nevis®

Making security an experience

White Paper

Entscheidender Faktor für mehr Sicherheit: Multi-Faktor-Authentifizierung

Wie Multi-Faktor-Authentifizierung in CIAM-Lösungen das Kundenerlebnis verbessert

Die Mehrheit der Kunden ist in grosser Sorge um die Sicherheit ihrer Daten im Internet. Eine einfache, aber sehr effiziente Massnahme für mehr Datenschutz ist die Multi-Faktor-Authentifizierung. Doch was genau verbirgt sich dahinter? Und wie lässt sich für eine gute Customer Experience erhöhte Sicherheit durch Multi-Faktor-Authentifizierung perfekt mit User-Komfort in Einklang bringen? Die Antworten auf diese Fragen finden Sie in diesem White Paper.

Inhalt

Vorwort

Shoppen, Geld überweisen, Versicherungen abschliessen und, und, und – wir alle erledigen heute zahllose Dinge online. Dafür ist meist ein Online-Account samt Anmeldeinformationen nötig. Zudem liegen aus dem gleichen Grund sensible Daten auf zahllosen Servern. Mit Blick auf den erneuten **dramatischen Anstieg von Cyber-Attacken in Europa** verwundert es nicht, dass bei den Nutzern die Sorge um ihre Daten steigt.

Unter anderem mit Phishing- oder Brute Force-Attacken versuchen Kriminelle Nutzerkonten zu kompromittieren. Eine zusätzliche Schutzebene dagegen bietet die Multi-Faktor-Authentifizierung (MFA). Doch wie bei jeder Massnahme, mit denen Sie die Sicherheit der Daten Ihrer Kunden erhöhen, dürfen Sie auch bei der MFA nicht vergessen: Der bessere Schutz darf nicht auf Kosten der Customer Experience gehen. Denn Kunden sind keine Mitarbeitenden, die verpflichtet sind, zusätzliche Sicherheitsmassnahmen zu akzeptieren. Haben sie den Eindruck, dass ihre Benutzererfahrung dadurch leidet, wechseln sie zu einem anderen Anbieter mit höherem Komfort.

Es kommt also darauf an, die MFA so zu implementieren, dass sich Datensicherheit und Benutzerfreundlichkeit die Waage halten. In modernen Customer Identity and Acces Management-Lösungen ist der Einsatz von MFA als Sicherheitsebene selbstverständlich. Gleichzeitig verfügen sie über die Möglichkeit, MFA mit passwortfreien Identifikationsmassnahmen zu kombinieren, sodass nicht nur eine weitere Sicherheitsebene eingezogen wird, sondern der Login-Prozess sich zusätzlich vereinfacht. Auf den folgenden Seiten erläutern wir Ihnen, wie MFA genau funktioniert und wie Sie innerhalb Ihres CIAM perfekt auf die Anforderungen Ihrer Nutzer abgestimmt werden kann – für eine optimale Customer Experience und treue Kunden.

Eine informative Lektüre wünscht

Stephan Schweizer
CEO, Nevis Security AG

Einleitung

In diesem White Paper erklären wir Ihnen ausführlich, warum MFA für Unternehmen heute ein unverzichtbarer Bestandteil Ihrer Sicherheitsmassnahmen sein sollte und wie sie funktioniert. Ausserdem zeigen wir auf, wie Sie im Rahmen von CIAM Ihre MFA-Massnahmen mit der passwortfreien Authentifizierung verbinden können. Damit lässt sich der Wunsch Ihrer Kunden nach hoher Sicherheit bei maximalem Login-Komfort massgeschneidert erfüllen.

Warum sollten Unternehmen auf MFA setzen?

Die Antwort darauf ist einfach: Weil Passwörter allein nicht sicher sind und kompromittierte Nutzerkonten immer noch eine der grössten Bedrohungen für Datensicherheit darstellen.

Obwohl viele Kunden sich um die Sicherheit ihrer Daten sorgen, legen sie selbst nicht immer die grösste Vorsicht an den Tag. Noch immer erfreuen sich bei den Passwörtern zum Beispiel leicht zu knackende Zahlenfolgen wie „123456" oder einfache Wort-Zahlen-Kombinationen wie „hallo123" grosser Beliebtheit. Auch gaben 44 Prozent von 1'000 befragten Konsumenten im Rahmen unserer Studie für das **Nevis Sicherheitsbarometer 2021** an, dass sie ein und dasselbe Passwort für mehrere Konten benutzen.

Risikofaktor Passwort

44,3%

der befragten Konsumenten nutzen **ein und dasselbe Passwort** für mehrere Konten.

Quelle: Nevis Sicherheitsbarometer 2021

Mit diesem Verhalten spielen sie Cyber-Kriminellen und ihren häufigsten Angriffsmethoden in die Hände. Nach den Angaben der für das Nevis Sicherheitsbarometer befragten 500 IT-Entscheider gehören dazu Brute-Force-Angriffe (rund 27 Prozent) und Credential-Stuffing-Attacken (rund 23 Prozent).

Brute-Force-Angriffe

Bei Brute-Force-Angriffen gehen Hacker mit roher Gewalt vor. Anhand einer Liste mit gültigen Benutzernamen versucht ein Bot durch automatisiertes Ausprobieren die dazugehörigen Passwörter herauszufinden.

Phishing-Angriffe

Phishing ist führend bei den Social-Engineering-Attacken, die sich menschlicher Schwächen bedienen, um unrechtmässig in den Besitz von Anmeldedaten zu kommen. Phishing-Mails, hinter denen angeblich vertrauenswürdige Absender stecken, sollen die Empfänger dazu verleiten, auf gefälschten Seiten zum Beispiel sensible Login-Daten preiszugeben.

Credential Stuffing

Daneben machen Hacker sich auch den Umstand zunutze, dass eine erschreckend hohe Userzahl dieselben Benutzernamen und Kennwörter bei unterschiedlichen Anbietern nutzt. Haben die Kriminellen durch Brute-Force- oder Phishing bereits Nutzerdaten erbeutet, versuchen sie sich möglicherweise im nächsten Schritt mittels Credential Stuffing auf anderen Websites einzuloggen – mit fatalen Konsequenzen für die Nutzer.

Eine gegen alle

Allen diesen Angriffsmethoden ist eins gemeinsam: Mit MFA kann den Kriminellen bei ihrem Tun ein wirkungsvoller Riegel vorgeschoben werden. Ganz einfach, weil die Multi-Faktor-Authentifizierung mindestens einen zweiten Identifikationsfaktor zusätzlich zum Passwort verlangt. Mit der leider noch weit verbreiteten Ein-Faktor-Authentifizierung haben Hacker leichtes Spiel, sobald ihnen das Passwort bekannt ist. Wird aber im Rahmen der MFA ein weiterer Faktor für die Identifizierung der Nutzeridentität gefordert, beispielsweise die Verifizierung biometrischer Daten in einer Access App auf dem Smartphone, sind die Online-Kriminellen ausgesperrt.

Sicherheitslücken können teure Imageschäden werden

Kann infolge eines Hacks nicht auf Daten oder Dienste zugegriffen werden, bedeutet das etwa für den Online-Handel enorme Umsatzeinbussen. Schätzungsweise **10,5 Billionen Dollar pro Jahr soll Cyber-Kriminalität Unternehmen weltweit bis zum Jahr 2025 kosten**. Im Jahr 2015 waren es „nur" 3 Billionen Dollar.

Nicht zu vergessen sind die Folgen der Imageschäden, die Ihrem Unternehmen drohen, wenn Sicherheitslücken in grossem Umfang bekannt werden und Kunden abwandern.

Ausserdem drohen Organisationen mittlerweile beträchtliche Geldstrafen, wenn sie wegen mangelnder Sicherheit gegen gesetzliche Datenschutzbestimmungen verstossen. **Laut dem jüngsten Jahresbericht der Anwaltskanzlei DLA Piper** wurden im vergangenen Jahr Bussgelder in Höhe von fast 1,1 Milliarden Euro (1,2 Milliarden US-Dollar) gegen Unternehmen wegen Verstössen gegen die Allgemeine Datenschutzverordnung der Europäischen Union (DSGVO) verhängt. Das ist ein neues Rekordhoch.

Wie funktioniert MFA?

Bei der MFA authentifizieren sich die Nutzer durch mindestens zwei verschiedene Sicherheits- und Validierungsverfahren. Grundsätzlich unterscheidet man vier Arten von Authentisierungstechnologien. Sie basieren auf den Faktoren Wissen, Besitz, biometrische Merkmale und Standort. Werden nur zwei verschiedene Varianten genutzt, wird das Zwei-Faktor-Authentifizierung (2FA) genannt.

Die vier Kategorien der MFA

→ Wissen

Dabei handelt es sich um etwas, das nur der Nutzer kennt. Dazu gehören Passwörter, PIN, die Antworten auf Sicherheitsfragen oder die User-Kennung. Auch die Transaktionsnummer (TAN) beziehungsweise das One-Time-Password (OTP) fallen in diese Kategorie. Dafür werden heute in der Regel TAN-Generatoren oder Authenticator Apps genutzt. Sie generieren die Kennwörter zeit- und ereignisbasiert immer neu. Noch sicherer wird das TAN-Verfahren, wenn in den Prozess auch die Kontonummer und der Betrag einbezogen werden.

→ Haben

Dafür muss der Nutzer im Besitz eines bestimmten Gegenstandes sein. Dabei kann es sich zum Beispiel um ein Smartphone, eine Chipkarte, einen USB-Token oder einen TAN-Generator handeln. Mittels des Hardware-Tokens wird ein Einmalpasswort oder ein One-Time-Passcode (OTP) generiert. Heute wird statt eines separaten Hardware-Tokens oft das Smartphone genutzt, weil es viele Menschen immer mit sich führen. Eine Authentifizierungs-App, die der Nutzer vorher installiert hat, stellt dann den OTP bereit. Separate Zusatzgeräte wie ein USB-Token oder ein TAN-Generator sind nicht mehr zeitgemäss. Sie werden in der Regel zu Hause verwahrt, was den Nutzer etwa bei Bankgeschäften zeitlich und räumlich einschränkt.

→ Sein

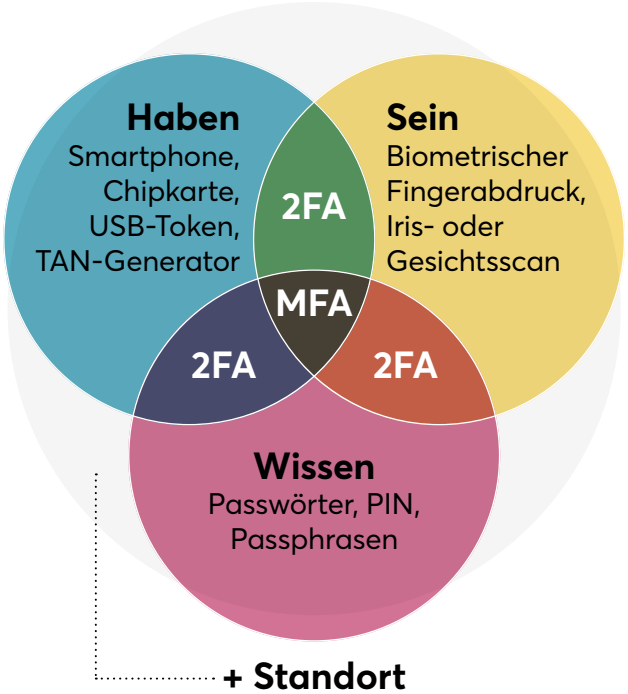
Etwas, das der Anwender ist. Er weist sich also mit seinen einzigartigen biometrischen Merkmalen aus. Dazu zählt sein Fingerabdruck, die Iris oder das Gesicht. Sind diese Faktoren einmal gescannt und gespeichert, kann der Nutzer nur durch eine Lebenderkennung identifiziert werden. Dafür muss er vor Ort sein und sich mit seinen biometrischen Merkmalen zum aktuellen Zeitpunkt ausweisen. Das System kann also nicht zum Beispiel durch ein Foto überlistet werden. Für die biometrische Authentifizierung sind in der Regel moderne Mobilgeräte erforderlich, die über die nötigen Technologien verfügen.

→ Standort

Insbesondere in der Finanzbranche werden auch Faktoren wie die IP-Adresse, falls möglich der Standort mittels GPS-Daten und in einigen Fällen ebenfalls die Nutzungsdauer im Vergleich mit früheren Online-Sitzungen zur Identitätsüberprüfung genutzt.

Zusammenspiel mehrfacher Faktoren

Beim eigentlichen Prozess der MFA kombiniert der Anbieter nun zwei oder mehr Faktoren beispielsweise wie folgt: Für die Nutzung einer Kreditkarte ist ihr Besitz genauso erforderlich wie das Wissen zur PIN, zur Gültigkeit und zur Prüfnummer. Als zusätzliche Sicherheitsschranke wird oft eine TAN-Nummer (Wissen) abgefragt, die mittels eines TAN-Generators (Besitz) generiert wird. Je mehr Faktoren dabei zusammenspielen, desto besser ist der Schutz vor Datenmissbrauch.



Grundlegende Überlegungen zum Einsatz der MFA

Von den Vorteilen der MFA können Unternehmen aus verschiedenen Branchen profitieren. Dazu gehören Anbieter von Financial Services und Banking, Behörden, Versicherungen, Maschinenbauer ebenso wie Akteure des Online-Handels, des Gesundheitswesens oder von Online-Casinos.

Unabhängig von der Branche müssen sie bei der Einführung der zusätzlichen Schutzebene durch MFA sicherstellen, dass sie eine Balance zwischen Sicherheit und Komfort für die Kunden schaffen. Damit dies gelingt, ist eine sorgfältige Planung erforderlich. Folgende Punkte sollten Sie daher vorab festlegen.

Obligatorisch oder optional?

Da die MFA immer ein gewisses Mass an zusätzlichem Aufwand für Ihre Kunden bedeutet, gilt es zu entscheiden, wie in einzelnen Anwendungsfällen Schutz und Bedienerkomfort optimal gewichtet werden. Zum Start müssen sich Unternehmen Gedanken darüber machen, wie sie die MFA für ihre Kunden einführen: Soll diese Technologie obligatorisch oder optional sein?

Es gibt schliesslich zahlreiche Anwendungsfälle, in denen die MFA theoretisch genutzt werden kann. Doch wo ist sie sinnvoll? Um die Benutzeridentifikation nicht unnötig zu verkomplizieren, was möglicherweise eine schlechte Kundenerfahrung nach sich zieht, sollte sorgfältig abgewogen werden, wann MFA wirklich erforderlich ist und wann nicht.

Selbst in der Finanzbranche, wo die meisten Transaktionen mit einem hohen Risiko verbunden sind, muss die MFA nicht überall das Mittel der Wahl sein. Es ist empfehlenswert, immer verschiedene Optionen anzubieten. Zum Beispiel könnten Sie den Kunden die Möglichkeit geben, die Art des zweiten Faktors selbst zu wählen. Dann entscheiden die Verbraucher selbst, ob sie etwa eine SMS-Nachricht erhalten, die aber weniger sicher ist, oder ob sie doch lieber Push-Benachrichtigungen über ihre mobile App für die Authentifizierung erhalten.

Selbstverständlich müssen Unternehmen die Folgen für die Sicherheit bedenken, wenn sie ihren Kunden zwischen verschiedenen MFA-Wegen die Wahl lassen, und mögliche Sicherheitsrisiken klar und deutlich kommunizieren.

Adaptive kontext- und risikobasierte MFA

Das Gute ist, dass moderne MFA die Möglichkeit bietet, die Authentifizierungsanforderungen kontext- und risikobasiert zu erhöhen.

Versucht ein Nutzer beispielsweise sich von einem Gerät aus zu authentifizieren, das er schon oft benutzt hat, kann sofortiger Zugriff gewährt werden. Falls der Authentifizierungsversuch über ein neues Gerät erfolgt, kann eine Genehmigung von einem bekannten vertrauenswürdigen Gerät verlangt werden.

Mit kontext- und risikobasierter MFA können Unternehmen bei verschiedenen Anwendungsfällen eine Flexibilität erreichen, die dabei hilft, dass Kunden ihre Bedürfnisse im Hinblick auf Sicherheit und Bedienerkomfort bestens erfüllt sehen.

Mit MFA in modernen CIAM-Lösungen die Customer Experience verbessern

Moderne CIAM-Lösungen wie die Nevis Authentication Cloud beinhalten für die grösstmögliche Sicherheit bei der Erfassung und Verwaltung von Kundenidentitätsdaten natürlich die MFA als zusätzliche Sicherheitsschranke. Dabei erfüllt sie folgende wichtige Voraussetzungen, die generell beim Einsatz von MFA für Kunden notwendig sind.

Mobile First

Ihre Mobiltelefone haben viele Menschen heute fast immer dabei. Am sinnvollsten ist es daher, für die MFA auf eine Anwendung auf dem Handy zu setzen. Dann besteht so gut wie keine Gefahr, dass die Nutzer ein externes Zusatzgerät im Anwendungsfall nicht dabeihaben. Ausserdem steigt die Akzeptanz bei Ihren Kunden für die MFA, wenn sie sie auf ihrem ohnehin immer griffbereiten Smartphone nutzen können.

Bequeme Verwaltung aller Funktionen

Mit der in der Nevis Authentication Cloud enthaltenen Management Console hat Ihr Unternehmen ein komfortables Tool, um alle integrierten Anwendungen inklusive der MFA zu verwalten. Denn es ist nicht sinnvoll, die MFA-Implementierung einzelnen App-Entwicklungsteams zu überlassen, die nicht über die nötige Erfahrung im Hinblick auf Datensicherheit verfügen. Mit der Management Console können Sie zum Beispiel Benutzer und Geräte verwalten und inaktive Nutzer oder nicht mehr in Nutzung befindliche Geräte aus dem System entfernen. Auch die Verwaltung von Zugriffs-Token, welche etwa die Anwendungen für Log-in-Genehmigungen verwenden, ist möglich.

Bewahren Sie Ihr Branding

Der Aufbau einer erfolgreichen Marke dauert Jahre. Jedes MFA-Tool, das Ihre Kunden nutzen, etwa Ihre Access-App, sollte daher nach Ihren Vorgaben gebrandet sein. Lösungen von Anbietern, die nicht an Ihre Corporate Identity angepasst werden können, verwässern unweigerlich das Kundenerlebnis mit Ihrer Marke. Auch könnten Nutzern bei einer namenlosen, unbekannten App Zweifel kommen, ob sie wirklich mit Ihrer Marke und Ihrem Unternehmen in Zusammenhang steht. Daher ist die in der Nevis Authentication Cloud enthaltene Access App für Ihre Kunden so konzipiert, dass Sie ohne grossen Programmieraufwand Ihr Logo, Ihre Farben und die Schriftart Ihrer Wahl tragen kann. Zudem ist die Nevis Access App gehärtet, End-to-End-verschlüsselt und FIDO-zertifiziert. Mittels Software Development Kit (SDK) kann sie ohne hohen Zeitaufwand integriert werden.

Passwortwortfreie, biometrische Authentifizierung

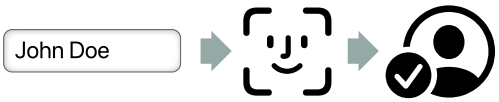
Mit der Möglichkeit der passwortfreien, Biometrie-basierten MFA bietet die Authentication Cloud sowohl ein Optimum an Sicherheit als auch ein Optimum an Komfort.

Am häufigsten wird die sogenannte Out-of-Band-Authentifizierung verwendet. Dahinter verbirgt sich eine bestimmte Form der MFA beziehungsweise Zwei-Faktor-Authentifizierung (2FA). Für den Erhalt des zweiten Authentifizierungsfaktors ist der Einsatz eines separaten Kommunikationskanals erforderlich. Der Nutzer erhält zum Beispiel nach Eingabe von Benutzername und Passwort auf einem vertrauenswürdigen Gerät eine Push-Nachricht oder muss sich darauf mittels seines Fingerabdrucks identifizieren.

Als besonders komfortable Form der Nutzeridentifikation bietet die Nevis Authentication Cloud die Möglichkeit kennwortloser Authentifizierung und Transaktionssignierung. Die Notwendigkeit eines unsicheren Passworts entfällt komplett.

Der passwortfreie Authentifizierungsvorgang dauert für den Nutzer nur wenige Sekunden. Die Kunden geben ihren Benutzernamen auf der Anmeldeseite ein und tippen auf ihrem Smartphone auf die Schaltfläche „Anmelden". Die Nevis Authentication Cloud-Instanz schickt eine Push-Benachrichtigung an das Mobiltelefon des Benutzers (Faktor „Haben"). Wenn er sie öffnet, kann er sich mit der von ihm gewählten biometrischen Methode (Faktor „Sein") authentifizieren. Ist die Authentifizierung erfolgreich, bestätigt die Nevis Access App dies und der User ist automatisch eingeloggt.

Passwortfreie Authentifizierung mittels biometrischer Merkmale in der Access App

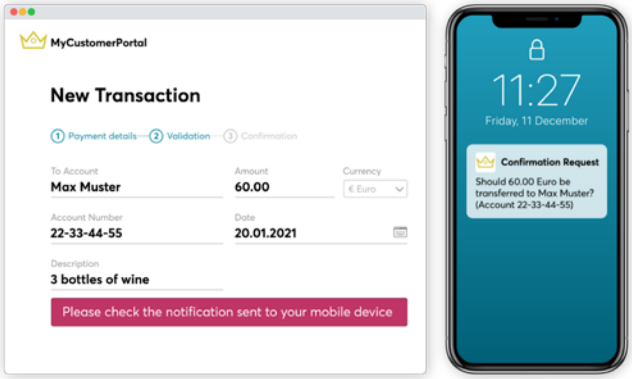


- Eine echte passwortlose Alternative die das Konto vor Credential Stuffing und Kontoübernahmeangriffen schützt
- Es ist lediglich die Eingabe eines Benutzernamens und Authentifizierung notwendig

Transaktionsbestätigung

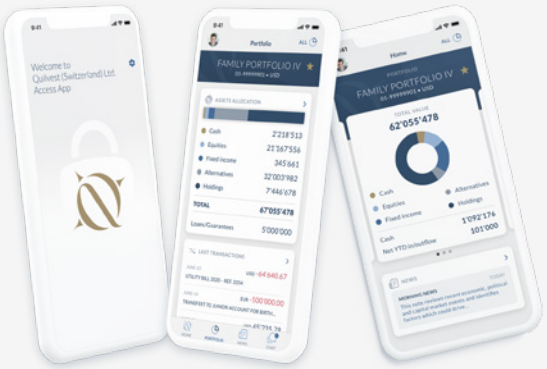
Bei Transaktionen mit besonders hohem Sicherheitsniveau wie Finanzgeschäften oder Informationsaktualisierungen sollte für ein Sicherheitsplus zusätzlich eine Transaktionsbestätigung Usus sein. Auch dabei spielt die MFA eine wichtige Rolle. Wie beim Login mit MFA informiert eine Push-Benachrichtigung den User über die bevorstehende Transaktion und über wichtige Einzelheiten wie etwa die Höhe des Geldbetrags oder die Kontonummer des Empfängers. So hat der Kunde noch die Möglichkeit korrigierend einzugreifen, bevor er durch seine gewählte biometrische Authentifizierung die Transaktion bestätigt. Weiterer Vorteil der Transaktionsbestätigung: Sie erhöht nicht nur die Sicherheit, sie schützt auch vor fehlerhaften Eingaben und sorgt so für ein positives Kundenerlebnis.

Transaktionsbestätigung mit der Nevis Authentication Cloud



Erfolgsbeispiel:
Sichere Authentifizierung im E-Banking mit der Nevis Authentication Cloud

QUILVEST
SWITZERLAND



Insbesondere in der Finanzbranche ist die Digitalisierung mit besonderen Anforderungen verbunden. Quilvest (Schweiz) AG, ein renommierter unabhängiger Vermögensverwalter, hat eine neue Plattform entwickelt, in der eine gesicherte Kommunikation auch per Chat-Funktion möglich ist. Damit wurde der Wunsch der Nutzer erfüllt, schnell und unkompliziert mit ihren Beratern in Kontakt zu treten – und dies in rechtssicherer Form, was durch externe Messenger-Dienste nicht gewährleistet werden könnte. Parallel wurde dem Bedarf nach einer neuen Authentifizierungsmöglichkeit samt Firewall für die Etablierung von E-Banking Rechnung getragen. Nevis überzeugte Quilvest unter anderem mit der Usability, der Sicherheit, der stabilen Verfügbarkeit der Authentication Cloud sowie der Möglichkeit, die App zu branden.

Sicher, flexibel und anwenderfreundlich

Nevis unterstützt Quilvest mit einer kombinierten Lösung aus Proxyserver, IDM, WebAuth Firewall-Infrastruktur und AccessApp mit Cloudlösung. Für die Authentifizierung wird die Nevis Authentication Cloud genutzt. Die Identifikation erfolgt mit Username und Passwort, mit Fingerprint/Face ID oder PIN. Es gibt zwei Möglichkeiten zur Authentifizierung: Entweder der Kunde loggt sich im Webportal ein und gibt seine Vertragsnummer sowie sein Passwort an. Dann wird ihm in der App eine Push-Authentifizierung zugeschickt. Zum Ausweisen nutzt er seine PIN oder Fingerabdruck/Face ID.

Alternativ kann der Kunde die Mobile Banking App öffnen. Dort gibt er seine Vertragsnummer an und erhält in der App eine Push-Nachricht, die er bestätigen muss – auch hier via PIN oder Fingerabdruck/Face ID. Via automatischem „App to App Switch" werden die Nutzer nach erfolgreich abgeschlossener Authentifizierung automatisiert zur Banking-App zurückgeleitet. Transaktionen an neue Empfänger sowie Beträge oberhalb einer festgelegten Höhe werden über die AccessApp ebenfalls zusätzlich autorisiert.

Das Ergebnis: Die Nutzer sind gegenüber dem E-Banking und Mobile Banking aufgeschlossener, weil es im Vergleich zu früher nicht mehr so komplex ist. Zudem sind Mobile- und E-Banking in einer einzigen App nutzbar, was die Handhabung vereinfacht.

MFA – mit komfortabler Sicherheit punkten

In Anbetracht der weiterhin steigenden Zahl von Cyber-Angriffen ist die Bedeutung von Sicherheit insbesondere beim Login-Prozess und bei Online-Transaktionen mit erhöhtem Schutzlevel nicht zu vernachlässigen. Deshalb kommen Unternehmen um den Einsatz der MFA nicht mehr herum. Da damit allerdings – je nach Art der Umsetzung – ein gewisser Mehraufwand für die User verbunden ist, sollten Sie bei der Wahl Ihrer MFA-Lösung wohlüberlegt vorgehen. Das Hantieren mit unterschiedlichen Geräten und ein umständliches Eintippen von Codes oder Passwörtern kann bei den Nutzern Frust aufkommen lassen. Das führt nicht nur zu einer schlechten Customer Experience, sondern möglicherweise dazu, dass die Nutzer auf unsicherere Identifikationsverfahren ausweichen.

Eine Lösung für diese Herausforderung sind MFA-Systeme, die durch den Einsatz von Biometrie maximale Sicherheit und hohen Bedienerkomfort auf höchstem Niveau verbinden.

Zielgruppenspezifisch sicher

Natürlich sollten Sie beim Einsatz von 2FA/MFA-Konzepten die Anforderungen Ihrer Zielgruppe im Auge behalten und Folgendes bedenken:

- Nicht alle Kunden haben aktuelle Smartphone-Modelle, sodass sie die biometrische Authentifizierung gegebenenfalls nicht anwenden können
- Komplizierte Passwörter, PIN und TAN auf dem Handy einzugeben, ist umständlich

Dennoch überwiegen die Vorteile von MFA die Nachteile. Letztere lassen sich durch die wohlüberlegte Wahl anwenderfreundlicher Verfahren, Stichwort Biometrie, sowie den kontext- und risikobasierten Einsatz gut ausgleichen. Mit CIAM-Lösungen wie der Nevis Authentication Cloud gelingt Ihnen nicht nur eine nah an der Zielgruppe orientierte Umsetzung der MFA. Sie profitieren unter anderem von Features wie einer App, die sich komplett in Ihrem Design gestalten lässt oder der Möglichkeit von Transaktionsbestätigungen. Damit gelingt es einfach und unkompliziert, die richtige Balance zwischen Datensicherheit und Usability zu verwirklichen.

nevis®

Making security an experience

Über Nevis

Nevis entwickelt Sicherheitslösungen für die digitale Welt von morgen: Das Portfolio umfasst passwortfreie Logins, die sich intuitiv bedienen lassen und Nutzerdaten optimal schützen. In der Schweiz ist Nevis Marktführer für Identity und Access Management und sichert über 80 Prozent aller E-Banking-Transaktionen. Weltweit setzen Behörden sowie führende Dienstleistungs- und Industrieunternehmen auf Lösungen von Nevis. Der Spezialist für Authentisierung unterhält Standorte in der Schweiz, Deutschland und Ungarn.

Follow us

www.nevis.net