NUANCE

Beheben Sie die Schwachstellen der Zwei-Faktor-Authentifizierung.

Wußten Sie, dass per SMS versandte Einmalpasswörter Ihre Kunden gefährden?

E-Book
Nuance Gatekeeper

SMS sind nicht sicher

Viele Unternehmen setzen zur Authentifizierung bei Banking- und E-Commerce-Transaktionen auf Zwei-Faktor-Authentifizierung (2FA) mit Einmalpasswörtern (One-Time Passcodes, OTPs), die per Short Message Service (SMS) versandt werden. Diese Art der 2FA ist schnell und unkompliziert, aber SMS waren nie als Sicherheitstool gedacht. Beim Versenden von OTPs per SMS wird davon ausgegangen, dass es sich beim Empfänger um den Kontoinhaber handelt – was jedoch nicht gewährleistet ist.

Betrüger nutzen die Schwachstellen von SMS auf verschiedene Weisen aus: Sie können persönliche Kundendaten einfach im Dark Web kaufen und damit Kontoübernahmen veranlassen, um SMS mit OTPs abzufangen. Betrüger verschaffen sich zudem mit zielgerichteten Malware-Bots Zugriff auf Kundengeräte, stehlen ihre Daten und fangen OTPs sowie Authentifizierungscodes ab.

Betrugstaktiken wie diese nutzen die SMS-basierte 2FA aus. Dazu zählen auch SIM-Swapping und Portierungs-Maschen, bei denen Betrüger sich als Kunden ausgeben, um deren Nachrichten an eine von ihnen kontrollierte Telefonnummer weiterzuleiten. Diese Methoden machen Schlagzeilen und Behörden greifen ein. In den USA z. B. übt die Federal Communications Commission (FCC) Druck auf Telekommunikationsanbieter aus, die den Austausch von SIM-Karten verhindern sollen, wenn der Netzbetreiber nicht über eine sichere Authentifizierungsmethode verfügt.

Die Schwachstellen von SMS sind allerdings nicht nur für Telekommunikationsanbieter problematisch. Sie betreffen jedes Unternehmen, das auf SMS-basierte 2FA setzt.

Schnell handeln und Vertrauen gewinnen

Kund*innen erwarten von Ihnen Sicherheit. Die Unternehmen mit dem besten Schutz ernten das höchste Vertrauen und die stärkste Kundenbindung.

Betrüger stehen nicht still, wie an der raschen Ausbreitung von Banking-Trojanern zu erkennen ist. Diese Malware-Bots infizieren die Geräte ihrer Opfer und verschaffen sich Zugriff auf all ihre persönlichen Daten, Kreditkarten und Banking-Apps. Die Verbreitung von FluBot, TeaBot und jüngst SharkBot zeigt, dass Cyberkriminelle einen neuen Weg gefunden haben, die Schwachstellen von SMS-OTPs auszunutzen.

Unternehmen müssen ihre Sicherheitsmaßnahmen schnell aktualisieren, um diese Bedrohungen abzuwehren und das Vertrauen ihrer Kund*innen zurückzugewinnen. Zunächst gilt es zu verstehen, wie Betrüger SMS-basierte 2FA ausnutzen und warum besitzbasierte Authentifizierung an sich riskant sein kann.

Die Authentifizierung per Handy und SMS ist unzuverlässig und unsicher

12% der Kund*innen wurden kürzlich Opfer von Handy- oder Mobilfunkbetrug

19% der SMS-basierten Kontowiederherstellungen schlagen fehl[1]

37% der gesamten erfolgreichen Betrugsversuche erfolgten möglicherweise durch die Offenlegung von OTPs[2]

1 Quelle: Gemeinsame Studie von Stanford und Google, aus dem Jahr 2015, aber nach wie vor relevant.
2 Quelle: Pressemeldung der HSBC UK, 15. September 2021: https://www.about.hsbc.co.uk/news-and-media/hsbc-uk-issues-customer-warning-as-one-time-passcode-fraud-increases

Die Facetten des Betrugs per SMS-2FA

In den letzten Jahren wurde immer offensichtlicher, dass SMS-OTPs ein großes Betrugsrisiko darstellen. HSBC, eine der größten Banken in Großbritannien, warnte vor Betrügern, die Kunden dazu brachten, ihre OTPs am Telefon preiszugeben. Die Bank gab an, innerhalb von sechs Monaten über 3.000 erfolgreiche OTP-Betrugsfälle verzeichnet zu haben.

Passwort-Phishing ist jedoch nur eine der diversen Methoden, mit denen Betrüger die inhärenten Schwachstellen von SMS ausnutzen. Zu den anderen gängigen Betrugsmaschen zählen:

— **SIM-Swapping:** Betrüger geben sich als Kunden aus und bitten um die Portierung einer Handynummer auf ein neues Gerät in ihrem Besitz, sodass sie alle eingehenden Anrufe und Nachrichten erhalten.

— **Portierungsbetrug:** Betrüger erstellen mit gestohlenen Kundendaten ein Konto bei einem anderen Anbieter und lassen die Handynummer des Opfers auf ein Gerät beim neuen Anbieter übertragen.

— **Rufumleitungen:** Betrüger geben sich als Kunden aus und behaupten, ihr legitimes Gerät verloren oder beschädigt zu haben. Sie bitten dann um die Umleitung aller Anrufe und Nachrichten auf eine andere Nummer.

— **Whaling:** Ein Betrüger gibt sich als Mitarbeiter aus der Abteilung für Betrugsprävention aus und bittet das Opfer, eine nicht legitime Transaktion zu bestätigen. Der Betrüger erzählt dem Opfer, dass es zum Abschluss der Transaktion einen Sicherheitscode per SMS erhält, und leitet dann den Vorgang zum Zurücksetzen des Passworts ein. Dadurch erhält das Opfer ein OTP per SMS, das es sodann dem Betrüger vorlesen soll.

— **Malware:** Betrüger überzeugen Opfer durch Phishing oder Social Engineering, Malware wie FluBot, TeaBot oder SharkBot auf ihre Geräte herunterzuladen. Diese Malware gewährt den Betrügern Zugriff auf die Kreditkartendaten und persönlichen Informationen der Opfer sowie die Möglichkeit, ihre SMS abzufangen.

Betrug auf dem Vormarsch am Beispiel USA

47% der Erwachsenen sind in den letzten zwei Jahren Opfer von Identitätsdiebstahl geworden[3]

57% der Unternehmen verzeichneten steigende Verluste durch Betrug im Zusammenhang mit Kontoübernahmen und -eröffnungen im Jahr 2020[4]

712,4 Mrd. $ Verlust durch Identitätsdiebstahl in 2020, 42 % mehr als im Vorjahr[5]

3 Quelle: Aite Group, U.S. Identity Theft: The Stark Reality, March 2021
4 Quelle: Experian 2020 Global Identity and Fraud Report
5 Quelle: Aite Group, U.S. Identity Theft: The Stark Reality, March 2021

Die verheerenden Folgen von Betrug
2016 verlor Tech-Investor Bob Ross eines Freitagabends ca. 1 Mio. Dollar in nur einer Stunde und das Leben seiner Familie veränderte sich für immer. Der Grund? SIM-Swapping. Erfahren Sie, wie ein gebildeter, technikaffiner Mensch zum Betrugsopfer wurde, und warum er sich für Stimmbiometrie als Standardoption für 2FA einsetzt.

Hören Sie hier seine Geschichte.

Zeit für eine neue biometrische 2FA

Die Identitätsprüfung über OTPs, die an Kundengeräte gesendet werden, ist grundsätzlich unzuverlässig und unsicher. Stattdessen stellen immer mehr Unternehmen auf Biometrie als Identitätsnachweis um.

Bei der Biometrie werden Personen anhand einzigartiger menschlicher Merkmale authentifiziert. Biometrie als zweiter Authentifizierungsfaktor ist schneller, sicherer und praktischer als wissensbasierte Authentifizierung (Knowledge-Based Authentication, KBA, also mit Passwörtern oder Sicherheitsfragen) oder besitzbasierte Authentifizierung (z. B. mit SMS-OTPs). Allerdings bieten nicht alle biometrischen Verfahren dasselbe Maß an Komfort oder Sicherheit.

Gesichtserkennung und Fingerabdruckleser erfreuen sich großer Beliebtheit bei Kund*innen, haben jedoch kritische Einschränkungen: Sie binden Kunden an einzelne Geräte und müssen bei einem Wechsel (oder Diebstahl) immer neu konfiguriert werden. Zudem lassen sich diese Methoden oft von Betrügern aushebeln oder umgehen.

Stimmbiometrie hingegen eignet sich ideal für Step-up- und Zwei-Faktor-Authentifizierung, selbst über digitale Kanäle. Diese Systeme authentifizieren legitime Kund*innen und erkennen Betrüger anhand des einzigartigen „Stimmabdrucks“ einer Person. Kund*innen sind somit nicht mehr von KBA abhängig und können sich mühelos und sicher authentifizieren, unabhängig vom genutzten Gerät oder Kanal.

Viele Unternehmen setzen zudem auf Verhaltensbiometrie, um Kund*innen fortlaufend zu authentifizieren und Betrug in digitalen Kanälen zu erkennen. Diese Lösungen arbeiten passiv im Hintergrund und analysieren, wie Nutzer mit ihren Geräten interagieren, um ungewöhnliches oder betrügerisches Verhalten schnell zu erkennen.

Die Wahl der passenden Biometrielösung

Unabhängig davon, welche biometrischen Verfahren Sie nutzen: Denken Sie daran, dass nicht jeder Lösungsanbieter Ihren Anforderungen gerecht wird. Bei der Auswahl einer Lösung für biometrische Authentifizierung stellen Sie potenziellen Technologiepartnern folgende wichtige Fragen:

- Wie verfahren Sie mit Einwilligung und Compliance bezüglich der Erfassung, Speicherung und Verarbeitung biometrischer Daten?
- Können Sie Referenzen nennen, die Sie unterstützen, und können wir diese sprechen?
- Wie oft veröffentlichen Sie neue Algorithmen?
- Haben Sie Erfahrung mit Deepfakes?
- Bieten Sie mehrere biometrische Verfahren, um Kund*innen über Sprach- und digitale Kanäle hinweg zu authentifizieren?
- Wie einfach lassen sich Ihre Lösungen in unsere bestehende Customer-Engagement-Infrastruktur integrieren?
- Bieten Sie flexible Bereitstellungsoptionen, einschließlich Edge-Bereitstellungen?

„Betrüger suchen immer nach dem schwächsten Glied der Sicherheitskette. Oft ist es die 2FA per SMS. Stimmbiometrie nimmt Betrügern den Wind aus den Segeln und schließt Sicherheitslücken der wissensbasierten Authentifizierung, auf die sie sich für ihre Machenschaften verlassen.“

— Simon Marchand, CFE, Chief Fraud Prevention Officer, Nuance

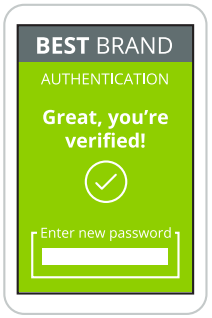
Mehrschichtige Sicherheit

1

Führen Kund*innen risikoreiche Aktionen wie das Zurücksetzen von Passwörtern oder den Wechsel bzw. die Portierung einer Handynummer durch, fordern Sie sie zur Authentifizierung mit ihrer Stimme auf, anstatt Einmal-Passwörter zu versenden.

Eine KI-gestützte Risiko-Engine analysiert die biometrischen Merkmale ihrer Stimme und untersucht das Gerät, Verhalten und andere Faktoren auf Anzeichen von Betrug.

2



3

Das System authentifiziert Kund*innen innerhalb von Sekunden und gibt das OK oder meldet einen vermeintlichen oder bekannten Betrüger an die Abteilung für Betrugsprävention.

Eine effektive Lösung zur Authentifizierung und Betrugserkennung sollte einen mehrschichtigen, ganzheitlichen Ansatz verfolgen. Es gibt kein Allheilmittel für jedes Authentifizierungs- und Betrugsproblem auf jedem Kanal und viele Lösungen sind auf bestimmte Kanäle beschränkt, greifen also nur an bestimmten Punkten der Customer Journey. Die derzeit fortschrittlichsten Lösungen vereinen Stimm-, Verhaltens- und Sprachbiometrie mit verschiedenen nicht-biometrischen Faktoren wie der Validierung von Anrufen und Umfelderkennung zu einer zentralen KI-gestützten Risiko-Engine.

Mit einer einheitlichen, kanalübergreifenden Lösung können Unternehmen sämtliche Interaktionen von Kunden und Mitarbeitenden optimieren und schützen, egal wann, wo und wie der Kontakt erfolgt.

Der echte Effekt von biometrischer 2FA

90% erkannte Betrugsversuche

99% erfolgreiche Authentifizierungen

92% Reduzierung der Betrugsverluste

* Statistiken von Nuance-Kunden

Seien Sie Betrügern einen Schritt voraus

Die problematischen Schwachstellen der 2FA per SMS sind seit Jahren bekannt und Betrüger sind erfinderisch dabei, sie auf immer neue Weisen auszunutzen. Banking-Trojaner wie SharkBot haben derzeit hauptsächlich europäische Banken im Visier, aber erfolgreiche Betrugsmaschen verbreiten sich bekanntermaßen schnell auf der ganzen Welt.

Zögern Sie also nicht und riskieren Sie damit, dass Kund*innen zur Konkurrenz wechseln – bekämpfen Sie das Problem jetzt. Handeln Sie sofort und Sie können aus einer Bedrohung eine Chance gewinnen, Ihre Kund*innen zu schützen und deren Vertrauen in Sie zu stärken. Damit schaffen Sie einen beträchtlichen Wettbewerbsvorteil durch bessere Customer Experience, reibungslosere Abläufe für Contact-Center-Agenten und einen höheren NPS.

WEITERE INFORMATIONEN
Mehr darüber, wie Sie jede Kundeninteraktion optimieren, schützen und personalisieren können, erfahren Sie per E-Mail an cxexperts@nuance.com oder auf unserer Homepage.

Quellen

Coronavirus-Related Spear Phishing Attacks See 667% Increase in March 2020. Security Magazine. Abgerufen am 17. November 2021 unter: https://www.securitymagazine.com/articles/92157-coronavirus-related-spear-phishing-attacks-see-667-increase-in-march-2020

Skiba, Katherine. (5. Februar, 2021). Pandemic Proves to Be Fertile Ground for Identity Thieves. AARP. Abgerufen am 17. November unter: https://www.aarp.org/money/scams-fraud/info-2021/ftc-fraud-report-identity-theft-pandemic.html

Inscoe, Shirley. (9. März 2021). U.S. Identity Theft: The Stark Reality. Aite Group.

HSBC UK customer warning: one time passcode fraud increases. HSBC UK. Abgerufen am 17. November unter: https://www.about.hsbc.co.uk/news-and-media/hsbc-uk-issues-customer-warning-as-one-time-passcode-fraud-increases

Über Nuance Communications, Inc.
Nuance Communications (Nuance) ist Technologie-Pionier und Marktführer im Bereich der dialogorientierten KI und Ambient Intelligence. 77 Prozent der Krankenhäuser in den USA und 85 Prozent aller Fortune-100 Unternehmen weltweit vertrauen Nuance als Full-Service-Partner. Wir liefern intuitive Lösungen, die Menschen ermöglichen, andere zu unterstützen.

ENT_4510_01_EB_GER, Feb 23, 2022