What's next

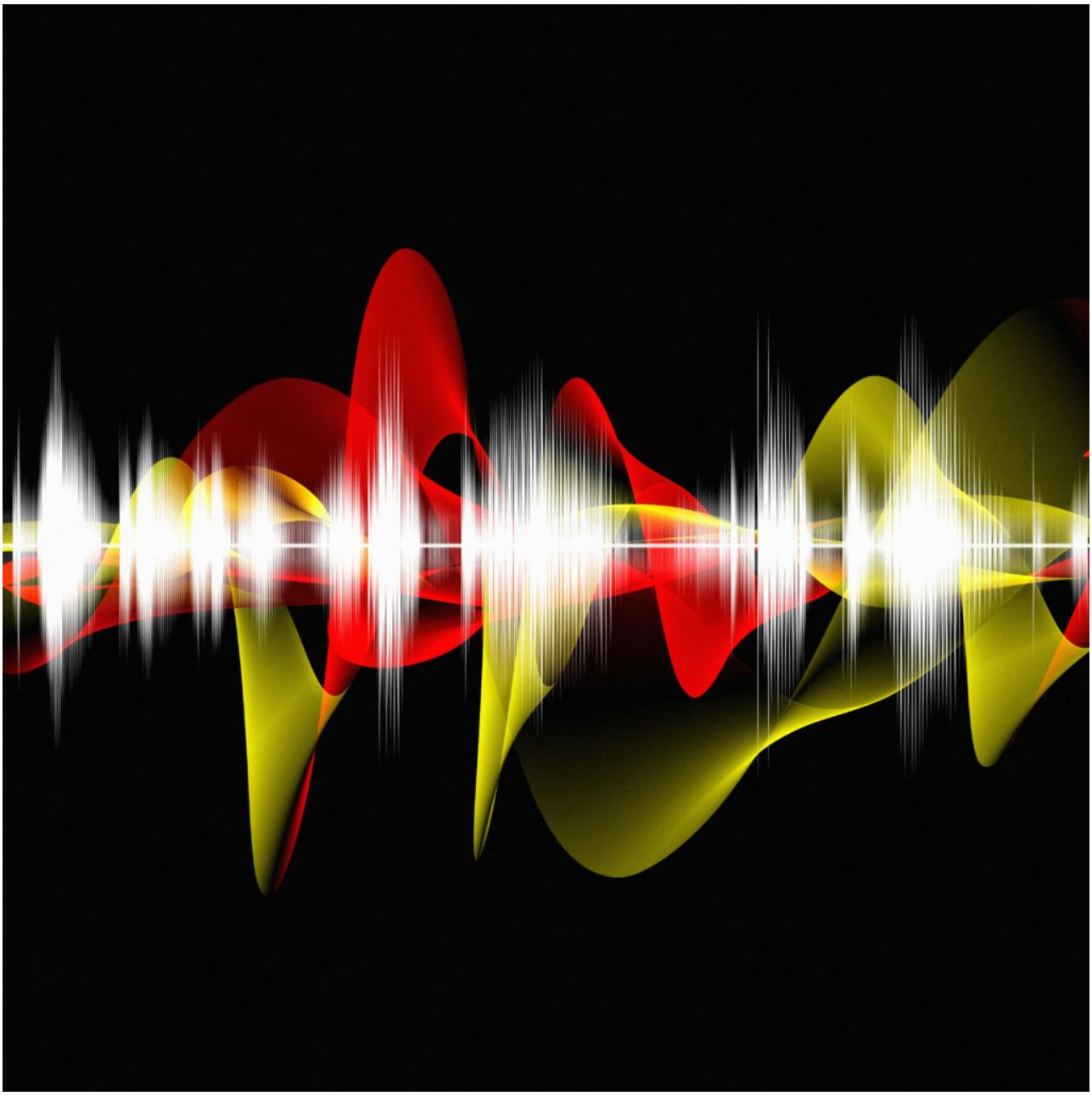
Enterprise

Betrug bei der Kundeninteraktion: Die ungebannte Gefahr

Seit Jahren nehmen betrügerische Aktivitäten bei der Kundeninteraktion länder- und kanalübergreifend zu. Davon ist insbesondere die Finanzbranche betroffen, doch die Kriminellen machen auch vor Branchen wie dem Einzelhandel, der Telekommunikation oder dem Dienstleistungssektor nicht halt. Deshalb ist eine wirksame Betrugsprävention unabdingbar, um Unternehmen vor finanziellen Schäden und dem Verlust des Kundenvertrauens zu schützen.

Sylvia Lohr

Posted 18 August 2020



Aktuelle Untersuchungen zeigen, wie groß die Gefahr für Unternehmen tatsächlich ist, Opfer eines Betrugs zu werden. Es wird geschätzt, dass durch manipulierte Kundenauthentifizierungen alljährlich Schäden in Milliardenhöhe entstehen. Dabei handelt es sich um ein weltweites Problem, denn die Intensität der kriminellen Angriffe nimmt auf globaler Ebene rasant zu.

BANKINGNEWS Nr. 278 / JUNI 2020

BETRUG OHNE GRENZEN

Banken verzeichnen seit Jahren Rekordschäden durch Betrug und Cyberkriminalität. Trotz hoher Investitionen in IT-Sicherheit und Betrugsprävention bleibt die Gefahr bestehen. Denn der moderne Betrüger kennt weder Länder- noch Kanal-Grenzen.

Ein globales Problem

Es ist beinahe unerheblich, in welchem Teil der Welt die Unternehmen ihre Geschäfte abwickeln, denn die Gefahren lauern nahezu überall. So ist beispielsweise Mexiko das Land mit dem weltweit höchsten Anteil an Firmen, die einer kriminellen Attacke zum Opfer fallen. Mit einem Wert von 93,9 % führt das mittelamerikanische Land die Liste der am stärksten betroffenen Nationen an – vor Spanien (87,5 %) und Italien (85,7 %). Dass auch deutsche Unternehmen in hohem Maße Angriffen ausgeliefert sind, zeigt sich daran, dass hierzulande immerhin 79,2 % von ihnen im vergangenen Jahr erfolgreich attackiert wurden.

Beunruhigend für die Sicherheitsexperten in Unternehmen, Organisationen und Regierungen ist, dass diese Zahl trotz umfangreicher Schutzmaßnahmen weiter zunimmt. Während 2016 weltweit 71,6 % von ihnen Betrugsschäden erlitten, schnellte dieser Wert bis zu diesem Jahr auf über 80 % in die Höhe. Dabei traf es überproportional häufig Unternehmen aus der Finanzbranche, gefolgt vom Einzelhandel sowie dem Telekommunikations- und IT-Sektor. Gleichzeitig stehen zunehmend Regierungen im Fokus der Betrüger, was dafürspricht, dass die Verbrecher in immer größeren Maßstäben denken.

Kanalübergreifende Attacken

Die Zeiten, in denen sich Kriminelle bei ihren Angriffen auf einen Kanal beschränkten, sind längst passé. Stattdessen werden inzwischen aus allen Bereichen Betrugsversuche vermeldet. Dabei lassen sich die Betrüger auch vor ausgereiften Schutzmaßnahmen bei der Kundenauthentifizierung nicht abschrecken. So erfolgen die Angriffe sowohl auf digitalen Kanälen – wie Webseiten, mobilen Apps und Chats – als auch per Telefon oder im persönlichen Gespräch.

Darauf müssen Unternehmen ihre Schutzmaßnahmen einstellen, denn in all diesen Bereichen werden seit 2017 mitunter erheblich erhöhte Betrugsaktivitäten registriert. Dabei stellen sich die Angreifer individuell auf die jeweiligen Kanäle ein. Während sie im Onlinebereich auf Kontoübernahmen oder Identitätsdiebstahl zurückgreifen, arbeiten sie am Telefon mit Ausreden oder täuschen ihre Ansprechpartner bei persönlichen Kontakten mit gefälschten Ausweisen.

Zudem zeigt sich, dass die Betrüger besonders gerne wiederholt bei gleichen Unternehmen zuschlagen. So wurden im Jahr 2019 über ein Drittel der betroffenen Unternehmen mehr als sechs Mal angegriffen. Ein Grund dafür ist, dass sich noch immer viel zu viele von ihnen bei der Authentifizierung ihrer Kunden auf herkömmliche Methoden wie PIN- oder Passwort-Abfragen verlassen. Doch darauf haben sich die Betrüger längst eingestellt und Wege gefunden, die veralteten Schutzmechanismen erfolgreich zu umgehen.

Wie unsicher PINs und Passwörter mittlerweile sind, zeigt eine Studie von Forrester Research. Ihr zufolge kann ein achtstelliges, zufällig zusammengesetztes und mit Großbuchstaben, Ziffern sowie Sonderzeichen kombiniertes Passwort innerhalb von nur neun Stunden geknackt werden.

Wirksame Betrugsprävention

Gegen Identitätsbetrug und betrügerische Kontenübernahmen helfen moderne Tools zur eindeutigen Kundenauthentifizierung. Eine effiziente Methode ist die biometrische Authentifizierung und Betrugsbekämpfung, mit deren Hilfe Unternehmen kriminelle Attacken bereits im Vorfeld und über alle Kanäle erkennen sowie bekämpfen können.

Biometrische Verfahren erlauben es, die Identität einer interagierenden Person anhand spezifischer Merkmale eindeutig zu erkennen und zu verifizieren. Dabei können biometrische Methoden zur Kundenauthentifizierung sowohl über eine Spracherkennung im Gespräch als auch über die Prüfung individueller Verhaltensmerkmale im Onlinebereich eingesetzt werden. Eine Kombination beider Verfahren im Omni-Channel-Kundenkontakt erzeugt somit einen wirksamen Schutzschild, der für Betrüger nur äußerst schwer zu überwinden ist.

Tags: Betrug, Betrugsprävention, Betrugsschutz, Biometrie, Finanzdienstleister, Identitätsbetrug, Kundenauthentifizierung, Kundeninteraktion, stimmbiometrie, Verhaltensbiometrie

More Information

Betrug ohne Grenzen
Sehen Sie hierzu mehr Informationen in der aktuellen Infografik vom Bankingclub Deutschland.
Learn more

About Sylvia Lohr

Sylvia Lohr ist Regional Marketing Managerin in der Enterprise Division bei Nuance. Neben den Ländern Deutschland, Österreich und Schweiz verantwortet sie auch die osteuropäischen Länder und die Türkei. Ursprünglich aus der analogen Welt kommend, hat sie die digitale Kommunikation maßgeblich vorangetrieben und versteht die Anforderungen der Transformation. Sie ist überzeugt, dass nur integrierte, kundenzentrierte Kampagnen erfolgreich sind und entwickelt innovative, zielgruppen-spezifische und vertriebsorientierte Marketingstrategien und setzt diese um. Sie lebt in der Nähe von Frankfurt und fährt in ihrer Freizeit gerne Motorrad.

View all posts by Sylvia Lohr