REGELN BRECHEN MIT KI

ZAHLUNGSBETRÜGERN VORAUS SEIN DURCH VERHALTENSANALYSEN

Zahlungsbetrug ist nicht nur aufgrund der zunehmenden Digitalisierung zu einer immer größeren Bedrohung für Banken und ihre Kunden geworden und kostet jedes Jahr Milliarden. Einige Banken kommen für den Schaden ihrer Klienten auf, andere verweisen auf die Verantwortung des Kunden für die Initiierung der Transaktionen. Entweder verlieren die Banken Profite oder das Vertrauen der Kunden. Ulrich Parthier, Herausgeber it management, sprach mit Achim Thienel, Geschäftsführer und Product Manager Cloud & Core Banking SaaS bei Finastra und Joël Winteregg, CEO und Founder von NetGuardians, einem Schweizer Fintech, das Lösungen zur Betrugsprävention von Banken entwickelt. Gemeinsam haben die beiden Firmen eine App herausgebracht, die künstliche Intelligenz (KI) einsetzt, um Betrug effizienter zu verhindern.

AUSWERTUNGEN ZEIGEN, DASS KI IM VERGLEICH ZU HERKÖMMLICHEN ZAHLUNGSBETRUGSPRÄVENTIONS-ANGEBOTEN DIE ANZAHL DER FEHLALARME UM BIS ZU 83 PROZENT REDUZIEREN KANN.

Joël Winteregg,
CEO und Founder, NetGuardians,
https://netguardians.ch/

Ulrich Parthier: *Täter finden immer neue Wege, um Betrug zu begehen. Welche Zahlungsbetrugsmethoden lassen sich aktuell beobachten?*

Achim Thienel: Neben Hightech-Hacking nutzen Betrüger nun auch Social Engineering, um Privatpersonen und Unternehmen mit gefälschten Rechnungen, vorgetäuschten Autoritäten und Business E-Mail Compromise (BEC) dazu zu bringen, direkt an sie zu zahlen. Kontoübernahmebetrug ist ebenfalls ein sehr häufiger Fall. Betrüger verschaffen sich durch verschiedene Techniken, wie zum Beispiel dem Einschleusen von schadhaften Codes auf die Computer der Opfer oder Phishing-Angriffe auf die E-Banking-Zugangsdaten der Kunden, Zugriff auf fremde Konten.

Ulrich Parthier: *Wie lässt sich KI zum Erkennen von Zahlungsbetrug einsetzen?*

Joël Winteregg: KI-gestützte Betrugsprävention funktioniert durch das Verständnis des normalen Zahlungsverhaltens eines Kunden und nutzt Verhaltensrisikomodelle, um betrügerische Transaktionen zu erkennen, die außerhalb der Norm liegen. Durch die Analyse von ungewöhnlichen Verhalten, wie zum Beispiel unverhältnismäßiger Überweisungsbetrag, unbekannter Begünstigter, fremdes Land der Empfängerbank, andere Währung, neuer Vorgangstyp, gelingt es Betrugsfälle auf Kundenkonten anhand einer Kombination dieser Faktoren zu erkennen. Eine auf diese Weise analysierte betrügerische Transaktion wird blockiert und gleichzeitig eine Warnung in Echtzeit generiert, welche dann über das Risiko-Dashboard und Forensik-Tools an die zuständigen Mitarbeiter weitergeleitet wird, um den Grund für die Blockierung der Transaktion zu ermitteln.

Ulrich Parthier: *Welche Vorteile gegenüber herkömmlichen Präventions-Modellen bietet KI?*

Achim Thienel: Durch KI und maschinelles Lernen gelingt es, betrügerischen Transaktionen stets einen Schritt voraus statt hinterher zu sein, so wie das bei herkömmlichen Lösungen zur Betrugsprävention der Fall ist. In der Vergangenheit verloren Banken viel Geld, um jeweils neue Regeln zum Erkennen von neuen Betrugsmethoden zu konfigurieren. Die vordefinierten Regeln erkennen jedoch nur bereits bekannte Szenarien. Traditionelle

Lösungen zur Betrugsprävention basieren auf statischen Regeln, die Zahlungen blockieren, die bestimmte Kriterien für betrügerische Zahlungsszenarien erfüllen. Täglich treten jedoch neue Fälle von Zahlungsbetrug auf gegen die Banken schutzlos sind. Zudem blockieren die vordefinierten Betrugsregeln oftmals auch legitime Kundenzahlungen, was nicht nur für die Kunden unangenehm ist, sondern zusätzliche Kosten für die Banken verursacht, da zum Teil Mitarbeiter ausschließlich für irrtümlich fehlgeschlagene Zahlungen von Kunden beschäftigt werden müssen. Unabhängig von der Art und Weise, wie der Betrug begangen wird, erkennen neue Verhaltensrisikomodelle mithilfe von künstlicher Intelligenz die Anomalie und markieren sie für eine Kundenüberprüfung.

Joël Winteregg: Auswertungen zeigen, dass künstliche Intelligenz im Vergleich zu herkömmlichen Zahlungsbetrugspräventions-Angeboten die Anzahl der Fehlalarme um bis zu 83 Prozent reduzieren kann und dazu führt, dass Bank-Angestellte schätzungsweise 93 Prozent weniger Zeit mit der Untersuchung verdächtiger Zahlungen verbringen. Zudem lernen KI-Modelle von selbst, man muss nicht jeden Tag mit einem Data-Scientist-Team im Rücken statische Regeln anpassen. Dadurch konnten eigenen Studien zufolge Banken ihre Ausgaben zur Betrugsprävention um bis zu 77 Prozent senken.

? **Ulrich Parthier:** *Wie hoch ist der technische Aufwand des Einsatzes von KI für Finanzdienstleister?*

Achim Thienel: Die Anschaffung und Implementierung innovativer KI-Lösungen erforderte früher ein Projektteam, das viele Personalressourcen verbrauchte und über ein Jahr bis zum Go-Live brauchte. Natürlich war dies für die Banken mit hohen Kosten verbunden. Durch die Bereitstellung von innovativen Lösungen als App über eine Plattform können Banken jedoch in wenigen Wochen live gehen.

? **Ulrich Parthier:** *Inwiefern eignet sich zur Entwicklung und Bereitstellung von innovativen Lösungen eine Plattform?*

Achim Thienel: Über eine offene und kollaborative Entwicklerplattform und Marktplatz, wie sie Finastra bereitstellt, wird es aufstrebenden Fintechs, wie NetGuardians ermöglicht, einfacher zu experimentieren, ihre Apps mit bereits vorhandenen, anonymisierten Bankdaten zu verfeinern und neue Kunden über einen offenen Marktplatz zu erreichen. Finanzinstitute und andere Akteure im Fintech-Ökosystem können von den auf diese Weise entwickelten Anwendungen profitieren und so den Wert ihrer Kunden steigern. Der auf Finanzdienstleister spezialisierte Plattform-Anbieter bringt die Expertise bei der Implementierung und dem Management von SaaS-Umgebungen sowie eine breite Kundenbasis aus den Bereichen Retail Banking, Payments, Lending, Corporate Banking und Treasury & Capital Markets ein. Das jeweilige Fintech bringt die fachliche Expertise und die Reputation in seinem Gebiet mit.

Joël Winteregg: Die Bereitstellung über eine offene Entwicklerplattform ermöglicht, dass Kosten bei der Implementierung eingespart, die Anwendungen besonders schnell in Betrieb genommen und einfach bedient werden können. Die Zeit bis zum Go-Live für den Kunden dauert im Vergleich zu alternativen Angeboten von bis zu einem Jahr über die Plattform nur ein paar Wochen. Zudem profitiert die Lösung durch die über die Plattform angeschlossene Banken-Community von einer sogenannten „kollektiven KI", die eine noch höhere Genauigkeit bei der Betrugseinschätzung und Reduzierung von Falschmeldungen ermöglicht. Nicht nur künstlicher Intelligenz sondern auch der Zusammenarbeit über Plattformen gehört die Zukunft - in der Bekämpfung von Zahlungsbetrug und in vielen weiteren Problemen aber auch Möglichkeiten, die unsere zunehmend digitale Welt mit sich bringt.

DURCH KI UND MASCHINELLES LERNEN GELINGT ES, BETRÜGERISCHEN TRANSAKTIONEN STETS EINEN SCHRITT VORAUS STATT HINTERHER ZU SEIN.

Achim Thienel, Geschäftsführer und Product Manager Cloud & Core Banking SaaS, Finastra, www.finastra.com

! **Ulrich Parthier:** *Herr Winteregg, Herr Thienel, wir danken für dieses Interview!*

FAZIT

KI führt durch effizientere Erkennung von Zahlungsbetrug dazu mehr Umsatz für Finanzinstitute zu generieren. Die über Finastra's offene Entwickler-Plattform und Marktplatz, FusionFabric.cloud, bereitgestellte App zur Prävention vor Zahlungsbetrug von NetGuardians nutzt künstliche Intelligenz, um proaktiv betrügerische Zahlungen in Echtzeit zu erkennen und Betrugsverluste zu reduzieren.