Operationalisierung von Machine Learning in der Betrugsbekämpfung – Woran scheitern Banken?

Abstract: Wir suchen nach dem Grund, warum Machine Learning in der Betrugsbekämpfung in der Praxis so wenig eingesetzt wird und sehen den Grund in der Schnittstelle zwischen analytischer Modellierung und den Fraud Monitoring Anwendungen.

Aktuelle, rein regelbasierte Fraud Monitoring Systeme liefern oft schlechte Erkennungsraten. Unternehmen beschäftigen sich deshalb seit geraumer Zeit mit Machine Learning zur Fraud Erkennung. Hybride Erkennungsmodelle, die Business Regeln und Machine Learning Modelle kombinieren, versprechen in der Praxis die besten Erkennungsraten. Die Kombination aus Mensch und Maschine, d.h. die Verknüpfung von menschlicher und künstlicher Intelligenz, ist ein Erfolgsfaktor.

Dennoch nutzen viele Systeme immer noch Erkennungsmodelle, die keinerlei maschinelles Lernen nutzen - ein Grund, mal genauer nach den Ursachen zu suchen. Wir als spotixx haben bei unseren Kunden Erfahrungen gemacht, die wir mit Ihnen teilen möchten.

Es macht Sinn, das Pferd mal von hinten aufzuzäumen. Wir schauen also nicht auf die wohl bekannten Herausforderungen bei der Erstellung von Machine Learning Modellen selbst, sondern vielmehr auf deren praktische Anwendung im Monitoring. Denn genau dieser Aspekt wird häufig erst nachgelagert betrachtet.

Hierbei ist es wichtig zu verstehen, dass die Ergebnisse moderner Machine Learning Algorithmen (z.B. Gradient Boosting, Neuronale Netzwerke etc.) meist weder leicht zu interpretieren sind noch als einfache Business Regeln abbildbar sind! Auf „traditionellere“ Algorithmen, wie z.B. Entscheidungsbaum-Verfahren oder die logistische Regression, wie sie z.B. auch meist im Credit Scoring eingesetzt werden, trifft dies sehr wohl zu.

Ein genauer Blick auf das Transaktions-monitoring, d.h. das Zielsystem für das Fraud Detection Modell, ist daher bereits zu Beginn der analytischen Modellierung wichtig.

Folgende Fragen sind im Vorfeld zu beantworten:

Wie sieht das Transaktionsmonitoring in Finanzinstituten heute meist aus?
Die Monitoring-Systeme in Finanzinstituten sind „mission-critical“, etabliert und gesetzt. Oft stehen sie bei einem externen Provider (z.B. im Falle von Kreditkarten) oder im Bereich Payments handelt es sich um Standard-Software von der Stange.

Wie integrieren und verarbeiten Transaktionsmonitoring-Systeme Machine Learning Modelle?
Ist das vorhandene Monitoring-System überhaupt technisch in der Lage Machine Learning Modelle auszuführen oder ist es auf Business Rules beschränkt? Welche Schnittstellen zur Integration von analytischen Scoring-Modellen stehen zur Verfügung und passen diese zu unseren Export-Schnittstellen? Oder im Falle, externer Systeme: Welche Services bietet der externe Prozessor zur Integration kundenspezifischer Erkennungs-modelle?

Welche Informationen stehen dem Fraud Detection Modell zur Laufzeit zur Verfügung?
Auf welche Daten kann das System (in Echtzeit?) zugreifen? Welche Berechnungen als Modell-

Input kann das Transaktionsmonitoring selbst ausführen?

Ein Machine Learning Modell, das diese Überlegungen nicht berücksichtigt, beweist lediglich theoretisch hohe Erkennungsraten, liefert aber keinerlei praktischen und kommerziellen Nutzen.

Unsere eigenen Praxiserfahrungen aus jüngerer Vergangenheit zeigen genau dies:

- Software-Vendoren verlangen zusätzliche Lizenzgebühren, um ihre Scoring-Engine für Machine Learning Modelle zu öffnen.
- Die Integration von Machine Learning Modellen ist komplex und zeitaufwändig und muss oft als Projekt umgesetzt werden, was eine häufige und schnelle Aktualisierung von Detection Modellen ad absurdum führt.
- Kunden meiden Änderungen an ihren operativen Monitoring-Systemen, weil sie die Auswirkungen auf die Produktion nicht abschätzen können.
- Zahlungsverkehrsdienstleister, die auf Skaleneffekte setzen, scheuen kunden-spezifische Modelle, obwohl diese auf kundenspezifischen (Teil-)Portfolien meist besser performen als die Konsortialmodelle der Provider.
- Viele Machine Learning Algorithmen erzeugen Scoring-Modelle mit tausenden Code-Zeilen. Aus Performance-Aspekten sind deren Anwendung in vielen Monitoring-Systemen sehr problematisch.
- Zur Laufzeit stehen dem Entscheidungs-modell oft weniger Daten zur Verfügung als dem Data Scientist bei der analytischen Modellierung im Labor.

Wie sehen nun mögliche Antworten aus?

Ein Lösungsansatz sind Fraud Detection Modelle, die Ergebnisse in Form von Business Regeln liefern und so einfach in Transaktions-monitoring-Systeme integrierbar sind.

Der spotixx Fraud Analytics Service verfolgt genau diesen Ansatz. Die genannten Praxis-erfahrungen waren der Inkubator für den spotixx Fraud Analytics Service. Die Idee ist es, hoch-moderne, komplexe Machine Learning Verfahren greifbar zu machen. Das Ergebnis ist ein einfach interpretierbares und in jedes Fraud Monitoring System integrierbares Regelwerk zur Fraud Detection.

Der spotixx Fraud Analytics Service liefert automatisiert und maschinell erzeugte Fraud Detection Business Regeln.

Maschinell erzeugte Business Regeln sind:

- Transparent und einfach interpretierbar
- Performant in der Ausführung
- Präzis: Hohe Betrugserkennungsraten bei geringen False-Positive-Raten
- Schnell aktualisierbar, um auf neue Betrugs-muster zu reagieren
- Schnell integrierbar in das Fraud-Monitoring
- Beherrschbar, im Gegensatz zu manuell gepflegten, kontinuierlich wachsenden Regelwerken
- Preiswert in Erstellung und Betrieb

Andere Ansätze erfordern meist Erweiterungen oder Änderungen im Transaktionsmonitoring. Diese Investitionen müssen durch bessere Erkennungsraten gerechtfertigt sein.

Mehr über den spotixx Fraud Analytics Service erfahren sie hier:

https://spotixx.com/de/#sfas

Autoren: Ruppert Jaeschke (rj@spotixx.com)
Stefan Klaeser (sk@spotixx.com)