nevis®

Solution Paper

Nevis Authentication Cloud

Making security an experience.

Inhalt

3 Einleitung

3 Die digitale Revolution

5 Kunden wollen es einfach und sicher

5 Sind Customer Experience und IT Security unvereinbare Paradigmen?

7 Was will der Endkunde, wie profitiert der Anbieter?

9 Authentifizierung

9 Was ist Multi-Faktor-Authentifizierung?

9 Benutzername und Passwort – noch zeitgemäss?

10 2FA – 2-Faktor-Authentifizierung

10 2FA ohne Passwort

11 FIDO (Fast Identity Online) – der Standard zur passwortfreien Authentifizierung

11 Was kann die Authentication Cloud?

11 Nevis Authentication Cloud

12 Passwortfreie Authentifizierung

13 Transaktionsbestätigung (Transaction Confirmation)

14 Branded Access App

16 Management Console

16 FIDO und Nevis

17 Wie Nevis dem Unternehmen hilft

17 Was ist der Nutzen für den Endkunden?

17 Was ist der Businessnutzen?

18 Was ist der Nutzen für die IT?

19 Wie profitieren Branchen?

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Einleitung

Die digitale Revolution

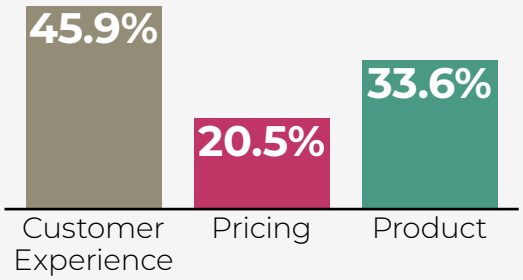
Wie oft nutzen wir digitale Geräte, wie lang sind wir täglich mit der Online-Welt verbunden? Schrittzähler, Schlafüberwachung, Online-Meetings, Social Media, Shopping, Banking, Haustechnik: Was immer Sie wollen, ist heute auch online möglich. Digitalisierung ist überall. Und nicht nur das. Wir stecken mitten in einer Digitalen Revolution, die einen noch gewaltigeren Wandel mit sich bringen wird als die Industrielle Revolution. Während technische Innovationen damals in einigen Branchen zu disruptiven Veränderungen geführt haben, verändert Digitalisierung heute die Welt als Ganzes.

Es gilt, die Kunden in dieser digitalisierten Welt abzuholen und sie überzeugend zu bedienen. Sie steuern den Markt und fordern. Der nächste Anbieter ist nur einen Klick entfernt, wenn es nicht passt. Wenn Anbieter also nicht mithalten, gehen sie unter. Jeden Tag. Noch nie verschwanden Fortune-500-Unternehmen so schnell wieder in der Versenkung wie heute. Experten des MIT und von Deloitte erwarten, dass 2025 40 Prozent der heutigen Fortune-500-Unternehmen nicht mehr existieren werden, weil sie sich nicht schnell genug anpassen konnten.

Aber wie holt man potenzielle und bestehende Kunden digital so ab, dass sie sich für eine Marke entscheiden und dieser treu bleiben? Es reicht schon lange nicht mehr aus, das innovativste Produkt herzustellen oder einfach einen guten Service zu bieten, um sich als Unternehmen zu differenzieren. Den Unterschied macht das Kundenerlebnis!

Gemäss einer Studie von Walker[1] überholte das Kundenerlebnis 2020 den Preis und das Produkt als wichtigster Key Brand Differentiator (Markendifferenzierungsmerkmal). Das klingt einleuchtend und zahlt sich auch aus. Einer Studie der Temkin Group[2] zufolge würden 86 Prozent der Kunden, die ihre Erlebnisse mit einem Unternehmen als positiv bewerten, bei diesem erneut einkaufen. Zum Vergleich: Bei nur einer negativen Erfahrung würde schon fast jeder fünfte Konsument sich von der Marke abwenden. Die Schlussfolgerung lautet also: Der Zugang zu jeder Online-Dienstleistung muss so bequem und sicher wie möglich gestaltet werden. Die Digitale Customer Experience (DCX) darf nichts zu wünschen übrig lassen. Beim Thema Sicherheit sieht es eindeutiger aus. Wo immer persönliche Daten gespeichert und Logins verwaltet werden, erwartet der Kunde möglichst hohe Sicherheit. Der Sicherheitsaspekt ist sozusagen das Minimum, um im Spiel zu sein – gewonnen wird über das Kundenerlebnis. Mit ein Grund, warum Best-of-breed Unternehmen in ihrer strategischen Ausrichtung auch hier den Fokus setzen.

Was sind in Ihrem Business die Top-Prioritäten der kommenden 5 Jahre?[1]



1: Customers 2020: A Progress Report, 2020, Walker
2: ROI of Customer Experience, 2018, Temkin Group

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Passwörter nicht mehr zeitgemäss?

Ob beim Online-Einkauf, auf Social-Media-Kanälen oder beim Online-Banking: Benutzer müssen sich anmelden. Immer wieder und wieder. Gemäss einer Studie von Gartner[1] hat eine Person im Durchschnitt 130 verschiedene Nutzerkonten. Und die meisten dieser Accounts sind simpel mit Benutzernamen und Passwort geschützt.

Passwörter sind unpraktisch

Im Schnitt müssen Menschen acht Mal pro Tag Passwörter für die zehn verschiedenen Online-Konten oder Applikationen eingeben, die sie jede Woche regelmässig benutzen[2]. Die Fülle der Passwörter, die sich Endanwender merken müssen, um auf eine wachsende Zahl von Diensten im Internet zuzugreifen, ist überwältigend. Allein mit der Suche oder dem Zurücksetzen von Passwörtern verbringt der durchschnittliche User ca. 12 Tage seines Lebens[3].

Aber es sind nicht nur die User, die während der Registrierung und der Authentisierungsprozesse viel Zeit verlieren. Anbieter aller Branchen sind gleichermassen davon betroffen, und sie verlieren zusätzlich Geld. Denn aufgrund fehlender Benutzernamen und Passwörter sowie mühsamer Registrierungsprozesse oder auch ungenügender Sicherheit bei diversen Transaktionen werden ca. ein Drittel der Online-Vorgänge abgebrochen[4]. Folgende Situationen können Kosten, Umsatzverlust und Mehraufwand verursachen:

- Der volle Warenkorb kommt nicht bis zur Kasse
- Das Upgrade zum Abonnement kann nicht gebucht werden
- Beim E-Banking greift der Benutzer zum Telefon, statt sich online zu informieren oder das Passwort selbständig zurückzusetzen
- Versicherungsfälle werden auf Papier statt elektronisch abgewickelt, und die Zusatzversicherung wird bei der Konkurrenz abgeschlossen
- Für Behördengänge müssen mehr Schalter als nötig besetzt werden

66% „Eine schlechte Erfahrung auf einer Webseite beeinträchtigt meine Meinung zur gesamten Marke“

Quelle: SilverCloud

Passwörter sind unsicher

Passwörter beeinträchtigen nicht nur die Customer Experience, sondern verursachen auch grosse Sicherheitsprobleme. Sie stecken oft hinter Datenschutzverletzungen. Laut Verizon Data Breach Investigations Report 2019[5] waren kompromittierte und schwache Anmeldedaten der Grund für 80% der mit Hacking verbundenen Verstösse. Und 29% aller Verstösse, unabhängig von der Art des Angriffs, beruhten auf der Verwendung gestohlener Anmeldedaten.

1: *Gartner Identity & Access Management Summit, Gartner 2018*
2: *A Large-Scale Study of Web Password Habits*
3: *Openwave Mobility Research*
4: *TNS Research im Auftrag von VeriSign, Inc.*
5: *World Economic Forum - Passwordless Authentication: The Next Breakthrough in Secure Digital Transformation, S. 5*

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Traditionelle Passwort-Gepflogenheiten nutzten da wenig, ganz im Gegenteil: Die Anwender haben sich im Lauf der Zeit einige schlechte Angewohnheiten angeeignet. Jeder, der schon mal ein komplexes Passwort auf dem Mobiltelefon eingeben musste, kennt das. Das ist so mühsam, dass man riskante Kompromisse eingeht und kurze oder immer wieder dieselben Passwörter verwendet. Die Anwender gehen mit Passwörtern nachweislich immer leichtsinniger um. Die Analyse einer halben Milliarde geknackter Konten ergab, dass nur wenige Passwörter mehr als 8 bis 10 Zeichen umfassen. Weniger als 6% der Passwörter enthalten Großbuchstaben oder Symbole[1]. Das macht sie extrem anfällig für Brute-Force-Angriffe. Denn kurze und einfache Passwörter kann man viel einfacher durchprobieren.
Durch Brute-Force-Angriffe, Phishing oder andere Methoden des Social Hacking kommen Kriminelle leicht an Benutzernamen und Passwörter. Sehr bedenklich: Eine Studie ergab Anfang Juni 2020, dass zwei Drittel der Studienteilnehmer, die wussten, dass ihre Passwörter geknackt worden waren, diese drei Monate später immer noch nicht geändert hatten[2].
Fazit: Passwörter sind heute als Hauptauthentisierungslösung für Endkunden nicht mehr tragbar. Es ist ratsam, weitere Authentifizierungsfaktoren hinzuzufügen oder auf Passwörter gänzlich zu verzichten, wie das Nevis mit der passwortlosen Mobile Authentication Solution macht. Wir setzen auf biometrie-basierte Multi-Faktor-Authentifizierung (MFA), um die Sicherheit und Customer Experience zu optimieren.

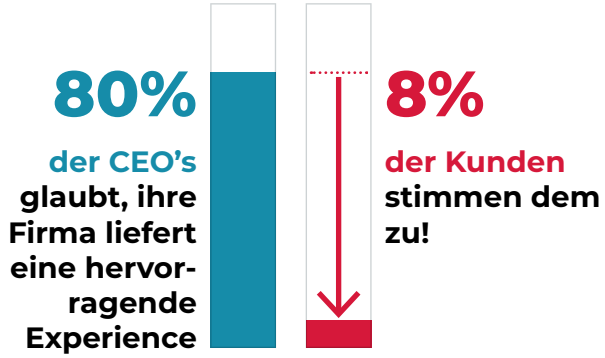
Kunden wollen es einfach und sicher

Sind Customer Experience und IT Security unvereinbare Paradigmen?

Das Anwendererlebnis und die Sicherheit sind wichtige Kriterien, die ausbalanciert werden müssen, wenn man Kunden gewinnen und halten will. Leider gilt immer noch das Paradigma, dass die Erhöhung der Sicherheit oft das Nutzererlebnis beeinträchtigt. Und dass umgekehrt ein grossartiges Nutzererlebnis nicht sicher sein kann. Müssen die Forderungen der Anwender nach einfachem, schnellem und unkompliziertem Online-Zugriff um der Sicherheit und Einhaltung der Vorschriften willen hinten anstehen?

Den Anbietern verschiedenster Branchen ist die Kluft zwischen den Kundenerwartungen und der tatsächlichen Kundenerfahrung nicht bewusst.

Der „Experience Gap“



Bain & Company via Craig McVoy, CCXP

1: *Duo Labs Security Analysis*
2: *Studie des Security and Privacy Institute der Carnegie Mellon University - Artikel der Netzwoche*

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

27%

Fast ein Drittel der Konsumenten glauben, dass die Erlebnisse mit Marken mit der Zeit schlimmer geworden sind, nicht besser

62%

würden die Marke wechseln, wenn sie den Eindruck hätten, dass sie ein besseres Erlebnis bekommen würden

Quelle: Experience Gap Report 2018, clearstrategy.com

Veraltete Multifaktor-Authentisierung (MFA) vs. Biometrie

Sicherheit ist ein kontinuierlicher Entwicklungsprozess, ein ewiges Katz-und-Maus-Spiel zwischen Angreifer und Verteidiger. Die Angreifer sind in der Lage, Passwörter zu ermitteln, zu stehlen oder diese brachial auszuhebeln. Die Lösung sollte daher eine Kombination von mehreren Faktoren zur Identifizierung des Users sein: die Multifaktor-Authentisierung.

In den letzten Jahren wurden jedoch Studien publiziert, welche Probleme mit veralteten MFA-Methoden aufzeigen[1]. Letztere sind nicht benutzerfreundlich genug. Beispiele sind die manuelle Eingabe des dynamischen Passworts und die Verwendung von Zusatzgeräten (Hardware-Token) zur Erstellung von Einmalpasswörtern (OTP). Die Schwächen: nicht einfach zu bedienen, nicht einfach ins tägliche Leben zu integrieren, nicht mobil. Oft werden diese MFA-Mechanismen für Anwendungen mit hohem Sicherheitsbedarf, wie Online-Banking, verwendet. Die Kunden verwahren das erforderliche Zusatzgerät entsprechend zuhause an einem sicheren Ort. Dies schränkt die Nutzbarkeit zeitlich und räumlich massiv ein. Die Interaktionsmöglichkeiten mit der Bank sind sehr begrenzt.

Moderne Multifaktor-Authentisierung nutzt Biometrie. Die heute in mobilen Geräten verbauten biometrischen Identifikationstechnologien ermöglichen komplett neue Ansätze im Bereich der Authentisierung. Der Trend wird zusätzlich befeuert durch neue Standards wie z. B. FIDO (Fast IDentity Online). Gartner empfiehlt den Anbietern, dem Thema der passwortlosen Authentisierung höchste Priorität einzuräumen. Das Ersetzen eines Passworts durch biometrische Authentifizierung kann sowohl die Benutzerfreundlichkeit als auch die Sicherheit verbessern – ein Effekt, der bei Sicherheits- und IAM-Tools nicht häufig zu beobachten ist[2]. Zum ersten Mal ist es möglich, dass höhere Sicherheit und Benutzerfreundlichkeit Hand in Hand gehen!

Wie erfolgreich das ist, zeigt sich am Beispiel des langjährigen Nevis-Kunden PostFinance:

PostFinance

„Unsere Kunden erwarten den passwortfreien und sicheren Zugang zu ihrem Konto: Die Zahl der Kundeninteraktionen hat sich verdoppelt."

Eric Müller
Lead Solutions Architect
PostFinance

1: *World Economic Forum - Passwordless Authentication: The Next Breakthrough in Secure Digital Transformation, S. 5*
2: *Gartner: 2020 Planning Guide for Identity and Access Management*

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Was will der Endkunde, wie profitiert der Anbieter?

Das Vertrauen der Endkunden in die digitalen Kanäle muss ständig verfestigt werden. Besonders wichtig ist dabei ein zusätzlicher Schutz bei „allem, was mit Geld, was mit hohem Wert, dem Bereich der Gesundheit oder der Privatsphäre“[1] zu tun hat.

Egal ob sich ein Endkunde über einen Browser, sein Smartphone oder einen digitalen Kiosk[2] einloggt: Die Anmeldung soll einfach vonstatten gehen und zudem – unabhängig vom gewählten Endgerät – eine möglichst schlanke und hürdenlose Kaufabwicklung ermöglichen.

Der Fokus der Anbieter liegt heute auf der neuen Erwartungshaltung der Kunden bei der Authentifizierung: schnell, unkompliziert, von überall zugänglich, ohne das lästige Eintippen von Passwörtern, ohne zusätzliche Geräte, immer zur Hand.

Nichts bietet sich dazu besser an als das Smartphone. Es gibt derzeit weltweit geschätzt 3,5 Milliarden Smartphones (mehr als Zahnbürsten). Durchschnittlich verbringt ein User täglich nahezu drei Stunden am Smartphone und hat dabei mehr als 2’600 Interaktionen (Tippen, Wischen, Schieben). Das Smartphone ist ein integraler Bestandteil unseres Lebens, ein Gerät, welches wir immer dabei haben, egal wo wir uns befinden, immer griffbereit, leicht zu bedienen und sehr persönlich.

Diese mobilen Geräte verfügen über separate, geschlossene, geschützte Bereiche: Sicherheits-Chips. Diese sind physisch vom Haupt-Chip getrennt und enthalten das kryptografische Material (sogenannte Private Keys[3]). Um an das kryptografische Material zu gelangen, muss der Bereich mittels Biometrie erschlossen werden. Selbst wenn also ein Gerät abhanden kommt, ist der Sicherheits-Chip manipulationssicher, und die Private Keys können nicht gestohlen werden.

Das Smartphone verfügt über sichere biometrische Eingabemöglichkeiten, die Passwörter bestens ersetzen können. Die biometrischen Informationen verlassen das Gerät niemals. Dies erlaubt uns, den Sicherheits-Chip als ideales Werkzeug zu nutzen, um Kunden sicher und geschützt online zu authentifizieren.

1: *Prof. Christoph Meinel, Direktor des Hasso-Plattner-Instituts (HPI)*
2: *Der digitale Kiosk, auch Thin Client, ist z. B. eine Arbeitsstation zur Eingabe medizinischer Daten, ein Check-in-Schalter, eine Selbstbedienungsstation oder ein Informationsterminal mit öffentlichem Zugriff.*
3: *Ein Private Key ermöglicht es seinem Besitzer, mit dem Public Key verschlüsselte Daten zu entschlüsseln, digitale Signaturen zu erzeugen oder sich zu authentisieren.*

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

1. Die Nutzer haben sich an die biometrischen Eingaben auf Smartphones und Tablets gewöhnt. Über 80 Prozent verwenden bereits ihren Finger oder ihr Gesicht, um ihre Geräte zu entsperren[1]. Zusätzlich ist die Technologie mittlerweile allgegenwärtig und auf den meisten Geräten verfügbar. Studien zeigen, dass sich die Benutzer diese positive, einfache Variante auch für die Authentifizierung wünschen.

2. Benutzerinnen und Benutzer wollen keine Passwörter auf ihrem Mobiltelefon tippen. Wir alle wissen, wie umständlich es ist, eine lange Nachricht zu tippen, zum Beispiel im Bus, auf dem Weg nach Hause nach einem anstrengenden Arbeitstag. Viele Studien zeigen, wie schlecht es um Passwörter steht. Eine Studie der Universität München hat speziell den Umgang mit Passwörtern auf dem Smartphone untersucht und herausgefunden, dass die User dort noch kürzere und noch einfachere Passwörter verwenden, als sie dies auf dem Computer tun[2]. Dies bedeutet, dass Passwörter, welche auf einem Smartphone erstellt werden, noch einfacher zu knacken sind.

3. Für sichere Transaktionen, insbesondere im Banking oder im Gesundheitswesen, werden heute oft zusätzliche Geräte oder Verfahren verwendet, wie zum Beispiel RSA-Tokens, Smartcard Reader, USB-Keys, SMS oder Ähnliches. Diese lassen sich aber selten bis nie kombiniert auf einem Smartphone anwenden – und SMS ist aus Sicherheitsgründen nicht mehr zu empfehlen. Eine Studie zeigt zudem, dass ein Drittel der Teilnehmerinnen und Teilnehmer das Hardware-Token nicht dabei hat, wenn es gebraucht wird.

4. In der „Mobile-First"-Welt, in welcher wir heute bereits agieren, muss für die Benutzerinnen und Benutzer ein passwortfreies Erlebnis ermöglicht werden. Eine Studie von Mastercard offenbart, dass in Deutschland fast jede zweite Person eine Bestellung oder einen Vorgang abbricht, weil das Passwort nicht mehr präsent ist[3].

Ein modernes Authentifizierungssystem ist nicht nur aus Sicherheitsgründen erforderlich, sondern auch das wichtigste Instrument der Digitalisierung. Es ermöglicht uneingeschränkte Mobilität, reduziert Reibungsverluste und verbessert damit die Kundenerfahrung. Es steigert die betriebliche Effizienz und gewährleistet eine bessere Einhaltung von Vorschriften. Wir unterstützen Sie dabei, all diese Aufgaben, die nicht zu Ihrem Kerngeschäft gehören, so effizient wie möglich zu erfüllen. Denn wenn Sie das Verlangen Ihrer Kunden nach Bequemlichkeit und Sicherheit ignorieren, verlieren Sie diese an die Konkurrenz und gewinnen keine neuen hinzu.

1: Google Umfrage unter 1'000 Kunden
2: Manuel von Zezschwitz, Alexander De Luca und Heinrich Hussmann: „2014. Honey, I shrunk the keys..."
3: Mastercard-Studie

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Authentifizierung

Was ist Multi-Faktor-Authentifizierung?

Die Multi-Faktor-Authentifizierung (MFA) ist ein Sicherheitsmechanismus, bei dem Personen durch mehr als ein erforderliches Sicherheits- und Validierungsverfahren authentifiziert werden. Die wichtigsten Identifikationsmittel basieren auf den Prinzipien Wissen, Haben und Sein. Darüber hinaus können sowohl der Ort als auch die Zeit als Überprüfungsmerkmale dienen und als weitere Faktoren hinzugezogen werden.

Die Kombination dieser Identifikationsfaktoren stellt zuverlässig sicher, dass die Person, die auf vertrauliche Daten zugreifen will, wirklich der Mensch ist, den sie zu sein vorgibt:

- **Haben** – Besitz eines Gerätes (Mobiletelefon, Bankkarte etc.)
- **Wissen** – ein Passwort, Sicherheitsfragen, PIN
- **Sein** – Biometrische Merkmale (Fingerabdruck, Face-ID, Iris-Muster)

Weitere Faktoren, die zur Überprüfung der Identität genutzt und vor allem im Finanzumfeld eingesetzt werden, um Betrugsabsichten aufzudecken (adaptive MFA):

- **Location** – bestimmte IP-Adresse
- **Zeit** – im Vergleich zur letzten oder zu üblichen Sessions

Die Zwei-Faktor-Authentifizierung (2FA) ist den meisten Anwendern als Variante von MFA bekannt, auch wenn der Begriff vielleicht noch nicht so geläufig ist. Beim Geldabheben am Automaten verwenden wir seit Jahren 2FA: Nur wenn die Bankkarte benutzt wird (etwas, das man besitzt) und der korrekte PIN-Code eingegeben wird (etwas, das man weiss), lässt sich die Transaktion durchführen.

Der Markt bietet eine Vielzahl unterschiedlicher Varianten der Authentifizierung an, und je nach Anwendungsfall kann der zweite Faktor ganz unterschiedlich gewählt werden. So gibt es zahllose Geräte und Lösungen, die sich zur Zwei-Faktor-Authentifizierung einsetzen lassen: von Tokens über Einmal-Passwörter (OTP) via SMS und RFID-Karten bis hin zu Smartphone-Apps oder Mobile ID. Die meisten dieser Methoden bringen jedoch auch bestimmte Nachteile mit sich, wie:

- Medienbruch
- Zusätzliche Hardware
- Verzögerte Zustellung / E-Mails nicht zuverlässig (Spam)
- Kein direkter Bezug zum Unternehmen → Vertrauensverlust
- Kostenfaktoren

Benutzername und Passwort – noch zeitgemäss?

Ob beim Online-Einkauf, auf Social-Media-Kanälen oder beim Online-Banking: Benutzername und Passwort dienen häufig zur Legitimation bzw. zur Überprüfung der Identität. Diese sogenannte Ein-Faktor-Authentifizierung basiert zwar auf der Kombination von zwei Merkmalen – 1. Benutzername und 2. Passwort. Beide Merkmale gehören aber zum selben Faktor – dem Wissensfaktor.

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Die einfache Implementierung und geringen Kosten sind die wichtigsten Gründe, warum Passwörter bis heute die häufigste Form der Ein-Faktor-Authentifizierung sind. Sie rechtfertigen diese jedoch nicht. Fällt ein Passwort in die falschen Hände, kann das schwerwiegende Folgen haben. So können Cyber-Kriminelle unter falscher Identität Waren einkaufen, Online-Konten plündern oder Chats für ihre persönlichen Zwecke missbrauchen. Somit gilt: Wer beim Zugang zu Systemen nur auf Benutzername und Kennwort vertraut, ist nur bedingt sicher. Auch ein sorgfältig ausgewähltes Passwort allein kann heute nicht mehr als sicher eingestuft werden.

Hinzu kommt, dass je nach Branche oder Geschäftsprozess ein Faktor unter Umständen regulatorisch nicht mehr ausreicht. Zwei Merkmale aus dem Bereich Wissen (Benutzername und Passwort) genügen nicht. Multi-Faktor-Authentifizierung ist zwingend erforderlich. Dies spielt insbesondere beim Schutz von Sozialdaten sowie bei Geldtransaktionen eine entscheidende Rolle.

2FA – 2-Faktor-Authentifizierung

Der Authentisierungsprozess bei der 2-Faktor-Authentifizierung beginnt normalerweise mit der Eingabe eines sicheren Passworts – dem ersten Faktor. Bestätigt das System die Richtigkeit des eingegebenen Kennworts, führt dies nicht direkt zum gewünschten Inhalt, sondern zu einer zusätzlichen Sicherheitsschranke – dem zweiten Faktor. So lässt sich verhindern, dass jemand, der unbefugt im Besitz des Passworts ist, Zugang zu Daten oder Funktionen erhält. 2FA funktioniert aber auch ganz ohne Passwort.

2FA ohne Passwort

Der zweite Faktor kann, wie oben erwähnt, ein Zusatzgerät (Besitz) erfordern. Im Gegensatz zum Smartphone ist das allerdings nicht immer zur Hand. Alternativ bietet die passwortfreie Authentisierung mit einem biometrischen Merkmal (Sein) eine einfache und sichere Identifikation und beantwortet die Frage „Wer sind Sie?“ mit diesem zweiten Faktor. Die passwortfreie Authentifizierung zielt darauf ab, biometrische Daten (ein Set von Fingerabdrücken, das Gesicht oder das Muster der Iris) zu erfassen, mit denen Personen klar und eindeutig identifiziert werden können. Bei der Authentisierung werden diese biometrischen Merkmale mit Hilfe biometrischer Sensoren erfasst und dann mit den bereits auf dem Gerät gespeicherten Daten abgeglichen. Stimmen die gescannten Daten mit den gespeicherten Merkmalen überein, werden sie authentifiziert.

Um Kunden durch die optimale Kombination aus Benutzerfreundlichkeit und Sicherheit zu gewinnen und zu halten, kommt es darauf an, eine langfristige Sicherheitsstrategie zu entwickeln. Dabei ist es längst überfällig, sich von der rein wissensbasierten Authentisierung zu verabschieden.

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Die passwortlose Authentisierung bietet vier entscheidende Vorteile gegenüber der traditionellen, wissensbasierten Authentisierung:

- Wirtschaftlichkeit: Sie erhöht die Einnahmen und senkt die Kosten (z.B. entfallen SMS-Gebühren)
- Bessere Benutzererfahrung: Sicheres Einloggen und Shoppen ohne Hindernisse
- Strategischen Wettbewerbsvorsprung: Höhere Interoperabilität dank FIDO-Standard
- Optimierte Sicherheit[1]

FIDO (Fast Identity Online) – der Standard zur passwortfreien Authentifizierung

FIDO ist das weltweit grösste Ökosystem für standardbasierte, interoperable Authentisierung, mit dem Ziel, das Passwort-Problem der Welt zu lösen. Der FIDO-Standard ist ein offener Industriestandard für die sichere, schnelle und einfache Authentisierung im Internet. Er gibt Unternehmen die Möglichkeit, in ihren Produkten hardwaregestützte Authentisierung wie Fingerabdruck- oder Gesichtserkennung einzusetzen. Die Benutzer der Produkte können sich so einfach bei Online-Services anmelden und müssen sich dafür keine komplizierten Passwörter merken.

Was kann die Authentication Cloud?

Nevis Authentication Cloud

Authentifizierung bedeutet, dass die digitale Identität eines Benutzers erkannt wird und sichergestellt ist, dass die Person tatsächlich diejenige ist, die sie vorgibt zu sein. Im Zusammenhang mit Online-Diensten kann Nevis demnach garantieren, dass die Person, die sich anmeldet, auch die Person ist, die das jeweilige Konto erstellt hat – und nicht zum Beispiel ein Bot, der mittels Brute Force Attack (Durchprobieren unzähliger Passwörter) einzudringen versucht.

Wenn sich ein Benutzer das erste Mal für ein Konto anmeldet, ist es üblich, ein Passwort festzulegen. Für die Einrichtung eines Kontos kann als Alternative die Nevis Access App zur Authentifizierung verwendet werden. User füllen wie üblich das Anmeldeformular aus, aber als Teil des Prozesses wird das Konto mit der Nevis Access App verbunden (z.B. über Scanning eines QR-Codes). Mittels Biometrie greift das System dann auf den Sicherheits-Chip im Smartphone zu und erstellt die Verlinkung zum Konto. Ab diesem Zeitpunkt kann der Benutzer komplett auf Passwörter verzichten.

Die Nevis Authentication Cloud...
...erweitert Ihre Infrastruktur mit kennwortloser Authentifizierung und Transaktionssignierung als Service. Unsere FIDO-zertifizierte Lösung bietet die Authentifizierungserfahrung, die Endbenutzer heute erwarten. Ihre Kunden können sich ohne Passwort anmelden. Und

1: *World Economic Forum - Passwordless Authentication: The next breakthrough in secure digital transformation, S. 13*

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

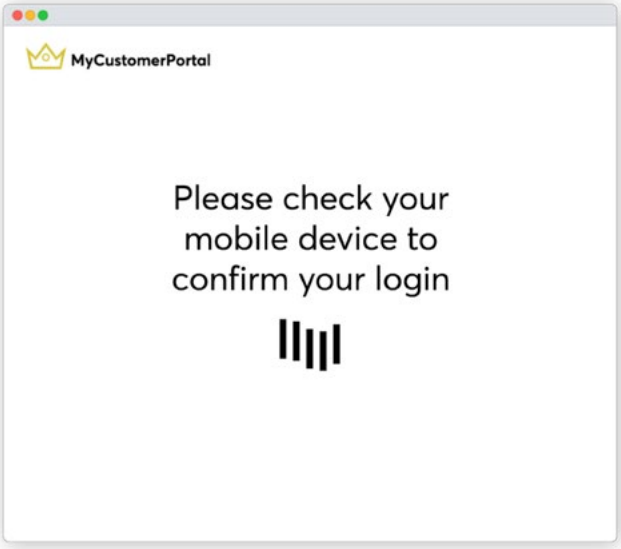
weil sie dazu nur das Mobiltelefon mit seinem Sicherheits-Chip benötigen, ist der Prozess komfortabler und zuverlässiger. Diese Multi-Faktor-Methode ist viel sicherer als die alten, passwortbasierten Lösungen. Mit modernster serverseitiger Technologie kann das System zudem für besonders sensible Bereiche zur Transaktionsbestätigung genutzt werden.

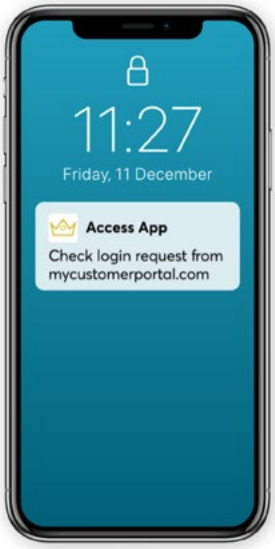
Nevis bietet eine passwortfreie Login-Erfahrung, die die biometrischen Authentifizierungsmöglichkeiten moderner Smartphones nutzt. Die zugrundeliegende Technologie basiert auf dem bewährten FIDO-Standard, der Interoperabilität und langfristigen Investitionsschutz gewährleistet. Als Mitglied der FIDO-Allianz engagiert sich Nevis stark für die Unterstützung aktueller und zukünftiger FIDO-Standards. Mit seiner zertifizierten FIDO-Implementierung garantiert Nevis die Erfüllung der anspruchsvollen Sicherheits- und Interoperabilitätsanforderungen des FIDO-Sicherheitsstandards. Die mobile Authentisierungslösung von Nevis ist als SaaS-Angebot (Software as a Service) oder alternativ On-Premise (vor Ort) erhältlich.

Passwortfreie Authentifizierung

Passwortfreie Authentifizierung ist eine Angelegenheit von wenigen Sekunden, wobei die meisten davon auf die Eingabe des Benutzernamens oder einer E-Mail-Adresse entfallen. Wenn der Browser ab der zweiten Anmeldung die E-Mail-Adresse automatisch ergänzt, geht es noch schneller.

Das Zukunftsszenario wird geprägt durch maximale Benutzerfreundlichkeit: Ihre Kunden geben ihren Benutzernamen auf der Anmeldeseite ein und tippen auf ihrem Mobiltelefon auf die Schaltfläche „Anmelden“. Die Nevis Authentication Cloud-Instanz schickt eine Push-Benachrichtigung (bei Mobile First einen Deep Link) an das Mobiltelefon des Benutzers. Nach dem Öffnen der Benachrichtigung kann sich der Benutzer mit der von ihm gewählten biometrischen Methode authentifizieren. Wenn der Vorgang abgeschlossen ist, bestätigt die Nevis Access App die Identität, und die Authentifizierung ist erfolgreich. Der Benutzer wird automatisch eingeloggt.





Video Clip ansehen

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

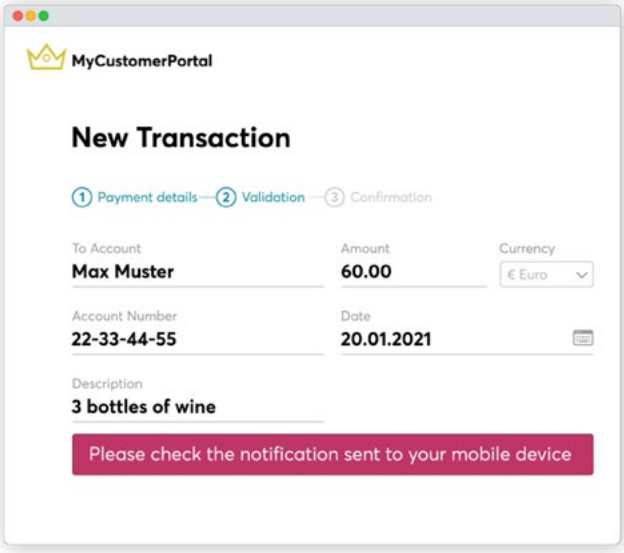
Transaktionsbestätigung (Transaction Confirmation)

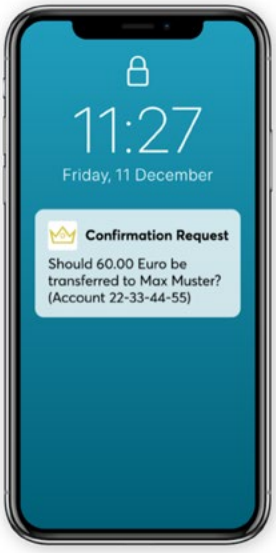
Die Transaktionsbestätigung (englisch: Transaction Confirmation) ist eine zusätzliche Sicherheitsmassnahme, die für bestimmte Finanztransaktionen und Informationsaktualisierungen erforderlich ist. Diese wird verwendet, wenn der Benutzer zusätzlich zur Authentisierung bestimmte Informationen prüfen und bestätigen muss. Die Transaktionsbestätigung ermöglicht, mit nur einem Klick, sowohl finanzielle als auch betriebliche Transaktionen sicher und eindeutig zu bestätigen.

Eine Push-Benachrichtigung informiert den Nutzer über die bevorstehende Transaktion. Anschliessend werden alle notwendigen Einzelheiten zur Transaktion angezeigt, sodass der Kunde vor der Freigabe die Angaben einsehen und gegebenenfalls korrigieren kann. Nach Prüfung der Daten kann die Transaktion ganz einfach durch Scannen des Fingerabdrucks, des Gesichts oder durch die Eingabe eines PINs bestätigt oder abgelehnt werden.

Mit der Transaktionsbestätigung wird nicht nur die Sicherheit gegen mögliche Betrugsangriffe erhöht, sondern auch menschlichen Fehlern oder Vertippen vorgebeugt.

Neben der erhöhten Sicherheit für Kunden bietet die Einführung der Transaktionsbestätigung auch massgebliche Vorteile für Unternehmen. Alle Transaktionen, ob bestätigt oder abgelehnt, werden im Hintergrund protokolliert und archiviert. Dies ermöglicht es, im Zweifelsfall zu beweisen, ob und wann eine Transaktion genehmigt oder abgelehnt wurde. Besonders praktisch ist dies auch in Hinblick auf einzuhaltende Compliance- und Wirtschaftsprüfungsrichtlinien.





Video Clip ansehen

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Sogenannter Friendly Fraud, bei welchem Kunden fälschlicherweise Rückvergütungsansprüche stellen, wird durch Transaction Confirmation ebenfalls verhindert. Zudem werden Kunden vor Phishing-, Social-Engineering- und Data-Switching-Attacken geschützt. Auch bekannte Sicherheitsprobleme, mit welchen SMS-OTP-Anbieter zu kämpfen haben (z. B. Abfangen von SMS oder SIM-Swapping), stellen bei Mobile Transaction Confirmation kein Problem dar.

Offen bleibt noch die Frage, wie man beweisen kann, dass die Person, die die Transaktion initiiert hat, die richtige Person ist. Dieses Problem kann durch eine biometrische Verifikation des Benutzers gelöst werden, ganz ähnlich wie bei der Authentifizierung beim Login. Die Funktionalität der Transaktionssignierung setzt also nicht nur das Prinzip „What you see is what you sign" um, sondern garantiert auch die Unleugbarkeit bestätigter Transaktionen. Die möglichen Anwendungsfälle sind nahezu endlos:

- Bestätigung von Zahlungen
- E-Commerce-Transaktionen
- Erteilung von DSGVO[1]-Einwilligungen
- Bestätigung von ZertES-konformen Dokumentensignierungsprozessen und viele mehr

Branded Access App

Eine erfolgreiche Marke aufzubauen kann Jahre dauern. Es gilt, die gewünschte Markenwahrnehmung bei den Kunden zu erzielen, Vertrauen und Loyalität zu schaffen, positive Emotionen zu erzeugen und sich gleichzeitig von der Konkurrenz abzugrenzen. Dazu gehört, dass Sie unabhängig von Kanal oder Endgerät mit einem konsistenten Markenauftritt an die Kunden herantreten. Sowohl die Kernbotschaft als auch visuelle Elemente der Markenidentität sollten die Kunden in der einen oder anderen Form immer wiederfinden können.

Ihre Marke muss Vertrauen vermitteln. Vertrauen, das Sie sich bei Ihren Kunden erworben haben. Deshalb haben wir unsere Access App nach Ihren Vorgaben markenfähig gestaltet. Sie trägt ohne Programmieraufwand Ihr Logo, Ihre Farben und die Schriftart Ihrer Wahl. Der einheitliche Auftritt unterstützt Sie dabei, von Ihren Kunden das gewünschte Vertrauen zu erhalten. Die Sicherheitsmerkmale in der App werden Ihnen helfen, dieses Vertrauen weiter zu stärken.

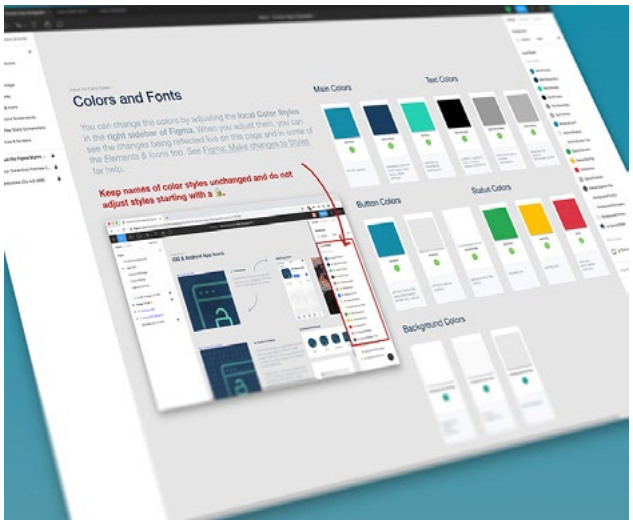
Darüber hinaus unterscheiden Sie sich deutlich von Ihren Mitbewerbern, wenn die Access App Ihre Corporate Identity kommuniziert und in Ihrem Design gestaltet ist. Dies gibt Ihren Benutzern die nötige Gewissheit, dass ihre Daten und ihr Konto bei Ihnen sicher sind. Denn wer würde sich schon bei einer namenlosen, unbekannten App authentifizieren wollen, bei der unklar ist, ob sie wirklich mit der gewünschten Marke und dem zugehörigen Unternehmen in Zusammenhang steht?

1: Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union ist seit dem 25. Mai 2018 in Kraft.

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Damit Sie weder bei Markenauftritt und beim Kundenerlebnis noch bei der Sicherheit Kompromisse eingehen müssen, können Sie unsere Access App komplett nach Ihren visuellen und kommunikativen Anforderungen gestalten: Unsere App ist komplett „brandable“. Aber was bedeutet das genau?

Komplett „brandable“ heisst, dass Sie jedes Detail der App flexibel und nach Belieben an Ihr Corporate Design anpassen können: Farben, Schriftarten, Texte, Bilder, Icons und Hintergrund. Sogar die Sprache, in welcher Nachrichten und Inhalte in der App angezeigt werden, können Sie frei wählen.



Ist es nicht grossartig, so viele Möglichkeiten beim individuellen Branding und Design der Access App zu haben? In der Gestaltung führt unbegrenzte Freiheit jedoch oft dazu, dass man viel Zeit zum Konfigurieren investiert, bevor man erste Ergebnisse vorweisen kann. Deshalb haben wir für Sie eine Figma-Vorlage der App erstellt. Diese ermöglicht Ihnen, alle App-Bildschirme mit wenigen Klicks anzupassen. Mit der praktischen Vorschau-Funktion können Sie jeden einzelnen App-Screen auf Herz und Nieren testen, bevor Sie die App im Apple App Store oder auf Google Play veröffentlichen.

Für Unternehmen mit sehr anspruchsvollen CI/CD-Anforderungen gibt es zusätzlich die Möglichkeit, benutzerdefinierte Icons hochzuladen, App-Hintergründe zu erstellen sowie Texte und Benachrichtigungen, welche in der App angezeigt werden, selbst festzulegen. Das Einzige, was Sie in der Nevis Access App nicht ändern können, ist das Layout und die Form der einzelnen Felder sowie die Anzahl der Bildschirme in der App.

Die wichtigsten Eigenschaften der Nevis Access App:

- White Label Mobile App, komplett brandable
- Mobile SDK (integriert in bestehende Geschäftsanwendung)
- Folgt dem Branchenstandard und ist FIDO-zertifiziert
- Entspricht DSGVO, SCA[1], PSD2[2] und anderen Vorschriften
- Passwortfrei (implizite MFA)
- Biometrische Authentifizierung
- Die Anwendung ist gehärtet und End-to-End verschlüsselt

1: Strong Customer Authentication (SCA) bietet eine zusätzliche Sicherheitsebene, wenn Kunden eine Online-Transaktion vornehmen.
2: Die zweite Zahlungsdiensterichtlinie von 2015 (Payment Services Directive, PSD2) reguliert Zahlungsdienste in der EU.

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Zusätzlich zur brandable White Label Access App bieten wir Ihnen die Option, unsere Authentication Cloud mittels eines nach FIDO UAF 1.1 zertifizierten Software-Entwicklungs-Kits (SDK) in Ihre native Mobile App zu integrieren. Die Verwendung des SDK bietet sich speziell für jene Unternehmen an, die bereits eine native Mobile App für ihre Kunden in Betrieb haben oder daran sind, eine solche zu entwickeln.
Ob Sie nun unsere brandable White Label Access App nutzen oder den Authentication Cloud SDK in Ihre native App einbauen, spielt für Ihre Kunden keine Rolle. Mit beiden Varianten signalisieren Sie, dass bei Ihnen Sicherheit und Convenience an erster Stelle stehen und Sie bei keinem der beiden Aspekte Kompromisse eingehen.

Management Console

Die Nevis Authentication Cloud Management Console gibt Systemadministratoren alle erforderlichen Werkzeuge an die Hand, um die von Ihnen integrierten Anwendungen zu verwalten und das Branding der White-Label-App anzupassen. Sie können damit ferner alle Benutzerkonten einsehen, ändern oder löschen.

Die Konsole eröffnet komfortable Optionen, neue Web-Anwendungen zu integrieren – sowohl für massgeschneiderte Applikationen als auch für bestehende Nevis Security-Suite-Instanzen. Sie können über die Konsole auch die Zugriffs-Token verwalten, welche die Anwendungen für Login-Genehmigungen und Transaktionssignierung verwenden.

Die Konsole bietet darüber hinaus eine einfach zu bedienende Schnittstelle für die Benutzer- und Geräteverwaltung. Admins haben die Möglichkeit, nach Benutzern und Geräten zu suchen, um etwa inaktive Benutzer und veraltete Authentifikatoren (d.h. alte Telefone) aus dem System zu entfernen.

Außerdem können Unternehmen die Konsole verwenden, um das Branding ihrer White Label App zu gestalten und anzupassen. So kann die App anschliessend ohne jeglichen Programmieraufwand in die App-Stores von Apple und Google gestellt werden.

FIDO und Nevis

Das Mobilgerät wird zunehmend der primäre oder sogar alleinige Kanal für den Kontakt zu Unternehmen. Nevis ermöglicht dem Kunden eine benutzerfreundliche, starke Authentisierung auf dem Mobilgerät mit Fingerabdruck- und Gesichtserkennung, und zwar basierend auf dem FIDO-Standard.

Auf mobilen Geräten gibt es zu diesem Zweck einen separaten, sicheren Chip, der völlig unabhängig von den anderen Komponenten des Geräts arbeitet. Er dient ausschliesslich der Speicherung und Verarbeitung der biometrischen Daten und Authentifizierungsanfragen. Die Daten verlassen das Gerät nie, können nicht manipuliert werden und sind nicht einmal für die Authentisierungsanwendung (z.B. Ihre Access App) zugänglich. So behält der Benutzer die alleinige Kontrolle über seine biometrischen Merkmale.

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Im Hintergrund, während des Anmeldeprozesses, erweitert sich der Informationsfluss zur Nevis Authentication Cloud-Instanz, in der die Benutzeridentität DSGVO-konform gespeichert und ein benutzerspezifischer QR-Code bzw. Deep Link generiert wird. Die Nevis Access-Anwendung liest diesen Code und authentisiert den Nutzer anschliessend anhand seiner hinterlegten biometrischen Merkmale. Auf diese Weise werden der private kryptografische Schlüssel auf dem Sicherheits-Chip des Geräts und der öffentliche Schlüssel auf dem Server gepaart, um eine passwortfreie Anmeldung zu ermöglichen.

Wie Nevis dem Unternehmen hilft

Was ist der Nutzen für den Endkunden?

Kunden wollen mit minimalem Aufwand und maximaler Sicherheit auf Online-Angebote zugreifen. Sie erwarten innovative und aussergewöhnliche Erlebnisse, wenn es um ihre Kundenidentität geht, aber auch den höchsten Standard bei Sicherheit, Datenschutz und Compliance. Kunden erwarten…

- ein reibungsloses Erlebnis über alle Kanäle
- einen intuitiven, benutzerfreundlichen und sicheren digitalen Zugang
- Schutz vor Identitätsdiebstahl
- passwortfreie, sekundenschnelle Anmeldung, so einfach wie die Entsperrung des Smartphones
- keine zusätzlichen Geräte oder Verfahren
- bequeme Transaktionsbestätigungen

Was ist der Businessnutzen?

Unternehmen müssen das Vertrauen und die Loyalität der Kunden gewinnen, um neue Möglichkeiten für Wachstum und Wettbewerbsvorteile zu erschliessen. Es ist von entscheidender Bedeutung, eine führende Rolle im digitalen Ökosystem zu übernehmen und den heutigen Anforderungen der digitalen Transformation gerecht zu werden. Neue Angebote müssen schnell verfügbar sein, und die Kosten sollten auf ein Minimum beschränkt werden. Mit der Authentication Cloud gewinnen Sie viele Vorteile. Einige Highlights:

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

- Deutlich bessere Usability durch Eliminierung unnötiger Schritte
  - Steigert Kunden-Loyalität
  - Steigert Bereitschaft, Premium Price zu bezahlen
- Niedriger TCO (Total Cost of Ownership), da in nur wenigen Schritten in Ihre IT-Umgebung integriert
- Verfügbar als App mit benutzerdefiniertem Branding oder mit SDK integrierbar in bestehende App
- Die Kombination von High-End-Sicherheit mit großer Benutzerfreundlichkeit wird dazu beitragen, die Interaktionsraten mit Kunden zu erhöhen und gleichzeitig alle gesetzlichen Anforderungen zu erfüllen
- Verkürzte Markteinführungszeit für digitale Angebote
- Mehr Kundeninteraktionen ohne SMS-Mehrkosten
- Weniger abgebrochene Conversion-Prozesse mit sicherer und einfacher Transaktionsbestätigung (FIDO)
- Sichere und intuitive Online-Geschäfte dank PSD2-, SCA- und DSGVO-konformer Transaktionsbestätigung
- Investitionsschutz: Die FIDO-basierte Implementierung ermöglicht eine schnelle Anpassung an die zukünftigen Fähigkeiten mobiler Geräte
- Die FIDO-Zertifizierung garantiert die Erfüllung anspruchsvoller Sicherheits- und Interoperabilitätsanforderungen.

Was ist der Nutzen für die IT?

Ohne IT ist Innovation durch Digitalisierung kaum realisierbar. Doch die Anforderungen sind vielfältig: Eine kohärente Sicherheitsinfrastruktur muss einen einfachen und sicheren Zugang zu Online-Diensten bieten, den gesetzlichen Richtlinien und der Compliance entsprechen und möglichst wenig Wartungs- und Helpdesk-Aufwand generieren. Die Authentication Cloud bietet maximale Unterstützung bei der Erreichung dieser Ziele. Sie spart Kosten und bietet gleichzeitig Rechtssicherheit:

- In wenigen Schritten in Ihre IT-Umgebung integriert, ohne zusätzliche Investitionen in die Infrastruktur
- Out-of-the-Box-Integration für Azure AD B2C
- Schnelle Einbindung mittels Widget in E-Commerce-Shops, Portale usw.
- Automatisierte Standardprozesse reduzieren den Helpdesk-Aufwand
- Verfügbar als App mit individuellem Branding und als Software Development Kit (SDK)
- Rechenzentrum entweder in der EU oder in der Schweiz
- Erfüllt alle Bestimmungen bezüglich Datenschutz, Einwilligung und Löschung, wie DSGVO, PSD2, GKV-SV usw.
- Die FIDO-Zertifizierung garantiert die Erfüllung anspruchsvoller Sicherheits- und Interoperabilitätsanforderungen

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Wie profitieren Branchen?

Unternehmen aller Branchen müssen sich der Herausforderung stellen, dass ihre Kunden immer öfter und immer länger online und mobil unterwegs sind. Bieten Sie den Kunden online keinen komfortablen und sicheren Zugriff auf Ihre Dienstleistungen, wechseln sie schnell zur Konkurrenz.

Nutzen Sie die Nevis Authentication Cloud. So können Ihre Kunden rund um die Uhr von unterwegs auf einfache Weise und gut geschützt ihre Online-Geschäfte mit Ihnen abwickeln. Die Nevis Authentication Cloud bietet Ihren Kunden:

- Zugriff rund um die Uhr
- Zugriff von unterwegs
- Passwortfreien Zugriff
- Sicheren Zugriff

Ein gutes Kundenerlebnis wird die Interaktionen erhöhen. Weil die Authentication Cloud ohne SMS auskommt, ist das „Return on Investment“ (ROI) oft nach dem 1. Monat schon erreicht.

Jede Branche ist jedoch einzigartig und hat ihre Herausforderungen. Die Nevis Authentication Cloud bietet für die spezifischen Probleme Ihrer Branche Lösungen, mit denen Sie sich von der Konkurrenz abheben:

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Branche	Problem	Lösung	Vorteil
Financial Services und Banking	Komplizierter Konto-Zugriff via externes Tool	passwortfreie Login-App	Steigerung der Benutzer-interaktionen
	Identitätsdiebstahl	passwortlose Login-App: Transaktionen biometrisch genehmigen	Vertrauen der Kunden bleibt. Gute Reputation
	Einhalten von Regulatorien	2FA mit passwortloser Transaktionsbestätigung (FIDO-Standard)	PSD2- und DSGVO-Konformität
Behörden	Schaltergeschäfte sind zeitlich aufwändig	Online-Geschäfte abgesichert mit Transaction Confirmation, auch für Dokumenten-Bestätigung 2FA für alle Geschäfte	Beschleunigung von Prozessen Absicherung von Transaktionen Einsparung von Zeit, Aufwand und Geld Gesteigerte Kundenfreundlichkeit und Reputationsgewinn
	Klassische Dokumentensignierung kann nicht eindeutig einer Person zugeordnet werden	Nur Transaktionen, die biometrisch authentifiziert werden, werden auch durchgeführt	Absicherung von Transaktionen Einsparung von Zeit, Aufwand und Geld Gesteigerte Kundenfreundlichkeit und Reputationsgewinn
Versicherungen	Komplizierter Zugriff auf das Versicherungsportal	Passwortlose Login-App	Steigerung der Benutzer-interaktionen
	Kommunikation mit Kunden via E-Mail ist umständlich	Push-Notifikationen via Login-App	Steigerung der Benutzer-interaktionen
	Hochladen von sensitiven Informationen ist heikel	Passwortfreie, biometrische 2FA	Compliance/Datenschutz
ICM und Maschinenbau	Zugriff auf das Industrieportal ist unsicher und kompliziert	Passwortfreie, biometrische 2FA	Schutz für geistiges Eigentum Zeitgewinn für Partner, Händler usw. SMS-Gebühren entfallen
Gesundheitswesen	Zugriff ins E-Health-Portal ist kompliziert	Passwortfreie, biometrische 2FA	Zeitgewinn für Kunden SMS-Gebühren entfallen
	Keine Kontrolle darüber, wer Zugriff auf persönliche Daten erhält	Bestätigung der Einsicht für Drittpersonen Transaktionsbestätigung bei Bedarf	Kontrolle für Patienten. Reduzierung von Support-Aufwand und -Kosten für Anbieter Kürzere Wege, schnellere Entscheidungen Vertrauensgewinn

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Branche	Problem	Lösung	Vorteil
E-Commerce	Shop-Login ist kompliziert bzw. Benutzername und Passwort sind oft nicht zur Hand	Passwortfreie Anmeldung	Weniger Transaktionsabbrüche und mehr Umsatz
	SMS-Nachrichten verursachen Kosten	Passwortfreie Bestätigung	SMS-Transaktionskosten entfallen
	Integration von Sicherheitsmechanismen ist kompliziert	Shopware-Plugin verwenden[1]	Schnelle Einbindung von bequemer Verbesserung der Sicherheit
Glückspielanbieter	Familienmitglieder mit Login-Daten können auf Spielerkonto zugreifen	Biometrische, passwortfreie Authentifizierung	Compliance: Zugriff ist geschützt und nur für autorisierten Spieler möglich
	Spieleinsätze sind nicht abgesichert	Transaktionsbestätigung	Sensible Transaktionen sind sicher Der Spieler ist abgesichert

1: Funktioniert nur mit „Shopware"-Systemen.

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

nevis®

Making security an experience.

Über Nevis

Die Nevis Security AG ist ein Pionier in der digitalen Sicherheit und macht sich weltweit für den Einsatz passwortloser, benutzerfreundlicher Zugangslösungen stark. Als Schweizer Marktführer im Bereich Customer Identity and Access Management (CIAM) stattet Nevis Organisationen aus dem Finanz-, Versicherungs- und iGaming-Sektor mit einem Höchstmass an Datenschutz und nahtlosen Authentifizierungsverfahren aus. Nevis-Technologie sichert mehr als 80 Prozent der Online-Banking-Transaktionen in der Schweiz ab – ein Indiz für Expertise und Engagement für Innovation. Mit Hauptsitz in Zürich/Schweiz und Niederlassungen in ganz Europa baut Nevis seine globale Präsenz durch ein schnell wachsendes Partnernetzwerk permanent aus und unterstreicht damit seine Rolle als wichtiger Akteur im digitalen Ökosystem. Nevis strebt danach, seine Stellung als führende Instanz im Bereich der digitalen Identitätssicherheit weltweit zu stärken und skalierbare, zukunftsweisende Lösungen bereitzustellen, die den wachsenden Anforderungen seiner Kunden gerecht werden.

www.nevis.net

© 2024 Nevis Security AG. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch Nevis Security AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden. Die von Nevis Security AG angebotenen Softwareprodukte können Softwarekomponenten auch anderer Softwarehersteller enthalten. Produkte können länderspezifische Unterschiede aufweisen.

Die vorliegenden Unterlagen werden von der Nevis Security AG bereitgestellt und dienen ausschliesslich zu Informationszwecken. Die Nevis Security AG übernimmt keinerlei Haftung oder Gewährleistung für Fehler oder Unvollständigkeiten in dieser Publikation. Die Nevis Security AG steht lediglich für Produkte und Dienstleistungen nach der Massgabe ein, die in der Vereinbarung über die jeweiligen Produkte und Dienstleistungen ausdrücklich geregelt ist. Keine der hierin enthaltenen Informationen ist als zusätzliche Garantie zu interpretieren.

Insbesondere ist die Nevis Security AG in keiner Weise verpflichtet, in dieser Publikation oder einer zugehörigen Präsentation dargestellte Geschäftsabläufe zu verfolgen oder hierin wiedergegebene Funktionen zu entwickeln oder zu veröffentlichen.

Diese Publikation oder eine zugehörige Präsentation, die Strategie und etwaige künftige Entwicklungen, Produkte und/oder Plattformen können von der Nevis Security AG jederzeit und ohne Angabe von Gründen unangekündigt geändert werden. Die in dieser Publikation enthaltenen Informationen stellen keine Zusage, kein Versprechen und keine rechtliche Verpflichtung zur Lieferung von Material, Code oder Funktionen dar. Sämtliche vorausschauenden Aussagen unterliegen unterschiedlichen Risiken und Unsicherheiten, durch die die tatsächlichen Ergebnisse von den Erwartungen abweichen können. Dem Leser wird empfohlen, diesen vorausschauenden Aussagen kein übertriebenes Vertrauen zu schenken und sich bei Kaufentscheidungen nicht auf sie zu stützen.