FORRESTER®

Orientierung in der kanalübergreifenden Betrugs- und Authentifizierungslandschaft

Wie Biometrie moderne Authentifizierungs- und Betrugspräventionsstrategien antreibt

Einstieg →

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

Das Paradigma der Authentifizierung und Betrugsprävention verändert sich

Bisher haben sich Unternehmen traditionell auf die Sprachübertragung im Contact Center konzentriert, um Kunden zu authentifizieren und Betrug zu verhindern. Mit steigenden Kundenerwartungen an zeitnahe, reibungslose Interaktionen hat die Nutzung von digitalen Self-Service-Kanälen wie mobilen Apps und Chat-Foren rasant zugenommen — und damit auch das Betrugsrisiko. Unternehmen arbeiten daran, die Erwartungen an schnelle und reibungslose digitale Erlebnisse zu erfüllen. Sie müssen dabei ihre Authentifizierungsstrategien ändern, um die Kunden und das Unternehmen kanalübergreifend zu schützen.

Im April 2019 beauftragte Nuance Forrester Consulting mit der Bewertung von Betrug und Authentifizierung. Mit unserer Befragung von 561 internationalen Entscheidungsträgern zu Betrug und Authentifizierung wollten wir erfahren, welche Kanäle besonders betroffen sind, wie die Organisationen darauf reagieren und welche Verbesserungen Unternehmen vornehmen können.

Wesentliche Ergebnisse

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. Eine kanalübergreifende Authentifizierung ist von wesentlicher Bedeutung.

Unternehmen sind auf die Bekämpfung von kanalübergreifendem Betrug nur schlecht vorbereitet. Obwohl sie von ihrer Betrugsprävention in einzelnen Kanälen überzeugt sind, zeigen sie weitaus weniger Vertrauen in ihre kanalübergreifende Betrugsprävention.

Für eine moderne kanalübergreifende Strategie sind biometrische Authentifizierungsmethoden unumgänglich. Unternehmen, die Biometrik in mehr als einem Kanal einsetzen, tendieren eher dazu, ihre kanalübergreifende Betrugsprävention als vollständig oder fast optimal zu beschreiben.

Mit zunehmender digitaler Authentifizierung entstehen neue Betrugsrisiken

Mobile und digitale Erfahrungen sind sehr gefragt-und das Wachstum der Authentifizierung auf diesen Kanälen ist beträchtlich: 67 % der Unternehmen haben innerhalb von 24 Monaten einen Anstieg der Authentifizierung ihrer mobilen Anwendungen um 10 % oder mehr verzeichnet. Sobald Unternehmen die Art und Weise, wie sie mit ihren Kunden in Kontakt treten, ändern, ändern sie auch die Art und Weise, wie sie das Betrugsrisiko betrachten und managen:

- 70 % sind sich einig, dass die traditionellen Sprachkanäle im Mittelpunkt der Strategie zur Betrugsprävention stehen.
- 74 % stimmen zu, dass mit der Erschließung neuer Kanäle zur Kundenbindung ihre Betrugsanfälligkeit gestiegen ist.
- 87 % bestätigten, dass sie ihren Fokus auf die Betrugsprävention in den digitalen Kanälen gelenkt haben.

Rang der Kanäle, in denen Unternehmen die höchste Stufe der Kundenauthentifizierung erleben	Prozentanteil der Firmen, in denen die Kundenauthentifizierung in den vergangenen 24 Monaten in diesem Kanal um mindestens 10 % gestiegen ist
Website	55 %
Mobile Anwendung	67 %
Persönlich	25 %
Telefon	28 %
Chat	54 %

Basis: Verschiedene Führungskräfte mit Zuständigkeit für Betrugsprävention und Kundenauthentifizierung in internationalen Unternehmen
Quelle: Studie im Auftrag von Nuance, durchgeführt im April 2019 von Forrester Consulting.

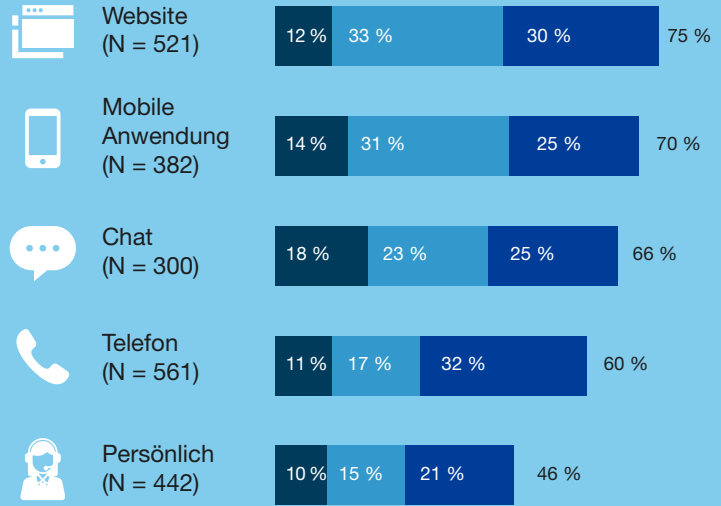
Betrug ist im Aufwind — und kein Kanal ist sicher

Leider hat die schnelle Akzeptanz von digitalen On-Demand-Diensten seitens der Kunden zu vergleichbarem Zuwachs an Betrug in den Digitalkanälen geführt: 45 % der Unternehmen sahen in den vergangenen 24 Monaten in ihren Mobilanwendungen und Websites eine Steigerung der Betrugsrate um mindestens 4 %.

Trotz des Erfolgs von „mobile-first“-Strategien zur Stärkung digital versierter Kunden wachsen in vielen Unternehmen auch die Telefon- und In-Person-Kanäle sowohl in Bezug auf die Authentifizierung als auch auf Betrug. Obwohl 87 % der Unternehmen angaben, dass sie sich vorrangig mit Betrugsprävention in den digitalen Kanälen befassen, müssen auch die etablierten Kanäle der Unternehmen geschützt bleiben.

Auch wenn betrügerische Aktivitäten es in erster Linie auf digitale Kanäle absehen, dürfen die etablierten Kanäle nicht außer Acht gelassen werden.

„Wie hat sich die Betrugsrate (einschließlich Betrugsversuche, die im Vorfeld verhindert werden konnten, und Vorfälle, die erst nach Eintreten erkannt wurden) in den vergangenen 24 Monaten in den folgenden Kanälen verändert?“



Basis: Verschiedene Führungskräfte verantwortlich für Betrugsprävention und Kundenauthentifizierung in internationalen Unternehmen
Quelle: Studie im Auftrag von Nuance, durchgeführt im April 2019 von Forrester Consulting.

Unternehmen sind sich ihrer Fähigkeit, Betrug in einzelnen Kanälen zu verhindern, sehr sicher

Trotz steigenden Betrugs sind Unternehmen der Meinung, dass ihr Betrugsschutz ausgereift ist: Bis zu 84 % geben an, der Schutz vor Betrug in beliebigen Kanälen sei fast oder vollständig optimiert.[1] Unternehmen sind jedoch zu optimistisch — sie vertrauen auf viele gleiche, leicht zu umgehende Authentifizierungsmethoden:[2]

- **Personenbezogene Daten:** Bestätigung des Geburtsdatums, PLZ, usw.; Daten, die sich häufig aus sozialen Medien abrufen lassen oder nach einem Datenverstoß aus dem Dark Web erworben werden können.
- **Knowledge-Based Authentication (KBA):** z. B. „Welche Farbe hatte Ihr erstes Auto?“; diese Angaben sind aufgrund weitreichender Datenverstöße immer weniger verlässlich oder so unklar, dass Benutzer irritiert sind.
- **Passwörter:** oft nicht komplex genug oder Benutzer schreiben sie an unsicheren Orten auf; Betrüger werden versuchen, Passwort-Kombinationen auf vielen Seiten durchzuprobieren, in der Hoffnung, dass das gleiche Passwort wiederverwendet wurde.

„Wählen Sie für jeden der aufgeführten Kanäle aus, wie Ihr Unternehmen Kunden in diesem Kanal anmeldet, authentifiziert und/oder autorisiert.“

Top 5 Authentifizierungsmethoden-die riskantesten Methoden sind weiß

TELEFON

Identitätsprüfung

Personenbezogene Daten

Knowledge-Based Authentication

Risiko-basierte Authentifizierung

Passwörter

WEBSITE

Passwörter

Identitätsprüfung

Personenbezogene Daten

Knowledge-Based Authentication

Software-basierte OTP

MOBIL-APP

Passwörter

Identitätsprüfung

Personenbezogene Daten

Knowledge-Based Authentication

Software-basierte OTP

PERSÖNLICH

Identitätsprüfung

Personenbezogene Daten

Knowledge-Based Authentication

Biometrischer Fingerabdruck

Biometrische Gesichtserkennung

Basis: Verschiedene Führungskräfte verantwortlich für Betrugsprävention und Kundenauthentifizierung in internationalen Unternehmen
Quelle: Studie im Auftrag von Nuance, durchgeführt im April 2019 von Forrester Consulting.

Kanalübergreifender Betrug ist die größere Gefahr

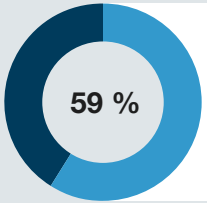
Auch wenn die meisten Unternehmen der Meinung sind, dass sie einzelne Kanäle unter Kontrolle haben, Betrüger arbeiten kanalübergreifend und suchen in den einzelnen Kanälen nach Schwachstellen. So ist beispielsweise das Nichtvorhandensein von Karten (z. B. die Verwendung einer gestohlenen Kreditkartennummer ohne physische Karte) eine alte Betrugsmethode, die auf dem Telefonkanal wirksam bleibt, während die Übernahme von Konten (z. B. Passwort-Hacking) auf Websites und mobilen Anwendungen wirksam ist.

Daher stimmen 82 % der Unternehmen zu, dass eine kanalübergreifende Authentifizierung immer wichtiger wird, um Betrug zu verhindern. Doch nur 59 % bezeichnen ihren kanalübergreifenden Betrugsschutz als fast oder vollständig optimiert — damit weitaus weniger ausgereift als für einen einzelnen Kanal. Unternehmen sind auf die Bekämpfung der sich wandelnden Betrugsformen nur schlecht vorbereitet.

„Welche Art des Betrugs ist in den vergangenen 24 Monaten in den einzelnen Kanälen am häufigsten aufgetreten?“

Kanal	Häufigste Form von Betrug
Mobile App und Website	Kontoübernahme
Telefon	Karte nicht vorhanden
Chat	Identitätsdiebstahl
Persönlich	Betrug mit synthetischen Ausweisen

Nur 59 % beschreiben ihre Fähigkeit, kanalübergreifenden Betrug in ihrem Unternehmen zu verhindern, als fast oder vollständig optimiert.



Deutlich unter der durchschnittlichen Reife eines einzelnen Kanals (81,2 %)

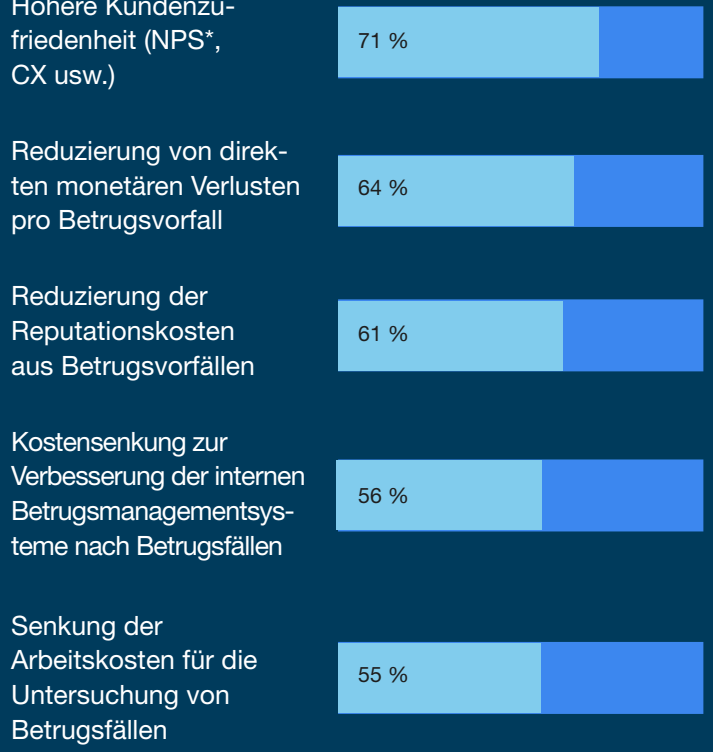
Basis: 561 Führungskräfte verantwortlich für Betrugsprävention und Kundenauthentifizierung in internationalen Unternehmen
Quelle: Studie im Auftrag von Nuance, durchgeführt im April 2019 von Forrester Consulting.

Verhinderung von kanalübergreifendem Betrug verbessert das Kundenerlebnis

Wenn Unternehmen an ihrer kanalübergreifenden Betrugsprävention arbeiten, sehen sie das verbesserte Kundenerlebnis (CX) als entscheidendes Ergebnis. Es überrascht nicht, dass es jeden Kostensenkungsvorteil übertrifft, wahrscheinlich aufgrund der etablierten Verbindung von CX und Umsatzwachstum.[3] Verbesserte CX wird erzeugt durch kanalübergreifende Authentifizierungserfahrungen:

- **Effektiv:** Begrenzung von Fehlabweisungen und Fehlannahmen, auch wenn Kunden über verschiedene Kanäle gehen.
- **Einfach:** Authentifizierungsmethoden, die weder frustrierend noch aufwändig und in allen Kanälen konstant sind.
- **Emotionale Resonanz:** Kunden haben ein gutes Gefühl bei dem Erlebnis – so ist Vertrauen in Zusammenhang mit Authentifizierung eine besonders wichtige Emotion.[4]

„Welche Geschäftsvorteile sollen durch eine bessere Prävention von kanalübergreifendem Betrug gewonnen werden?“



Basis: 561 Führungskräfte verantwortlich für Betrugsprävention und Kundenauthentifizierung in internationalen Unternehmen
*Hinweis: Net Promoter und NPS sind eingetragene Servicemarken und Net Promoter Score ist eine Servicemarke von Bain & Company, Inc., Satmetrix Systems, Inc. und Fred Reichheld.
Quelle: Studie im Auftrag von Nuance, durchgeführt im April 2019 von Forrester Consulting.

Biometrie hilft Unternehmen, Sicherheit und Kundenzufriedenheit in Einklang zu bringen

Unternehmen evaluieren ältere und neue Authentifizierungsmethoden, um die kanalübergreifende Authentifizierung zu verbessern, Betrug zu verhindern und dadurch ein besseres Kundenerlebnis zu gewinnen. Trotz klarer Mängel sehen Unternehmen Passwörter, personenbezogene Daten und KBA immer noch als betrugsverhindernd an. Jedoch erkennen sie auch den Wert der Biometrie. Basierend auf angeborenen Merkmalen fügen diese Methoden der Interaktion keine Reibung hinzu.[5] Darüber hinaus kann die Biometrie Betrüger identifizieren, unabhängig von ihrem Wissen oder ihren sozialtechnischen Fähigkeiten. Unternehmen, die Biometrie kanalübergreifend einsetzen:

- verwenden weniger häufig Passwörter und personenbezogene Daten für mobile Anwendungen, Websites und Telefone (um bis zu 24 Punkte).
- bezeichnen ihre Betrugsprävention in jedem Kanal wahrscheinlich als optimal (um bis zu 20 Punkte).
- bezeichnen ihre Betrugsprävention in jedem Kanal wahrscheinlich als vollständig oder fast optimal (um bis zu 9 Punkte).

Unternehmen sind weiter der Meinung, dass ältere Formen der Authentifizierung wichtig sind, aber viele erkennen auch den Wert von Biometrie

Basis: 561 Führungskräfte verantwortlich für Betrugsprävention und Kundenauthentifizierung in internationalen Unternehmen
Quelle: Studie im Auftrag von Nuance, durchgeführt im April 2019 von Forrester Consulting.

Schlussfolgerung

Unternehmen sind in einem ständigen Wettlauf, um Dienstleistungen anzubieten, wann, wo und wie ihre Kunden es wünschen. Das hat dazu geführt, dass Unternehmen ihre Vorgehensweise in Bezug auf Authentifizierung und Betrugsprävention überdenken. Sowohl legitimierte Kunden als auch Betrüger bewegen sich frei über die Kanäle- Unternehmen benötigen ein modernes Authentifizierungs-Toolset, das die Sicherheitsbedürfnisse mit den Anforderungen von CX in Einklang bringen kann. Neue Tools wie die Biometrie gewinnen an Bedeutung, nicht nur wegen ihrer relativen Sicherheit im Vergleich zu veralteten Methoden, sondern auch wegen ihrer Fähigkeit, das Kundenerlebnis reibungslos und angenehmer zu gestalten. Unternehmen, die Biometrie in mehr als einem Kanal einsetzen, sind auf dem Weg zu kanalübergreifender Betrugsprävention.

Projektleiterin:
Emma Van Pelt,
Market Impact Consultant

Forschungsbeitrag:
Forresters Sicherheits- und Risiko-Forschungsgruppe

Methodik

Dieser Opportunity Snapshot wurde von Nuance in Auftrag gegeben. Zur Profilerstellung nutzte Forrester Consulting vorhandene Forschungsergebnisse der Sicherheits- und Risikoforschungsgruppe bei Forrester. Die Forschung wurde von uns durch eine angepasste Befragung von 561 internationalen Entscheidungsträgern aus dem Bereich Betrugserkennung und Authentifizierung ergänzt. Die kundenspezifische Umfrage wurde im April 2019 begonnen und abgeschlossen.

ANMERKUNGEN

ZURÜCK 1. Ein optimiertes Betrugspräventionsprogramm ist definiert als eines, das kontinuierlich und effektiv, integriert, proaktiv und in der Regel automatisiert ist.
ZURÜCK 2. Quelle: „Top Cybersecurity Threats In 2018“, Forrester Research, Inc., 27. November 2017.
ZURÜCK 3. Quelle: „The US Customer Experience Index, 2018“, Forrester Research, Inc., 19. Juni 2018.
ZURÜCK 4. Quelle: „Drive Growth With Customer Trust And Build Brand Resilience“, Forrester Research, Inc., 25. September 2018.
ZURÜCK 5. Quelle: „Best Practices: Behavioral Biometrics“, Forrester Research, Inc., 5. Mai 2018.

WISSENSWERTES ZU FORRESTER CONSULTING

Forrester Consulting bietet unabhängige objektive, auf Forschungsergebnisse gestützte Beratungsdienstleistungen und hilft damit Führungskräften, ihre Organisationen zum Erfolg zu führen. Die Beratungsdienste von Forrester reichen von kurzen Strategiesitzungen bis hin zu speziell auf den Kunden abgestimmten Projekten. Bei Forrester kommunizieren Sie direkt mit unseren Forschungsanalysten, die ihr Fachwissen auf die speziellen Herausforderungen Ihres Unternehmens anwenden. Weitere Informationen finden Sie unter forrester.com/consulting.

Demografie

REGIONEN

- Europa: 55 %
- Nord-, Mittel- und Südamerika: 36 %
- Australien: 9 %

POSITION

- Leitungsebene (C-Level): 39 %
- Stellvertretender Direktor (VP): 24 %
- Generaldirektor (Director): 37 %

ANZAHL MITARBEITER

- 500 bis 999: 1 %
- 1.000 bis 4.999: 54 %
- 5.000 bis 19.999: 29 %
- 20.000 oder mehr: 16 %

BRANCHE

Es sind verschiedene Branchen vertreten, einschließlich Finanzdienstleister, Einzelhandel, Telekommunikation, Fertigung, Technologie, Professional Services, Versand und Gesundheitswesen.

FORRESTER®