwaffe-gegen-geldwaesche>

02.09.2020

Rubrik: Künstliche Intelligenz

Autor: Stefan Bottler

Geheimwaffe gegen Geldwäsche

Beim Aufspüren von illegalen Transaktionen unterlaufen immer wieder Fehler. Künstliche Intelligenz soll weiterhelfen, die ersten Erfahrungen mit solchen Tools liegen jetzt vor.



Jeder Kontoinhaber kann in Verdacht geraten. Wenn ein einziges Mal eine einzige ungewöhnlich hohe Geldsumme eingeht, läuten bei manchem Bankmitarbeiter die Alarmglocken. Soll er an die Zentralstelle für Finanztransaktionsuntersuchung (FIU) in Köln eine Verdachtsmeldung wegen Geldwäsche schicken? Das kann schnell passieren, wie im Frühjahr 2020 einige Kleinunternehmen und Freiberufler erfahren mussten.

Weil sie während des Lockdowns keine Aufträge akquirieren konnten beziehungsweise ihren Betrieb schließen mussten, hatten sie Corona-Soforthilfen in vier- oder gar fünfstelliger Höhe beantragt. Als diese Gelder eintrafen, mussten die Empfänger den örtlichen Polizei- und Zollbehörden Rede und Antwort stehen. Ein misstrauischer Sachbearbeiter ihrer Hausbank hatte offenbar die FIU informiert.

Schlagzeilen machte der Fall eines freiberuflichen TV-Autoren in Nordrhein-Westfalen, dem das Bundesland 9000 Euro auf sein Privatkonto bei der örtlichen Sparkasse überwiesen hatte. Das Institut sperrte vorübergehend sogar das Konto dieses Kunden.



© Shutterstock

Ein Geldwäscheverdacht kann zur sofortigen Sperrung des Kundenkontos führen.

Ausdrücklich berief eine Mitarbeiterin sich auf das Geldwäschegesetz (GWG) von 2017, das Banken das Einfrieren von verdächtigen Geldern erlaubt. Die Meldungen über unzählige Betrugsversuche gerade in Nordrhein-Westfalen hatten bei ihr den Verdacht geweckt, dass sich ein Betrüger Zugang zu den Daten des Kunden verschafft hatte.

Bisher wird nur ein Bruchteil aufgedeckt

Solche Vorgänge sind möglicherweise auch eine Folge der verschärften Meldepflicht, welche das GWG seit Anfang 2020 vorschreibt. Weit mehr Marktteilnehmer, darunter Makler und Kunsthändler, müssen der FIU nun verdächtige Vorgänge melden, außerdem sind die Sorgfaltspflichten für die Prävention nochmals verschärft worden.

Ohnehin ist der Kampf gegen Geldwäsche immer aufwendiger geworden. Kein Wunder: Internationale Organisationen schätzen, dass weltweit jährlich zwischen 720 Millionen und zwei Milliarden Euro illegal erwirtschaftet und mit Kontoeinzahlungen, Währungsumtausch und anderen Transaktionen „gewaschen“ werden.

Allenfalls ein Bruchteil dieser Betrugsfälle wird aufgedeckt. An Lösungen, die verdächtige Vorgänge einwandfrei identifizieren und fehlerhafte Meldungen an den FIU verhindern, herrscht großes Interesse. Als neue Geheimwaffe gelten digitale Lösungen, welche mit Deep Learning, Predictive Analytics und weiteren Tools der künstlichen Intelligenz (KI) Geldströme permanent überwachen und kriminelle Transaktionen von nicht kriminellen abgrenzen.

Mit entsprechenden Lösungen beschäftigt sich das KI-Competence Center der Sparkassen-Finanzgruppe (KIXpertS). Gegenwärtig führen die IT-Experten mit Software-Unternehmen und ausgesuchten Sparkassen zwei Studien zu diesem kniffligen Thema durch.

Erste marktreife Lösung

Auch mehrere Fintechs arbeiten an KI-gestützten Produkten zur Identifikation von Geldwäsche. Eine marktreife Lösung bietet das von erfahrenen Zahlungsverkehrsspezialisten gegründete Münchner Unternehmen Hawk:AI an. Mit KI-Tools der neuesten Generation lernt diese Plattform permanent, was illegale Transaktionen von legalen unterscheidet, und kann Kriminalitätsmuster in Echtzeit erkennen und überwachen.

Die Anforderungen der EU-Richtlinie gegen Geldwäsche und Terrorismusbekämpfung (AML-Richtlinie), die eine permanente Optimierung von Anti-Geldwäsche-Prozessen fordert, sehen die Macher von Hawk:AI erfüllt. „Jeder Finanzdienstleister kann mit unserer Lösung arbeiten“, versichert Tobias Schweiger, Gründer und Geschäftsführer des Unternehmens. Im Gegensatz zu vielen anderen IT-Anbietern verzichtet die Münchner Plattform auf Lizenzmodelle und bietet ausschließlich eine „Software as a Service (SaaS)“-Lösung.

Für Schweiger ist dies nicht nur aus Kostengründen ein Vorteil. „Unser Cloud-Produkt erkennt institutsübergreifend Geldwäsche- oder Betrugsmuster“, sagt der CEO. Per Machine Learning sei es möglich, mehrere Banken auf Basis von großen Datenmengen nach Anomalien und ungewöhnlichen Verhaltensmustern zu checken. Mit diesem Konzept könne Hawk.AI branchenweiten Betrügereien auf die Spur kommen, versichert Schweiger.



© Shutterstock

KI-gestützte Lösungen, die Geldwäsche und Betrugsmuster erkennen, könnten Bank- und Sparkassenmitarbeitern aus einer altbekannten Bredouille helfen.

Ein Beispiel sind die sogenannten „Money Mules“. Übers Internet oder auf der Straße werden Personen angeworben, welche gegen eine Provision kleinere Barbeträge auf ihr Konto einzahlen und diese Gelder anschließend auf Drittkonten überweisen.

Solche Argumente überzeugen offenbar. Eine Handvoll Finanzdienstleister arbeitet bereits mit der Lösung der Münchner, mit knapp einem Dutzend weiterer Anbieter, darunter zwei Sparkassen in Metropolregionen, werden gerade Gespräche geführt. Das große Interesse verwundert nicht. KI-gestützte Lösungen können Bank- und Sparkassenmitarbeitern aus einer altbekannten Bredouille helfen.

Mitarbeiter auf sich allein gestellt

Bei der Identifikation von verdächtigen Vorgängen sind diese weitgehend auf sich allein gestellt und müssen sich fast ausschließlich auf ihre berufliche Erfahrung verlassen. Die Behörden nennen nur sehr allgemeine Verdachtsmomente. Die Mitarbeiter sollen demnach grundsätzlich prüfen, ob ein Sachverhalt „ungewöhnlich und/oder auffällig“ ist. Solche Kriterien können auf Geschäfte zutreffen, welche nicht zum Kunden beziehungsweise seinen (vermuteten) wirtschaftlichen Verhältnissen passen.

Oder aber auf bargeldlose Rückzahlungen, wenn ein Produkt zuvor bar bezahlt worden ist. Auch fehlende Kundendaten, die Vermeidung von persönlichen Kontakten, mangelhafte Produktkenntnisse oder nicht nachvollziehbare Vertragsbeziehungen können verdächtig machen.

Gleiches gilt für Zahlungen in Kryptowährungen. Weil bislang für Bitcoins & Co. kein zentrales Clearing von Geldbewegungen entwickelt worden ist, wurden mit diesen virtuellen Währungen in den letzten Jahren immer mehr Gelder „gewaschen“.

Der Mitarbeiter muss weiterhin prüfen

KI-gestützte Lösungen können die Entscheidung, welche „ungewöhnlichen“ beziehungsweise „auffälligen“ Transaktionen der FIU gemeldet werden müssen, erleichtern. Die Tools lernen nicht nur auf Basis von historischen Daten und bisherigen Entscheidungen. Sie können außerdem anhand von vorhandenen Kriminalitätsmustern neue Anomalien im Zahlungsverkehr ermitteln und arbeiten hierbei mit Transaktions-Screenings in Echtzeit. Kurzum: Sie reichern Statistikzahlen mit übergreifenden Analysen an, welche ständig aktualisiert beziehungsweise verfeinert werden.



© Shutterstock

KI: Auffälligkeiten auf Kundenkonten werden dem Mitarbeiter sofort auf dem Bildschirm angezeigt. Dieser prüft und entscheidet dann das weitere Vorgehen.

„Unsere Lösung packt zwei große Herausforderungen in der Geldwäscheprävention an“, so Schweiger. Das Produkt der Münchner lernt einerseits aus den Fallbearbeitungen der Bank, sodass die festgestellten Verdachtsfälle immer zielgenauer werden, wie Schweiger versichert. Das verhindere Fehlalarme und steigere die Prozesseffizienz. Außerdem nutzt das Produkt algorithmische Verfahren, um Auffälligkeiten im Verhalten einzelner Kontoinhaber oder im Zusammenspiel mehrerer Konten aufzudecken.

„Das regelmäßige Trainieren unserer Modelle auf der Transaktionslandschaft der einzelnen Bank und zukünftig auch bankenübergreifend steht dabei im Vordergrund“, sagt Schweiger. Im Idealfall weiß demnach eine KI-gestützte Lösung über neue Verdachtsmomente bereits vor deren ersten Auftreten Bescheid. Der Anwender muss allerdings die Weichen für solche Präventivlösungen stellen und die richtigen technischen Filter einsetzen.

Dann werden besonders brenzlige Fälle sofort auf seinem Bildschirm angezeigt. „Jede auffällige Transaktion, welche unsere Lösung ermittelt, muss auch in Zukunft von einem Mitarbeiter nochmals überprüft werden“, betont der Geschäftsführer von Hawk:AI ausdrücklich. Das schreibt das GWG vor. Eine KI-gestützte Lösung macht diese also nicht überflüssig.

Es gibt auch Grenzen

Auf die Grenzen solcher Lösungen, solcher Präventivkonzepte macht Silvia Frömbgen aufmerksam. „Wir werden weiterhin neue Tatbestände nicht verhindern können, weil ihre kriminellen Ziele erst im Nachhinein erkannt werden“, betont die Abteilungsdirektorin des Deutschen Sparkassen- und Giroverbands (DSGV). „Deshalb müssen wir die Hürden für solche Vorgänge weiter erhöhen.“ Auch in Zukunft könnten verdächtige Transaktionen nur anhand von Indizien ermittelt werden, welche der Sparkassenmitarbeiter „abarbeiten“ muss.

„Häufig kann er gemeldete Transaktionen nicht abschließend beurteilen, weil keine Rückmeldung der FIU vorliegt.“ Das aber sei die Mindestvoraussetzung für „lernende Systeme“. Eine KI-gestützte Lösung müsse deshalb auch den Austausch zwischen Bank und Behörden effizient unterstützen. Solche Konzepte werden mittlerweile von der 2019 gegründeten Anti Financial Crime Alliance (AF-CA) angedacht. Ihr gehören außer der Bafin und dem BKA 14 Banken an.

Auch das KIXpertS-Projektteam dürfte sich mit diesem Thema bei seinen Studien für die Sparkassen-Finanzgruppe beschäftigen. Als Allheilmittel können KI-gestützte Lösungen erst gelten, wenn dieses Problem gelöst ist.