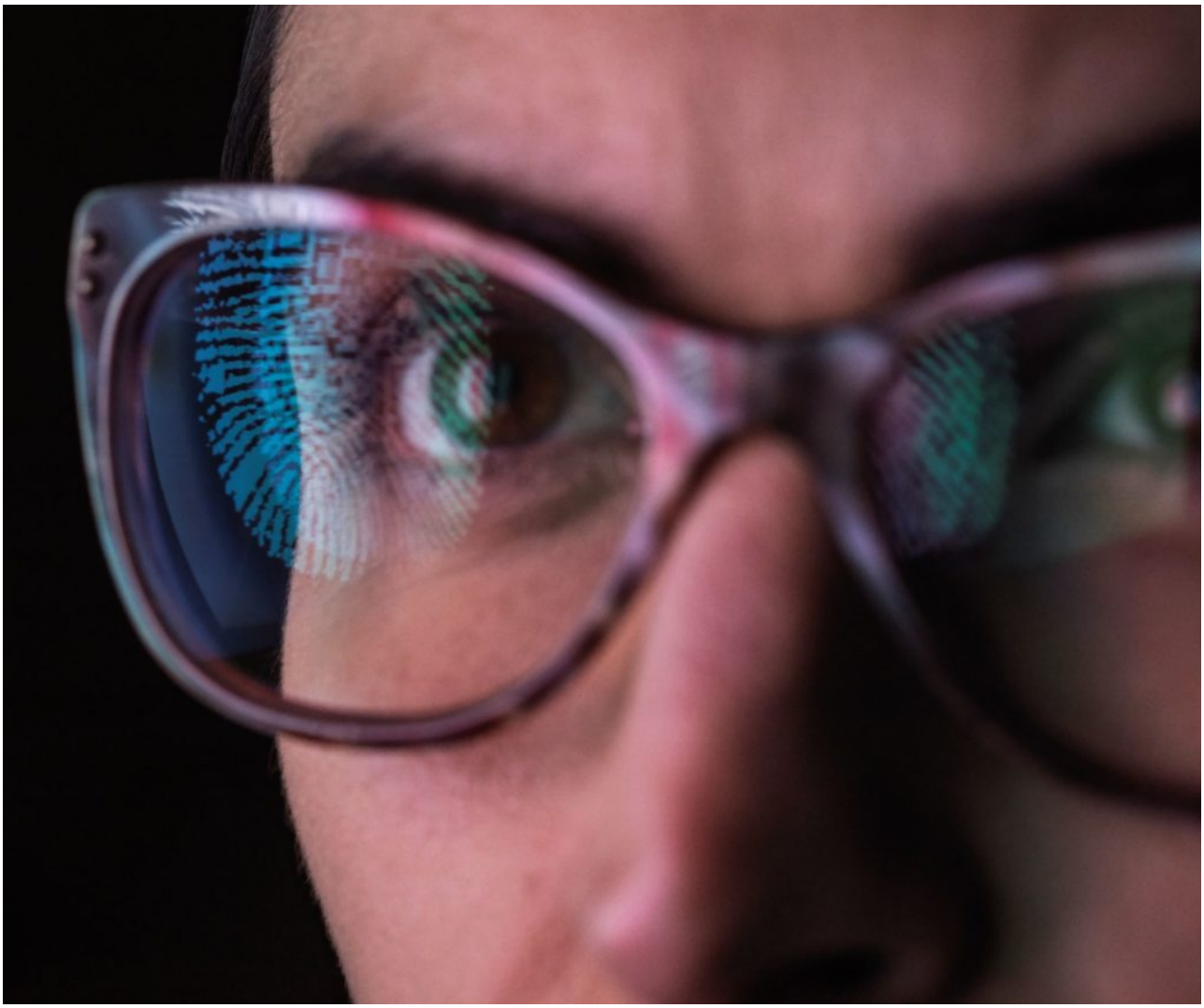
What's next

Enterprise

Digitale Sicherheitstrends für 2021

Jedes Jahr werden unzählige Technologienutzer im Internet zu Kriminalitäts- und Betrugsopfern. In Zeiten der COVID-19 Pandemie steigen die Fallzahlen von Cyberkriminalität stetig an, da Interaktionen, wie Online-Banking und -Shopping, in einem Ausmaß wie noch nie zuvor genutzt werden. Vor diesem Hintergrund stellen wir unsere wichtigsten Prognosen für die Cybersicherheit im Jahr 2021.

Brett Beranek
Posted 6 Januar 2021



Von Cybersicherheit über Betrugsprävention bis hin zum Risikomanagement: Hier eine Zusammenfassung der wichtigstendigitalen Sicherheitstrends

Sicherheit durch passwortfreie Authentifizierung

Vorausschauende CISOs werden ihre Systeme, im Sinne der Bedienerfreundlichkeit für Kunden und Sicherheit für Unternehmen, auf eine passwortfreie Authentifizierung umstellen. Verbraucher wünschen eine digitale Erfahrung, die einfach, sicher und passwortfrei ist. Tägliche Passwörter und PINs (z.B. E-Mail, Geldautomaten) sind fast schon Relikte aus grauer Vorzeit. Da Verbraucher vermehrt Online-Kanäle für ihre Bankgeschäfte, sozialen Kontakte, Spiele und Einkäufe nutzen, wächst auf der Sicherheitsebene der Bedarf an technisch ausgefeilten, sicheren Systemen. Passwörter wiegen Verbraucher seit Jahren in einem trügerischen Gefühl der Sicherheit. Insbesondere angesichts des drastischen Anstiegs der Geräteanzahl und Vielfältigkeit für die Nutzung von Apps. All diese Geräte benötigen für eine

dauerhafte Nutzung sensible Daten und sind ständig der Gefahr ausgesetzt, dass diese Daten verfolgt und gestohlen werden. Unternehmen müssen ihren Kunden nachweisen, dass sie deren Sicherheit ernst nehmen. Verbraucher sind sich mittlerweile der Gefahren rund um ihre Identität wesentlich bewusster als zuvor. Daher steigen auch ihre Anforderungen an die Unternehmen, mit denen sie geschäftlich verbunden sind. Unternehmen können sich ein ausschließlich renditeorientiertes Handeln nicht länger leisten. Mittlerweile ist größere Sicherheit ein wesentliches Kriterium für Kundenbindung, Kundentreue und eine sozialverantwortliche Unternehmensführung.

Zusammenspiel von Betrugsprävention und Authentifizierung

Ein integrierter Ansatz für Betrugsprävention und Authentifizierung wird der Schlüssel für den Schutz vor einer schwachen gerätebasierten Biometrie sein. Kunden werden Sicherheitsprotokolle fordern, die ihre tatsächliche Person identifizieren statt jemanden, der eventuell ihre Identität vorgibt. Wir erkennen eine deutliche Abwendung von einer Technologie, die nicht die tatsächliche, mit dem Sicherheitssystem interagierende Person identifiziert. Eine Authentifizierung beispielsweise durch Passwörter, PINs oder SMS-Bestätigungen ist nicht mehr ausreichend. Diese Daten lassen sich zu einfach beschaffen. Biometrische Verfahren, wie Sprach- oder Verhaltenserkennung, Fingerabdrücke und Iris-Scans sind für eine sichere Online-Präsenz unverzichtbar. Aufgrund ihres jahrelangen Umgangs mit smarten Geräten sind Kunden häufig bereits vertraut mit einer Identifizierung durch Fingerabdruck oder Gesichtserkennung. Leider bieten die meisten dieser gerätebasierten biometrischen Verfahren der Authentifizierung keinen wirksamen Schutz vor Betrügern. Erstens ist die Feststellung schwierig, wer den biometrischen Abdruck erstellt hat, und zweitens sind diese Abdrücke auf ein bestimmtes Gerät beschränkt. Dadurch lassen sie sich nicht über mehrere Kanäle nutzen oder von einem Gerät in ein anderes übertragen. Ihr „Wert“ steht und fällt mit ihrer Kostenfreiheit. Es ist die serverbasierte Biometrie, wie beispielsweise die Stimmbiometrie, die sowohl eine signifikante Betrugsprävention als auch reibungslose, bedienerfreundliche Kundenerfahrungen zum Ergebnis hat.

Der Kunde ist König dank hochentwickelter KI

Hochentwickelte Künstliche Intelligenz wird biometrischen Verfahren ermöglichen, die immer komplexeren Sicherheitsprobleme zu lösen. Anfang des Jahres hat die Telefónica, S.A., ein multinationales spanisches Telekommunikationsunternehmen und einer der weltweit größten Netzanbieter, Nuance damit beauftragt, mit der Stimmbiometrie anhand des Klangs der Stimmen von Kunden zu analysieren, ob diese 65 Jahre oder älter sind. Diese wichtige Feststellung unterstützt das Unternehmen darin, einer Altersgruppe, die höchst anfällig für Betrugsversuche ist, einen hochwirksamen Betrugsschutz zu bieten.

Die Ausrüstung mit hoch entwickelten Technologien ermöglicht Unternehmen durch zusätzlich zu erwägende biometrische Faktoren nicht nur die Priorisierung oder Adaption von Diensten für spezifische Kundengruppen, sondern auch die Verstärkung von Maßnahmen zur Betrugsprävention.

Der Kundendienst wird eine drastische Umstellung auf Video-/virtuelle Einrichtungen erfahren. Wenn virtuelle Konsultationen, Transaktionen und Interaktionen zwischen Marken und Verbrauchern zur Norm werden, müssen digitale Kanäle so sicher und bequem sein, als würden diese Interaktionen mit einem tatsächlichen Personenkontakt stattfinden. Kundendienst per Video ist ein Trend, der sich als eine Folge von COVID-19 abzeichnet, die Stimmbiometrie ist ein unverzichtbarer Faktor der Authentifizierung und Wahrung der Kundensicherheit.

Ein Beispiel: Angesichts des hohen Anstiegs von virtuellen Transaktionen hat die IBK (Industrial Bank of Korea), zur Sicherstellung einer robusten, technisch ausgereiften Kundenauthentifizierung, die Technologie der Stimmbiometrie von Nuance implementiert. Mit einer Bewertungseinheitlichkeit von 100 % hat die IBK die Erfahrungen mit dem Online-Banking revolutioniert.

Sicherheit im Homeoffice

Sicherheitsbeauftragte brauchen aufgrund einer vermehrten Verlagerung der Arbeit in ein Homeoffice, einen langen Arm für den Schutz vor einem Anstieg von Betrugsversuchen. Da Unternehmen die Arbeit ihrer Mitarbeiter auf unbestimmte Zeit ins Homeoffice verlegen, eine Maßnahme, die der „Harvard Business Review“ in seiner aktuellen Ausgabe (Nov./Dez. 2020) mit „The Work From Anywhere Future“ betitelt, werden Betrugsversuche gegen Telearbeiter und Frontline-Agents zunehmen. Telearbeit bietet aber auch selbst ein Potenzial für Betrug am Arbeitsplatz. Unbeaufsichtigten Mitarbeitern mit Zugriff auf persönlich identifizierende Daten (PII) eröffnet sich die neue Möglichkeit, ihre Arbeitgeber zu hintergehen und wertvolle Informationen zu stehlen. Unter dem zunehmenden Druck, den gesellschaftlich und wirtschaftlich schwierige Zeiten mit sich bringen, entstehen die richtigen Bedingungen für einen Anstieg der Betrugsversuche am Arbeitsplatz. Forrester Research bestätigt diese Annahme mit der Prognose, dass von internen Handlungen verursachte Datenlecks von aktuell 25 % auf 33 % ansteigen werden. Damit Unternehmen weltweit nahtlos mit Mitarbeitern interagieren können, müssen sie schnell mit Maßnahmen gegen Stimmfälschungen (wie durch ein extrem realistisches Speach-Cloning oder die Deep-Voices-Methode, die Künstliche Intelligenz für eine Stimmfälschung auf der Grundlage von Sprache, Akzenten und Tönen nutzt) reagieren. Herkömmliche Sicherheitsmaßnahmen müssen angesichts vieler außerhalb der Firewall eines Unternehmens tätigen Mitarbeiter ebenfalls auf höchstem Leistungsniveau funktionieren.

Das Jahr 2021 wird im Zeichen einer größeren digitalen Sicherheit und Sorgenfreiheit stehen. Traditionelle Handlungsweisen, selbst wenn sie so rudimentär und fundamental sind, wie das Online-Passwort, sind nicht länger ausreichend. Biometrische Sicherheitssysteme, die auf verifizierbaren Merkmalen basieren, wie Iris-Scans, Fingerabdrücken und Sprachmustern, werden subjektive Codes, die viel zu leicht gestohlen und missbraucht werden können, ersetzen. Unternehmen, die diese Systeme implementieren, werden einen reibungslosen Übergang in eine sichere digitale Gegenwart schaffen.

Tags: Biometrie, digitale Sicherheit, digitales Engagement, KI, Kundenerfahrung, Stimmauthentifizierung

More Information

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