PRODUCT SHEET
ID & Fraud Management | Lösungen für Banken

arvato BERTELSMANN Financial Solutions

Schutz vor Cybercrime im Online-Banking

Ihre Herausforderungen

Weil Betrüger mit echten, illegal beschafften Daten arbeiten, reichen die üblichen Risiko-Management-Verfahren nicht mehr aus, um betrügerisches Verhalten zu erkennen und zu unterbinden. In der digitalen Welt nimmt jedoch genau diese Gefahr, dass mit gestohlenen Account-Daten betrügerische Aktionen durchgeführt werden, stetig zu. Daher wird der Schutz von Kunden- und Kontodaten immer wichtiger.

Typische Betrugsphänomene

- **Account Takeover:** Betrüger verschaffen sich die Zugangsdaten zu Online-Banking-Accounts (z. B. Phishing-Mails) und missbrauchen die digitale Identität des Kunden zur Durchführung von Transaktionen.
- **New Account /Application Fraud:** Betrüger eröffnen Konten oder beantragen Kredite / Kreditkarten mit falschen oder gestohlenen Identitäten.
- **Man-in-the-Middle:** Betrüger schleusen sich in die Kommunikation zwischen Kunde und Online-Banking-System ein und manipulieren den Datenverkehr für betrügerische Zwecke.
- **Mobile Malware:** Betrüger nutzen Sicherheitslücken auf mobilen Endgeräten und platzieren Schadsoftware, um unbemerkt Kundendaten zu sammeln.

Aufwändige Prozesse

- **User Authentication:** Die Implementierung eines höheren Sicherheitsniveaus kann mit aufwändigeren Prozessen verbunden sein und führt bei Good-Usern zu einem negativen Kundenerlebnis.
- **Transaction Monitoring:** Die Analyse und Verlinkung von historischen Transaktionsdaten ist mit zeitintensiven Verfahren und höheren Kosten verbunden.

Unsere Lösung

Arvato Financial Solutions verfügt über eine Betrugspräventions-Lösung, mit der illegal erworbene Kunden- und Kontodaten nutzlos werden. Mit Hilfe von verschiedenen Lösungsmodulen lassen sich nicht nur die Betrüger identifizieren – für den legitimen User wird aufgrund von vereinfachten Authentifizierungsprozessen auch ein besseres Kundenerlebnis ermöglicht. Zusätzlich wird eine Einschätzung der Betrugsgefahr bei Transaktionen in Echtzeit abgegeben, sodass Unternehmen finanzielle Verluste und Reputationsschäden verhindern und ihren Umsatz steigern können. Unsere Lösung bietet eine modulare Plattform mit diversen Technologien und Tools, die zu einer Gesamtlösung integriert werden können, um spezifische Anwendungsfälle abzubilden.

Ihre Vorteile

- **Frühzeitige Betrugsprävention**
- **Automatisierte Betrugserkennung**
- **Datenschutzrechtliche Konformität**
- **Optimierung des Kundenerlebnisses**

So funktioniert intelligentes Fraud Management

Device Tracking

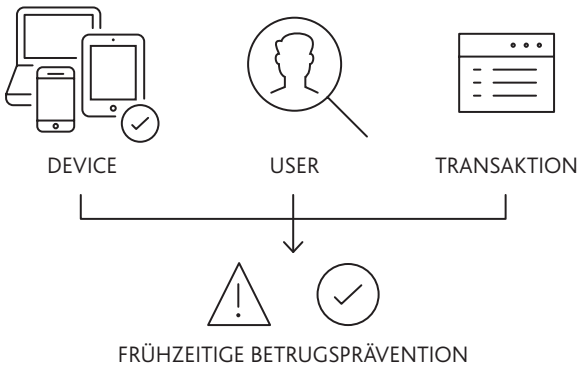
Das Tracking dient der Erkennung und Wiedererkennung eines Devices in Echtzeit anhand spezifischer Attribute (Device-Art, Geo-Location, Browserdaten etc.). Mit den Geräteinformationen wird eine Device-ID generiert, die in Verbindung mit den Personen- und Transaktionsdaten ausgewertet wird. Durch die Verknüpfung von mehreren Datenarten können Betrugsversuche identifiziert werden, bei denen eine „univariate" Betrachtung keine Hinweise liefern würde.

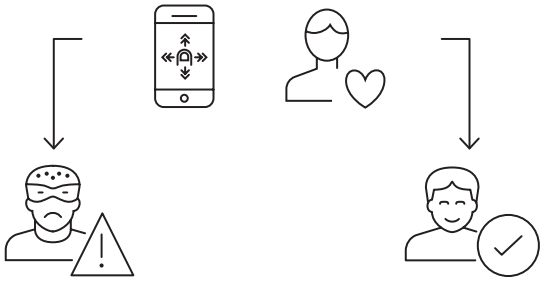
Passive Biometrics & Behavioral Analysis

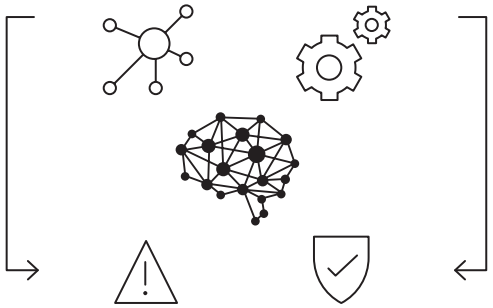
Der User kann anhand seines passiven biometrischen Profils (z. B. Tippen, Klicken, Zoomen, Wischen) identifiziert werden. Mit Hilfe einer Verhaltensanalyse werden die Navigationsstrukturen während der Websession aufgezeichnet und können mit historischen und durchschnittlichen Kundenverhaltensmustern abgeglichen werden. Diese Identifizierung ermöglicht die Unterscheidung zwischen vertrauenswürdigen und betrügerischen Usern in Echtzeit. Mit Hilfe dieser Verfahren kann zudem automatisch erfasst werden, ob es sich um menschliches Verhalten handelt oder ein automatisiertes Programm genutzt wird.

Artificial Intelligence & Machine Learning

Die automatische Entwicklung und der Einsatz von selbstlernenden Algorithmen sind eine Ergänzung zu den Regelwerken und erlauben verbesserte Prognosen. Dank analytischer Modelle ist es möglich, Betrug vorherzusagen und in Echtzeit einen Risikoscore zu generieren. Auf dieser Grundlage wird eine Handlungsempfehlung ausgesprochen. Die Entscheidung, ob eine Transaktion durchgeführt werden soll, kann automatisch oder manuell getroffen werden. Artificial Intelligence ermöglicht eine automatisierte Betrugserkennung und eine schnelle Anpassung an neue Betrugsmuster, sodass Entscheidungsprozesse schneller und effizienter gestaltet werden können.







Unsere Leistungen

- Multi-Layered-Betrugsprävention
- Echtzeit-User-Authentication
- Bedarfsspezifische und flexible Konfigurierung
- Beratungsdienstleistungen

Weitere Fragen? Nehmen Sie Kontakt mit uns auf.

Arvato Financial Solutions
Dominik Coenen | Vice President Sales, Finance & Payment
Telefon: +49 7221 5040-3354 | dominik.coenen@arvato.com

finance.arvato.com

Your backbone for growth.