Technische Systeme unterstützen die **Betrugsprävention**

Von Andreas Unterreitmeier

Betrugsversuche bei Kontoeröffnungen, Überweisungen und Kreditanträgen müssen von Kreditinstituten effizient erkannt und verhindert werden. Andreas Unterreitmeier entwirft das Bild eines schnell anpassbaren Systems, das sowohl interne als auch externe Daten nutzt. Dieses umfasst unter anderem die Analyse von Transaktionsdaten, um bestimmte Muster zu erkennen, beispielsweise die Einordnung von Objekten, für die Kredite vergeben werden, nach Merkmalsähnlichkeiten. Dadurch könnten eventuelle Netzwerke erkannt werden. In letzter Instanz jedoch könnten technische Systeme stets nur den gesunden Menschenverstand unterstützen, ihn aber keineswegs ersetzen. Red.

Betrügerische Handlungen nehmen in Deutschland immer mehr zu. Laut polizeilicher Kriminalstatistik wurden mit 968 162 Betrugsfällen im Jahr 2010 die höchsten Fallzahlen seit Bestehen einer gesamtdeutschen Statistik im Jahr 1993 erfasst. Betroffen ist davon zu einem Großteil auch die Finanzbranche: So dokumentierte man 2010 etwa 19 520 Fälle von Kontoeröffnungs- und Überweisungsbetrug. Die Gründe liegen vor allem in der zunehmenden Anonymisierung, Automatisierung, Internationalisierung sowie dem Outsourcing im Antragsprozess. Dadurch entstehen Schlupflöcher und Lücken, die Betrüger gerne nutzen.

War ein Betrugsversuch erfolgreich, verbreitet er sich rasend schnell im Netzwerk der Kriminellen und animiert zum Nachahmen. Die Gefahr der „Ansteckung" für Banken steigt. Selbst wenn diese sich umfangreich schützen, finden Betrüger immer neue Wege, die Sicherheitsvorkehrungen zu umgehen – ein nie endendes Wettrennen zwischen Hase und Igel beginnt.

Aufsichtsbehörden und Gesetzgeber haben die Problematik bereits erkannt und entsprechend neue Anforderungen zur Betrugsprävention in den Gesetzen verankert. Sie verlangen insbesondere risikoorientierte und transparente Präventionsmaßnahmen, um Geldwäschevorfälle, Terrorismusfinanzierung oder sonstige strafbare Handlungen, wie etwa Betrug, frühzeitig zu erkennen. Banken müssen wirtschaftlich Berechtigte und politisch exponierte Personen identifizieren können, Transaktionen fortlaufend überwachen können und auf Verdachtsfälle hinweisen. Eine weitere große Herausforderung besteht für Finanzinstitute darin, die im Gesetz geforderte „zentrale Stelle" im Unternehmen einzurichten, die alle Entscheidungen für die Bereiche Compliance sowie interner und externer Betrug trifft, prüft und dokumentiert.

Zum Autor

Dr. Andreas Unterreitmeier ist Competence Leader für Risk Analytics bei der SHS VIVEON AG, München.

Um den geforderten Präventionsmaßnahmen gerecht zu werden und der steigenden Zahl an Betrugsfällen entgegenzuwirken, ist es im ersten Schritt wichtig, dass Banken beim Antragsprozess zwischen Bonität und Betrug unterscheiden, also letztendlich zwischen „nicht zahlen können" und „nicht zahlen wollen". Da Betrug anderen Gesetzmäßigkeiten unterliegt als die reine Bonitätsprüfung, sollten Banken die Betrugsprävention im Prüfprozess separat adressieren. Eine Betrugsprüfung sollte demnach fester Bestandteil innerhalb des Antragsmanagements werden.

Im zweiten Schritt geht es dann darum, die richtigen Prüfungskriterien festzulegen. Dafür müssen Banken wissen, wie Betrug funktioniert. Denn Betrugsfälle zeichnen sich häufig dadurch aus, dass sie zwar im Vorfeld per se nicht auffallen, aber dennoch bestimmten Mustern folgen, die wiederum durchaus auffällig sind. Um diese zu identifizieren, müssen Banken sich der unterschiedlichen Betrugstypen bewusst werden und deren Vorgehensweisen kennen. Grob lassen sich drei Typen unterscheiden:

- „Der Privaterschleicher" versucht, eine Leistung für sich selbst zu optimieren oder

zu erschleichen. Dafür variiert er häufig seine Daten, etwa indem er die Schreibweise seines Nachnamens ändert.

- „Der Verlegensheitsoptimierer" ist Kunde mit bestehender Geschäftsbeziehung, der kurz- oder mittelfristige Probleme hat und diese mittels Betrug verlagern will. Dafür verschleiert er seine Daten.

- „Der Gewerbliche Betrüger": Hierbei handelt es sich um einen geschäftsmäßigen Betrüger, bei dem es um hohe Stückzahlen innerhalb eines kurzen Zeitraums geht. Der Betrugsversuch ist gut durchgeplant und weist eine hohe kriminelle Energie auf. Das Vorgehen ist dabei immer wieder neu. Meist werden nicht existente Personen und Unternehmen geschaffen.

Bei jedem dieser Typen lassen sich bestimmte Muster in den Vorgehensweisen erkennen. Dabei geht es in weniger schlimmen Fällen lediglich darum, dass sich abgelehnte Antragssteller für ein Girokonto möglicherweise ein paar Jahre älter machen, Vor- und Nachnamen vertauschen oder ihre Kontaktdaten in einer leicht veränderten Schreibweise angeben – in der Hoffnung, nicht in der Datenbank gefunden zu werden und als Neukunden aufzutauchen. Weit schwerwiegender sind jedoch ausgefallene Kreditverträge durch betrügerische Handlungen, etwa durch Mehrfachfinanzierung. Letzteres bedeutet immer auch einen großen finanziellen Schaden für die betroffene Bank.

Ansatzpunkte zur Erkennung der Betrugsmuster

Um die Muster in den Vorgehensweisen zu identifizieren und erfolgreich zu bekämpfen, gibt es verschiedene Ansatzpunkte. Diese reichen von manuellen Prüfprozessen bis hin zur systematischen und automatisierten Analyse von Antrags- und Kundendaten. Grundlage für alle Methoden sind die sogenannten Risk Analytics, also statistische Analysen und Data-Mining-Verfahren. Sie eignen sich besonders dazu, Risiken wie Betrug oder Zahlungsausfall zu analysieren. Zudem können sie neue Anträge mit Hilfe von Modellen wie etwa Scorecards bewerten und dadurch Betrugsverdachtsfälle automatisiert erkennen und aussteuern.

In der Praxis hat sich hierbei ein Stufenmodell bewährt, das nach und nach umgesetzt werden kann und so die Betrugsprävention schrittweise verbessert. Dafür sollten Banken folgende Schritte gehen:

Stufe 1 – Festlegen von Geschäftsregeln: Eine grundlegende Voraussetzung für den Umgang mit Betrug ist die Etablierung von Geschäftsregeln (auch: Policy Rules oder Business Rules). Durch diese werden Fälle identifiziert, die zunächst nur als Betrugsverdacht zu klassifizieren sind und dann zur manuellen Überprüfung ausgesteuert werden müssen. Policy Rules werden als harte Prüflogiken formuliert. Dies können etwa Unter- oder Obergrenzen für ein Merkmal (zum Beispiel Mindestalter von 18 Jahren für bestimmte Verträge) sein oder aber Plausibilisierungsregeln für Merkmalskombinationen (beispielsweise dass das Bruttoeinkommen eines Antragstellers innerhalb einer marktüblichen Bandbreite in der Branche liegen muss).

Diese Geschäftsregeln dienen der Betrugsprävention und identifizieren relativ offensichtliche Betrugsverdachtsfälle, die ausgesteuert und anschließend manuell bearbeitet werden müssen. Denn ob beispielsweise eine Schreinerei, die einen Umsatz von mehreren Millionen Euro angibt, tatsächlich einen Betrugsversuch unternimmt oder nicht, muss im Rahmen der manuellen Prüfung geklärt werden.

Stufe 2 – Aufbau eines Fraud Caches: Im nächsten Schritt sollten Banken einen sogenannten Fraud Cache aufbauen. Ein Fraud Cache ist ein Speicher etwa in Form einer täglich aktualisierten Tabelle im Data Warehouse, in dem alle Neukundenanträge eines definierten Zeitraums, zum Beispiel der vergangenen 15 Monate, gesammelt werden. Kommt nun ein neuer Antrag in das System, wird der Speicher auf bereits vorhandene Anträge des potenziellen Neukunden überprüft. Mit Hilfe einer unscharfen Suche werden absichtliche oder versehentliche Namensvariationen sowie „plötzlich gealterte" Antragsteller identifiziert. Auf diese Weise können Mehrfachanträge unter gleichen oder veränderten Identitäten erkannt werden.

Mit schärferen Suchregeln identifiziert man Personen, bei denen alle Merkmale exakt übereinstimmen. Etwas weichere Suchregeln erkennen Kunden, die mit hoher Wahrscheinlichkeit identisch sind – etwa wenn eine sehr ähnliche Schreibweise des Namens und der Adresse sowie ein gleiches Geburtsdatum vorliegen. Schließlich können noch weichere Suchregeln definiert werden, die lediglich Name und Adresse auf Ähnlichkeit prüfen und dann vermeintlich identische Personen zur manuellen Bearbeitung übergeben.

Stufe 3 – Etablierung einer Netzwerk-Analyse: Ziel dieser Analyse ist es, Auffälligkeiten in Netzwerken zu entdecken. Hierfür werden beispielsweise mehrfach genutzte Telefonnummern, Mailadressen oder Ausweisnummern bei unterschiedlichen Neukundenanträgen oder Bestandskundendaten gesucht. Auch wenn sich in vielen Fällen plausible Erklärungen finden lassen – etwa eine gleiche Adresse bei Ehepartnern –, so können sich dennoch auch Indizien für Betrugsversuche ergeben. Auffällig wäre beispielsweise, wenn die Kontaktdaten eines Neukunden auch bei einem erst kürzlich gestellten, aber abgelehnten Antrag mit unterschiedlichen Personendaten zu finden sind. Für die Netzwerk-Analyse können sowohl die gesamten Bestandskundendaten als auch der Fraud Cache aus der zweiten Stufe genutzt werden.

Stufe 4 – Einführen von Data Mining: Mit Data-Mining-Verfahren lassen sich gezielt Transaktionsdaten analysieren und auswerten. Data Mining bedeutet eine syste-

matische Anwendung von bestimmten Methoden auf einen Datenbestand, um dadurch neue Muster zu erkennen. Das Ziel hierbei ist die Identifikation eines Fraud-Netzwerks mit Hilfe von Kontakten bekannter Betrugsfälle zu beziehungsweise deren Interaktionen mit anderen Kunden.

Diese Formen von Risk Analytics sind an enge Voraussetzungen gebunden: Erstens sind sie nur dann einsetzbar, wenn Transaktionsdaten zwischen Kunden vorhanden sind – beispielsweise Überweisungsdaten bei Finanzdienstleistern. Zweitens dürfen derartige Analysen unter keinen Umständen für Marketingzwecke durchgeführt oder genutzt werden, sondern ausschließlich, um das Unternehmen vor Schaden zu bewahren. Für die Analyse bieten sich verschiedene Data-Mining-Verfahren an, durch die Objekte nach Merkmalsähnlichkeiten und Transaktionen untereinander gruppiert werden können. Die Ergebnisse lassen sich anschließend in Form von Landkarten visualisieren. Ist ein Fraud-Netzwerk identifiziert, müssen Banken sich geeignete Maßnahmen überlegen, mit denen sie der Gefahr der „Ansteckung" von Krediten entgegenwirken können.

Stufe 5 – Entwicklung einer Scorecard: In einem nächsten Schritt können im Rahmen der Risk Analytics auch Scorecards zur Betrugserkennung eingesetzt werden. Voraussetzung dafür ist, dass bereits eine größere Zahl an Betrugsverdachtsfällen vorhanden ist. So können Scorecards mit möglichst hoher Trennschärfe entwickelt werden, auf deren Basis alle Anfragen zu Neuverträgen einer verlässlichen Betrugsbewertung unterzogen werden. Bei genügend großen Fallzahlen können zudem mehrere Scorecards für verschiedene Segmente oder Gruppen entwickelt werden, etwa getrennt nach Produktarten oder Privat- und Firmenkunden.

Die Scorecard liefert eine Aussage über die Betrugswahrscheinlichkeit eines neuen Antrags – diese wird dann beispielsweise auf einer sechsstufigen Rating-Skala analog dem Schulnotensystem abgebildet. So ist es mit Hilfe der Scorecard möglich, eine einfache, schnelle, reproduzierbare und automatisierbare Entscheidung über einen Betrugsverdacht bei Neuanträgen zu treffen. Zudem lassen sich aus den Analyseergebnissen bei der Erstellung einer Scorecard häufig auch Geschäftsregeln ableiten und in die bereits bestehenden integrieren. Auf Basis der Fraud-Scorecard kann anschließend ein Fachkonzept zur Implementierung eines IT-gestützten Fraud-Management-Systems konzipiert werden.

Stufe 6 – Entwicklung eines IT-gestützten Fraud-Management-Systems: Die höchste Stufe im Betrugspräventions-Modell ist ein permanentes IT-gestütztes Entscheidungs- und Monitoring-System, das auf den zuvor genannten Analyseergebnissen und Scoring-Werkzeugen aufbaut. Ein solches System gewährleistet eine automatisierte Bewertung der Betrugswahrscheinlichkeit und ermöglicht es Banken, trotz der großen Menge an Neuanträgen und Bestandskunden die regulatorischen Anforderungen – etwa aus § 25 c Kreditwesengesetz – einzuhalten.

Durch die Einbindung interner sowie externer Daten, beispielsweise von Auskunfteien und Terrorismuslisten, können Neukunden automatisch überprüft und identifiziert und Geschäftsbeziehungen kontinuierlich überwacht werden. Dabei garantiert das System die vom Gesetz geforderte Dokumentation aller Aktionen und Daten und damit die Nachvollziehbarkeit der Entscheidungen. Findet das System während der automatischen Prüfung Auffälligkeiten innerhalb eines Neuantrags, so leitet es den manuellen Prüfprozess ein. Dabei wird der Antrag von Sachbearbeitern im Detail geprüft und individuell entschieden. Ziel ist es jedoch, den manuellen Aufwand so weit wie möglich zu reduzieren und nur zweifelhafte Fälle manuell zu bearbeiten.

Damit ein solches System einen wirklichen Mehrwert bietet, sollte es schnell anpassbar sein und externe sowie interne Daten ohne Probleme einbinden. Des Weiteren sollten die Prozesse und auch die einzelnen Dienste in den Prozessen den Anforderungen eines international agierenden Unternehmens Rechnung tragen. Die Pflege und Anpassung von Betrugspräventionsprozessen sollte sowohl bei der Konzeption als auch bei der späteren Umsetzung möglich sein. So bleiben Finanzinstitute flexibel und können schnell auf regulatorische Änderungen oder neues Betrugsvorgehen reagieren.

Betrugsszenarien immer komplexer

Werden die Maßnahmen nach und nach umgesetzt, haben Banken die besten Voraussetzungen, um betrügerische Handlungen wirksam zu identifizieren, zu bekämpfen und zu reduzieren. Sie können die regulatorischen Anforderungen zur Betrugsprävention einhalten und Vermögens- und Reputationsschäden vermeiden. Zudem lassen sich durch die Maßnahmen auch mögliche weitere Betrugsfälle im Netzwerk bekannter Betrüger frühzeitig feststellen.

Grundsätzlich gilt aber: Die Kreativität von Betrügern wird von deren krimineller Energie bestimmt. Dadurch werden die Betrugsszenarien immer komplexer und ihre Erkennung und Bekämpfung immer schwieriger. Banken müssen ihre Präventionsmaßnahmen entsprechend einfach, schnell und effektiv anpassen können. Technische Systeme können dabei lediglich die Einhaltung der gesetzlichen Anforderungen unterstützen, eine gleichbleibende Qualität von Prozessen gewährleisten, die richtigen Daten sammeln, die Prozessausführung gesetzeskonform dokumentieren und die interne Prüfung unterstützen. Damit legen sie die „Hürde" für Betrüger höher. Aber sie können nicht den „gesunden Menschenverstand" ersetzen, denn durch eine automatisierte Bewertung lassen sich nur Verdachtsfälle erzeugen – die finale Prüfung obliegt immer noch dem Menschen.