Ingrid Riehl

Schutz vor **Onlinebetrug**

Ingrid Riehl, Geschäftsführerin, CRIFBÜRGEL GmbH, München

Wer früher ein Konto oder ein Depot eröffnen wollte, musste dafür entweder in eine Bankfiliale gehen oder – im Fall von Direktbanken ohne Filialnetz – zur Post. Dort prüfte ein Mitarbeiter den Ausweis und bestätigte in einem Formular die Identität des angehenden Bankkunden. Dank Videoidentifizierung geht das nun auch vom heimischen Sofa aus: Dafür benötigt der Kunde nur einen PC mit Webcam oder ein Smartphone mit Kamera. Er muss seinen Ausweis in die Kamera halten, ihn ein wenig kippen, damit die Hologramme sichtbar werden, und einige Fragen beantworten. Mehr als diesen kurzen Videochat braucht es oft nicht, um sich als Kunde zu identifizieren und gegebenenfalls ein Angebot sofort nutzen zu können.

Carsharing als Vorreiter

Die Anwendungsmöglichkeiten sind vielfältig: So wird das Verfahren bereits bei Carsharing-Anbietern und Mobilitätsdienstleistern genutzt, beim Erwerb von Prepaidkarten für das Mobiltelefon – oder eben bei Banken für Konto- und Depoteröffnungen. Der Vorteil: Der Prozess ist einfach und schnell und verläuft ohne Medienbruch, sodass die Abbrecherquote deutlich gemindert werden kann.

Eine weitere Anwendung für das Video-Ident-Verfahren bieten Kreditanträge. Ein attraktives Marktsegment für Banken, weil sie hiermit selbst in der aktuellen Niedrigzinsphase noch Geld verdienen können – anders als etwa beim Girokonto. Und der Markt wächst, wie etwa die Zahlen der Deutschen Bundesbank zeigen. Ende 2016 hatten Privatpersonen in Deutschland Konsumentenkredite in Höhe von 231 Milliarden Euro aufgenommen, Baufinanzierungen nicht mitgerechnet. Schon mehr als jeder vierte Verbraucherkredit (27 Prozent) kommt dabei online zustande, so eine aktuelle Studie des Bankenfachverbands. Tendenz weiter steigend, denn die Internetaffinität der Deutschen bei ihren Finanzgeschäften nimmt generell weiter zu. So nutzen aktuell schon 27 Prozent der Verbraucher Apps, vor allem für das Onlinebanking. Noch vor fünf Jahren waren dies nur fünf Prozent. Eine Kreditaufnahme per Smartphone können sich heute bereits sieben Prozent der Verbraucher vorstellen.

Allerdings sind mit diesen bequemen Services oft auch dem Datenklau Tür und Tor geöffnet. Betrugsfälle, wie etwa fingierte Kreditanträge, gab es schon immer. Doch durch die Verfügbarkeit von persönlichen Daten im Internet nimmt vor allem die Identitätsübernahme immer weiter zu. Und wo gut gefälschte Ausweise im persönlichen Kontakt in der Filiale im Schnitt etwa fünfmal verwendet werden, können damit im Internet eine Vielzahl von Anträgen bei diversen Banken gleichzeitig gestellt werden. Der Schaden geht so ganz schnell in die Millionen. Daher ist es klug, wenn Banken ihre bestehenden Sicherheitsmaßnahmen mit externen Lösungen ergänzen und erweitern, um Betrügern bestenfalls einen Schritt voraus zu sein. Das ist möglich mit modularen Lösungen, die Banken und ihre Kunden durch intelligente Mustererkennung vor Datendiebstahl, Identitätsmissbrauch und unbefugtem Kontozugriff schützen.

Das Thema Datendiebstahl beschäftigt ja nicht nur Banken, sondern auch Onlinehändler, Streaming-Dienste und vergleichbare Anbieter, wo Betrüger gestohlene Identitäten nutzen könnten, um unter falschen Namen einen Account anzulegen und sich so Geld und Gut zu erschleichen. Zentrale Fragen bei jedem Onlinegeschäftskontakt sind also: Existiert der neue Nutzer wirklich? Sind die angegebenen Daten korrekt? Oder wird eine falsche Identität verwendet?

Hier setzen wirksame Fraud-Prevention-Lösungen an. So kann mittels eines koordinierten Identifikations- und Prüfprozesses Identitätsmissbrauch im Internet in Echtzeit erkannt werden: Im Fall der international agierenden Wirtschaftsauskunftei Crifbürgel werden dabei innerhalb von Millisekunden aus sämtlichen Datenquellen die Angaben zur entsprechenden Person abgefragt und durch die Kombination verschiedener, sich ergänzender Module betrügerische Identitäten erkannt. Um Firmen und ihre Kunden vor Onlinebetrügern zu schützen, geht das Fraud-Prevention-System aber noch weiter: Die digitale Identität jedes Nutzers kann auf Basis eines Netzes von Daten und Transaktionen ermittelt werden. Die Fähigkeit, diese Daten zu verknüpfen und neue Transaktionen mit bereits bestehenden Identitäten zu verbinden, ist das Herzstück der Betrugsprävention. Gemäß dem Credo „Kenne deinen Kunden!" werden die Geräteidentifikation, die Verhaltensanalyse und andere Datensätze verbunden und liefern so Klarheit über die digitale Identität und die Endgeräte des Nutzers.

Missbrauch von Kunden-Accounts verhindern

Schutz bietet die Lösung auch beim sogenannten Account Takeover, wo Betrüger versuchen, sich mit gestohlenen Login-Daten oder durch den Einsatz von Schadsoftware Zugang zum Konto argloser Verbraucher zu verschaffen. Dem beugen ein permanentes Konten-Monitoring und der automatisierte Abgleich mit historischen Daten bei jedem Login wirksam vor. Dieser „digitale Wachhund" kennt seinen Herrn genau: Er kennt die individuelle Kunden-DNA, dazu gehören etwa dessen IP-Adresse, seine Endgeräte und typischen Verhaltensmuster. Der Account Protector prüft laufend auf Angriffe auf das Kundenkonto, auf Trojaner und Malware, er erkennt Anomalien, wie etwa eine andere IP-Adresse, eine untypische Location oder unplausible Änderungen in den Stammdaten und benachrichtigt – je nach Voreinstellung – die Bank oder den Kunden direkt. So wird dem Betrug durch Cyberattacken ein Riegel vorgeschoben.

Betrügerische Handlungen wird zwar kaum ein System komplett verhindern können, doch mit kontinuierlichem Monitoring und cleverem Datenmanagement gelingt in vielen Fällen die Erkennung von Betrug – damit nach Möglichkeit gar nicht erst ein Schaden entsteht.