

Fingerabdruck? Sprachbiometrie? Gesichtsbiometrie?

Was haben Finger, Gesicht und Stimme gemeinsam?

Sie alle sind biometrische Merkmale, die bei jedem einzigartig sind und anhand derer die Identität verifiziert werden kann.

Die Praxis und mehrere Datenschutzverletzungen haben gezeigt, dass Passwörter, ID-Nummern oder PINs nicht sicher sind und als eigenständiger Authentifizierungsfaktor nicht ausreichen. Egal wie komplex unsere Passwörter auch sind – es besteht nach wie vor Bedarf an zusätzlichen Sicherheitsebenen. Genau das macht die Biometrie so beliebt. Vom Zugriff auf unsere mobilen Geräte, über das Öffnen unserer Bürotür, den Zugriff auf unser Bankkonto bis hin zum Gespräch mit einem Contact-Center-Mitarbeiter – es gibt immer mehr alltägliche Anwendungsmöglichkeiten für die Biometrie als Authentifizierungsmittel. Die biometriebasierte Authentifizierung ist sicherer als jede andere Methode und verknüpft eine Identität mit einer bestimmten Person anstatt mit einem Passwort oder Code, die von jedermann verwendet werden können.

Biometrie soll es also sein. Aber welche Art von Biometrie?

Obwohl jedem klar ist, dass es jetzt an der Zeit ist, auf Biometrie umzusteigen, herrscht bei Unternehmen große Unsicherheit darüber, für welche Biometrietechnologie sie sich entscheiden sollen. Wie bei vielem gibt es auch hier nicht die eine richtige Antwort. Um Licht ins Dunkel zu bringen, habe ich die wichtigsten Informationen über gängige biometrische Technologien in einer einfachen Tabelle zusammengefasst.*

 Eigenschaften	 Stimme	 Fingerabdruck	 Gesicht
Benutzerfreundlichkeit	Hoch	Hoch	Mittel
Fehlerursachen	Hintergrundgeräusche	Trockenheit, Schmutz, Alter	Beleuchtung, Alter, Brille, Haare
Genauigkeit	Hoch	Hoch	Hoch
Falschrückweisungsrate (FRR)	Niedrig	Hoch	Hoch
Körperlich aufdringlich	Niedrig	Mittel	Hoch
Benutzerakzeptanz	Hoch	Hoch	Mittel
Langfristige Stabilität	Hoch	Hoch	Mittel
Geräteabhängigkeit	Niedrig	Hoch	Mittel
Benutzerfreundlichkeit Lebendigkeitserkennung	Hoch	Hoch	Mittel
Registrierungsaufwand	Keiner (passiv) – Mittel (aktiv)	Niedrig – Mittel	Niedrig
Nutzererlebnis	Passiv oder aktiv	Aktiv	Aktiv
Anwendbare Kanäle (im Contact Center)	Unmittelbar: Anruf, IVR, mobile App Potenziell: Web	Unmittelbar: Mobile App Potenziell: Web, IVR	Unmittelbar: Mobile App Potenziell: Web, IVR

*Die Tabelle basiert auf Informationen, die Sie [hier](#) finden.

Jede der Technologien hat ihre Vor- und Nachteile. Die Fingerabdruck-Technologie ist beispielsweise sehr benutzerfreundlich, erfordert aber ein bestimmtes Gerät, auf das nicht alle Verbraucher Zugriff haben. Die passive Sprachbiometrie erfordert keine Hardware und keinen Aufwand seitens des Anwenders, aber es ist sinnvoll, sie nur in bestimmten Kanälen einzusetzen. Die Gesichtsbiometrie eignet sich zwar sehr gut für Millenials, aber weniger für ältere Menschen, die sich unwohler fühlen, wenn sie ein Selfie machen.

Lebendigkeitserkennung und Customer Experience (CX) als Priorität

Sie fragen sich nun wahrscheinlich: „Es gibt so viele verschiedene Parameter, welche sind für mein Unternehmen am wichtigsten?“ In Anbetracht aktueller Branchentrends (siehe Beispiel [hier](#)) und konkreter Risiken wie Spoofing und gefälschte Fingerabdrücke auf Grundlage von Social-Media-Bildern (ja, [das kann tatsächlich passieren!](#)) empfehle ich, in eine Technologie zu investieren, die die Lebendigkeitserkennung beinhaltet. Je mehr eine Technologie auf der Lebendigkeitserkennung basiert, desto besser. Auf der anderen Seite müssen die Interaktionen Kundenerfahrungsorientiert, intuitiv und benutzerfreundlich sein, da heute die Kundenerfahrung an erster Stelle steht. In diesem Fall ist die beste Lösung diejenige, bei der der Kunde so wenig Aufwand wie möglich hat und die dennoch eine verbesserte Kundenerfahrung bietet, unabhängig von dem verwendeten Gerät und ohne zeitaufwendige Registrierung.

Registrierungsaufwand – der Schlüssel zu mehr Nutzerakzeptanz

Die Registrierung sollte ein Schlüsselparameter sein, wenn man sich für eine biometrische Technologie zur Kundenauthentifizierung entscheidet. Wenn es darum geht, die Identität von Kunden mithilfe von Biometrie zu verifizieren, kann die Registrierung entscheidend dabei sein, eine erfolgreiche Implementierung bei Millionen von Nutzern sicherzustellen. Die Registrierungsrate ist der wichtigste prädiktive Indikator. Dieser lässt darauf schließen, wie viele Kunden bei ihrer nächsten Interaktion mit dem Unternehmen eine biometriebasierte Authentifizierung nutzen werden. Eine hohe Registrierungsrate (z. B. 70 % der Kunden) bedeutet, dass die meisten Kunden sie nutzen würden. Eine niedrige Registrierungsrate bedeutet dagegen, dass die meisten Kunden sie nicht nutzen werden und die Investition in die neue Technologie umsonst war. Das bringt es auf den Punkt: Sie müssen eine Technologie wählen, die sowohl eine einfache Nutzung als auch eine einfache Registrierung gewährleistet.

Insbesondere im Bereich der Sprachbiometrie ist NICE der einzige Anbieter, der die passive Registrierung auf alle Kanäle anwendet, was bedeutet, dass Kunden nichts weiter tun müssen, um sich für die neue biometrische Technologie zu registrieren. Sie erfolgt nahtlos, erfordert keinen Aufwand seitens des Verbrauchers und verschafft Unternehmen die höchstmögliche Registrierungsrate.

Sprachbiometrie als ultimative Lösung

Jede der hier besprochenen biometrischen Technologien hat ihre Stärken und Schwächen. Es kommt also darauf an, welche Parameter für Ihre spezifischen Ziele und Anforderungen am wichtigsten sind. Ein aktueller [Bericht von Opus Research](#), der die Bedrohungen, Schwachstellen und Angriffsvektoren im Zusammenhang mit der Sprachbiometrie behandelt, besagt: „Die Biometrie ist im Allgemeinen nie zu 100 Prozent sicher, da es sowohl False Rejects (Ablehnung der Authentifizierung eines echten Benutzers) als auch False Accepts (Akzeptanz der Authentifizierung eines betrügerischen Benutzers) gibt. Die Sprachbiometrie ist jedoch sicherer und benutzerfreundlicher als ihre Alternativen. Und wenn sie als Teil einer ganzheitlichen multimodalen, Opti-Channel-Strategie und nicht als Einzellösung implementiert wird, bietet das Gesamtergebnis nachweislich ein Höchstmaß an Sicherheit mit einem verbesserten Kundenerlebnis.“

Autor: Rotem Shemesh, Product Marketing Manager, Real-Time Authentication, NICE.

Über NICE

NICE (Nasdaq: NICE) ist der weltweit führende Anbieter von cloudbasierten und lokal installierten Unternehmenssoftwarelösungen. Mit diesen Lösungen können Unternehmen auf Grundlage von Analysen strukturierter und unstrukturierter Daten fundierte Entscheidungen treffen. Mit den Lösungen von NICE können Unternehmen jeder Größenordnung einen besseren Kundenservice bieten, Compliance sicherstellen, Betrug verhindern und Bürger schützen. NICE-Lösungen werden von mehr als 25.000 Unternehmen in über [150 Ländern](#) verwendet, darunter mehr als 85 Fortune-100-Unternehmen. www.nice.com