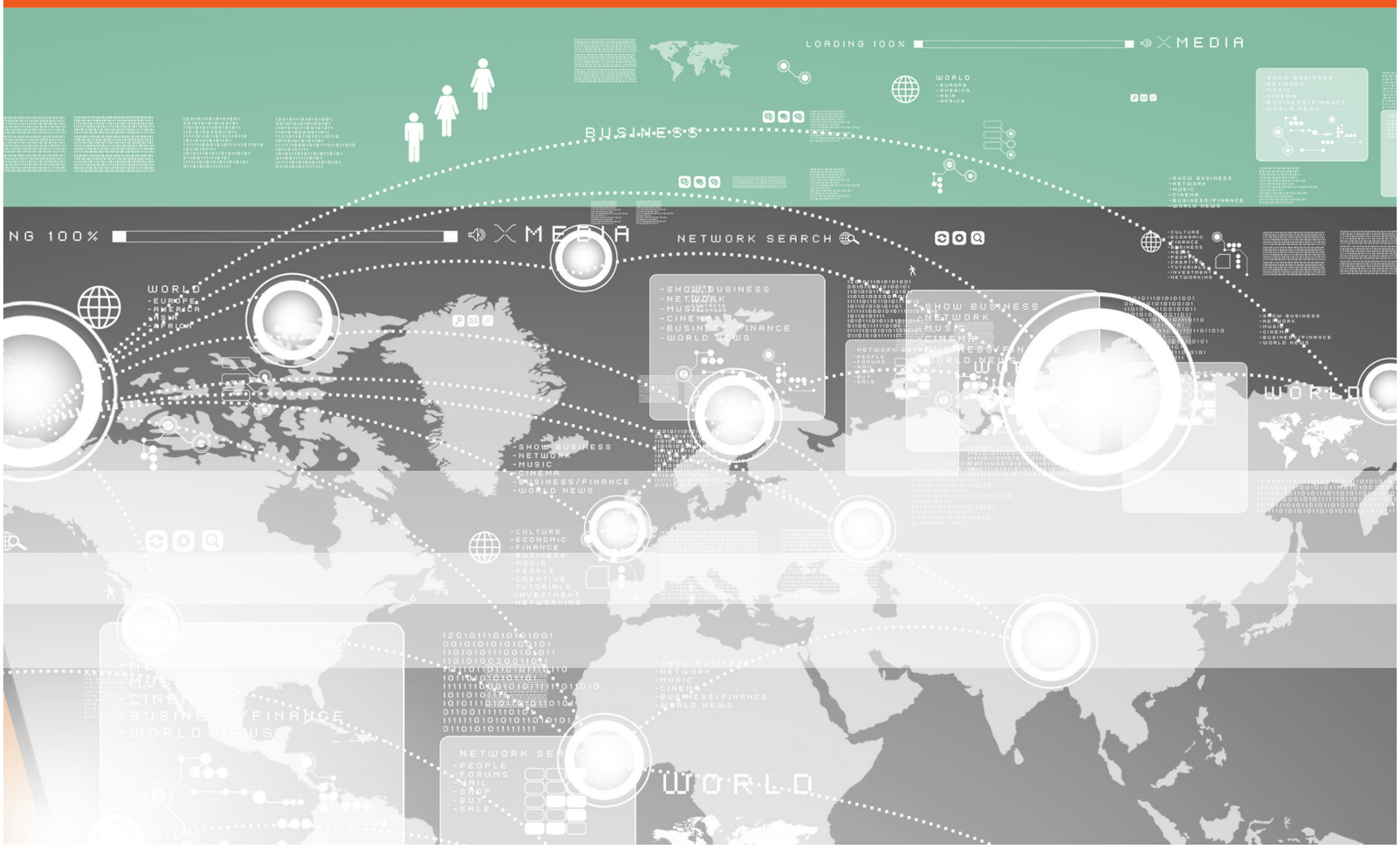
Seien Sie cleverer als Contact-Center-Betrüger - mit Supercharged Voice Biometrics

opusresearch



opusresearch | Bericht »

Seien Sie cleverer als Contact-Center-Betrüger - mit Supercharged Voice Biometrics »

Durch die Nutzung der neuesten Fortschritte auf dem Gebiet der Machine-Learning-Technologien zusammen mit Sprachbiometrie für die Authentifizierung von Anrufern können Contact Center jetzt betrügerische Absichten von Anrufern erkennen. Im Rahmen des Kampfes gegen ausgeklügelte betrügerische Angriffe ist die Erstellung hochwertiger Beobachtungslisten von Betrügern auf der Grundlage historischer Aufzeichnungen nicht nur ein sehr effektives Verteidigungsinstrument, sondern auch ein wirksames Hilfsmittel für die Strafverfolgung. Solchen Angreifern das Handwerk legen zu können ist eine echte Revolution im Kampf gegen Betrugsversuche.

»

November 2018

Ravin Sanjith, Intelligent Authentication, Opus Research

Opus Research, Inc.
350 Brannan St., Suite 340
San Francisco, CA 94107

www.opusresearch.net

Betrüger sind sehr wachsam und entschlossen, alle Schwachstellen in den Kundenkanälen eines Unternehmens auszunutzen. Während die Stimmbiometrie eine der wirksamsten Waffen gegen den Contact-Center-Betrug ist, kann ihre Wirksamkeit durch die Stimmanalyse von Anrufern von bereits vergangenen Interaktionen deutlich erhöht werden.

Bislang werden „Voiceprints“ für Authentifizierungszwecke verwendet und analysiert, um Einblicke für den Kundenservice zu gewinnen. Die neuesten Fortschritte der Machine-Learning-Technologien ermöglichen jetzt aber auch, bisher unvermutete betrügerische Absichten aufzudecken. Mithilfe dieser Technologien können beeindruckende Beobachtungslisten erstellt werden, um bisher unbekannte Betrüger zu entlarven und zukünftige Angriffe zu verhindern. Darüber hinaus ermöglicht die Automatisierung dieses Prozesses Unternehmen, mit der Zunahme von Contact-Center-Betrug Schritt zu halten, die Qualität und der Umfang der stimmbasierten Beobachtungslisten von Betrügern ständig zu verbessern und so außergewöhnliche geschäftliche Vorteile zu erzielen.

Die Sprachkommunikation wird immer wichtiger

Während die Bedeutung digitaler Self-Service-Kanäle in den letzten Jahren deutlich zugenommen hat, wächst auch die Nutzung von Sprache zur Interaktionen mit dem Contact Center stetig. Dieser Trend kann auf folgende Gründe zurückgeführt werden auf:

- Früher – Die einzige Alternative für Kunden um mit einem Unternehmen zu interagieren, bestand, neben telefonischer Kontaktaufnahme, darin, eine Niederlassung
- Heute – Generationsübergreifender Komfort im persönlichen Gespräch, insbesondere bei der Lösung komplexer Fragestellungen, die sich nicht digitalisieren lassen
- Morgen – Erhebliche Verbesserungen der Sprachverarbeitung, die nicht nur erkennt, was gesagt wird, sondern auch den mit der Sprache verbundenen Kontext und die Emotionen erkennen kann. Diese sorgen für die zunehmende Verfügbarkeit von „Voice first“-Technologien (Smart Speakers, Voice-Bots, Siri, Alexa usw.), was zur Entwicklung einer neuen „Gen-V“, eine „Voice-Generation“ beiträgt, die es gewohnt ist und kein Problem damit hat, mit einer Maschine zu kommunizieren.

Mitarbeiter sind entscheidend für die optimale Kundenerfahrung

Futurologen sagen voraus, dass bald die meisten Kundeninteraktionen über eine Art virtuellen Mitarbeiter stattfinden werden, und verschiedene Live-Chat-Einrichtungen wie virtuelle Assistenten, Chatbots und andere intelligente digitale Hilfsmittel wie das Internet, E-Mail, Instant Messaging und soziale Medien unterstreichen diesen Trend schon heute. Im Bereich der Sprach- und Stimmerkennung wird diese Revolution derzeit aber hauptsächlich von Geräten übernommen, etwa von Sprachassistenten wie Siri, Alexa, Google Assistant u. dgl. Nach wie vor bildet das Contact Center das Rückgrat für die Kundenerfahrung, und im Mittelpunkt steht immer noch der Mitarbeiter.

Auch wenn oft anderes behauptet wird, ist selbst im Zuge der allgemeinen Digitalisierung der Mitarbeiter weiterhin die tragende Säule für die Kundenerfahrung, da nur reale Menschen als wirklich angenehm empfundene Beziehungen zu Kunden aufrechterhalten können. In praktischer Hinsicht sind die Mitarbeiter derzeit die einzige Alternative für Fälle, in denen digitale Technologien versagen. Als Stütze und Ersatz für sowohl digitale als auch andere Self-Service-Kanäle (einschließlich IVR) müssen die Mitarbeiter eine optimale Kundenerfahrung gewährleisten und dabei gleichzeitig Anrufer authentifizieren und Betrugsversuche erkennen, um Compliance und Sicherheit zu wahren.

Der Sprachkanal ist der am stärksten gefährdete Kanal

Die Anforderungen an die Mitarbeiter sind, gelinde gesagt, extrem und führen zu Fluktuationsraten von über 30 %. Dies wiederum hat die Kosten in die Höhe getrieben, was zu einer Vielzahl von outgesourcten Contact Center-Lösungen rund um den Globus geführt hat Zwar lassen sich damit einige Contact-Center-Kosten senken, die Auswirkungen auf die Kundenerfahrung sind im Allgemeinen allerdings eher negativ. Der Grund hierfür ist, dass Unternehmen in ihren Möglichkeiten eingeschränkt sind, um innerhalb ihrer outgesourcten Service-Anbietern sowohl die Einhaltung von Prozessen als auch die Handhabung von sensitiven Kundeninformationen zu kontrollieren.

Dieses Dilemma wird dadurch noch weiter verstärkt, dass von Mitarbeitern (oft durch Anreize unterstützt) erwartet wird, für eine bessere Kundenerfahrung, basierend auf geschäftlichen Zielen wie etwa den Net Promotor Score (NPS) und die Anrufeffizienz (Agent Handling Time - AHT), zu sorgen. Authentifizierungsprozesse resultieren oft in einer Art von Anrufer-Befragung, wie zum Beispiel Knowledge-Based Authentication (KBA) oder One-Time-Password-Verfahren (OTP). Solche Verfahren widersprechen völlig den geschäftlichen Zielen einer optimalen Kundenerfahrung und Mitarbeitereffizienz. Oft führt dies zu Kompromissen innerhalb der Sicherheitsprozesse, was Mitarbeiter anfälliger für Social-Engineering-Angriffe macht. Betrüger wissen dies und richten daher ihre Angriffe bevorzugt gegen Contact Center als das schwächste Element der Omnichannel-Struktur eines Unternehmens.

Multifaktor-Authentifizierung im Contact Center

In Reaktion auf diese Herausforderungen werden derzeit zahlreiche Innovationen eingeführt, um die Kundenerfahrung und die Sicherheit zu verbessern, während aber auch die betriebliche Effizienz gesteigert oder zumindest gewahrt werden soll. Dazu gehören physische und digitale Tokens – Letzteres wird versandt über USSD Codes, in einer App oder per SMS-Pushbenachrichtigung. Solche Verfahren beeinträchtigen die Kundenerfahrung und sind zudem mit höheren Kosten für Unternehmen verbunden. Ein anderes Verfahren ist die gerätegebundene biometrische Authentifizierung mit Verbindung zu den Anrufdaten, wofür allerdings die modernsten Netzwerke und Infrastrukturen benötigt werden. Die vielversprechendsten Methoden nutzen SIM-Validierung und Phone Profiling in Verbindung mit Netzwerkdaten. Diese Methoden werden jedoch immer noch auf den Sprachkanal verschoben, wenn die Systeme ausfallen.

Betrüger sind sich dieses wesentlichen Problems bewusst und nutzen eine Reihe verschiedener Techniken, um diese Prozesse zu beeinträchtigen oder zu maskieren, so dass sie nur noch das Problem haben, einen Mitarbeiter in direkter Interaktion zu überzeugen. Obwohl die meisten Sicherheitsexperten eine multimodale Sicherheitsarchitektur mit mehreren Ebenen als End-Design anstreben, ist der damit verbundene Zeit-, Kosten- und Ressourcenaufwand für die meisten Unternehmen oft zu groß.

MIT DER KUNDENERFAHRUNG ALS ZENTRALEM FAKTOR FÜR DEN GESCHÄFTLICHEN ERFOLG, IST DIE SPRACHBIOMETRIE EIN ENTSCHEIDENDES VERFAHREN FÜR DIE AUTHENTIFIZIERUNG IN CONTACT CENTERN.

Was für einen einzelnen betrügerischen Angriff benötigt wird

Live-Anrufe von Betrügern sind oft so aufgebaut, dass sie als absolut legitime und harmlose Anfragen erscheinen. Tatsächlich sind sie jedoch Teil einer größeren Kampagne, die dazu dient, systematisch Informationen über die Sicherheitsprozesse eines Unternehmens zu sammeln und die Daten zu ergänzen, die ein Betrüger sich möglicherweise bereits mit anderen Mitteln, etwa im Rahmen größerer Datenschutzverletzungen, verschafft hat. Solche Angriffe, bei denen nach Angaben von shapesecurity.com allein in 2017 mehr als 2,8 Millionen persönliche Anmeldedatensätze gestohlen wurden, erhöhen die Anzahl betrügerischer Aktivitäten immens.

Oft verwenden Syndikate „Call-Miner“, welche die mit diesen verschiedenen Methoden erfassten Informationen in einem als „Dump Checking“ bezeichneten Prozess validieren - einem Verfahren, bei dem, wie beim bekannten „Containern“, sozusagen im Müll nach Brauchbarem gesucht wird. Diese Data-Miner (oder auch „Data Mules“) sind äußerst geschickt bei der Anwendung von Social Engineering-Techniken gegenüber den Mitarbeitern und oft auch angenehmer im Umgang als - oft wütende - reale Kunden. Hierdurch ist der allgemeine Erfolg größer, da die Mitarbeiter eifrig und motiviert sind, die Anrufer zufriedenzustellen.

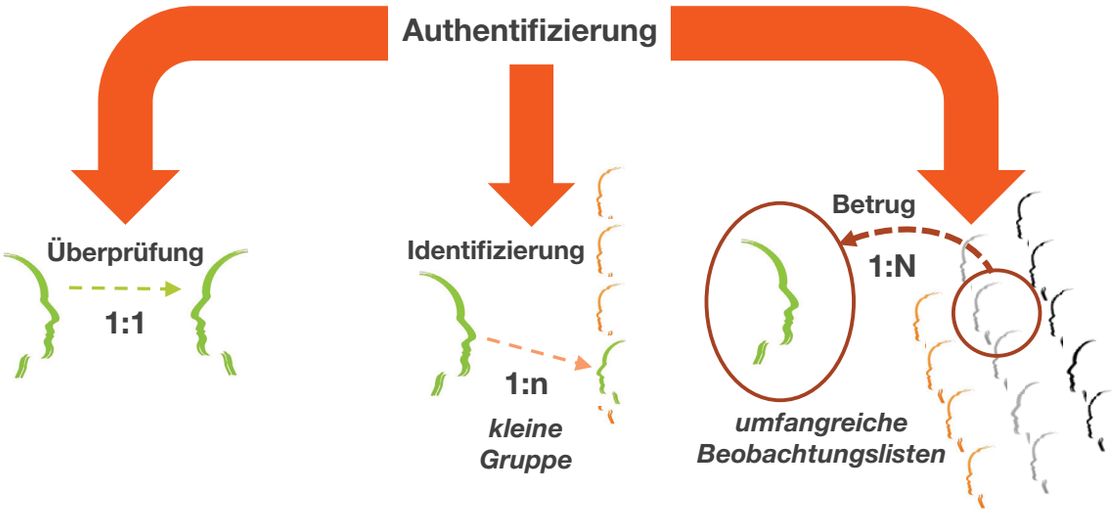
Selbst Betrug, der außerhalb des Sprachkanals stattfindet, etwa über eine Website, App oder sogar in der Niederlassung, ist häufig auf Daten angewiesen, die über ein Contact Center überprüft wurden. Oft erfolgen bis zu fünf Anrufe, bevor ein solcher realer Angriff auf die Ressourcen eines Unternehmens stattfinden kann.

Sprachbiometrie: Authentifizierung und Betrugserkennung

Die meisten Prozesse für die Betrugserkennung basieren auf der Identifizierung von Besonderheiten in Transaktions-, Kanal- und Kundenverhalten. Mit der Zeit wurden manuelle Prozesse durch regelbasierten Automatisierungen ersetzt, die immer mehr von den revolutionären Entwicklungen auf dem Gebiet des maschinellen Lernens profitieren. Zu diesen Kennzeichen gehören u.a. die Anrufer-ID (ANI/CLI), die Geräteidentifizierung, aktuelles Timing und Häufigkeit von Aktivitäten, Authentifizierungsergebnisse aus anderen Kanälen zu demselben Kunden sowie die immer stärker werdende Verknüpfung bislang separater Datenquellen zur Erkennung von jeglichen Irregularitäten. Daraufhin werden ausführlichere Untersuchungen durchgeführt, für die weitere Informationsquellen genutzt werden, und die datenhungrige Spirale dreht sich so immer weiter.

Die Sprachbiometrie hat vor über einem Jahrzehnt einen schleppenden Start genommen und wächst nun weltweit äußerst schnell. Opus Research schätzt, dass bis 2020 mehr als 500 Millionen verschiedene Stimmen erfasst sein werden. Dies ist eine sehr wertvolle Datenquelle für Sprach- und Stimmdaten, die ursprünglich für Authentifizierungszwecke gedacht war, jetzt aber auch zur Betrugserkennung eingesetzt werden kann. Die Sprachbiometrie unterstützt Forscher durch die Bereitstellung einer völlig neuen Art von Daten, welche zur Ergänzung dieser Untersuchungen verwendet werden kann. Dies gilt sowohl für Anrufer, welche die Authentifizierung durch Sprachbiometrie bestehen also auch für solche, die sie nicht bestehen – die einen dienen als Referenzpunkte für die Prüfung mutmaßlicher Betrüger, und die anderen sind die Quelle für die Erstellung von Stimm-Beobachtungslisten.

Abbildung 1: Modelle für die Sprach-Authentifizierung



Verbesserung des Umfangs und der Qualität von Sprachbiometrie-Beobachtungslisten

Markierte „Voiceprints“ sind die Inputs für stetig wachsende Beobachtungslisten von bestätigten und verdächtigen Betrügern. Eine Herausforderung besteht jedoch darin, dass die Geschwindigkeit, mit der diese Beobachtungslisten aufgebaut werden, von der Geschwindigkeit der Verbreitung der Sprachbiometrie-Authentifizierung begrenzt wird. Dies wird durch die (bislang) geringe Kundenakzeptanz der Sprachbiometrie aufgrund von Datenschutzbedenken und anderen „Technologie zu früh“-Einwänden verstärkt.

Eine weitere Herausforderung ist der Umfang der Ressourcen, die für Analysen der Sprachkanäle benötigt werden; wie alle Strategien für das Betrugsmanagement belastet dies die wenigen Ermittlungsteams bei der Durchführung hochwertiger und schneller Untersuchungen sehr. Unabhängig vom Sprachkanal führte das massive Wachstum des Digital Commerce-Sektors zu Mengen von Daten, wobei hoch entwickelte Filterverfahren angewandt werden müssen, um die Balance zwischen „False Negatives“ (Angriffe, die durch die Betrugserkennungsnetze schlüpfen) und „False Positives“ (legitime Transaktionen, die fälschlich als mögliche Betrugsversuche markiert werden) zu erreichen.

Bislang wurde der Sprachkanal verwendet, um Betrugsuntersuchungen zu verbessern, indem manuell auf die Historie aufgezeichneter Anrufe zugegriffen wurde, und indem diese Anrufe angehört wurden, um Gesprächsinhalte zu ermitteln. Auch wurde eine manuelle, qualitative Bewertung durchgeführt, ob der Anrufer verdächtig oder anders klang als ein bekannter oder bestätigter legitimer Kunde. Ein solcher Prozess ist natürlich nicht nur sehr subjektiv, sondern auch äußerst zeitraubend.

Die jüngsten Entwicklungen bei der Kombination der Sprachverarbeitung und der Sprachbiometrie ermöglichen mittlerweile die Analyse sehr großer Datenbanken von historischen Anrufaufzeichnungen, um Stimmen miteinander zu verknüpfen und somit hochwertige Stimmprofile für alle früheren Anrufer zu erstellen.

Ein einzelner Vergleich dieser Stimmprofile mit Transaktionsdaten aus CRM- und anderen unterstützenden Systemen ermöglicht eine Vielzahl von Einsichten, wie etwa:

- Unterschiede bei dem oder den Stimmprofil(en) für dasselbe Kundenkonto
- Wiederholte Anrufe mit demselben Stimmprofil für unterschiedliche Accounts
- Sehr häufige Anrufe mit demselben Stimmprofil – besonders, wenn die Authentifizierung fehlgeschlagen ist
- Zeit, Ort, ANI/CLI, Gerät und andere deutliche Muster, die zu einem bestimmten Stimmprofil passen

Diese Methoden bieten Betrugsuntersuchungsteams völlig neue Möglichkeiten, die Geschwindigkeit und die Qualität ihrer Ermittlungen zu verbessern und mit der stetigen Zunahme der Angriffe auf Sprachkanäle Schritt zu halten.

Abbildung 2: Neue Methoden zur umfassenden Betrugsverhinderung

Quelle: NICE Systems Ltd

Historische Aufzeichnungen: Eine Fundgrube wertvoller Identifizierungsdaten

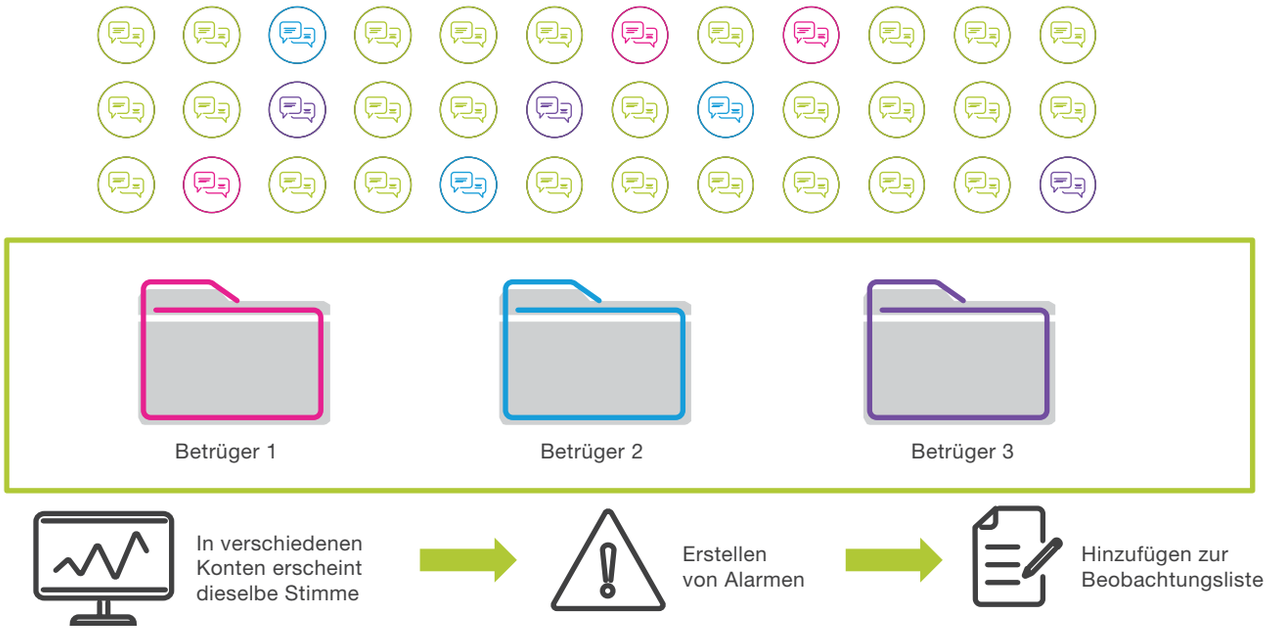
Neben dem Gesprächsinhalt selbst enthalten Sprachaufzeichnungen wertvolle Informationen zur Identität des Anrufers. Diese können zur Erkennung unterschiedlicher verdächtiger Verhaltensweisen verwendet werden:

- Prüfung, ob an einem Anruf mehr als ein Anrufer teilnimmt
- Identifizierung des Anrufers aus einer bekannten Gruppe (z. B. Familienkonten, Geschäftspartner und andere „im Auftrag von“-Szenarien)
- Vergleich identifizierter Stimmen mit registrierten „Voiceprints“
- Erkennen von „Bot“-Aktivitäten und anderen Versuchen zur Verschleierung von Stimmen durch Audiosynthese

Da die meisten Betrugsversuche von einer relativ kleinen Gruppe von Kriminellen verübt werden, besteht die Herausforderung darin, diese Personen in einer riesigen Menge von Datenquellen, Inputs und genialen Methoden zur Verschleierung ihrer Aktivitäten und Identitäten zu identifizieren. Wenn sich die Geschichte tatsächlich wiederholt, dann gilt dies auch für Betrüger, die ein Contact Center anrufen – Unabhängig davon, ob es sich um einen sich wiederholten Angriff, „roher Gewalt“ auf ein einzelnes Konto, oder um die systematische Sammlung von Informationen aus mehreren Konten durch „Vishing“ handelt.

Durch die Analyse einer Vielzahl solcher Aufzeichnungen und die kontinuierliche Optimierung, um größere Präzision zu erzielen, sowie die ständige Ergänzung zusätzlicher Verhaltens-, Transaktions- und Authentifizierungsdaten konnten bahnbrechende Ergebnisse bei der Identifizierung bekannter Krimineller und der Erkennung bislang unvermuteter betrügerischer Aktivitäten erzielt werden.

Abbildung 3: Proaktive Erkennung von Betrügern durch die Auswahl von Anrufen mit hohem Risiko



Quelle: NICE Systems Ltd

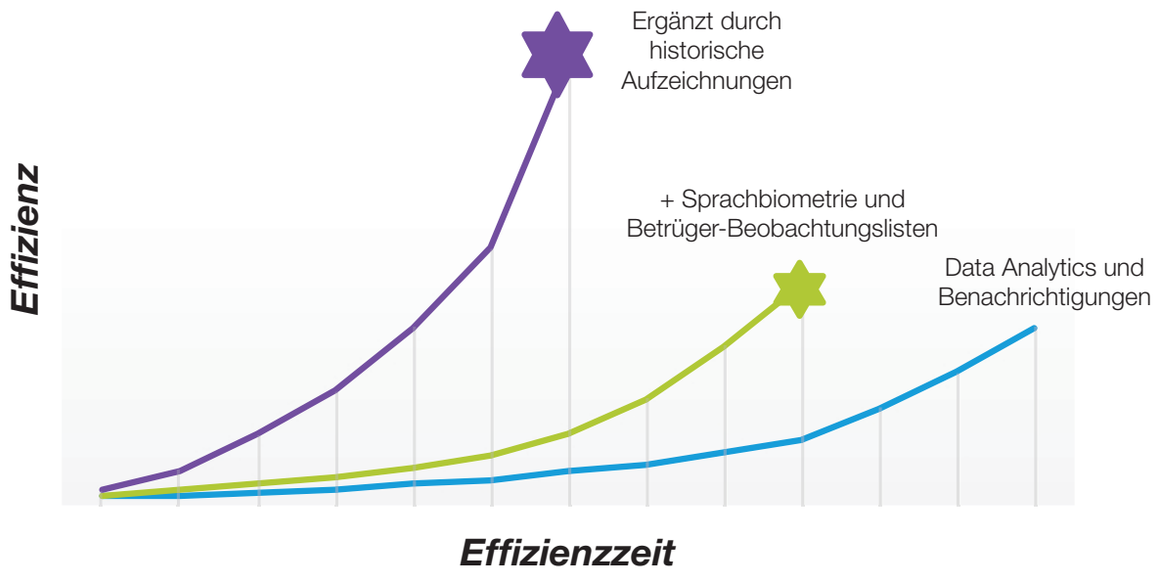
Die Automatisierung dieses Prozesses ermöglicht Unternehmen, mit der Zunahme von Betrügen in Contact Centern Schritt zu halten, und zwar nicht nur zum Zeitpunkt des Angriffs selbst, sondern auch während der zahlreichen Anrufe, die dem eigentlichen Angriff vorangehen. Die Möglichkeit zur Nutzung historischer Aufzeichnungen liefert äußerst schnell positive Ergebnisse, da dies inkrementelle Verfahren, die auf den organischen Eingang von Anrufen und der anschließenden manuellen Analyse basieren, außen vor lässt.

Exponentielle Effizienz mithilfe von Sprachbiometrie über Betrugserkennung bis hin zur Betrugsverhinderung

Die sprach- und stimmbasierte Betrugserkennung ist der Ausgangspunkt für eine nachhaltige Betrugsverhinderung. Im Rahmen der „3. Faktor – Biometrie"-Familie von Authentifizierungsverfahren können Sprachbiometrie und Betrugserkennung dazu genutzt werden, die tatsächliche Person hinter der Stimme zu identifizieren – anders als bei den meisten anderen Verfahren, die lediglich den Abgleich von Daten erlauben. Wie bereits erwähnt, werden die meisten Betrugsangriffe von einer relativ kleinen Zahl von Kriminellen durchgeführt, die, sobald sie erkannt wurden, den Sprachkanal nicht erneut angreifen können; dies nimmt Täter „aus dem Spiel" und schafft so eine Grundlage für eine nachhaltige Betrugsverhinderung.

Die Verbesserung des Umfangs und der Qualität von Stimm-Beobachtungslisten von Betrügern ermöglicht daher exponentielle Vorteile der Effizienz und Zeit.

Abbildung 4: Kürzere Effizienzzeiten dank historischer Aufzeichnungen



Im Rahmen des Kampfes gegen ausgeklügelte betrügerische Angriffe ist die Erstellung hochwertiger Beobachtungslisten von Betrügern auf der Grundlage historischer Aufzeichnungen nicht nur ein sehr effektives Verteidigungsmittel, sondern auch eine verbesserte Möglichkeit, Betrüger strafrechtlich zu verfolgen. Solchen Angreifern das Handwerk legen zu können ist eine echte Revolution für den Kampf gegen Betrug.

Über Opus Research

Opus Research ist ein diversifiziertes Beratungs- und Analyseunternehmen, das wichtige Einblicke in Software und Services zur Unterstützung multimodaler Kundendienste ermöglicht. Opus Research konzentriert sich auf „Conversational Commerce“, die Zusammenführung intelligenter Assistententechnologien, von Conversational Intelligence, intelligenter Authentifizierung, Unternehmenszusammenarbeit und Digital Commerce.

Wenden Sie sich für Vertriebsanfragen bitte per E-Mail an info@opusresearch.net oder telefonisch an +1(415) 904-7666