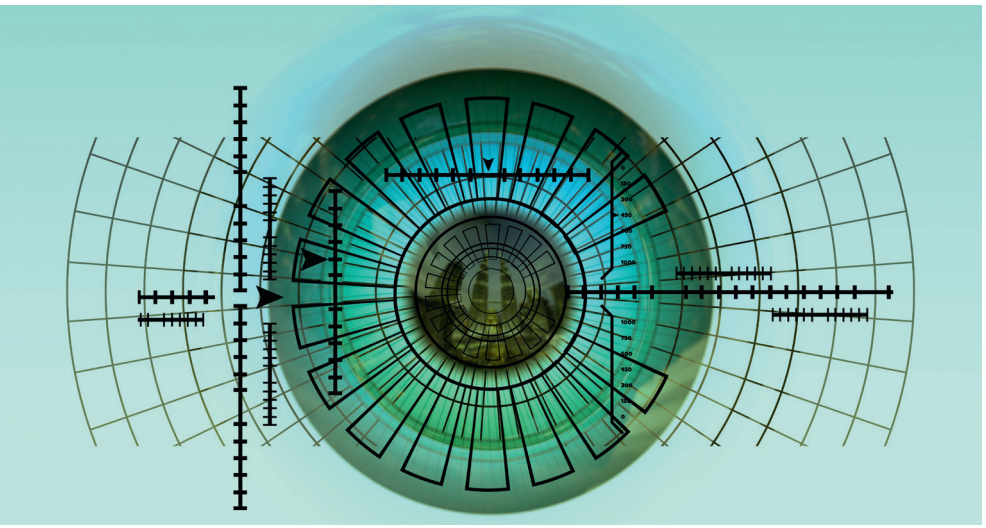
Selbstlernende Betrugsprävention im E-Commerce

Von Ralf Gladis



Hohe Chargeback-Raten können für Händler teuer werden. Betrugsprävention hat deshalb hohe Priorität. Regelbasierte Systeme stoßen aber schnell an ihre Grenzen. Entweder lassen sie durch False-Positive-Meldungen die Konversionsraten sinken oder zu laxe Regeln geben zu viele betrügerische Transaktionen frei. Hohes Potenzial sieht Ralf Gladis deshalb in der Künstlichen Intelligenz. Algorithmen ermöglichen die risikobasierte Beurteilung auf einer individuellen Bewertung der einzelnen Transaktion und sie sind auch in der Lage, Betrugsmuster aufzudecken, die Menschen nicht erkennen können. Red.

Zahlungsbetrug ist so alt wie das Geld selbst und unabhängig von der gewählten Zahlungsmethode. Gerade bei Kreditkartentransaktionen besteht für Händler und Kunden ein nicht zu unterschätzendes Risiko. Um zu verhindern, dass Kriminelle mit gestohlenen Karten und Datensätzen Schindluder treiben, setzte die Betrugsprävention bislang auf die sogenannte Rule Based Fraud Prevention. Hierbei bestimmen feste Regeln, ob eine Kreditkartenzahlung akzeptiert wird oder nicht.

Das ist jedoch weder für Händler noch für Kunden die Ideallösung. Denn immer wieder kommt es vor, dass die Methode harmlose Transaktionen verweigert oder umgekehrt betrügerische Vorgänge durch das teilweise weitmaschige Netz der Regeln schlüpfen. Abhilfe schafft die risikobasierte Betrugsprävention (Risk Based Fraud Prevention). Sie setzt auf Machine Learning und arbeitet wesentlich exakter.

Drakonische Strafen bei hohen Chargeback-Raten

Für Händler ist Kreditkartenkriminalität ein großes Ärgernis. Neben gestohlenen Daten bedrohen vor allem Chargebacks in Form von Friendly Fraud die Geschäfte.

– Chargebacks selbst sind einfache Rückbelastungen und erst einmal kein Grund zur Sorge.

– Beim Friendly Fraud hingegen kaufen Nutzer Waren mit ihrer eigenen Kreditkarte und verlangen von der Issuer-Bank eine Rückbuchung nachdem sie die Produkte erhalten haben. Auf diese Weise behalten sie die Ware und erhalten dennoch das gezahlte Geld zurück. Heutzutage fallen bereits 70 Prozent aller Kreditkartenbetrugsfälle in diese Kategorie.

Händler fürchten zu Recht den Effekt einer hohen Chargeback-Rate auf das Geschäft, sie haften selbst für den entstandenen Schaden. Die Folgen sind ein beeinträchtigter Cash-Flow, eingeschränkte Optionen der Zahlungsakzeptanz und ein sinkender Umsatz, kurz: dem Verkäufer gehen Geld und Güter verloren. Die Faustregel: Steigt die Betrugsrate über ein Prozent aller abgewickelten Kreditkartenzahlungen, muss der Acquirer gegenüber dem Kreditkartennetzwerk Rechenschaft in Form von monatlichen Berichten ablegen. Wer unter derartiger Beobachtung steht, muss drakonische Strafen zahlen.

Aussitzen ist keine Lösung. Reichen die schwarzen Schafe ihre Berichte nicht beim Netzwerk ein, steigen die Strafen für den Verzug auf bis zu 1 000 Euro pro versäumtem Tag.

Prävention ist oberstes Gebot

Für den Acquirer, der als Mittler zwischen beiden Parteien steht, ist es in manchen Fällen einfacher, die Kreditkarten-Akzeptanz gleich ganz aufzukündigen. Für die Händler ist der Schritt

Ralf Gladis, CEO, Computop Wirtschaftsinformatik GmbH, Bamberg

hingegen verheerend. Sie können fortan keine Kreditkartenzahlungen über den bisherigen Partner-Acquirer mehr akzeptieren und landen im Falle von Mastercard und Visa für mindestens fünf Jahre in einer „Sünder-Kartei", der Terminated Merchants File.

Dort vorzeitig wieder herauszukommen, ist schwierig. Wer sich in besagtem Zeitraum an einen anderen Acquirer wenden möchte, scheitert oft an seinem negativen TMF-Eintrag. Die Auswahlmöglichkeit der Partner schränkt sich dadurch oft erheblich ein. Prävention ist deshalb oberstes Gebot.

Die gute Nachricht: Dieses Risiko können Betroffene deutlich senken. Dank Machine Learning verbessern sich moderne Systeme kontinuierlich und sind effektiv wie nie zuvor.

Rule-Based war gestern

Bisher galt der regelbasierte Ansatz der Betrugsprävention als Standardlösung. Er legte Bedingungen fest, die erfüllt werden mussten, um eine Transaktion zu genehmigen. Treten im Zahlungsprozess Auffälligkeiten auf, lehnt der Händler die Zahlung ab.

Ein Beispiel: Verwendet ein Nutzer die Karte aus einem bestimmten Land heraus, das über Regeln als kritisch eingestuft wurde oder ist das Gerät, mit dem er online bezahlt, unbekannt, steigt die Wahrscheinlichkeit, dass die Transaktion scheitert. Auch wenn er eine Karte mehrmals in kurzen Abständen nutzt, besteht insbesondere in Kombination mit dem gerade genannten Kriterium das Risiko einer Ablehnung. Hier greifen sogenannte Velocity Checks, die Transaktionen innerhalb eines definierten Zeitraumes auf wiederkehrende Muster prüfen.

In der Praxis existieren noch viele weitere Bedingungen, die als Sicherheitsschranken fungieren. Ein großes Problem ist aber, dass ein derartiges Modell oft auch die Falschen trifft. Sind die Regeln zu lax ausgelegt, steigt die Betrugsrate. Sind sie zu streng, sinkt die Konversion.

Mehr Konversion durch weniger False Positives

Für Händler ist „Künstliche Intelligenz (KI)" aber nicht nur für die Betrugsprävention interessant. Der Risk-Based-Ansatz hilft auch, die Zahl der False Positives zu reduzieren. Hierbei handelt es sich um fälschlicherweise zurückgewiesene Transaktionen, von denen eigentlich keine Gefahr ausging, die jedoch von regelbasierten Herangehensweisen als kriminell eingestuft wurden. Umgekehrt sind False Negatives nichts anderes als Betrüger, die das System als unbedenkliche Kunden klassifiziert hat.

Für die Händler ist die genauere Einschätzung über risikobasierte Lösungen deshalb eine große Erleichterung, da sie für eine höhere Konversionsrate und damit für mehr Umsatz sorgt.

Die neue Generation des Risikomanagements arbeitet mit Künstlicher Intelligenz und setzt auf Machine Learning. Einfacher ausgedrückt: Ein Algorithmus übernimmt die Risikokalkulation und lernt mit jeder durchgeführten Transaktion dazu, indem er aus der Historie der durchgeführten Zahlungen sowohl Betrugsfälle als auch erfolgreiche Geschäfte identifiziert und dabei Muster erkennt. Das hat viele Vorteile, denn die Methode ist nicht nur genauer als der regelbasierte Ansatz, sie erkennt auch Betrugsszenarien, die bisher unter dem Radar flogen und passt sich verändertem Käuferverhalten und Kriminalitätsentwicklungen an.

»Risikobasierte Lösungen sorgen für höhere Konversionsraten.«

Transaktionen werden individuell bewertet

Den Unterschied zwischen den beiden Herangehensweisen illustriert ein Klassiker der regelbasierten Prävention: das Kriterium der Kartenherkunft. Hierbei blockten Anbieter per Regelsetzung Kartenzahlungen aus bestimmten Ländern, die auf einer Blacklist stehen. Auch die Höhe des Betrages spielte in die Entscheidung hinein. So könnte eine konkrete Regel lauten: Wird eine Zahlung über mehr als 500 Euro aus Afghanistan angefragt, lehnt das System sie automatisch ab.

Der risikobasierte Ansatz errechnet hingegen Wahrscheinlichkeiten. Die Frage lautete also nunmehr: Welchen Anteil haben Beträge über 500 Euro an der Gesamtheit der verzeichneten betrügerischen Transaktionen und wieviel Prozent der erfolgreichen Zahlungen liegen über 500 Euro? Die Betrugspräventionslogik der Künstlichen Intelligenz nutzt dieses Datenpaar und errechnet, wie die Chancen stehen, dass eine neue Transaktion über 500 Euro betrügerisch ist. Damit ersetzt die Berechnung eines Punktwertes auf der Grundlage bedingter Wahrscheinlichkeiten die Ja-/Nein-Entscheidung.

Die Kombinationsmöglichkeiten mit anderen Rechenoperationen sind praktisch unbegrenzt. So lässt sich erfragen, wie hoch das Risiko ist, dass eine neue Transaktion aus einem bestimmten Land gefährlich wird. Die Künstliche Intelligenz kombiniert diesen Wert mit den Informationen über den Geldbetrag und berechnet so eine Gesamteinschätzung für den Vorgang. Dabei kann sie beliebig viele weitere Kriterien ansetzen wie beispielsweise die allgemeine Betrugsrate, Betragsschwellen, Kartenherkunft, Einsatzort, Branche, die Verwendung eines Anonymisierungsdienstes, Transaktionsdauer und Übereinstimmung von Rechnungs- und Lieferadresse.

Mit jedem zusätzlichen Parameter erhöht sich die Genauigkeit der Betrugsvorhersage für genau diese Art der Transaktion. Zudem verbessert sich die Kalkulation mit jedem weiteren Zahlvorgang. Anhand der stetig wachsenden Datenhistorie steigt die Präzision der Wahrscheinlichkeitsberechnung für jeden einzelnen Parameter und dadurch auch die Qualität der Gesamtaussage kontinuierlich.

Hier liegt die große Stärke der Künstlichen Intelligenz. Sie ist im Vergleich zum Menschen in der Lage, viel größere Datenmengen in kürzester Zeit zu durchforsten, zu sortieren, zu analysieren und Schlüsse nach einer antrainierten Logik zu ziehen.

All diese komplexen Berechnungen laufen in Sekundenbruchteilen unmittelbar nach der Anfrage zur Autorisierung der Zahlung ab. Das Ergebnis drückt die Künstliche Intelligenz über einen Score-Wert aus, der entscheidet, ob die Transaktion der kartenausgebenden Bank über 3D Secure verifiziert werden muss oder nicht.

»Machine Learning reagiert in Echtzeit auf neue Gefahren.«

Bewertet die Engine den Vorgang als unbedenklich, kommt die Passworteingabe gar nicht erst zum Einsatz. Bei einem mittleren Scoring kann es sein, dass Banken den Vorgang nach eigenen Kriterien überprüfen oder den Käufer auffordern, sein Passwort einzugeben. Sobald 3D Secure greift, geht die Haftung vom Händler auf die Bank über. Bei einem Score im roten Bereich wird die Zahlung ohne Umschweife abgelehnt.

Die risikobasierte Herangehensweise verändert die Betrugsprävention grundlegend und bewegt sich weg vom manuellen und händlerindividuellen Prozess. Sie nutzt für ihre Kalkulationen die Gesamtheit aller anonymisierten Transaktionen. Gleichzeitig baut sie, falls gewünscht, weiterhin auf die händlerspezifische Risikoeinschätzung anhand der Transaktionshistorie jedes einzelnen Unternehmens auf.

Damit das gelingt, speichern Dienstleister sowohl die dafür benötigten anonymisierten Daten der erfolgreichen Transaktionen, aber auch der späteren Chargebacks, aus den Abrechnungsdateien der Acquirer. Dadurch wird Sicherheit auf einem konstant hohen Niveau garantiert, das mit den Entwicklungen des Marktes automatisch mitwächst, wie das folgende Beispiel illustriert.

Das KI-Auge sieht mehr

Bisher war es nötig, Änderungen hinsichtlich der Bedrohungslage manuell zu verfolgen. Somit mussten Menschen händisch neue Szenarien ausfindig machen, um sich im Dschungel der Betrugsmaschen einen Überblick zu verschaffen. Ein großer Nachteil, denn so sind nur stark verzögerte Reaktionen auf neue Gefahren und Entwicklungen möglich. Automatisiertes Machine Learning reagiert hingegen nahezu in Echtzeit und spürt Anomalien auf, die dem Menschen verborgen bleiben.

So ist eines der vielen erstaunlichen Ergebnisse der selbstlernenden Betrugsprävention, dass es kriminelle Vorgänge gibt, die über Schriftarten erkannt werden können. So haben Fraud Scoring Engines überraschenderweise Registrierungen von Usern abgelehnt, deren Browser sehr seltene Fonts nutzten. Auf den ersten Blick schien der Zusammenhang zwischen Schriftart und Betrug schwer nachvollziehbar. Bei genauerer Untersuchung stellte sich heraus, dass die fraglichen Fonts hauptsächlich bei illegalen Online-Spielcasinos zum Einsatz kommen. Die KI erkannte diesen Umstand und folgerte, dass die Wahrscheinlichkeit eines Betrugs außerordentlich hoch liegt. Dem Menschen wäre dieses bizarre Phänomen wohl verborgen geblieben.

»KI-Detektive können sogar zusammengeschlossen werden.«

Für Händler ergibt sich daraus ein klarer Sicherheitsgewinn, der erst durch den Einsatz der neuen Technologie möglich wurde. Die KI-Detektive können für noch mehr Sicherheit sogar zusammengeschlossen werden. So nutzt Computop neben der eigenen selbstlernenden Betrugsprävention auch die Expertise externer Dienstleister wie CRIF. Dadurch fällt die Betrugsvorhersage nochmals präziser aus und nutzt weitere Parameter, die über Schnittstellen ergänzt werden können.

Der selbstlernenden Betrugsprävention gehört die Zukunft. Sie sorgt für eine schlagkräftige Lösung im Kampf gegen die Kreditkartenkriminalität. Wo der regelbasierte Ansatz den aktuellen Entwicklungen teils deutlich hinterherhinkt, reagieren risikobasierte Systeme beinahe in Echtzeit auf neue Trends im Bereich Fraud. Dadurch haben Kriminelle deutlich weniger Spielraum. Für Händler bedeutet das eine höhere Konversionsrate, mehr Umsatz und ein geringeres Risiko, in den berüchtigten Terminated-Merchant-Listen zu landen. Künstliche Intelligenz hilft nicht nur, die Kriminalitätsfälle zu senken, sondern erkennt auch Muster, die der menschlichen Wahrnehmung verborgen bleiben.

Enormes Potenzial

Vollständig vermeiden können die neuen Technologien Betrug nicht, doch sie sind ein enormer Fortschritt, dessen Potenzial noch lange nicht ausgeschöpft ist. Je umfangreicher der Datenpool und je ausgefeilter die KI-Lösung, desto schwerer haben es Kriminelle, mit betrügerischen Transaktionen erfolgreich zu sein.

Mit der modernen Technologie stößt die ganze Branche jedoch ein Feld auf, das unglaubliches Potenzial für die Zukunft eröffnet. Interessant ist dieser Umstand allein schon deshalb, weil Künstliche Intelligenz eine vergleichsweise junge Disziplin der Computerforschung ist, die sich trotz ihrer jetzt schon bewiesenen Macht in vielerlei Hinsicht noch in den Kinderschuhen befindet. Anbieter wie Computop entwickeln ihre Lösungen deshalb kontinuierlich weiter, um ihren Kunden die maximale Sicherheit zu garantieren. ■

BEILAGENHINWEIS

Dieser Ausgabe liegt das Sachregister 2018 der Zeitschrift cards Karten cartes bei.

KARTEN
cards | cartes

SICHERHEIT

Biometrie ist die Zukunft

Von Ralf Gladis, Computop – Digitales Payment muss sicher sein. Mit zunehmender Beliebtheit elektronischer Zahlungen steigt jedoch das Risiko von Attacken auf Kundendaten. Benutzername, Passwort und PIN: Diese Kombination gilt unter Experten als vergleichsweise unsicher. Abgefangene E-Mails, ausgespähte Geldautomaten und ausgeklügelte Phishing-Praktiken verhelfen Kriminellen immer wieder zum Erfolg. Das erfordert neue Strategien. Die zweite europäische „Richtlinie über Zahlungsdienste im Binnenmarkt" (PSD2) schreibt deshalb vor, dass zur Authentifizierung des Zahlungsabsenders jeweils zwei von drei Faktoren überprüft werden müssen: Wissen (zum Beispiel ein Passwort), Besitz (zum Beispiel Chip-Karte), Inhärenz (zum Beispiel Fingerabdruck).

Sicherer und bequemer als Passwörter

Gerade der Faktor Inhärenz wird an Bedeutung gewinnen, denn auf vielen Smartphones ist die Authentisierung mittels eines Fingerabdrucks oder Gesichtserkennung bereits Realität. Auch in den niedrigeren Preisklassen wächst die Zahl der Geräte mit biometrischen Fähigkeiten, wodurch die Technologie im Massenmarkt immer stärkere Verbreitung findet. Da fast jeder ein Mobiltelefon besitzt, wird es zu einem wichtigen Baustein für die neue Zwei-Faktor-Sicherheitslösung nach PSD2.

Durch die einfache Handhabung sind Zahlungen nicht nur besser geschützt, sondern auch bequemer. Der Nutzer muss im Bezahlvorgang weder ein unhandliches Passwort noch eine PIN eingeben. Er legt zur Bestätigung lediglich seinen Finger auf den Scanner oder hält das Smartphone vor das Gesicht. Lösungen wie Apple Pay integrieren diese Art der Authentifizierung bereits jetzt in den Zahlungsvorgang.

Dieser Weg wird auch Händlern offenstehen, die im Zuge der neuen Richtlinie Zahlungen gemäß „Instant Payments" auslösen wollen. Diese sekundenschnellen, jederzeit verfügbaren Transaktionen ermöglichen im Namen des Bankkunden eine direkte Ausführung vom Bankkonto durch Dritte und unterliegen ebenfalls der Zwei-Faktor-Autorisierung.

Nutzen die Händler das Zusammenspiel zwischen Hardware-Herstellern und Zahlungsdienstleistern, sparen sie sich den Aufbau eigener Strukturen. Der Fingerabdruck, das Gesichts- oder

das Stimmenmuster der Nutzer wird hochverschlüsselt auf dem Endgerät gespeichert. Statt des Originalprofils erhält der Payment Service Provider lediglich nach einem bestimmten Muster verschlüsselte Zeichensequenzen, sogenannte Hashwerte. Um den Nutzer zu authentifizieren, prüft er, ob der erhaltene Hashwert mit dem anfänglich hinterlegten Wert zusammenpasst. Er kann nicht auf die biometrischen Rohdaten zugreifen und deshalb auch nicht den unverschlüsselten Fingerabdruck wiederherstellen.

Biometrie im Browser

Biometrische Authentifizierung ist praktisch überall einsetzbar. Beispielsweise für die Zugangskontrolle zu besonders schützenswerten Unternehmensbereichen oder für die sichere Identifizierung an einer 24-Stunden-Paketabholung, an der Poststation. Doch auch beim digitalen Shopping ergeben sich neue Möglichkeiten.

Die Non-Profit-Organisation Fast Identity Online (FIDO) bietet mit Web Authentication einen Authentisierungsstandard für Webbrowser mit FIDO-Anschluss, der die passwortlose biometrische Authentisierung und Authentifizierung über Fingerabdruck oder Gesichtserkennung erlaubt. Browser wie Microsoft Edge, Google Chrome und Mozilla Firefox unterstützen die Technologie bereits. Hersteller können die API für Smartphones und Tablets mit Fingerabdrucksensor (zum Beispiel Apples Touch ID) oder Gesichtserkennung (Windows Hello, Face ID) nutzen. Die biometrischen Nutzerdaten verlassen auch in diesem Fall niemals den gesicherten Bereich des Geräts. Lediglich die Hashwerte werden übermittelt.

Voice Commerce noch Zukunftsmusik

Während Fingerabdrücke und Gesichtserkennung bereits als Sicherheitsfeatures im Massenmarkt angekommen sind, bleibt die biometrische Authentifizierung über die Stimme vorerst noch dem Geschäftsbereich vorbehalten. Unternehmen wie Banken und auch die Telekom setzen aber schon heute Verfahren ein, bei denen die Stimme das Passwort ersetzt. Der Netzbetreiber spricht von bis zu 100 charakteristischen Merkmalen, die eine Stimme einzigartig machen und die im Zuge der Erstidentifikation in ihrem System erfasst werden, sollte ein Kunde sich für diese Form der Anmeldung entscheiden.

Das Profil speichert dabei nicht die Stimme selbst, sondern eine daraus generierte Zahlenkombination. Auch hier ist eine nachträgliche Nachbildung des biometrischen Ausgangsmaterials unmöglich. Im Konsumentenbereich ist eine ähnliche Anwendung im Voice Commerce und bei digitalen Assistenten wie Google Home oder Amazon Echo denkbar. Noch ist deren Technik nicht in der Lage, Stimmen hundertprozentig auseinanderzuhalten. Es ist aber nur eine Frage der Zeit, bis die Entwicklung auch auf diesem Bereich soweit ist.