



Biometrie 2.0: Worauf Banken achten müssen

Digitale Authentifizierung ist zur Schlüsselfrage im Bankwesen geworden. Biometrische Verfahren gelten als sicher und komfortabel – doch nicht jede Lösung hält, was sie verspricht. Worauf Kreditinstitute achten sollten, wenn sie auf Fingerabdruck, Gesichtserkennung & Co. setzen, erklärt Edwardcher Monreal, Principal Solutions Architect bei HID, im Gastbeitrag.

Status quo der Biometrie im Bankwesen

Die Sicherheit der persönlichen Daten und natürlich der finanziellen Mittel von Kundinnen und Kunden ist eine der zentralen Herausforderungen von Finanzinstituten im digitalen Zeitalter. Sie setzen daher zur Authentifizierung und zur Validierung von Kundenidentitäten auf biometrische Verfahren. Entsprechende Softwarelösungen verwenden in der Regel ein oder mehrere physische Merkmale zur Verifikation, darunter das Gesicht, den Fingerabdruck, die Handfläche, die Iris oder die Stimme. Doch ein reiner Abgleich zwischen den vom Kunden hinterlegten biometrischen Eigenschaften mit denen der Person am Endgerät ist längst nicht mehr das Ende der Fahnenstange. Auch bestimmte Verhaltensweisen werden mittlerweile getrackt, um die Sicherheit zu gewährleisten. Dazu gehören etwa der Tipprhythmus, die Art und Weise, wie eine Person das Endgerät in der Hand hält, oder an welchen Standorten sie gewöhnlich verkehrt.

Das Onboarding neuer Kunden beginnt heute in den allermeisten Fällen damit, dass sie persönliche Daten und Dokumente wie amtliche Ausweise zum Nachweis ihrer Identität einreichen. Die Bank prüft dann, ob es

sich bei den vorgelegten Dokumenten um gültige amtliche Unterlagen handelt und ob die biometrischen Daten ebenfalls unverfälscht sind. Sobald diese Prüfungen abgeschlossen sind, registriert das Finanzinstitut die Identität des Kunden, sodass die hinterlegten Daten zur Authentifizierung und Verifikation verwendet werden können. Dieser Vorgang ist heutzutage in wenigen Sekunden erledigt und findet entweder über spezielle Apps oder Remote-Onboarding-Services auf der Webseite der Kreditinstitute statt. Die spätere Überprüfung der User via Live-Scan und -Abgleich der hinterlegten Daten ist ebenfalls schnell durchgeführt.

Der Haken an der Sache

Während die Einrichtung und Nutzung biometrischer Sicherheitsverfahren und das Onboarding von neuen Kundinnen und Kunden in der Theorie reibungslos funktioniert, ist es in der Praxis oft nicht ganz so einfach. Gerade die Liveness Detection, also die eindeutige Feststellung, dass es sich um eine wirkliche Person handelt und diese auch wirklich gerade am Gerät tätig ist, ist eine große Herausforderung. Banken brauchen daher entsprechende Lösungen, die ihnen dabei helfen, die Liveness eindeutig nachzuweisen. Die gängigste Form der

Echtheitsprüfung ist das Stellen bestimmter Aufgaben, die ein User durchführen muss – zum Beispiel drei Finger heben oder den Kopf in eine bestimmte Richtung drehen. Auch die passive und aktive Gesichtserkennung oder die Eingabe einmaliger Passcodes sind gängige Verfahren.

Die Biometrie gilt zu Recht als absolutes State-of-the-Art-Verfahren für die sichere Identifikation von Nutzern. Tatsächlich wird sie von den Aufsichtsbehörden zunehmend als sichere Methode für die Remote-Kontoeröffnung befürwortet. Die Monetary Authority of Singapore (MAS) erlaubt Finanzinstituten etwa die Verwendung biometrischer Authentifizierung bei der Due-Diligence-Prüfung von Kunden ohne persönliche Vorsprache. Die Europäische Bankenaufsichtsbehörde (EBA) hat ebenfalls detaillierte Leitlinien zur Förderung biometrischer Lösungen für das Remote-Onboarding in der EU herausgegeben. Und auch die Zentralbank der Vereinigten Arabischen Emirate fördert den Einsatz biometrischer Technologien im Rahmen ihres Rahmenwerks für Grundlagentechnologien zur Stärkung der digitalen Identitätsprüfung.

Doch auch im Hinblick auf die User Experience sind biometrische Lösungen für die Identitätsprüfung ein Schritt in die richtige Richtung. Die Verfahren sind nicht nur sicher und schnell, sondern rationalisieren auch den Zugang zu den Bankdienstleistungen enorm und steigern somit den Komfort. Dennoch sind Anbieter dieser Lösungen angehalten, die Benutzerfreundlichkeit weiter zu steigern, indem sie eine höhere Genauigkeit und Präzision bieten: Nur so können sie dem Anspruch gerecht werden, validen Kunden Transaktionen möglichst reibungslos zu ermöglichen, Betrüger aber gleichzeitig in Echtzeit zu erkennen und zu blockieren.

Anbieter biometrischer Lösungen müssen darüber hinaus die strengen Compliance-Vorschriften des Bankensektors in ihren Anwendungen abbilden, ohne den Komfort für die Endnutzer zu verringern. Um diese Anforderungen unter einen Hut zu bringen, müssen biometrische Lösungen Audit-Logging- und Reporting-Funktionen bieten, die es dem Sicherheitsteam einer Bank leicht machen, ihrer Pflicht im Hinblick auf Compliance-Berichte nachzukommen. Die Anbieter von Lösungen für biometrische Sicherheitsverfahren müssen zudem sicherstellen, dass diese Funktionen je nach geografischem Standort oder Art der Dienstleistung den neuesten Vorschriften entsprechen.

Darüber hinaus bringt die zunehmende Verwendung persönlicher Daten, insbesondere biometrischer Daten, eine Vielzahl neuer Anforderungen an den Datenschutz und

die Datenverwaltung mit sich, mit denen sich einige Banken nicht auseinandersetzen können oder wollen. Dies hat zu einer Zunahme der Verwendung biometrischer Authentifizierungslösungen geführt, die es den Nutzern ermöglichen, ihre biometrischen Daten auf ihren eigenen Geräten zu verwalten und zu speichern. Dort können sie zudem kontrollieren, an wen ihre Banken diese Daten weitergeben und von wem sie abgerufen werden. Auf diese Weise können Banken biometrische Authentifizierung anbieten und gleichzeitig die Nutzer unterstützen, die Hoheit über ihre persönlichen Daten zu behalten.

Auf diese essenziellen Funktionen sollten Banken achten

Kreditinstitute, die aktuell neue Lösungen für die biometrische Authentifizierung evaluieren, sollten auf bestimmte Merkmale und Funktionen achten. Eine gute Lösung bietet nicht nur ein einziges Verfahren an, sondern lässt den Benutzern die Wahl, welchen biometrischen Faktor (also etwa Fingerabdruck- oder Gesichtsscan) sie verwenden möchten. Sie sollte es zudem unterstützen, mehrere biometrische Merkmale für eine einzelne Überprüfung der Identität vorzulegen, anstatt einen mehrstufigen Prozess zu initiieren. Umso besser, wenn diese Verfahren nicht nur mit neuen, sondern auch mit bereits vorhandenen Geräten in Bankfilialen in Verbindung mit mobilen Authentifikationssystemen durchgeführt werden können. Ein weiteres Merkmal guter Lösungen ist die Verwendung fortschrittlicher KI-Technologie, die die Genauigkeit von Biometrie-Scans steigern und in Echtzeit überprüfen können, ob diese von einer echten Person durchgeführt werden. Auf diese Weise steigert Künstliche Intelligenz die Anti-Spoofing-Fähigkeiten der Authentifizierungsplattform.

Neben diesen Sicherheitsaspekten ist auch wichtig, dass die User ihre bereits vorhandenen Edge-Geräte für die Überprüfung nutzen können. Wenn Anbieter die bereits vorhandenen Edge-Scan-Funktionen mit der Kamera oder dem integrierten Fingerabdruckscanner eines Smartphones nutzen, können sie sich auf die offene Integration mit diesen Geräten konzentrieren. Das ermöglicht hochpräzise Scans und eine Datenextraktion nahezu in Echtzeit. Zu guter Letzt sollten Banken die gewünschte Lösung daraufhin prüfen, ob sie implizierten Bias beim Identifikationsprozess reduziert und für alle Benutzergruppen gleichermaßen sicher und präzise funktioniert.

Die Finanzbranche ist seit vielen Jahren Vorreiter, wenn es darum geht, digitale Sicherheitsverfahren zu verbessern und

damit Kundinnen und Kunden besser vor Betrug oder Verlust zu schützen. Angesichts der rasanten technologischen Entwicklungen im Bereich der Biometrie sowie deren immer bequemere Nutzbarkeit sind treibende Faktoren für den Aufschwung entsprechender Systeme im Bankensektor. Gute Lösungen für biometrische Sicherheitsverfahren helfen Banken, die Herausforderungen der Nutzerauthentifizierung im digitalen Zeitalter zu meistern und Kunden ein nahtloses Erlebnis zu bieten – ohne den Schutz der höchstpersönlichen Daten zu vernachlässigen.

Über den Autor: Edwardcher Monreal ist Lösungsarchitekt und Experte für digitale Sicherheit mit einer instinktiven Leidenschaft für pragmatische Problemlösungen. Er verfügt über mehr als zwei Jahrzehnte Erfahrung in der Entwicklung von Software und der Bereitstellung von Lösungen und Dienstleistungen für das Militär, die Telekommunikation, Banken, Unternehmen und die Regierung mit Synergien in den Bereichen NFC, TSM und mobile Finanzdienstleistungen in Verbindung mit PKI, Risikomanagement und starker Authentifizierung.

Versicherungs- und Finanznachrichten

expertenReport



<https://www.experten.de/id/4946853/Biometrie-20-Worauf-Banken-achten-muessen/>