NUANCE | WHAT'S NEXT BLOG

Kundeninteraktion auf allen Kanälen, Verifizierung und Betrugsprävention

Unsichtbar für Sicherheitsbeauftragte und unüberwindbar für Betrüger

Nuance Communications

31 Januar 2020

Wie lässt sich ein Gleichgewicht zwischen reibungsloser Authentifizierung und wirksamer Betrugsprävention herstellen? Lassen Sie uns gemeinsam die unsichtbare Welt der KI-basierten Sicherheitsmethoden auf dem Nuance CXS 2020 erkunden.

Vergessen Sie für einen Moment (wenn Sie können) die Aufgabe, einen erstaunlichen Kundenservice zu bieten und gleichzeitig die Kosten für den Service zu reduzieren. Fakt ist, dass herausragende, kostenoptimierte Erlebnisse für die Kundenbindung nicht auf Kosten der Sicherheit gehen dürfen.

Aus diesem Grunde haben wir das Thema **Sicherheit** zu einem Schlüsselthema unseres diesjährigen Nuance Customer eXperience Summit am 10. März in London gemacht. Mit führenden Vertretern verantwortlich für herausragende Kundenengagements diskutieren wir Trends, Gefahren und Lösungen.

Warum ist omni-channel Sicherheit gerade jetzt ein so heißes Thema im Kundenkontakt?

Da Unternehmen ihren Kunden immer mehr Kontaktkanäle anbieten, haben sich auch Betrüger immer weiterentwickelt, um zwischen diesen Kanälen hin und her zu springen und ihre Straftaten zu begehen. Oftmals beeinflussen Betrüger Contact-Center-Agenten über sog. Social Engineering (Hervorrufen bestimmter Verhaltensweisen, um an vertrauliche Informationen zu kommen), bevor sie die gesammelten Informationen dazu verwenden, Betrug auf anderen, weniger geschützten Kanälen zu begehen.

Dazu sagt Forrester in einer Studie:

"82% der Unternehmen stimmen zu, dass die Authentifizierung über die verschiedenen Kanäle hinweg immer wichtiger für die Betrugsprävention wird. Doch nur 59% definieren ihre kanalübergreifende

Betrugsprävention als nahezu oder vollständig optimiert."

Laut Forrester besteht die größte Herausforderung für die kanalübergreifende Betrugsprävention darin, die traditionellen, wissensbasierten Authentifizierungsmethoden (KBA = knowledge based authentication), die derzeit hauptsächlich von Unternehmen eingesetzt werden, abzulösen. PINs, Passwörter und PII sind alle im Dark Web verfügbar, weshalb sie ungeeignet sind für die Kundenauthentifizierung. Außerdem werden sie von legalen Kunden leicht vergessen, was zu Reibungsverlusten bei der Kundenbindung führt und die Zahl der Fehlalarme, mit denen sich die Betrugspräventionsteams befassen müssen, erhöht.

Welche technischen Lösungen gibt es, die Ihren Ansatz zur Kundenauthentifizierung und Betrugsprävention revolutionieren können?

Biometrie kann eine Antwort sein
Viele Unternehmen setzen bereits auf biometrische Verfahren, um ihre kanalübergreifende Sicherheitsstrategie zu unterstützen. Die Verwendung mehrerer biometrischer Methoden im Contact Center und über digitale Kanäle hinweg kann eine effektive Möglichkeit sein, Kunden schnell und sicher zu authentifizieren und das Betrugsrisiko zu minimieren. Weniger Aufwand, weniger Betrug, das ist ein Thema über alle Industrien hinweg, doch insbesondere kann das für die Finanzinstitute einen entscheidenden Vorteil bringen.

Zum Beispiel können mithilfe von **Stimmbiometrie** Kunden authentifiziert und Betrüger identifiziert werden, indem Hunderte von Variablen in den Stimmen von Personen schnell analysiert werden. Unsere Nuance Lightning Engine basiert auf Algorithmen, die Anrufer in der IVR- oder im Contact Center mit weniger als zwei Sekunden Tonaufnahme und mit einer 25-40% höheren Genauigkeit authentifizieren können.

In digitalen Kanälen analysiert die **Verhaltensbiometrie** die Art und Weise, wie Personen mit Websites und Anwendungen auf ihrer Tastatur, Maus oder ihrem Smartphone (neben vielen anderen Verhaltensmerkmalen) interagieren, um eine Aufgabe zu erfüllen – Muster, die für Betrüger unglaublich schwer zu reproduzieren sind.

Doch die biometrischen Innovationen gehen sogar noch weiter. So haben wir hier bei Nuance eine völlig neue Art der Biometrie erfunden. Die Gesprächsbiometrie in unserer **ConversationPrint**-Lösung geht noch einen Schritt weiter und analysiert den Wortschatz, die Grammatik, die Satzstruktur und vieles mehr, um ein einzigartiges Profil des Sprachgebrauchs während Interaktionen zu erstellen.

Lesen Sie alles über diese spannende Insider-Geschichte seines Erfinders in unserer aktuellen digitalen Ausgabe Nuance IQ.

Das Potenzial für Unternehmen eine Kombination dieser biometrischen Technologien einzusetzen ist enorm, um somit die Sicherheit über alle Kanäle zu erhöhen und gleichzeitig den Aufwand für die Kunden zu reduzieren.

Diskutieren Sie mit uns die Zukunft der sicheren, omni-channel Authentifizierung auf dem Nuance CXS 2020 in London.

Tags: Stimmbiometrie, Biometrische Authentifizierung, Customer eXperience Summit