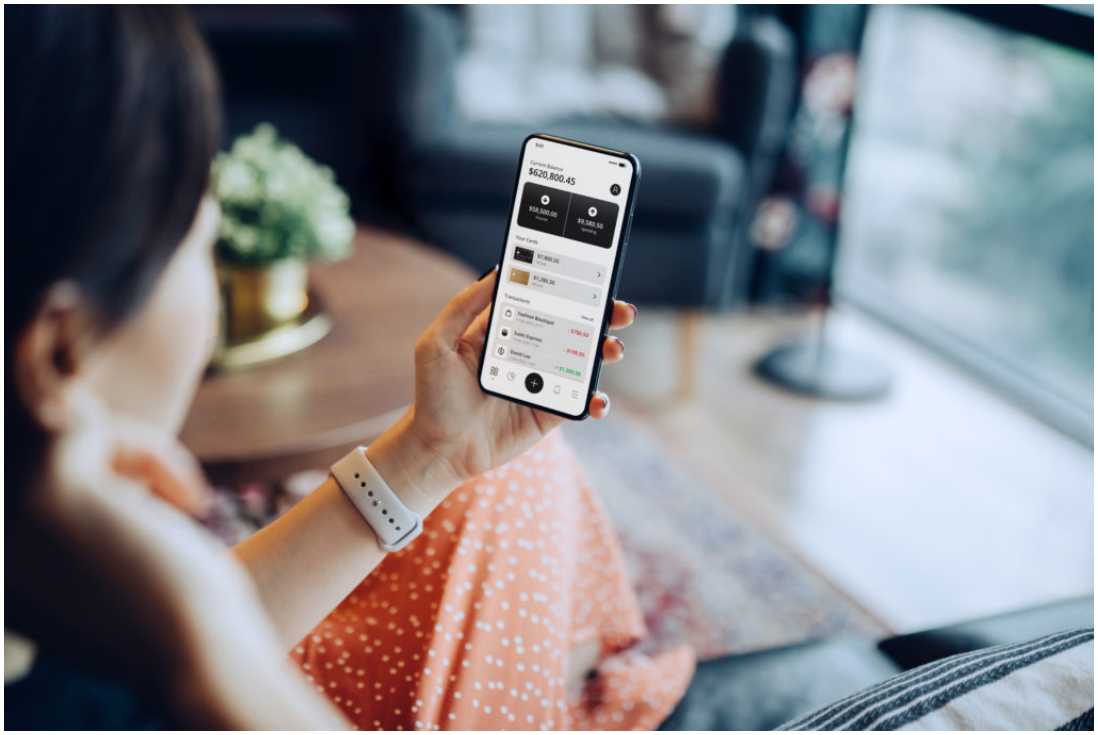
NUANCE | WHAT'S NEXT BLOG

Kundeninteraktion auf allen Kanälen, Verifizierung und Betrugsprävention

Es ist dringend an der Zeit, Authentifizierungsmethoden neu zu gestalten

Nuance Communications

18 November 2021



Unternehmen müssen mehr für ihren eigenen Schutz und den ihrer Kund*innen leisten – darauf macht die International Fraud Awareness Week jeden November aufmerksam. Obwohl sie ihnen noch immer vertrauen, bieten wissensbasierte Authentifizierungsmethoden nicht mehr genügend Schutz für Verbraucher*innen. Statt den Betrüger*innen das Feld zu überlassen, sollten Unternehmen neue Methoden zur biometrischen Authentifizierung einsetzen, denn damit schützen sie nicht nur ihre Kund*innen, sondern bieten ihnen zudem ein besseres Erlebnis.

Die Kosten von Betrug sollten den Expert*innen für IT-Security und Betrugsprävention während der International Fraud Awareness Week und darüber hinaus weiterhin Sorgen machen: Weltweit verlieren Verbraucher*innen jedes Jahr Milliarden und eine Studie von Nuance aus dem Frühjahr 2021 zeigt, dass in Deutschland knapp ein Fünftel der Befragten (17 Prozent) in den vorausgegangenen zwölf Monaten Opfer eines Betrugs geworden ist. Und das Problem wird immer schlimmer: Der Sicherheitsverantwortliche einer Privatkundenbank berichtet, dass die Anzahl der Betrugsversuche während der COVID-19-Pandemie um 400 Prozent gestiegen sei.

Einer der Gründe hierfür: viel zu viele Menschen und Unternehmen verlassen sich noch immer auf Authentifizierungsmethoden, die nicht mehr zeit- und zweckgemäß sind. Und die Veränderungen in den letzten zwanzig Monaten haben Kriminellen reichlich neue Möglichkeiten eröffnet, um dies auszunutzen.

Deshalb ist es für Unternehmen dringender denn je, sich von traditionellen Authentifizierungsmöglichkeiten, etwa PINs und Passwörtern, zu verabschieden und zu stärkeren, wie biometrischen, Merkmalen zu wechseln.

Es gibt kein wirklich starkes Passwort

Für Betrüger*innen ist es heute einfach im Dark Web an PINs, Passwörter oder persönlich identifizierbare Informationen (PII) zu gelangen. Dank schlechter Passworthygiene werden diese Daten für Kriminelle sogar noch wertvoller. In der Umfrage bestätigt – allen Warnungen und Aufklärungsversuchen zum Thema Cyber Security zum Trotz – ein Drittel der Befragten (32 Prozent) entweder nur ein einziges Passwort für alles zu verwenden oder zwischen Variationen von diesem zu wechseln. Zudem befolgen nur 18 Prozent die Anweisungen für die Erstellung eines besonders starken Passworts. Wenn traditionelle Authentifizierungsmethoden schon keine angemessene Sicherheit bieten, dann aber zumindest ein gutes Kund*innenerlebnis, oder?

Nein. Wissensbasierte Authentifizierungsmethoden stellen für entschlossene Betrüger*innen nicht nur kein Hindernis dar, weil sie über alle benötigten Informationen verfügen, sondern sind für tatsächliche Kund*innen auch oft mit Ärgernissen verbunden. Nicht selten vergessen oder verlieren sie die Informationen, die ihre Identität verifizieren sollen – wer erinnert sich tatsächlich noch an den Namen des Klassenlehrers aus der Grundschule oder die 16-stellige Kund*innennummer?

Daher überrascht es nicht, dass herkömmliche Authentifizierungsmethoden das Kund*innenerlebnis nachhaltig beeinträchtigen. Fast ein Drittel (30 Prozent) zeigt sich frustriert von der Groß- und Kleinschreibung von Passwörtern und der Notwendigkeit von Sonderzeichen, während ein Viertel (24 Prozent) Schwierigkeiten hat, sich Benutzernamen, PINs und Passwörter zu merken und sie deshalb regelmäßig zurücksetzen muss.

Die Zeit ist reif für die biometrische Authentifizierung

Um die inhärenten Schwachstellen traditioneller Authentifizierungsmethoden zu überwinden, implementieren immer mehr Unternehmen Lösungen für die biometrische Authentifizierung, wie Nuance Gatekeeper. Dabei wird die Identität von Personen auf Grundlage von Merkmalen verifiziert, die bei jedem Menschen einzigartig sind. Diese können nicht vergessen, gestohlen oder gefälscht werden und sind damit sicher und einfach zu verwenden.

Gerätebasierte biometrische Verfahren wie Systeme für die Identifikation von Fingerabdrücken oder dem Gesicht sind zwar bekannt und werden von vielen Verbraucher*innen bereits im Alltag genutzt, ihr Einsatz ist aber von Natur aus limitiert. Wer seinen Kontostand auf einem fremden Smartphone prüfen möchte, kann dies nur, wenn sein Fingerabdruck oder Gesicht auf dem Handy hinterlegt ist. Zudem schafft der gerätebasierte Ansatz auch neue Sicherheitslücken: Wer beispielsweise das Bankkonto eines älteren und hilflosen Verwandten leerräumen will, muss sich dafür einfach nur mit dessen Gesicht anmelden.

Unternehmen, die stattdessen einen serverbasierten Ansatz bei der biometrischen Authentifizierung verfolgen, können auf Faktoren wie Stimmbiometrie oder Verhaltensbiometrie setzen, um Kund*innen zu identifizieren – egal, von wo, wann und wie. Gleichzeitig können sie Betrüger*innen erkennen, unabhängig davon, hinter welchem Gerät oder welcher Identität sie sich verstecken.

Stimmbiometrie-Engines analysieren zum Beispiel Hunderte von Merkmalen der natürlichen Stimme einer Person und gleichen sie mit einer „Stimmprofil"-Bibliothek ab, in der die Stimmen von Kund*innen, aber auch Betrüger*innen hinterlegt sind. Die fortschrittlichsten Systeme können diese Analyse in weniger als einer Sekunde durchführen – während Kund*innen den Agent*innen am Telefon noch ihren Namen und ihr Anliegen mitteilen. Sobald die Mitarbeitenden sehen, dass die Authentifizierung erfolgreich war, können sie sich auf die Beratung und Hilfestellung konzentrieren, statt die Anrufenden mit Fragen zu löchern.

Lösungen für Verhaltensbiometrie analysieren dagegen die Art und Weise, wie Menschen tippen, über ihr Smartphone wischen, eine Maus bedienen und andere Faktoren ihres digitalen Verhaltens. Sie eignen sich ideal für die kontinuierliche Authentifizierung in digitalen Kanälen, da sie Sitzungen, die von Kriminellen übernommen wurden, schnell erkennen können.

Gesprächsbiometrie – der Neuling im Bereich Betrugsprävention – bietet eine weitere Möglichkeit, um festzustellen, ob eine Person tatsächlich diejenige ist, die sie vorgibt zu sein. Hierbei analysieren Lösungen die Art und Weise wie Menschen Sätze konstruieren, die gewählten Wörter und sogar die Emojis, die sie verwenden. Daher sind sie gut geeignet, um Betrüger*innen zu identifizieren, die Skripte verwenden.

Die biometrische Authentifizierung bietet allen Seiten Vorteile

Die gute Nachricht für alle Expert*innen aus dem Bereich der IT-Security und Betrugsprävention: Immerhin mehr als ein Drittel der Befragten (36 Prozent) fühlt sich heute eher bereit, biometrische Daten zur Authentifizierung zu verwenden als dies vor der Pandemie der Fall war. Zudem vertrauen 29 Prozent bei der Authentifizierung ihrer Identität einer Form der biometrischen Analyse. Verbraucher*innen schätzen, wie Biometrie Reibungen und Hindernisse bei der Interaktion mit Marken beseitigt, da sie sich nicht länger an Anmeldedaten erinnern oder Passwörter zurücksetzen müssen.

Der Telekommunikationsanbieter Teléfonica setzt sogar Stimmbiometrie ein, um sicherzustellen, dass seine schwächsten Kund*innen bei Konnektivitätsproblemen bevorzugt behandelt werden und sie den Service erhalten, den sie benötigten. Das System ermittelt das Alter einer oder eines Anrufenden anhand des Klangs der Stimme und leitet Anrufe von Senior*innen direkt an Live-Agent*innen weiter, die dann unmittelbar weiterhelfen.

Eine sichere Zukunft

Unternehmen können mithilfe einer Kombination aus biometrischen und anderen Authentifizierungsmethoden in einem mehrschichtigen Sicherheitsansatz, der durch den Einsatz von KI unterstützt wird, das Risiko einer bestimmten Interaktion in Echtzeit bewerten. Das Ergebnis ist eine drastische Reduzierung der durchschnittlichen Bearbeitungszeit, der Kosten für das Contact Center sowie der Verluste im Zusammenhang mit Betrug.

Es ist zu hoffen, dass biometrische Authentifizierungsmethoden bis zur nächsten Fraud Awareness Week noch stärker im Alltag vertreten sind als bislang. Und wenn immer mehr Unternehmen KI-gestützte, mehrschichtige Präventionsansätze zum Schutz ihrer Kund*innen verfolgen, wird die Fraud Awareness Week eines Tages vielleicht nicht mehr nötig sein.

Tags: Betrugsprävention, Biometrische Authentifizierung, International Fraud Awareness Week

More Information

Sie möchten mehr über Nuance-Lösungen zur Authentifizierung und Betrugsprävention lernen?

Erfahren Sie hier, wie Nuance biometrische Authentifizierung und KI gestützte Betrugsprävention durch eine einzige Gatekeeper Lösung kombiniert.

Learn more