NUANCE | WHAT'S NEXT BLOG

Kundeninteraktion auf allen Kanälen, Verifizierung und Betrugsprävention

Das goldene Zeitalter der Betrugsprävention

Brett Beranek | Vice President & General Manager, Security & Biometrics

7 Mai 2020

Das Jahr 2020 wurde als ein neues Jahrzehnt mit neuen Anfängen und neuen Möglichkeiten für Technologien eingeläutet. Es hat mit COVID-19 natürlich nicht ganz so begonnen, wie es viele von uns vorhergesagt hätten.

Das Jahr 2020 wurde als ein neues Jahrzehnt mit neuen Anfängen und neuen Möglichkeiten für Technologien eingeläutet. Es hat mit COVID-19 natürlich nicht ganz so begonnen, wie es viele von uns vorhergesagt hätten und hat massive Auswirkungen auf unser aller Gesundheit, Jobs und die globale Wirtschaft mit sich gebracht.

Die Ausbreitung des Coronavirus hat bei vielen zu einer erhöhten Unsicherheit geführt. Viele von uns werden womöglich ihre Banken anrufen, um zu prüfen, ob Zahlungen korrekt ausgeführt worden sind und sich beruhigen lassen, dass alles glatt gelaufen ist. Einige werden sich in ihre Arbeit stürzen, um produktiv zu bleiben und das Gefühl des Fortschritts aufrechtzuerhalten. Andere wiederum werden vielleicht sogar von den Nachrichten und dem Tagesgeschehen "abschalten" wollen, indem sie sich mit Netflix ablenken.

Während sich momentan alles um das Thema COVID-19 dreht, setzen Betrüger und Kriminelle beinahe unbemerkt immer raffiniertere Methoden ein, um Zugang zu sensiblen Daten und Informationen zu erhalten. Von E-Mail-Phishing und gefälschten Websites – Betrüger machen sich während der Epidemie Schwachstellen von Verbrauchern und Unternehmen zunutze.

Wir haben in den letzten Wochen tatsächlich einen deutlichen Anstieg von Betrugsfällen beobachtet – je nach Branche zwischen 200 Prozent und 400 Prozent. Einige davon stehen in direktem Zusammenhang mit der Pandemie, wobei jüngste Berichte vermuten lassen, dass es bisher Hunderte von Betrugsversuchen im Zusammenhang mit COVID-19 und Tausende von Phishing-Versuchen gegeben hat. Dies sind Zahlen, die mit der Zeit nur zunehmen werden.

Schwachstelle: traditionelle Authentifizierungsmethoden

In diesen schwierigen Zeiten und darüber hinaus ist es umso wichtiger, Kunden die Gewissheit bieten zu können, dass Ihr Unternehmen alles tut, um sie vor betrügerischen Aktivitäten zu schützen - Authentifizierung spielt dabei eine Schlüsselrolle. Der Duden definiert Authentifizierung als „beglaubigen; die Echtheit bezeugen".

Bisher haben wir uns traditionsgemäß auf wissensbasierte Identifikationsmittel verlassen, um zu beweisen, dass wir der sind, für den wir uns ausgeben – zum Beispiel durch die Verwendung von Namen und Adressen, Passwörtern oder PINs oder mit dem „Mädchennamens unserer Mutter".

Während der aktuellen Pandemie sind Verbraucher mit schwachen Zugangsdaten leichte Beute für Betrüger. Daten können leicht über E-Mail,Telefon oder SMS durch sogennante Phishing-Attacken abgegriffen werden. Diese Infos können Kriminelle dazu nutzen, um sich Zugang zu Bankkonten zu verschaffen.

"One-Time-Passwords" (OTP), die per SMS verschickt werden, vermitteln ein falsches Sicherheitsgefühl und sind kein wirksames Mittel, um Identitätsklau zu betreiben oder einen nicht erlaubten Zugang zu Bankkonten zu verhindern. Wenn Kriminielle genügend Informationen über eine Person haben, um sein Bankkonto zu knacken, dann hat er auch sicherhlich auch genug Informationen, um Handy zu hacken und so gesendete SMS abzufangen.

Im vergangenen Jahr, noch vor dem Ausbruch des Coronavirus, kosteten betrügerische Aktivitäten der Weltwirtschaft rund 5 Billionen US-Dollar. Laut einer von Nuance durchgeführten Umfrage, gaben rund ein Viertel (24 Prozent) der befragten Personen an, in den vergangenen zwölf Monaten Opfer von Betrug gewesen zu sein und durchschnittlich 2.000 US-Dollar aufgrund von geknackten Passwörtern verloren zu haben. Diese Zahl wird angesichts des Umfangs der betrügerischen Aktivitäten im Zusammenhang mit dem Coronavirus wahrscheinlich noch weiter steigen.

Dabei treffen Verluste durch Betrugsaktivitäten nicht nur den Verbraucher selbst, sondern die jeweiligen Anbieter, die eine Schwachstelle hatten. Zwei Drittel (62 Prozent) der Verbraucher gaben, an, dass sie den Anbieter wechseln würden, wenn sie durch Nutzung derer Services Betrügern zum Opfer fielen würden.

Biometrie für Sicherheit

Biometrie könnte die Antwort für Organisationen sein, die Betrüger und Kriminelle in Schach halten und die Sicherheit sowohl ihrer Kunden von Contact-Centern als auch ihrer Mitarbeiter während COVID-19 und darüber hinaus gewährleisten wollen.

Eine leistungsfähige und effektive Alternative zu Passwörtern und PINs, beispielsweise Stimmbiometrie, lässt sich nicht mit wissensbasierten Sicherheitsmethoden vergleichen. Das liegt daran, dass die menschliche Stimme so einzigartig ist wie ein Fingerabdruck. Durch den Einsatz ausgeklügelter Algorithmen zur Analyse von mehr als 1.000 Stimmmerkmalen nutzt die Stimmbiometrie-Technologie, die Stimme eines Anrufers nicht nur zur Überprüfung seiner Identität, sondern auch zum Schutz vor Hackern. OTP als Authentifizierungsmethode kann effizient sein, wenn sie mit Biometrie und Push-Benachrichtigungen gepaart wird.

Ein weiterer Schutz, der über Stimmbiometrie hinausläuft ist Verhaltensbiometrie. Diese Technologie misst, wie eine Person mit einem Gerät interagiert – wie sie schreibt, wie sie tippt, wie sie tippt und wie sie das Telefon durchzieht oder sogar hält -, um festzustellen, ob sie die Person ist, für die sie sich ausgibt.Wenn Biometrie gepaart mit anderen Methoden, wie beispielsweise Multi-Faktor-Authentifizierung, End-to-End-Verschlüsselung und Public-Key-Infrastruktur eingesetzt wird, kann sie zu einem effizienten Tool gegen betrügerische Aktivitäten eingesetzt werden.

Das goldene Zeitalter der Authentifizierung?

Biometrie könnte gerade jetzt eine immer größere Rolle für Unternehmen spielen. Die Nachfragen in Contact-Centern steigt, da Kunden mehr Service und Kontakt zu Unternehmen verlangen. Mitarbeitern, die nun gezwungen sind von zu Hause aus zu arbeiten, müssen sich gleichzeitig vielen Herausforderungen stellen: einen hervorragenden Kundendienst gewährleisten und gleichzeitig die richtigen Personen authentifizieren, um Betrug auszuschließen. Mitarbeitern in Contact-Centern, die biometrische Technologien zur Authentifizierung einsetzen, sparen Zeit und können sich auf ihre eigentliche Aufgabe konzentrieren – die Kundenbetreuung.

Die heutigen Umstände zwingen Unternehmen außergewöhnliche Maßnahmen zu ergreifen, um ihre Arbeitskräfte auch von zu Hause arbeiten zu lassen, neue Arbeitsweisen zuzulassen und in einigen Fällen auch Geschäftsmodelle neu zu überdenken. Jetzt ist der beste Zeitpunkt, über Authentifizierungsmethoden in Unternehmen nachzudenken, die Verbrauchern und Unternehmen vor betrügerischen Aktivitäten schützt. Ungewissheit zwingt oft zu Innovationen. Wenn diese Innovation dazu beiträgt, Kunden vor Betrügern zu schützen, haben wir zumindest einen Schritt nach vorn getan, um eine wachsende Bedrohung in dieser schwierigen Zeit zu verringern.

Tags: Betrugsprävention, Sprachbiometrie, Contact center strategie, Biometrische Authentifizierung

About Brett Beranek

Brett Beranek is responsible for overseeing every aspect of the security and biometric business at Nuance. Prior to joining Nuance, he has held over the past decade various business development & marketing positions within the enterprise B2B security software space. Beranek has extensive experience with biometric technologies, in particular in his role as a founding partner of Viion Systems, a startup focused on developing facial recognition software solutions for the enterprise market. Beranek also has in-depth experience with a wide range of other security technologies, including fingerprint biometrics, video analytics for the physical security space and license plate recognition technology. He has earned a Bachelor of Commerce, Information Systems Major, from McGill University as well as an Executive Marketing certificate from Massachusetts Institute of Technology's Sloan School of Management.

View all posts by Brett Beranek