Betrugsbekämpfung braucht **neue Modelle**

Von Jörg Floegel

Mit der wachsenden Vielfalt an Zahlungsmöglichkeiten steigt auch der Druck auf die Autorisierung der Zahlungen und die Betrugsbekämpfung. Das gilt umso mehr vor dem Hintergrund der mit der PSD II vorgesehenen Öffnung für Drittanbieter, die das Risiko für die Banken erheblich steigen lässt. Bisherige Systeme für die Betrugserkennung stoßen damit ans Limit. Und so werden neuronale Netze zunehmend durch Bayessche Modelle ersetzt, in die neue Bezahlkanäle leicht integriert werden können und die zudem durch weniger Fehlalarme auslösen. Red.

Die Betrugserkennung bei Kartenzahlungen ist komplex und damit kostenintensiv. Laut Europäischer Zentralbank wurden im Jahr 2013 in Europa 958 Millionen Euro bei Kartenzahlungen im Internet erbeutet.[1)] Aus Kulanz erstatten Banken und Sparkassen ihren Kunden die entstandenen Verluste, um das Vertrauen in ihre Dienstleistungen nicht zu gefährden. Doch das ist keine nachhaltige Lösung. Denn obwohl Beträge bis zu 20 Euro in Deutschland am liebsten mit Bargeld beglichen werden, nehmen Kartenzahlungen kontinuierlich zu. Im Jahr 2014 wurde bereits jeder zehnte Euro im Internet ausgeben[2)], im Fachhandel wird sogar jeder dritte Euro online ausgegeben und digital bezahlt.

Mit den Zahlungen wandern auch die kriminellen Angriffe ins Netz. Seit 2012 steigt die Zahl der Betrugsfälle mit Kartendaten im Internet – insbesondere bei Zahlungen aus dem Ausland. Obwohl 2013 nur zwei Prozent aller Überweisungen außerhalb des Sepa-Raums stammten, standen diese Transaktionen für 22 Prozent aller Betrugsfälle. Diese hohe Zahl ist darauf zurückzuführen, dass Betrüger niedrige Sicherheitsstandards in Ländern außerhalb Europas ausnutzen und beispielsweise Karteninformationen auf Magnetstreifen kopieren.

Card-not-present-Betrug auf Allzeithoch

In den USA, die kurz vor der flächendeckenden Einführung der EMV-Chips stehen, ist der Datenklau an Geldautomaten in den letzten Monaten sprunghaft angestiegen. Betrüger nutzen das kurze Zeitfenster, das ihnen noch bleibt, um mit gefälschten Karten Kasse zu machen.

Erfahrungen aus Deutschland zeigen, dass mit flächendeckender Einführung von EMV Betrugsfälle mit physischen Karten deutlich zurückgegangen sind.

Zum Autor

Jörg Floegel, Direktor Professional Services Deutschland, Österreich und Schweiz, NCR GmbH, Augsburg

Dafür steigt die Zahl der betrügerischen Card-not-present-Zahlungen kontinuierlich. 78 Prozent aller Kartenbetrugsfälle in Deutschland fanden 2013 ohne physische Karte statt.

Während die Angriffe immer ausgefeilter werden, deckelt die EU die Transaktionskosten bei Kartenzahlungen. Für Banken ist diese Entwicklung bedrohlich, da sie immer mehr Zahlungen abwickeln und verifizieren müssen, dabei aber weniger verdienen. Dabei müssen sie gerade jetzt ihre Systeme modernisieren, um sich gegen den steigenden Card-not-present-Betrug abzusichern. Eile ist geboten, denn mit der Öffnung von Karten-, Internet- und mobilen Zahlungen für Drittanbieter, die die PSD II Direktive fordert, steigt nicht nur die Zahl der Transaktionen, sondern das Risiko für Zahlungsbetrug.

Öffnung für Drittanbieter

Die PSD II deckelt nicht nur die Interbankenentgelte für Kartenzahlungen, sondern legt fest, dass Zahlungen nicht mehr über ein bestimmtes Konto bei einer spezifischen Bank abgewickelt werden müssen. Sie können künftig über neue Kanäle laufen, zum Beispiel direkt über Versorgungsunternehmen oder Telekommunikationsanbieter, die entsprechende Bestimmungen erfüllen. Dazu müssen Banken lizensierten Drittanbietern Zugriff auf die Kontodaten des Kunden einräumen.

Bei Schäden werden primär die Banken das Nachsehen haben, denn bei nicht autorisierten Kartenzahlungen darf der Verlust für den Verbraucher künftig 50 Euro nicht übersteigen.[3)] Gleichzeitig berichten Medien nahezu täglich über neue Bezahlmodelle und Angebote. Auch wenn sich nur einige davon durchsetzen, müssen sich Finanzinstitute auf eine Zahlungsvielfalt einstellen.

Nach Tests in Großstädten können Facebook-Nutzer in den USA seit August 2015 per Facebook Messenger Geld an andere Mitglieder des sozialen Netzwerkes senden. Das System selbst ist relativ einfach, da es auf bestehende Debit-Karten aufsetzt. Diese müssen im Nutzerprofil hinterlegt werden und schon kann mit wenigen Klicks Geld transferiert werden. Damit das Geld direkt vom eigenen Konto auf das des anderen Facebook-Nutzers übertragen werden kann, muss der Empfänger ebenfalls eine Karte in seinem Profil registrieren.

Bestehende Systeme am Limit

Mit Paypal, Google Wallet, Barclays Pingit und nun Facebook Messenger gibt es mittlerweile etliche Möglichkeiten, Geld direkt an andere Personen zu übertragen. Auch wenn hierzulande Paypal den größten Marktanteil hat, ist die Wahrscheinlichkeit recht hoch, dass die 700 Millionen Nutzer von Facebook weltweit dieses Angebot nutzen und damit diese Zahlungsform schnell etablieren. Einen besonderen Charme hat beispielsweise die Option, Zahlungen während eines laufenden Gruppenchat direkt anzustoßen, ohne den Chat zu verlassen. Jeder kann dabei sehen, wer wem wie viel gezahlt hat. Bei der Organisation einer Party oder beim Besorgen eines gemeinsamen Geburtstagsgeschenks ist die Funktion sehr praktisch.

Die Systeme vieler Banken sind allerdings nicht auf die Bewertung und Betrugsprävention bei Zahlungen aus einer ständig steigenden Zahl an Kanälen ausgerichtet. Um Betrugsszenarien zu erkennen, werden seit Jahren Algorithmen auf Basis neuronaler Netze eingesetzt, die Angriffe anhand von Verhaltens- und Ablaufmustern erkennen. Diese Methode ist bewährt, hat aber ihre Schwächen. So können oft nur begrenzte Datenmengen zur Mustererkennung ausgewertet werden.

Weicht der Angriff von bekannten Mustern ab, wird er nicht als solcher erkannt, da das Muster nicht auf seine zugrundeliegenden Regeln hin untersucht, sondern als Ganzes erkannt wird. Ein Lernen von neuen Mustern erfolgt erst durch umfassendes Training. Darüber hinaus können neuronale Netze keine präzise Vorhersage über die Interpretation eines Musters abgeben, solange nicht dieses spezifische Netz mit dieser spezifischen Lernerfahrung durchgerechnet wird. So entstehen komplexe, nicht lineare Strukturen.

Attacken automatisch aufspüren

Um solche Netze zu aktualisieren, müssen neue Verbindungen hergestellt, bestehende Verbindungen gelöscht oder die Gewichtung der einzelnen Informationen beziehungsweise Neuronen angepasst werden. Danach müssen diese neuen Verbindungen trainiert werden. Bei komplexen Neuronetzen kann das mehrere Monate dauern. Abgesehen von dem hohen Personalaufwand können sich Finanzinstitute heute solche Reaktionszeiten kaum noch leisten.

Einen anderen Ansatz verfolgt das sogenannte Bayes-Modell, das moderne Lösungen wie beispielsweise Fractals von NCR zugrunde legen. Die intelligente Betrugserkennungslösung wurde im Zuge der Übernahme von Alaric im Dezember 2013 ins NCR-Portfolio aufgenommen.

Bayessche Modelle machen sich einen mathematischen Satz aus der Wahrscheinlichkeitsrechnung zunutze, um zu ermitteln, mit welcher Sicherheit von einem Betrug auszugehen ist. Dieser Ansatz geht davon aus, dass eine Transaktion entweder legitim ist oder nicht. Einen Grad dazwischen gibt es nicht. Für jede Transaktion wird daher anhand von statistischen Erkenntnissen, Annahmen und Erfahrungswerten bewertet, mit welcher Wahrscheinlichkeit es sich um eine betrügerische Transaktion handelt, ganz unabhängig davon, ob sie im Internet, Online-Banking, am PoS-Terminal oder Geldautomaten initiiert wurde.

Anhand dieser Bewertung werden automatisch vordefinierte Aktionen ausgelöst: Die Transaktion wird genehmigt, abgewiesen oder zurückgestellt. Für zurückgehaltene Transaktionen können individuelle Regeln festgesetzt werden. Handelt es sich beispielsweise um eine ungewöhnlich hohe Transaktion für ein bestimmtes Kundenprofil, kann die Bank den Kunden per SMS oder E-Mail über die verdächtige Transaktion informieren und deren Authentizität abfragen. Handelt es sich aber um einen Fehlalarm, ist der Kunde verunsichert. Eine Alternative ist daher, Vorgänge zu beobachten und zusätzliche Filter anzusetzen. In dem Fall wird der Kunde erst alarmiert, wenn beispielsweise innerhalb von 30 Minuten in mehreren Transaktionen Summen bewegt werden, die die durchschnittlichen Tagesausgaben der letzten Monate um das Doppelte übersteigen.

Die Architektur der Lösung erlaubt eine kontinuierliche Integration neuer Technologien. Dank der modernen Architektur ist Fractals sehr flexibel einsetzbar und leicht zu konfigurieren. So können neue Bezahlkanäle problemlos integriert werden, um bei der Betrugserkennung einen ganzheitlichen Überblick zu gewährleisten.

Weniger Fehlalarme bei Bayesschen Modellen

Vergleichstests haben gezeigt, dass Bayessche Modelle andere gängige Lösungen bei der Erkennungsrate übertreffen und erheblich weniger Fehlalarme auslösen. Ergänzt um selbstlernende Funktio-

nen, kann sich so ein Modell automatisch beim ersten Auftreten eines neuen Betrugsszenarios darauf einstellen. Fractals bewertet Transaktionen nahezu in Echtzeit und kann sie im Betrugsfall noch während der Autorisierungsabfrage ablehnen.

Derzeit erfolgt die Bewertung der Transaktionen erst zeitversetzt über Nacht. Doch spätestens wenn Sofortzahlungen EU-weit verpflichtend werden, müssen Institute hierzulande reagieren. Bei kontaktlosen Bezahlmodellen werden Beträge heute schon in Echtzeit transferiert. Setzt sich Apple Pay durch, dann wird die Grenze von 20 Euro für kontaktlose Zahlungen schnell fallen.

Seit den neunziger Jahren wird an NFC-basierten (Near Field Communications) Zahlungen gearbeitet. Mit der Einführung von EMV kann die Technologie nun auch für sicheres, kontaktloses Bezahlen eingesetzt werden.

„Tap and go"-Zahlungen anfällig für Missbrauch

Gleichzeitig ist die Mobilfunktechnologie so weit fortgeschritten, dass kontaktlose Zahlungen nicht mehr an eine Karte gebunden sein müssen, sondern auch über ein Smartphone oder andere mobile Geräte erfolgen können. Damit wird der Anreiz erhöht, auch kleinere Beträge nicht mehr in bar zu begleichen.

Die Technologie wird aber nur genutzt, wenn sie auch einfach und unkompliziert funktioniert. Weder würde ein Kunde beim Kauf einer Tageszeitung zur Karte greifen und eine PIN eingeben oder am Kassenzettel unterschreiben noch würde der Händler sich angesichts der Kosten darüber freuen. Bei kontaktlosen Bezahlmodellen sind die Gebühren entsprechend dem Wert der Transaktion sehr niedrig. Doch Transaktionen, die weder durch eine PIN noch durch Unterschrift validiert werden, sind auch anfällig für Missbrauch. Aus diesem Grund ist die Transaktionssumme in der Regel auf 20 Euro begrenzt und es wird stichprobenartig nach der PIN oder einer Unterschrift gefragt.

Apple Pay und Tokenisierung: Knackpunkt Zahlungsautorisierung

Um Zahlungen besser abzusichern, wird verstärkt auf die sogenannte Tokenisierung gesetzt. Dabei wird die eigentliche Kartennummer (PAN) durch eine eingeschränkt nutzbare Pseudo-PAN ersetzt. Dieses Token enthält genug Informationen, um eine Transkation an einem gängigen Kartensystem abzuwickeln, kann aber nur von einem bestimmten Geschäft, einem bestimmten Gerät oder in einem bestimmten Zeitraum verwendet werden. Wird ein Token also abgefangen, ist es kaum von Nutzen für den Angreifer, da es weder die Kartennummer noch Informationen zum Konto enthält.

Apple Pay setzt beispielsweise auf Tokenisierung. Seit Juli können Besitzer eines i-Phone 6 oder einer Apple Watch in Großbritannien über ihre Geräte bezahlen und der Sprung auf den Kontinent lässt wohl nicht lange auf sich warten. Bei Apple Pay können Nutzer Zahlungen entweder über die bei i-Tunes hinterlegte Kreditkarte abrechnen oder eine neue Karte angeben. Beim Zahlungsvorgang wird ein einmaliges Token generiert und im Secure Element des Smartphones, einem speziell verschlüsselten Chip, gespeichert.

Das Token wird an keiner anderen Stelle gespeichert und auch nicht über eine Cloud synchronisiert. Für jeden Bezahlvorgang generiert das i-Phone eine neue Transaktionsnummer, die mit dem Token kombiniert wird. Auf diese Weise lässt sich die Zahlung der jeweiligen Kreditkarte und der entsprechenden Bank zuordnen. Apple erhält dabei weder Informationen über den Warenkorbinhalt noch die Rechnungshöhe. Der Händler wiederum hat keinen Zugriff auf die Kreditkartennummer oder den Namen des Kunden.

Der Bezahlvorgang ist für Nutzer einfach und die Sicherheitsmaßnahmen beeinträchtigen weder Komfort noch Geschwindigkeit. Dennoch hatte Apple Pay zum Start des Zahlungsdienstes in den USA erhebliche Probleme mit Betrugsfällen. So wurden gestohlene Kartendaten auf i-Phones hinterlegt und validiert. Für Apple und die Händler waren das legitime Apple-Pay-Konten, die innerhalb der Sicherheitssysteme genutzt werden konnten. Banken führten daraufhin eine Zwei-Faktor-Autorisierung ein, um sicher zu stellen, dass die Karte auch tatsächlich dem Nutzer gehört.[4)]

Das Beispiel zeigt, dass mit der Vielfalt an Zahlungsmöglichkeiten auch der Druck auf die Autorisierung der Zahlungen auf Bankenseite steigt. Da Tokens auch zunehmend bei Internetzahlungen eingesetzt werden, um Transaktionen mit gestohlenen Kartendaten zu verhindern, muss eine einwandfreie Validierung der hinterlegten Karte sichergestellt werden. Dazu müssen neue Autorisierungsstufen eingeführt werden, die Transaktionen, je nach Transaktionsart und -quelle bewerten.

Wird die Betrugserkennung mit der Autorisierung kombiniert, entsteht ein engmaschiges Sicherheitsnetz, dem auch bisher unbekannte Angriffsszenarien nicht verborgen bleiben. Gerade bei sinkenden Zahlungsentgelten ist es wichtig, keine Transaktion fälschlich zu blocken und die viel Handarbeit erfordernde Betrugserkennung so weit wie möglich zu automatisieren. Dann reduzieren Banken ihr Risiko bei Kartenzahlungen und gleichzeitig werden Zahlungen im Internet für Händler und Verbraucher billiger und sicherer.

Fußnoten

1) http://www.euractiv.de/finanzen-und-wachstum/linkdossier/psd-iban-sepa-die-neue-eu-richtlinie-ueber-zahlungsdienste-000148#group_summary
2) http://www.handelsblatt.com/unternehmen/handel-konsumgueter/online-shopping-wie-viel-wir-im-netz-ausgeben/11301594.html
3) http://www.euractiv.de/finanzen-und-wachstum/linkdossier/psd-iban-sepa-die-neue-eu-richtlinie-ueber-zahlungsdienste-000148#group_summary
4) http://www.technologytell.com/apple/147536/banks-take-steps-avoid-apple-pay-fraud/