Stimmbiometrie - maximale Sicherheit und maximale Flexibilität.

Optimieren Sie mit Stimmbiometrie sämtliche Prozesse und machen Ihre Kunden und Mitarbeiter glücklich.

NUANCE

TWINSOFT biometrics

Biometrie hat enorm an Bedeutung gewonnen. Zur Authentifizierung, aber auch zur Betrugsprävention hat sich der Einsatz biometrischer Technologien bewährt. In diesem Whitepaper erhalten Sie Einblicke in die Stimmbiometrie, die Vorteile und Einsatzmöglichkeiten. TWINSOFT *biometrics* und Nuance zeigen außerdem auf, wie Sie Biometrie in Ihrem Unternehmen integrieren können - sicher, schnell, kundenfreundlich und finanziell lohnenswert.

Was ist Sprachbiometrie?

BioShare

Biometrie ist die Wissenschaft zur Messung biometrischer Merkmale wie dem Fingerabdruck, Gesichts, der Stimme und vielem mehr. Ganz praktisch betrachtet, kann die Biometrie dazu benutzt werden, Personen zu identifizieren, beziehungsweise deren Identitäten zu verifizieren und ihnen somit Zugang/Zugriff oder eine Berechtigung zu gewähren, oder aber um schlichtweg ihre Anwesenheit zu erfassen.

Das bringt Sicherheits- und Bequemlichkeitsvorteile zugleich: Biometrische Merkmale sind einmalig und nur extrem schwer fälschbar. Dazu hat jeder Mensch die körpereigenen Merkmale immer bei sich – ein Szenario wie das Vergessen einer Schlüsselkarte oder ähnlichem ist somit hier nicht denkbar.

Die Stimme als Passwort
Für alle Merkmalsmessungen braucht es eine Person, die das jeweilige Merkmal scannen lässt, einen Sensor und im System hinterlegte Vergleichstemplates, mit denen das Scan-Ergebnis zur Identifikation/ Authentifizierung verglichen werden kann.

Die Stimme bietet die gleichen Sicherheitsvorteile wie die anderen biometrischen Merkmale und funktioniert darüber hinaus auch aus der Ferne – zum Beispiel über ein Telefongespräch.

Deshalb löst die Stimme die herkömmlichen Authentifizierungsmethoden PIN/Passwort ab, was viele namhafte Unternehmen, wie z.B. BITMARCK oder ITERGO, bereits täglich beweisen.

Über 100 verschiedene Sprachmerkmale
Über 100 verschiedene Sprachmerkmale können „gemessen“ werden, um die Identität der sprechenden Person zu verifizieren. Von der Aussprache bis hin zur Größe und Form des Nasengangs. Und weil Sprache nicht nur über den reinen „Ausstoß“ von Lauten funktioniert, sondern auch Inhalt transportiert, lässt sich die Stimme ideal – beispielsweise mit einem Passwort-Satz – kombinieren, um die Fälschungssicherheit noch einmal zu erhöhen.

Von Transaktionen bis hin zum Helpdesk
Es gibt diverse mögliche Anwendungsbeispiele für intelligent eingesetzte Biometrie-Lösungen. Von Finanztransaktionen über das Telefon/Internet über eine Passwort-Reset-Lösung bis hin zur kanalübergreifenden Authentifizierung im Homeoffice.

Ein Anwendungsbeispiel aus einer Passwort-Reset-Lösung: Erika Mustermann hat ihre Zugangsdaten zur Anwendung XY vergessen und muss sich nun ein neues Passwort bei der Kunden-Hotline besorgen. Etwa 4 Prozent der Mitarbeiter eines Unternehmens vergessen einmal im Monat ihr Passwort und müssen dieses zurücksetzen lassen.

Erika Mustermann könnte sich am Telefon also nun mit dem Satz „Bei Nuance und TWINSOFT ist meine Stimme mein Passwort“ authentifizieren. Stimm- und Sprachmerkmale sowie der korrekte Satz führen dann zu einer erfolgreichen Authentifizierung.

Hierbei spielen die Technologien von Nuance und TWINSOFT *biometrics* eine gewichtige Rolle:

Nuance Gatekeeper, eine Cloud-native, hochmoderne und entscheidungsfähige KI-gestützte Biometrielösung

BioShare von TWINSOFT *biometrics*, eine intelligente Biometrie-Management-Suite zur Verwaltung und Integration biometrischer Prozesse.

Etwa 4 Prozent der Mitarbeiter eines Unternehmens vergessen einmal im Monat ihr Passwort.

Vorteile von Stimmbiometrie

Stimme und Passphrase sorgt für maximale Sicherheit
Kein Verfahren ist absolut fälschungssicher. Und doch gibt es Möglichkeiten, den Aufwand für Betrüger so hoch zu schrauben, dass ein Angriff sich nicht mehr lohnt, beziehungsweise mit sehr hoher Wahrscheinlichkeit nicht gelingt. Dies gelingt zum Beispiel mit der Kombination verschiedener Authentifizierungsmethoden, wie z.B. wissensbasierter oder inhärenter Merkmale. Diese sogenannte „Zwei-Faktor-Authentifizierung“ wird auch in der neuesten Datenschutzgrundverordnung (DSGVO) empfohlen und laut der Zahlungsdiensterichtlinie PSD2 für Transaktionen durch Zahlungsdienstleister elementar wichtig.

Ein Betrüger kann sich den Namen des Haustiers oder den Geburtstag Ihrer Kunden beispielsweise in sozialen Netzwerken besorgt haben. Und vielleicht könnte der Betrüger im Gespräch sogar glaubhaft die Identität Ihres Kunden vortäuschen. Was er nicht kann: Wie Ihr Kunde sprechen und sich wie Ihr Kunde verhalten. Er müsste dafür mehr als 100 physikalische und verhaltensbedingte Merkmale, von denen viele nicht bewusst steuerbar sind, perfekt imitieren können. Daher gehört die Kombination Stimme mit einer wissensbasierten Frage zu den derzeit sichersten Authentifizierungsmethoden.

Kein Betrug „aus der Konserve“ möglich
Das System speichert keine Sprach-Aufnahme der Stimme. Stattdessen wird ein individuelles und mit einem Algorithmus verschlüsseltes Ergebnis verteilt gespeichert. Selbst wenn es einem Angreifer also irgendwie gelingen würde, an die gespeicherte Sprachdatei zu kommen, ließe sich diese nicht wieder „rekonstruieren“ und in eine Stimme verwandeln. Die Software kann durch das Monitoring der Tonfrequenz erkennen, ob gerade nur eine „Konserve“ abgespielt oder live gesprochen wird. Das System filtert sie heraus.

Compliance-Richtlinien und verschlüsselte Daten
Die Entscheidungshoheit über das „Ob“ und „Wie“ des konkreten Einsatzes unserer Lösungen **BioShare** und Gatekeeper trägt das Unternehmen. Für die Datenverarbeitung mittels unserer Produkte ist also der Kunde verantwortlich im datenschutzrechtlichen Sinne.

Unsere Anwendungen sind für verschiedenste Einsatzzwecke geeignet und lassen sich je nach Anforderung sehr individuell an die Bedürfnisse des jeweiligen Unternehmens anpassen.

Auch wenn personenbezogene Daten für die Interaktion mit ihren Kunden genutzt werden, sind diese niemals mit der Stimmbiometrie verknüpft – der Stimmabdruck ist separiert und somit sicher. Datentransfers von Unternehmen zu Unternehmen oder von Plattform zu Plattform sind im Nachhinein unmöglich – solche Anforderungen müssen vorher ausdrücklich eingeplant werden.

ROI in wenigen Monaten
Das Einsparungspotenzial durch den Einsatz einer Stimmbiometrie-Lösung ist insgesamt hoch. Wie hoch genau und wann der ROI erreicht werden kann, hängt letztendlich von Umfang und Einsatzfeld der Lösung ab.

90 Prozent der Betrugskosten reduziert
Eine Studie von Javelin Strategy & Research aus dem Jahr 2020 ergab, dass sich 2019 der Schaden durch Betrug auf 16,9 Mrd. US-Dollar belief. Die Kontoübernahmen (Account Takeovers, ATOs) haben sich im vergangenen Jahr verdreifacht, was zu Verlusten in Höhe von 6,8 Mrd. US-Dollar führte.[1]

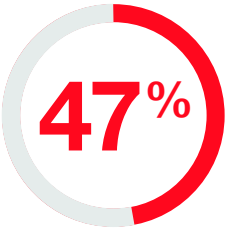
der Betrugskosten reduziert

Der Verlust eines Kontos beträgt dabei im Durchschnitt über 40.000 US-Dollar. Stimmbiometrie kann dazu beitragen, Betrugskosten per Telefon im Kundenservice um 90% zu reduzieren – eine Situation, in der sich das Investment also voraussichtlich schnell amortisiert hätte. Die meisten Unternehmen erreichen den ROI in weniger als sechs Monaten.

Einsparung durch Passwort-Reset um 70 Prozent
Ein anderes Beispiel aus der Praxis: Ein Passwort-Reset kostet ein Unternehmen zwischen 20 und 30 Euro – so Hochrechnungen. Darüber hinaus werden aber durch vergessene Passwörter ganze Workflows blockiert, die im schlimmsten Fall zu einem Auftragsverlust führen können, dessen Kosten auch in die Millionen gehen können. Durch den Einsatz von Stimmbiometrie lassen sich die Kosten auf 4 bis 8 Euro pro Reset senken und Workflows optimieren – je nach Umfang kann sich der Einsatz also ebenfalls bereits in wenigen Monaten finanziell rechnen.

geringere Kosten
für Passwort-Reset

Extrem schnelle Bearbeitungszeit
Der Schnelligkeitsvorteil, den Stimmbiometrie mit sich bringt, lässt sich an einem weiteren Beispiel untermauern: So kann beispielsweise ein Anrufer direkt zu Beginn des Telefonats anhand nur weniger Worte identifiziert und direkt dem richtigen Agenten für sein Anliegen zugeordnet und mit diesem verbunden werden. Ein Finanzinstitut konnte bereits 47 Prozent aller Anrufe nach nur einem Monat entsprechend weiterleiten. Ein enormer Service-Vorteil und eine enorme Zeitersparnis.



aller Anrufer wurden bereits
nach einem Monat direkt an einen
Agenten weitergeleitet

In nahezu jede Umgebung integrierbar
Unsere Stimmbiometrie-Lösung lässt sich über modernste Schnittstellentechnologie in Ihr bestehendes System integrieren und bietet Ihnen alle Vorteile ohne eine aufwändige Umstellung Ihres Systems. Dabei ist es ebenfalls möglich, bereits bestehende Anwendungen mit einer Authentifizierung über die Stimme zu koppeln – Biometrie also in Ihre Workflows zu integrieren oder gleich ganz neue Workflows zu erschaffen.

1. Krista Tedder, John Buzzard. 2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis. Abgerufen von: https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity#

Hohe User-Akzeptanz dank Schnelligkeit und geringer Fehlerquote
Der Forrester Report „TechRadar™: Biometric Authentication“[2] stellte schon 2017 fest: Nutzer erwarten überall eine reibungslose Authentifizierung. Verzögerungen oder technische Schwierigkeiten führen schnell zu Ärgernissen und Misstrauen in den Ablauf. Deshalb haben insbesondere Biometrie-Lösungen sowohl für die Authentifizierung als auch für die Betrugsprävention große Aufmerksamkeit erlangt. Für eine hohe Kundenakzeptanz ist also nicht nur die Sicherheit, sondern eben auch die Anwenderfreundlichkeit entscheidend.

> Verbraucher sind froh, dass sie von ihrer Bank geschützt werden, gleichzeitig nervt es sie aber, dass ihnen dieser Schutz erschwert, ein Konto zu eröffnen oder einzukaufen. Im Zuge der digitalen Transformation wird ein reibungsloses Kundenerlebnis entscheidend sein. Erfolgreich werden diejenigen Unternehmen, die dies mit den Anforderungen zur Betrugsbekämpfung unter einen Hut bringen können.“
>
> TJ Horan, Vize-Präsident im Produktmanagement des Analytics-Software-Unternehmen FICO

Dadurch, dass komplizierte Passwörter, fehleranfällige Schlüsselkarten und/oder lange Authentifizierungsprozesse durch den Einsatz von Stimmbiometrie nicht mehr notwendig sind, werden auch anfangs skeptische Nutzer schnell überzeugt.

In jeder Hinsicht *„social distancing“-konform*
Dadurch dass Authentifizierung via Stimmbiometrie, ähnlich wie Gesichts- oder Iriserkennung, keinen Körperkontakt mit dem Sensor erfordert und zudem auch ohne persönlichen Kontakt mit anderen Personen abläuft, erfüllt sie als Authentifizierungsmethode auch höchste Hygiene-Standards. In Zeiten von Covid-19 ein weiteres Argument, das zu einer deutlich höheren User-Akzeptanz führt.

Ausführliches Monitoring
Das Monitoring unserer Lösungen erfolgt über übersichtliche und in Echtzeit aktualisierende Dashboards – so lassen sich in Sekundenschnelle potenzielle Fehlerquellen wie möglicherweise defekte Sensoren o.ä. identifizieren. Gleichzeitig lassen sich durch das ausführliche Monitoring auch inhaltliche Rückschlüsse auf mögliche Gefahrenquellen ziehen: „In Woche X ist die Anzahl an fehlgeschlagenen Authentifizierungen besonders hoch – gab es hier vermehrt Betrugsversuche? Was könnten mögliche Ursachen sein?“ Gleichzeitig kann das Monitoring sogar für über die Authentifizierung hinaus inhaltlich relevante Erkenntnisse sorgen: „An Tag Y riefen besonders viele Kunden bei der Beschwerdehotline an – hier sollten wir auf Ursachenforschung gehen.“

2 TechRadarTM: Biometric Authentication, Q1 2018. Adoption of User-And Mobile-Friendly Biometrics Will Kill The Password https://www.forrester.com/report/TechRadar+Biometric+Authentication+Q1+2017/-/E-RES121267#

Was muss ein Unternehmen tun, um (Sprach-)Biometrie einzuführen?

Die Implementierung eines biometrischen Systems amortisiert sich für Sie am schnellsten, wenn Sie das richtige Verfahren und die richtige Integration in das bestehende System wählen. Auch hier gilt: Die Lösung muss zum Problem passen. Dabei müssen auch die unterschiedlichen Stärken der einzelnen Biometrie-Verfahren betrachtet werden, ehe endgültig entschieden werden kann, welche(s) Verfahren passt/passen.

Ein Passwort-Reset über einen Handvenenscan ist beispielsweise für eine/n Mitarbeiter/in im Homeoffice ggf. sehr umständlich umzusetzen, während der Zugriff auf einen Werkzeugschrank in einer sehr lauten Fertigungshalle für den Einsatz von Stimmbiometrie nicht optimal geeignet ist.

Wichtige Fragen:

- **Wie geht Ihr Unternehmen aktuell mit Betrug und Betrugsprävention um?**
- **Wo sind die Vor- und Nachteile Ihrer aktuellen Lösung(en)?**
- **Wie sieht die Angriffssituation aus/in welchen Zyklen kommen welche Art von Angriffen?**
- **Welche Nachteile wiegen besonders schwer?**
- **Durch welche (Kombination von) biometrische(n) Lösung(en) lassen sich die Nachteile beheben?**
- **Welche Schnittstellen gibt es in Ihrem System für das „Andocken“ einer passenden Lösung?**
- **Welche Lösung passt zu den äußeren Umständen der tatsächlichen Anwendungspraxis?**
- **Welche anderen Abläufe müssen gegebenenfalls an die biometrische Lösung angebunden werden?**

Analysieren Sie die Risiken und Betrugsvorkommen, gerne auch mit unseren Experten, um die passende biometrische Lösung umzusetzen.

Unter Berücksichtigung des Sicherheitskonzeptes, werden die biometrischen Hard- und Softwarekomponenten in das IT-System und den Arbeitsablauf integriert. Dabei werden auch die Schnittstellen überprüft, bei denen eine Benutzerauthentifizierung benötigt wird, um die Anbindung an das Biometrie-System zu schaffen. Mit einer Pilotimplementierung werden die Erkenntnisse dann nochmal auf einen praktischen Prüfstand gestellt, ehe der Rollout erfolgt.

Auch nach der Installation ein kompetenter Ansprechpartner
Nachdem die biometrische Authentifizierung in Ihre Prozesse eingebunden ist, stehen wir Ihnen für die Pflege sowie Wartung der Installationen, aber auch für die Beratung zu aktuellen Entwicklungen und die Beantwortung von Fragen als Ansprechpartner zur Verfügung.

Über Nuance Communications, Inc.
Nuance Communications (NASDAQ: NUAN) ist Pionier und Marktführer im Bereich der dialogorientiertenKI für alle Arbeits- und Lebensbereiche. Das Unternehmen liefert Lösungen, die verstehen, analysieren und reagieren, mit dem Ziel die menschliche Intelligenz zu bereichern sowie Produktivität und Sicherheit zu erhöhen. Nuance besitzt jahrzehntelange Erfahrung in der Entwicklung und Anwendung von KI und bietet Lösungen u.a. für das Gesundheits- und Rechtswesen, die Finanz- und Versicherungsbranche, Telekommunikation und Versorgungswirtschaft. Tausende von Unternehmen arbeiten mit Nuance zusammen, um engere Beziehungen und bessere Erfahrungen für Kunden und Mitarbeiter zu schaffen. Weitere Informationen finden Sie unter www.nuance.de.

TWINSOFT *biometrics*
Die TWINSOFT *biometrics* ist ein Tochterunternehmen der TWINSOFT GmbH & Co. KG mit dem Spezialgebiet Biometrie. Hier gibt es das Komplettpaket: Von allgemeiner Biometrie-Beratung über spezifische und individuelle Workshops oder KnowHow-Transfers bis hin zur ureigenen intelligenten Biometrie-Management-Suite „**BioShare**“, die das „liebste Kind“ der TWINSOFT *biometrics* sein dürfte. **BioShare** integriert biometrische Lösungen in bestehende Infrastrukturen von Unternehmen. Durch den anwenderfreundlichen und herstellerunabhängigen Einsatz sämtlicher unterschiedlicher biometrischer Merkmale und der entsprechenden Sensoren - wie Fingerprint, Handvenenscan, Gesichts- oder Stimmerkennung - wird die Unternehmensinfrastruktur auf leistungsstarkem Wege aufgefrischt, modernisiert und abgesichert.

Gemeinsam haben TWINSOFT und Nuance mit Password Reset eine Lösung entwickelt, die schon bei vielen führenden Unternehmer in Deutschland eingesetzt wird. Lesen Sie hierzu mehr.