5 Gründe, warum Ihre Stimme sicherer ist als jedes Passwort

Um einen Nutzer oder Kunden zu authentifizieren, setzen Unternehmen traditionell auf Passwörter, PINs und Sicherheitsfragen – und zahlen immer häufiger einen hohen Preis. Denn solche Barrieren knacken Hacker heute im Handumdrehen mit simplen Tools und greifen dann ungehindert auf sensible Daten zu. Stimmbiometrie bietet hier eine erstaunlich sichere Alternative. Sie ermöglicht eine zuverlässige Sprecherauthentifizierung in Sekundenschnelle und ist für den Anwender ausgesprochen bequem. Denn die zeitraubende Eingabe komplexer Zeichenfolgen oder die Beantwortung ausführlicher Sicherheitsfragen entfällt – ohne Abstriche in puncto Sicherheit.

Nuance liefert 5 Gründe, warum Stimmbiometrie die sicherere Variante ist, um Nutzer eindeutig zu identifizieren und Hackerangriffe effektiv abzuwehren.

1. **So eindeutig wie ein Fingerabdruck.**

Ein Stimmabdruck enthält mehr als 100 einzigartige Merkmale einer Person. Diese werden einerseits durch physische Faktoren wie die Länge des Stimmtraktes oder der Nasenpassage bestimmt. Andererseits erhält er seine Charakteristik durch Verhaltensmerkmale wie Tonhöhe, Rhythmus oder den Akzent des Sprechers. Die Authentifizierung ist damit einfach und sicher: Über bestimmte Eigenschaften identifiziert das System die Stimme innerhalb von Sekunden – und unter Umständen sogar unabhängig vom Inhalt des Gesagten. Auch eineiige Zwillinge oder der Sohn, der für den Zuhörer identisch wie sein Vater klingt, haben jeweils ihre eigene Stimmidentität. Diese erkennt ein biometrisches System zuverlässig.

2. **Für Cyberkriminelle wertlos.**

Hat ein Hacker unsichere PINs und Passwörter geknackt, stehen ihm praktisch alle Türen offen. Ganz anders bei der Stimmbiometrie: Bringen Cyberkriminelle den individuellen Stimmabdruck und die Passphrase in ihre Gewalt, so haben diese dennoch keinen Wert für sie. Zum einen stellen die gespeicherten Daten nur ein mathematisches Modell der Sprechereigenschaften dar. Eine Rekonstruktion der ursprünglichen Stimme ist daraus nicht möglich. Zum anderen sind die physikalischen Charakteristika einer Stimme absolut unnachahmlich – auch wenn sich etwa der Sprachrhythmus, die Intonation oder der Akzent imitieren lassen. Selbst Stimmaufzeichnungen kann die Stimmbiometrie dank Technologien wie Playback Detection und Liveness Detection zu mehr als 99 Prozent von Live-Stimmen unterscheiden.

3. **Hilft proaktiv, Betrug zu bekämpfen.**

Versucht ein Betrüger über ein Sprachdialogsystem, Call Center oder eine App mit der eigenen Stimme Zugang zu sensiblen Daten zu erlangen, hinterlässt er dabei seinen individuellen Stimmabdruck. Diesen können Unternehmen nutzen, um den Angreifer proaktiv aus ihren Systemen herauszuhalten. Gleichzeitig ist der Stimmabdruck ein sicheres Beweismittel, um den Betrugsversuch bei der Polizei anzuzeigen.

4. **Immer mit dabei und sogar bei Erkältungen einsatzbereit.**

Sicherheitslücken können zum Beispiel auch dann entstehen, wenn ein Anwender seine Zugangsdaten verloren hat und über eine ungesicherte Verbindung zurücksetzt. Oder wenn der Nutzer aus reiner Bequemlichkeit eine simple Zahlenkombination als Passwort gewählt hat, um es nicht zu vergessen.
Die Stimme als Schlüssel zum Kundenkonto führt dagegen jeder stets bei sich, und sie ist mit ihren individuellen Merkmalen kaum „zu knacken“. Auch Schwankungen in der Stimme – etwa bei einer Erkältung – führen in der Regel nicht zum Ausfall eines Stimmbiometrie-Systems. Denn bei über 100 geprüften Eigenschaften gibt es mit Sicherheit genügend „gesunde“ Prüfmerkmale. Damit erklärt sich, dass VocalPassword von Nuance auch einen erkälteten Nutzer in 94 Prozent der Fälle korrekt erkennt (unter normalen Bedingungen 97 Prozent).

5. **Im Rahmen der Multi-Faktor-Authentifizierung unschlagbar sicher.**

Stimmbiometrie kann als eine Methode zur Multi-Faktor-Authentifizierung verwendet werden. Die Stimme steht dabei für das, was man ist, und die Passphrase ist der Faktor für etwas, das man kennt. Diese Kombination gilt als die sicherste überhaupt. Zudem lässt sich Stimmbiometrie auch mit anderen Verfahren, wie der Verhaltensbiometrie, der Gesichtserkennung und dem Scan des Fingerabdrucks kombinieren. Und auch die Stimmbiometrie für sich genommen, ist im Vergleich zu herkömmlichen Verfahren wie PINs oder Passwörtern weniger anfällig für Betrugsversuche: Selbst wenn jemand die Passphrase kennt, kann er die Stimme des Sprechers nicht vollständig imitieren. Und auch wenn er Intonation, Rhythmus und Akzent perfekt nachzumachen vermag, finden sich noch immer genügend physikalische Merkmale, die jede Person individuell ausmachen.