What's next

Enterprise

Betrüger auf allen Kanälen bekämpfen

Simon Marchand, Verantwortlicher für Betrugsprävention bei Nuance, analysiert, wie sich der Kampf gegen Betrug verändert – und wie Unternehmen diesen mithilfe künstlicher Intelligenz (KI) gewinnen können.

Sylvia Lohr
Posted 17 Dezember 2019

Jedes Jahr verursachen Betrüger weltweit Schäden in Höhe mehrerer Mrd. Euro für Unternehmen. Während die finanziellen Verluste relativ einfach zu berechnen sind, fällt dies bei den indirekten Auswirkungen schwer. Die Bewertung von indirekten Einflüssen auf Markenimage oder Kundenvertrauen ist weitaus komplizierter – trotzdem sind sie absolut real.

Betrug, der durch Manipulation im Kontaktcenter oder anderen Kundenkontakt-Kanälen verübt wird, führt viel zu oft zur Finanzierung von Menschenhandel, Drogenschmuggel oder Terroranschlägen. In dieser neuen Welt, in der kriminelle und terroristische Netzwerke im Darknet kooperieren, haben Unternehmen nicht nur die Verantwortung, ihre Verluste zu minimieren. Sie müssen darüber hinaus ihren Teil dazu beitragen, die Welt vor diesen Verbrechen zu schützen.

Unternehmen benötigen eine gut durchdachte kanalübergreifende Strategie zur Betrugsprävention, die ihnen dabei hilft, sich, ihre Kunden und die Gesellschaft zu schützen.

Betrüger lieben neue Kanäle

Mehr Kontaktkanäle sind für Betrüger gleichbedeutend mit zusätzlichen Angriffsmöglichkeiten. Während Unternehmen bemüht waren, Kunden durch zusätzliche digitale Kanäle einen leichteren und bequemen Zugang zu bieten, haben sie damit auch den Betrügern das Handwerk erleichtert. Kriminelle sind äußerst clever darin, die vielfältigen Kanäle für ihre Betrügereien zu nutzen.

Aktuelle Studien von Forrester zeigen: “82 % der Unternehmen stimmen zu, dass die Authentifizierung über alle Kanäle immer wichtiger für die Betrugsabwehr wird. Doch nur 59% definieren ihre eigene Cross-Channel-Betrugsprävention als vollkommen oder annähernd optimal.”

Viele Unternehmen, die einen Kanal absichern, müssen deshalb erleben, dass die Betrüger einfach auf einen anderen, weniger geschützten Kanal ausweichen. Kriminelle suchen immer nach dem schwächsten Glied der Kette. Und sie sind äußerst geschickt darin, dieses zu finden und auszunutzen.

Zum Beispiel entdeckte das Betrugsbekämpfungsteam eines unserer Kunden, eine britische Großbank, dass ihr Kontaktcenter viele betrügerische Anrufe erhielt. Doch die tatsächlichen Betrugsversuche erfolgten über die digitalen Kanäle. Die Betrüger setzten bei ihren Anrufern auf die soziale Interaktion mit den Call Center-Agenten. Dabei versuchten sie, von diesen die benötigten Informationen zu erhalten, um damit einen Betrug auf anderen z. B. den digitalen Kanälen zu verüben.

Die Betrugs-Supply Chain

Zwar hat die Einführung von Chipkarten mit Geheimzahl, Verified by Visa, Mastercard SecureCode geholfen, das Ausmaß des traditionellen Betrugs bei Zahlungstransaktionen zu begrenzen. Doch nun gibt es ein neues Einfallstor, das kaum geschützt ist: Der Identitätsklau.

Das Darknet begünstigt eine Betrugs-Supply Chain, die die von Hackern gestohlenen personenbezogenen Daten und Passwörter mit Betrügern verbindet. Letztere verwenden die sensiblen Informationen, um daraus Einnahmen für ihre kriminellen Netzwerke zu erzielen. Und dabei geht es nicht nur um große Datenverluste wie beim Equifax-Vorfall, der das Unternehmen bis zu 700 Millionen US-Dollar an Kompensationszahlungen kosten dürfte.

Die Tatsache, dass viele von uns unterschiedlichste persönliche Informationen in den sozialen Medien teilen, erweist sich für Betrüger als wahre Goldgrube. Dabei wird deutlich, dass die Betrugstaktiken immer raffinierter werden und dass digitale Technologien immer stärker zum Einsatz kommen. Traditionelle Methoden zur Authentifizierung und Betrugsprävention werden deshalb in wachsendem Maße immer unzureichender.

Erkennung reicht nicht aus

Die Gefahr bei Passwörtern und personenbezogenen Daten ist, dass sie gestohlen werden können. Das macht sie für die sichere Authentifizierung ungeeignet und birgt die Gefahr einer Millionenstrafe wie zuletzt 1&1 in Deutschland erfahren musste. Gleichzeitig wurden die von den Unternehmen zur 2-Faktor-Authentifizierung genutzten Technologien und Werkzeuge (wie z. B. SMS) nicht für Sicherheitsaspekte konzipiert.

Darüber hinaus führen die traditionellen Strategien, mit denen Risiken erkannt und gebannt werden, lediglich zur Identifizierung von Betrugsversuchen – und dabei viel zu oft zu Fehlalarmen. Die Maßnahmen wirken jedoch nicht präventiv und können den an mehreren Fronten erfolgenden Cross-Channel-Betrug nicht wirksam bekämpfen. Deshalb ist mit wachsenden Verlusten durch Betrug und dem staatlichen Druck zur Prävention, ein neuer Ansatz erforderlich. Bei der KI-Technologie finden Unternehmen die geeignete Möglichkeit, um eine präventive Cross Channel-Methode einzusetzen.

KI-gestützte Cross Channel-Betrugsprävention

Dank der Verwendung von Sprachbiometrie in IVR und Contact Center können Anrufer innerhalb der ersten Sekunden authentifiziert werden. So können schnell und sicher betrügerische Interaktionen identifiziert und beendet werden, ohne dafür auf ein verdächtiges Verhalten warten zu müssen. Dies reduziert die Anfälligkeit und gleichzeitig den Aufwand für Anrufer sowie Agenten.

Die Kombination von Sprach- und Verhaltensbiometrie in digitalen Kanälen sowie der Aufbau einer wirksamen kanalübergreifenden Abwehr ist durchsetzungsstark. Technologien zur Sprach- und Verhaltensbiometrie entdecken dabei ungewöhnliches oder untypisches Verhalten. Daraufhin verifizieren sie mithilfe der Sprach-Authentifizierung die Identität des Kunden. Dies kann etwa geschehen, indem er aufgefordert wird, einen kurzen Satz vorzulesen oder während eines Gespräches.

Mit der Integration diese biometrischen Methoden in existierende Strategien und Maßnahmen zur Betrugsprävention (z. B. Erkennung von Anomalien oder Risikobewertung), können Betrüger effizient gestoppt werden – wo auch immer sie angreifen.

Es wird Zeit zu kooperieren – und die Betrüger zu stoppen

Biometrie-Technologien erkennen Betrug und können diesen wirksam verhindern. Das führt zu einer Reduzierung der Betrugsvorfälle und somit der Anzahl von Kunden, die über einen Kontobetrug informiert werden müssen. Vielleicht noch wichtiger ist, dass Biometrie direkt den Kampf gegen die Kriminellen aufnimmt. So helfen Beweismittel aus Contact Centern den

Ermittlungsbehörden, kriminelle Personen und Gruppen, die für Millionenverluste verantwortlich sind, vor Gericht zu bringen.

Neben der Zusammenarbeit mit Strafverfolgungsbehörden müssen Unternehmen deshalb beginnen, verstärkt miteinander zu kooperieren. Mit der richtigen Technologie, Strategie und Zusammenarbeit können wir die Betrugs-Supply Chain unterbrechen.

Tags: authentifizierung, Betrugsprävention, call center, KI, kundenservice, Künstliche Intelligenz, sprachbiometrie, Sprachtechnologie

More Information

Lesen Sie mehr zum Thema und weiteren Innovationen von Nuance.

Mit unserem IQ Magazine erhalten Sie Einblicke über die neuesten Innovationen für Ihren Kundenservice

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