

Kundeninteraktion auf allen Kanälen, Verifizierung und Betrugsprävention

# Sind Sie bereit für den Paradigmenwechsel in Authentifizierung und Betrugsprävention?

[Nuance Communications](#)

5 September 2019

FORRESTER

## Orientierung in der kanalübergreifenden Betrugs- und Authentifizierungslandschaft

Wie Biometrie moderne Authentifizierungs- und Betrugspräventionsstrategien antreibt

FORRESTER OPPORTUNITY SNAPSHOT: EINE BENUTZERDEFINIERTE STUDIE IM AUFTRAG VON NUANCE | JUNI 2019

Unternehmen konzentrieren sich traditionell auf die Sprachübertragung im Contact Center, um Kunden zu authentifizieren und Betrug zu verhindern. müssen ihre Authentifizierungsstrategien ändern, um ihre Kunden und sich selbst über alle Kanäle hinweg zu schützen

Wir sehen immer wieder, dass Unternehmen traditionell auf die Sprachübertragung im Contact Center bauen, um Kunden zu authentifizieren und Betrug zu verhindern. Doch sind mittlerweile die Kundenerwartungen an kanalübergreifende Services gestiegen. Unternehmen müssen ihre Authentifizierungsstrategien ändern, um ihre Kunden und sich selbst über alle Kanäle hinweg zu schützen.

In einer Forrester Studie, von uns im Frühjahr 2019 beauftragt, wurden weltweit über 500 Entscheidungsträger befragt. Wir wollten wissen wie die Authentifizierungs- und Betrugslandschaft von heute gesehen wird. Welche Kanäle besonders betroffen sind, wie die Organisationen darauf reagieren und welche Verbesserungen Unternehmen vornehmen können.

## Betrug geschieht immer und überall

Fast jeden Tag informieren uns die Medien über neue Datenlecks und Sicherheitslücken. Das sehen auch die befragten Studienteilnehmer so:

- Kanalübergreifender Betrug ist jetzt an der Tagesordnung. Genau wie die Kunden kanalübergreifend auf Dienste zugreifen, sind Betrüger auch über alle Kanäle hinweg unterwegs, um Schwachstellen aufzudecken.
- Unternehmen sind auf die Bekämpfung von Betrug nur schlecht vorbereitet. Obwohl sie von

ihrer Betrugsprävention in einzelnen Kanälen überzeugt sind, zeigen sie weitaus weniger Vertrauen in ihre kanalübergreifende Betrugsprävention.

- Biometrische, kanalunabhängige Authentifizierungsmethoden sind notwendig für moderne Strategien. Unternehmen, die Biometrie in mehr als einem Kanal einsetzen, tendieren eher dazu, ihre Betrugsprävention als vollständig oder fast optimal zu beschreiben.

## Neue Betrugsrisiken durch digitale Authentifizierung

Mobile und digitale Erfahrungen sind sehr gefragt. Authentifizierung auf diesen Kanälen wächst beträchtlich: 67% der Unternehmen haben innerhalb von 24 Monaten einen Anstieg der Authentifizierung ihrer mobilen Anwendungen um 10% oder mehr verzeichnet.

Die schnelle Akzeptanz digitaler On-Demand-Dienste seitens der Kunden hat auch zu vergleichbarem Zuwachs an Betrug in den Digitalkanälen geführt. So stellten 45% der Unternehmen 4% mehr Betrug in ihren Mobilanwendungen und Websites innerhalb von 24 Monaten fest.

87% der Unternehmen gaben an, dass sie sich vorrangig mit Betrugsprävention in den digitalen Kanälen befassen. Doch müssen auch die etablierten Kanäle der Unternehmen geschützt bleiben.

## Unternehmen glauben Betrug sicher zu bekämpfen

Erstaunlicherweise glauben Unternehmen trotz steigender Betrugszahlen, dass ihr Betrugsschutz ausgereift ist. Bis zu 84% geben an, der Schutz vor Betrug in beliebigen Kanälen sei fast oder vollständig optimiert. Doch Betrüger arbeiten kanalübergreifend und suchen in den einzelnen Kanälen nach Schwachstellen. Immerhin stimmen 82% der Unternehmen zu, dass eine omni-channel Authentifizierung Betrug verhindern kann. Fazit: Unternehmen sind auf die Bekämpfung der sich wandelnden Betrugsformen nur schlecht vorbereitet.

## Besseres Kundenerlebnis durch Omi-Channel-Betrugsprävention

Unternehmen, die an ihrer kanalübergreifenden Betrugsprävention arbeiten, erreichen direkt bessere Kundenerlebnisse (CX). Es überrascht nicht, dass die Resultate jeden Kostensenkungsvorteil übertrifft.

- Effektive Begrenzung von Fehlabweisungen und Fehlannahmen
- Konstant, einfach, weder frustrierend noch aufwendig in allen Kanälen
- Emotionale Resonanz, Vertrauensbildung, Kunden nehmen ein gutes Gefühl mit

## Biometrie unterstützt Unternehmen in puncto

### Sicherheit und Kundenzufriedenheit

Unternehmen evaluieren unterschiedliche Authentifizierungsmethoden, um kanalübergreifend Betrug zu verhindern und dadurch ein besseres Kundenerlebnis zu erreichen. Trotz klarer Mängel sehen Unternehmen Passwörter, personenbezogene Daten und KBA immer noch als betrugsverhindernd an. Jedoch wächst auch die Akzeptanz für Biometrie – wenn auch nur schleichend in Deutschland. Das haben wir auch auf der Opus Research Konferenz „Intelligent Authentication“ im Juni 2019 in München erfahren. Mehr als 60% der Deutschen empfinden biometrische Authentifizierung als angenehm, doch weniger als ein Viertel aller Unternehmen bieten diese Möglichkeit überhaupt an.

## Authentifizierungs- und Betrugslandschaft von heute

Wenn Sie mehr zu diesem Thema erfahren möchten, laden wir Sie zu unserem nächsten Webinar ein. Am **10. September 2019 von 11 bis 12 Uhr** erhalten Sie kostenfrei einen Einblick in die Resultate der Forrester Studie:

- Wie Betrug über Telefonkanäle im Contact Center auch zu Web-, Mobil- und anderen digitalen Kanälen führt.

- Über die Bereitschaft der Unternehmen, Betrug über alle Kanäle hinweg zu verhindern.
- Die Bedeutung von kanalübergreifender Authentifizierung in der Betrugsprävention.
- Strategien, mit denen Unternehmen Betrüger identifizieren und Betrug bekämpfen; u. a. auch durch die vermehrte Einführung von Biometrie, um finanzielle Risiken und Reputationsverluste durch Betrug zu senken, und dabei gleichzeitig die Customer Experience für legitime Kunden zu verbessern.

**Tags:** [Betrugsprävention](#), [Biometrische Authentifizierung](#)