NUANCE | WHAT'S NEXT BLOG

Kundeninteraktion auf allen Kanälen, Verifizierung und Betrugsprävention

Betrugsgefahr im Contact Center durch soziale Disruption

Nuance Communications

2 Dezember 2020

Die COVID-Pandemie hat gezeigt, wie schnell eine Krise zu sozialer Disruption führen kann. In Zeiten, in denen Menschen um ihre Gesundheit und finanzielle Zukunft bangen, herrscht in Contact Centern Hochbetrieb. Kriminelle wissen dies für ihre betrügerischen Aktivitäten zu nutzen, indem sie die überlasteten Systeme für ihre Zwecke missbrauchen. Methoden der biometrischen Identitäts- und Glaubwürdigkeitsprüfung helfen, Unternehmen und ihre Kunden vor Betrügern zu schützen. Ein Nuance-Whitepaper zeigt die Gefahren einer durch Disruption ausgelösten Betrugswelle auf und erklärt, wo wirksamer Schutz zu finden ist.

In Phasen wirtschaftlicher Not steigt die Betrugsaktivität, denn soziale Disruption löst einen rapiden wirtschaftlichen Abschwung und damit einschneidende Veränderungen der Lebens- und Arbeitsbedingungen aus. Diese Zeiten der Unruhe steigern die Belastung für Contact Center und ihre Mitarbeiter, da Kunden zusätzlichen Rat und Unterstützung benötigen. Das wachsende Anrufvolumen bringt Contact Center allerdings schnell an ihre Kapazitätsgrenze, was Betrugsversuche begünstigt.

Doch es sind nicht nur Kriminelle, die die Situation für sich ausnutzen. Auch bislang vertrauenswürdige Mitarbeiter können in der Not zur Bedrohung für Unternehmen werden, indem sie beispielsweise sensible Kundendaten stehlen. Gleiches gilt für Kunden, die etwa durch falsche Versicherungsansprüche einen „freundlichen" Betrug am Unternehmen begehen. Ob Kriminelle, Kunden oder Mitarbeiter –Studien zufolge lässt sich unter den Betrügern ein gewisses Muster erkennen: 68 % von ihnen stecken selbst in finanzielle Schwierigkeiten. Der durch den Betrug verursachte Schaden kann die Existenz von

Unternehmen ernsthaft gefährden. Zu den im Rahmen der Coronakrise gemeldeten Schäden zählen unter anderem:

- um 400 % angestiegene Betrugsversuche bei einer Privatkundenbank
- COVID-19-bedingte Betrugskosten in Höhe von 24 Mio. US-Dollar
- tägliche Verluste von 500.000 US-Dollar durch COVID-19-bedingten Betrug

Die Faktoren, die den Betrug begünstigen, sind vielschichtig. Einerseits führt die Überlastung in Contact Centern dazu, dass Maßnahmen zur Identitäts- und Glaubwürdigkeitsprüfung weniger konsequent angewandt werden. Zum anderen förderte die Pandemie einen starken Anstieg der Arbeit im Homeoffice, wodurch Betrüger ein zusätzliches Einfallstor erhielten, um an sensible Daten zu gelangen oder sich widerrechtlich zu authentifizieren. Deshalb gehen 90 % der Spezialisten für Betrugsbekämpfung davon aus, dass sich folgende Delikte bei Unternehmen und Organisationen bis ins kommende Jahr hinein häufen werden:

- Betrug bei Hilfsorganisationen und Spendenaktionen
- Phishing durch Identitätsfälschung bei Behörden und Gesundheitsämtern
- Cyberangriffe im Zusammenhang mit Heimarbeit

Innovative Technologien zur Betrugsbekämpfung

CX-Manager müssen der wachsenden Betrugsgefahr nicht tatenlos entgegensehen. Zur Bekämpfung professioneller Akteure stellen biometrische Lösungen eine effektive Alternative zur wissensbasierten Authentifizierung dar. Sie identifizieren Anrufer automatisch anhand ihrer Stimme oder der Art ihrer Tastatureingabe, anstatt sich auf die persönliche Abfrage von Kennwörtern oder PINs durch einen Mitarbeiter zu verlassen.

Diese Methoden bieten eine ganze Reihe von Vorteilen. Zum einen gewähren sie umfassenden Schutz, da biometrische Daten von Kriminellen nicht einzusehen oder zu manipulieren sind. Zudem stehen sie zuverlässig rund um die Uhr bereit, und nehmen so den Druck von Mitarbeitern im Contact Center, die sich statt um die Authentifizierung ihrer Kunden nun um die Belange ihrer Kunden kümmern können. Letztere profitieren ebenfalls, da die Gesprächszeiten nicht durch langwierige Authentifizierungsprozesse in die Länge gezogen werden.

Glaubwürdigkeitsauthentifizierung gegen Kundenbetrug

Um Kundenbetrug zu erkennen, leistet die biometrische Glaubwürdigkeitsauthentifizierung einen wertvollen Beitrag. Sie identifiziert unehrliche Handlungen von vertrauenswürdigen Kunden und verhindert so die Anerkennung widerrechtlich gestellter Ansprüche. Wie sicher dieses biometrische System ist, zeigt das Beispiel einer US-amerikanischen Bank, die bei der Glaubwürdigkeitsauthentifizierung laut eigenen Aussagen eine Treffergenauigkeit von 86 % erzielt.

Tags: Sprachbiometrie, Contact center strategie, Biometrische Authentifizierung