nevis®

Solution Paper

Nevis ID

Making security an experience.

Inhalt

Einleitung

Die Geschäftswelt entwickelt sich mit einer enormen Dynamik, die Digitalisierung schreitet voran. Immer mehr Dienstleistungen werden heute in digitaler Form angeboten. Dies hat Auswirkungen auf die Geschäftsprozesse und -modelle. Alles, was bisher analog in der realen Welt gekauft werden konnte, kann nun auch online erworben werden. Kunden sind zwar bei der Weitergabe ihrer eigenen Daten sehr zurückhaltend. Wenn sie jedoch Ihrer Marke **Vertrauen** schenken[1], sind sie bereit, persönliche Daten preiszugeben. Es versteht sich von selbst, dass der Zugriff auf Ihre Services dabei sicher und schnell erfolgen muss. Das Online-Portal sollte Schutz vor Angriffen jeglicher Art bieten. Sowohl persönliche Daten als auch Business-Anwendungen müssen sicher sein.

Generell gilt es, sensible Informationen in Unternehmen und Behörden wirksam vor unbefugtem Zugriff zu schützen. Gleichzeitig muss es auch möglich sein, diese sicher, rechtskonform, effizient, wirtschaftlich und anwenderfreundlich zu verarbeiten. Um das zu gewährleisten gilt es, die Identität der Kunden zu schützen. Und genau hier ist Sicherheit wichtiger als je zuvor. Oft vergisst man dabei, dass komplizierte Login-Prozesse das erstrebenswerte positive Kundenerlebnis beeinträchtigen.

Positive Kundenerfahrung entscheidend für den wirtschaftlichen Erfolg

Studien zeigen, dass der Wettbewerb zwischen Unternehmen heute zu zwei Dritteln über die Kundenerfahrung ausgetragen wird. 2010 waren es erst 36%[2]. Wer folglich im Markt bestehen will, sollte bei der Digitalen Customer Experience (DCX) keine Wünsche offen lassen. Die Unternehmen kommen nicht darum herum, den Spagat zwischen bestmöglicher User Experience und effizientem Datenschutz zu meistern.

Um dies zu erreichen, setzen Firmen auf leistungsstarke softwarebasierte Lösungen, wie sie Customer-Identity- und Access-Management-Systeme (CIAM) bieten. Diese können nicht nur viele Identitäten bzw. eine grosse Anzahl an Benutzern, sondern auch Zugriffsberechtigungen zentral und sicher verwalten. Wobei hier nicht nur der Kundenanspruch nach Schnelligkeit und Bequemlichkeit erfüllt wird, sondern als Pflichtaufgabe des CIAM-Systems auch die strenge **DSGVO-Einhaltung** beim Umgang mit persönlichen und vertraulichen Daten gegeben ist.

CIAM-Systeme unterstützen die Realisierung effizienter und sicherer Digitalisierungsinitiativen. Digitale Geschäftsprozesse werden dabei durch eine intuitive, auf Biometrie basierende Multi-Faktor-Authentifizierung (MFA) vorangetrieben und optimiert. Sie fungieren als Hebel zur Effizienzsteigerung bei gleichzeitiger Gewährleistung von Sicherheit, Qualität und Customer Experience. Ihr entscheidender Vorteil ist die Schaffung einer konsistenten und nahtlosen Kundenerfahrung über alle Kanäle hinweg – bis hin zum komfortablen mobilen Kundenerlebnis.

Für alle Unternehmen, die auf erstklassigen Kundenservice setzen und ihren Kunden eine abgesicherte, umfassende Kundenerfahrung geben wollen, bietet ein CIAM-System einen klaren Wettbewerbsvorteil.

1: *PwC: Experience is everything: Here's how to get it right*
2: *Superoffice: Customer Experience Statistics*

Kunden wollen es einfach und sicher

Customer Experience und Customer Trust als Schlüssel zum Erfolg

Das Kundenerlebnis hat sich schnell zu einer Top-Priorität für Unternehmen entwickelt. Denn der nächste Anbieter ist nur einen Klick entfernt. Ab dem ersten Berührungspunkt muss das Kundenerlebnis positiv gestaltet sein. Die Ansprüche der Verbraucher an Geschwindigkeit und Verfügbarkeit von Services und Dienstleistungen sind in den letzten Jahren deutlich gestiegen. Hinzu kommt der Wunsch nach Self-Service-Optionen, welche Kunden befähigen, ihre Daten selbständig zu verwalten und ihre Präferenzen festzulegen.

Als Anbieter müssen Sie sicherstellen, dass Ihre Kunden einen besseren Service erleben als bei den Mitbewerbern. Sie sollten dabei den Fokus auf die anspruchsvollen, digital affinen Kunden richten. Denn wenn diese Kunden zufrieden sind und Ihnen vertrauen, haben positive Empfehlungen eine grosse Reichweite – negative allerdings auch. Und darum sollten Sie erst recht in diesen Bereich investieren.

27%

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

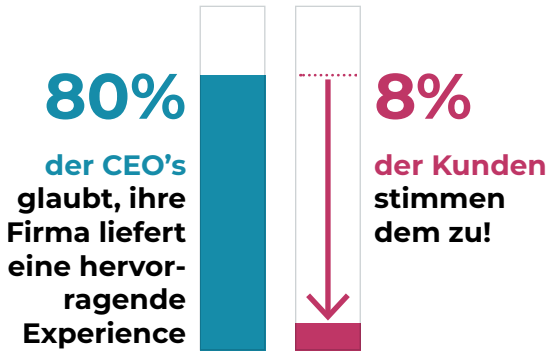
62%

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

Quelle: Experience Gap Report 2018, clearstrategy.com

Doch vielen Anbietern unterschiedlichster Branchen ist die Kluft zwischen den Kundenerwartungen und der tatsächlichen Kundenerfahrung bis heute nicht bewusst.

Der „Experience Gap“



Bain & Company via Craig McVoy, CCXP

Als Beispiel zeigt eine Untersuchung im E-Commerce, dass die Kunden „Service Transparency" – d.h. Einsicht in den Stand ihrer Bestellung – am höchsten priorisieren. Die Anbieter glauben jedoch, dass dieser Punkt bei ihren Kunden erst an dritter Stelle steht.

Um das Bedürfnis des Kunden nach einer herausragenden „Service Transparency" zu stillen, müsste ihm der Anbieter schnell und unkompliziert Zugriff gewähren, rund um die Uhr, von überall her. Kurzum: ein positives mobiles Erlebnis ist besonders wichtig. Wird das nicht erkannt, führt dies zu Fehlinvestitionen, Frust auf Kundenseite und Abwanderung zu anderen Wettbewerbern.

Aber warum ist es so schwierig zu erkennen, was Kunden wollen bzw. was sie verärgert? Weil die Kunden in den meisten Fällen das Unternehmen stillschweigend verlassen. Nur einer von 26 unzufriedenen Kunden beschwert sich wirklich beim Anbieter. Verstärkt wird das Problem dadurch, dass der Konsument eine negative Erfahrung in der Regel mit mehr Personen teilt als eine positive Erfahrung[1]. Damit haben alle Branchen zu kämpfen. Fehlt das positive Kundenerlebnis, ist das Geschäftswachstum gefährdet.

BRACK.CH

„Nevis kombiniert technischen Sachverstand und umfassende Beratung zu einem attraktiven Gesamtpaket. Nachhaltig beeindruckt hat uns die Dienstleistermentalität. Neben dem Kernthema Sicherheit hatten unsere Ansprechpartner immer zentrale Aspekte wie User Experience und Geschäftsprozesse im Blick."

Marcel Rassinger
CIO der Competec-Gruppe

Ein positives Kundenerlebnis ist verknüpft mit Customer Trust. Das Vertrauen der Kunden wird massgeblich geprägt von den Leistungen, die sie erhalten. Vertrauen entsteht, wenn Sie die Bedürfnisse Ihrer Kunden verstehen, sie respektieren und ihnen einen relevanten Service bieten. Das Vertrauen der Kunden zu gewinnen, ist nicht nur wichtig, damit sie loyal sind und wiederkommen, sondern auch, damit sie darauf bestehen, dass ihre Freunde ebenfalls mit Ihnen Geschäfte machen.

Ein Beispiel, wie verbesserte Customer Experience zu Customer Trust führen kann, ist die Eliminierung von Passwörtern beim Zugriff auf Dienstleistungen.

1: *Superoffice: Customer Experience Statistics*

Passwort als Bürde und Problemquelle

Wenn Sie Nachrichten über gestohlene Passwörter aufgrund eines Datenlecks hören, sind Sie dann erleichtert, dass Ihr Unternehmen nicht betroffen ist? Schön. Wenn Sie nur mit den Schultern zucken, weil Ihre Cybersecurity sowieso auf dem neusten Stand ist, ist das natürlich noch besser. Wenn Sie in beiden Fällen jedoch von den Benutzern Ihrer Dienstleistungen noch Passwörter verlangen, riskieren Sie trotzdem Schäden für Ihr Unternehmen. Weil Passwörter alles andere als benutzerfreundlich sind. Das führt dazu, dass eine grosse Anzahl Nutzer ein und dasselbe Passwort für mehrere Konten verwendet. Ist nun eines dieser Konten von einem Datenleck betroffen und nutzt der User für das Konto bei Ihrem Unternehmen dasselbe Passwort, werden Sie angreifbar. Cyberkriminelle werden gestohlene Passwörter überall dort einsetzen, wo sie die Möglichkeit sehen, Benutzerkonten zu übernehmen. Denn nur gerade 28% der von einem Datenleck betroffenen Nutzer wechseln innerhalb von drei Monaten ihr Passwort. Das riskante Nutzerverhalten bringt somit auch Ihr Unternehmen in Gefahr. Alleine in Q3 2020 gab es 770 Millionen Attacken auf Logins mittels Credential Stuffing[1]. Zu den am schwersten betroffen Industrien zählen dabei Retail, E-Commerce, Gaming und Financial Services. In Großbritannien gingen laut einer Statistik der City of London Police beim Online-Shopping am Black Friday und Cyber Monday allein 16,4 Millionen Pfund durch Cyber-Kriminelle verloren[2].

Nur 28% der User wechseln nach einem Datenleck ihre Passwörter.

Artikel von zdnet.com

Stellen Sie sich vor, Ihr Unternehmen entscheidet sich nun beim Login für eine sichere, passwortfreie Variante, basierend auf biometrischer Authentifizierung, z.B. mittels FaceID oder Fingerabdruck. So nehmen Sie Ihren Kunden die Bürde des Passworts ab. Niemand muss sich mehr mühsam ein Passwort merken oder es regelmässig erneuern oder stärker machen. Sie verbessern das Kundenerlebnis massgeblich. Zugleich wächst das Vertrauen, das der Kunden in Ihr Unternehmen und Ihr Vertrauen in Ihre Kunden.

Sind Customer Experience und IT Security unvereinbare Paradigmen?

Das Anwendererlebnis und die Sicherheit sind wichtige Kriterien, die miteinander ins Gleichgewicht gebracht 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 gross-artiges Nutzererlebnis nicht sicher sein kann. Müssen die Forderungen der Anwender nach einfachem, schnellem und unkompliziertem Online-Zugriff der Sicherheit und Einhaltung der Vorschriften weichen?

1: *Arkose Labs: Q4 2020 Fraud & Abuse Report*
2: *Artikel von Finance Digest*

Der Weg zum positiven und sicheren mobilen Kundenerlebnis führt über moderne Multi-Faktor-Authentifizierung mit Biometrie. Die heute in mobilen Geräten verbauten biometrischen Identifikationstechnologien ermöglichen komplett neue Ansätze im Bereich der Authentifizierung. Der Trend wird zusätzlich befeuert durch neue Standards wie z.B. FIDO (Fast IDentity Online). **Gartner empfiehlt den Anbietern, dem Thema der passwortlosen Authentifizierung 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[1]. 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

Unternehmen müssen heute schneller auf die neuen Anforderungen reagieren – sei es wegen neuer Initiativen oder neuer Bedrohungen. Der Zugang zum Kundenportal bzw. den Online-Dienstleistungen muss dabei rund um die Uhr gegeben, einfach und sicher sein. Sie profitieren davon, wenn Sie die Interaktionsmöglichkeiten mit den Lösungen, die ein CIAM-System bietet, erweitern und vereinfachen.

Eine gute CIAM-Lösung dient als strategisches Mittel für die Kundenbindung und erlaubt eine durchweg positive Erfahrung für den Endbenutzer. Es ist wichtig, das Kundenerlebnis vom ersten Moment an ansprechend zu gestalten.

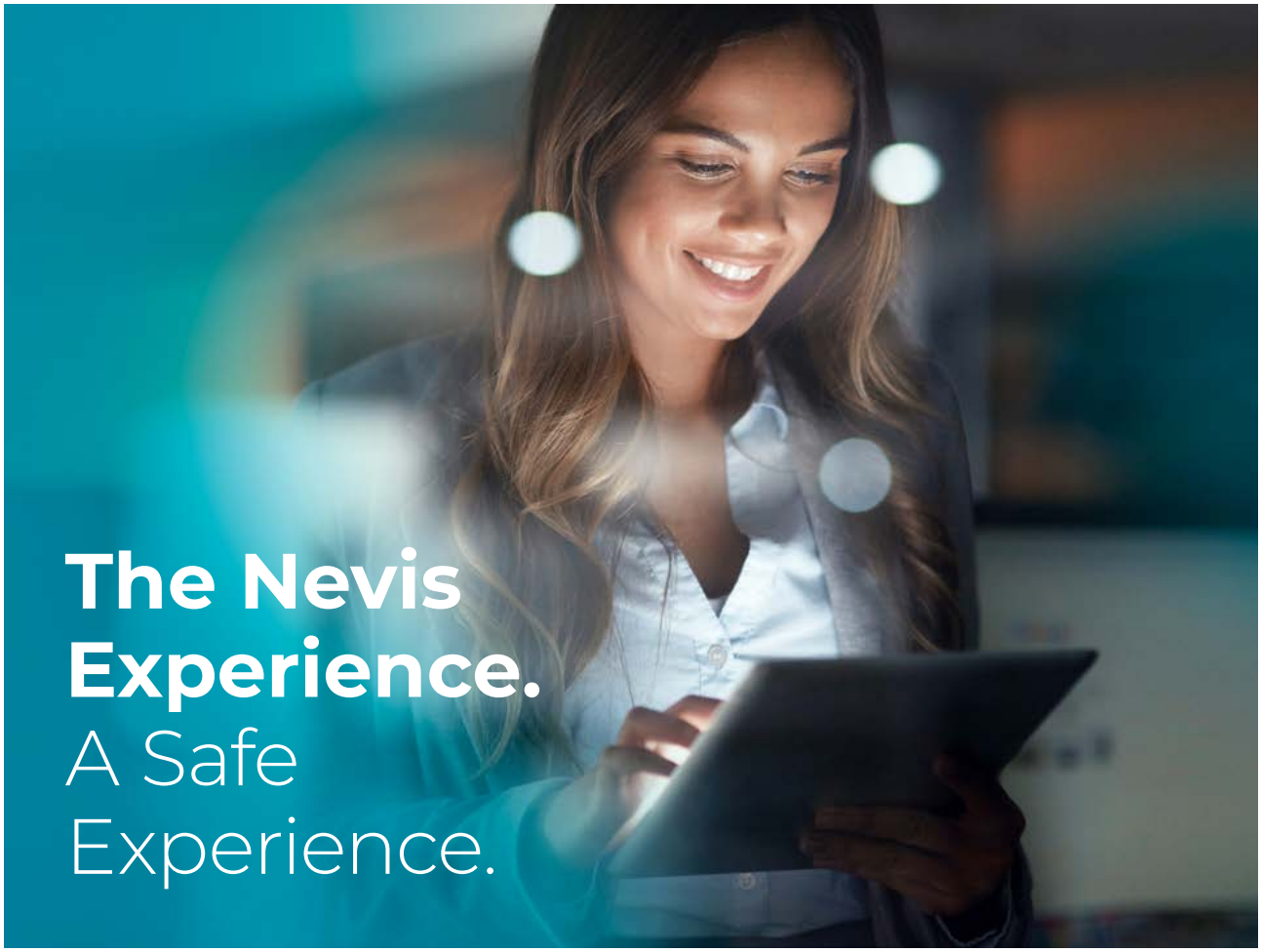
Die Identitäten und Zugänge der Nutzer müssen geschützt und kontrolliert werden, doch nicht auf Kosten des Kundenerlebnisses. Laut Aussagen des US-Analystenhauses Gartner ist Benutzerfreundlichkeit ein Schlüsselfaktor für die Wahl von CIAM-Software: „Customer Experience is the Battlefield"[2]. Aber die Budgets für Customer Experience hinken den gesteigerten Kundenansprüchen hinterher, sagt Gartner: „CX budgets are not increasing with increased expectations"[3] und gefährden somit den Erfolg des Unternehmens. Denn eine zu komplexe Bedienung und ein geschmälertes Nutzererlebnis können sich negativ auswirken – etwa durch Kundenverlust und Gewinneinbruch.

1: Gartner: 2020 Planning Guide for Identity and Access Management
2: Gartner Customer Experience Summit, 2019
3: Gartner Customer Experience Survey, 2018

Ein modernes CIAM-System 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, bietet die Möglichkeit schnellerer Reaktionen auf Veränderungen und somit die Verbesserung Ihrer Dienstleistungen. Darüber hinaus stellt es die Einhaltung komplexer Regularien und Vorschriften wie der DSGVO sicher.

Nutzen Sie die Nevis ID Plattform, um Ihren Benutzern sicheren Zugang zu Informationen und Anwendungen zu bieten, bei Bedarf das Sicherheitsniveau zu erhöhen sowie Identitäten mit allem, was dazu gehört, sicher und effizient zu verwalten.

Wir unterstützen Sie dabei, all diese Aufgaben, die nicht zu Ihrem Kerngeschäft gehören, professionell zu erfüllen. Und denken Sie daran: Wenn Sie das Verlangen Ihrer Kunden nach Komfort und Sicherheit ignorieren, verlieren Sie diese an die Konkurrenz und gewinnen keine neuen hinzu.



CIAM

White Paper **Was ist CIAM** herunterladen

Ein erfolgreiches Kundenerlebnis hängt massgeblich von einem ausgewogenen Verhältnis zwischen Sicherheit und Anwenderfreundlichkeit ab. Für eine personalisierte und relevante Benutzererfahrung sind personenbezogene Daten erforderlich. Um jedoch Zugriff auf diese personenbezogenen Daten zu erhalten, müssen Ihnen Kunden ihr Vertrauen entgegenbringen. Dieses Vertrauen bauen Sie mit einem grossartigen Benutzererlebnis auf. Es ist nicht sinnvoll, für die Usability bei der Sicherheit Abstriche zu machen oder umgekehrt. Das Problem mutet zunächst fast unlösbar an, lässt sich für Unternehmen aber durch die Integration von CIAM in den Griff bekommen.

Die Funktionsbereiche im Customer Identity and Access Management bezeichnen wir mit den drei „C“: Connect (verbinden), Collect (sammeln) und Convert (umwandeln). CIAM ist eine Lösung für die Verwaltung von digitalen Identitäten (Benutzer und die mit diesen Benutzern verknüpften Informationen) und Zugriffsberechtigungen der Benutzer auf Daten, die ein Unternehmen (oder ausgelagerter Cloud-Anbieter) sammelt und speichert. Dank dieser digitalen Identitäten erhalten Kunden komfortablen und dennoch sicheren Zugriff auf ihre Benutzerkonten und Daten. So legen Unternehmen ganz einfach den Grundstein für einzigartige und personalisierte Benutzererlebnisse.

Im Gegensatz zu Identity and Access Management (IAM) ist CIAM eine kundenorientierte Lösung, die einen Grossteil der Entscheidungen über Datenspeicherung und Zugriffsrechte in die Hände der Benutzer selbst legt. Indem die Benutzer ihre Wahl für oder gegen Zugriffs- und Sicherheitsprotokolle treffen, die eigenen Datenschutzeinstellungen konfigurieren und selbst bestimmen, welche Daten sie teilen und welche Informationen sie sehen möchten, können sie ihre eigene Erfahrung mit einer Marke oder einem Dienstanbieter gestalten.

Mit CIAM bieten Sie Ihren Kunden einen vereinfachten digitalen Zugang, ohne bei der Sicherheit Kompromisse eingehen zu müssen. Die besten Systeme ihrer Art umfassen Funktionen wie passwortloses Login, umfassende Self-Service-Möglichkeiten und biometrische Identifizierung. Sie gewährleisten ferner die Einhaltung gesetzlicher Vorschriften wie der Datenschutz-Grundverordnung (DSGVO). So wird es für Unternehmen möglich, ihre Sicherheitslevels individuell festzulegen – je nachdem, wie sensibel die Daten und Informationen sind, auf die zugegriffen werden soll. Beispielsweise können weniger vertrauliche Informationen mit einem Social Login geschützt werden (d.h. Anmeldung über ein Social-Media-Konto), während sensiblere Daten vor dem Zugriff möglicherweise eine zusätzliche Authentifizierung – etwa durch unverwechselbare biometrische Merkmale – erfordern, um die Identität eines Benutzers zu überprüfen.

Ein gutes CIAM-System wie die Nevis ID Plattform unterstützt Sie bei Herausforderungen in folgenden Themenbereichen:

- Digitale Identitäten
- Single Sign-on (SSO)/Social Login
- Passwortfreier Zugriff
- Verhaltensanalysen
- Multi-Faktor-Authentifizierung (MFA)

Technische Sicht auf CIAM

Folgende Standards haben sich mittlerweile bei modernen CIAM-Systemen etablieren können:

- FIDO für die Authentifizierungsbedürfnisse (Herstellung einer sicheren Verbindung)
- OAuth 2.0 für die Autorisierung
- OpenID Connect und SAML für die Föderation (Identity Federation)

FIDO (Fast Identity Online) ist das weltweit grösste Ökosystem für standardbasierte, interoperable Authentifizierung, mit dem Ziel, das Passwort-Problem der Welt zu lösen. Der FIDO-Standard ist ein offener Industriestandard für die sichere, schnelle und einfache Authentifizierung im Internet. Er gibt Unternehmen die Möglichkeit, in ihren Produkten hardwaregestützte Authentifizierung 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.

Das **OAuth 2.0-Framework**[1] ist ein Satz von definierten Prozessabläufen für die delegierte Autorisierung. Dieser verbessert den automatisierten Zugriff von Anwendungen, die weder dem Benutzer selbst noch dem Serviceanbieter, sondern einem Drittanbieter gehören. Dienstanbieter und andere abhängige Parteien können im Namen des Endbenutzers Aktionen durchführen und auf Ressourcen zugreifen, ohne dass der Endbenutzer seine Anmeldedaten offenlegen muss.

OpenID Connect (OIDC) ist ein Authentifizierungsprotokoll, das den Austausch von Berechtigungsnachweisen und grundlegenden Profilinformationen der Endbenutzer zwischen Identitätsanbietern und Dienstanbietern ermöglicht. OpenID Connect besteht aus einer Reihe von definierten Prozessabläufen für die Federation Authentification, die OAuth 2.0 als Basis nutzt und darauf aufbaut[2]. Diese Abläufe fügen eine einfache Identitätsschicht hinzu, um eine föderierte Authentifizierung zu ermöglichen[3]. OpenID Connect funktioniert sowohl für Web- als auch für mobile Anwendungen. OIDC ermöglicht es den „Relying Parties" (RPs), Benutzer über Websites und Apps hinweg zu authentifizieren, ohne Passwortdateien besitzen und verwalten zu müssen. Dank OIDC weiss die Relying Party jederzeit, welche Identität die Person hat, die gerade den Browser oder die native App benutzt, ohne die Identität des Anwenders selbst zu verwalten[4].

Security Assertion Markup Language (SAML) ist ein Authentifizierungsprotokoll, das den Identity Providern (IdP) erlaubt, Autorisierungsdaten an Service Provider (SP) weiterzugeben. SAML stellt die Verbindung zwischen der Authentifizierung der Identität eines Benutzers und der Autorisierung zur Nutzung eines Dienstes her. SAML beinhaltet einen Satz definierter Prozessabläufe für die föderierte Authentifizierung, völlig unabhängig von OAuth 2.0. Im Gegensatz zu OpenID Connect, das für CIAM-Szenarien eingesetzt wird, kommt SAML vorwiegend im Bereich Workforce-IAM zum Zug.

1: Definition von computerweekly.com
2: openid.net
3: hackernoon.com
4: OpenID FAQ

Was kann die Nevis ID Plattform?

Die Nevis ID Plattform ist eine moderne Lösung für ein effizientes Identitäts- und Zugriffsmanagement. Dank ihres modularen Aufbaus und der offenen Schnittstellen lässt sie sich flexibel an die unterschiedlichsten Anforderungen anpassen. Nevis wird der bestehenden Infrastruktur vorgeschaltet und fügt eine weitere Sicherheitsebene hinzu, indem es den gesamten Benutzerzugriff auf die Kundenzugänge und Portale kontrolliert.

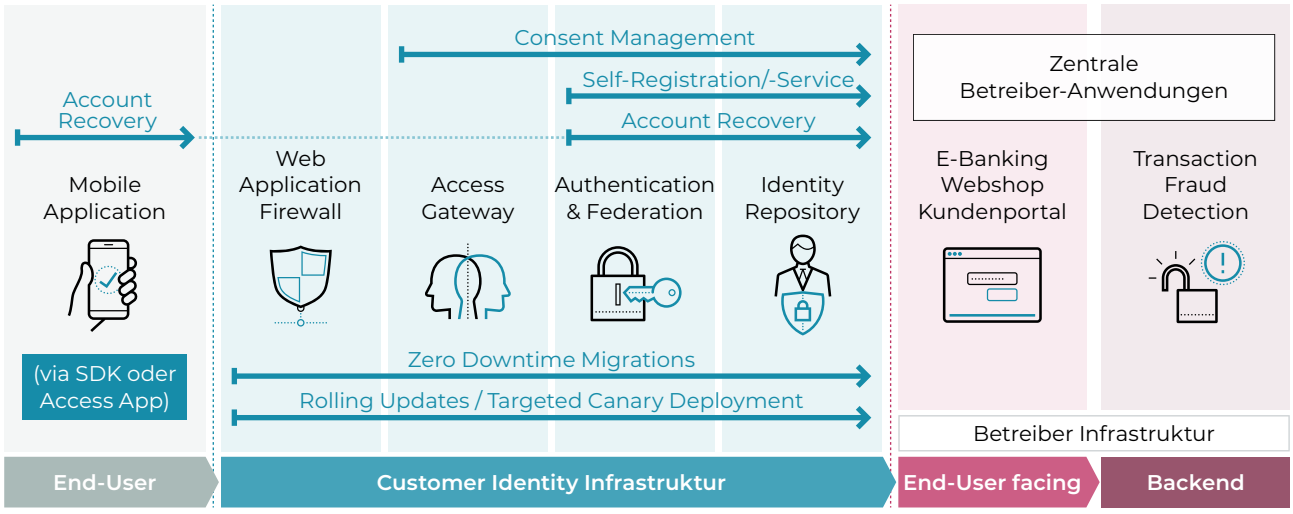
Die Authentifizierung und Autorisierung bilden den Kern eines erfolgreichen Customer Identity und Access Managements. Nevis besteht aus dem Secure Entry Gateway, kombiniert mit einer Web Application Firewall, einem Authentifizierungsdienst und dem Identitätsmanagement.

Die Nevis CIAM-Software beinhaltet jedoch weitere Funktionalitäten, um den gesamten Prozessablauf bei der Authentifizierung und Autorisierung effektiver zu gestalten. Im Folgenden erfahren Sie mehr über diese und weitere Funktionalitäten.

Die Nevis ID Plattform umfasst ausgereifte, bewährte Produktkomponenten im Bereich Customer Identity and Access Management und bietet Funktionen wie:

- Web Access Management und Federation
- Einstiegs-Gateway und Web-Anwendung/ Application Firewall (WAF)
- Starke Zwei-Faktor-Authentifizierung (2FA)
- Adaptive Authentifizierung
- Unterstützung für Social Login/Social Identities
- Mobile Authentifizierung nach FIDO-Standard mit unserer Access App und SDK
- Benutzerverwaltung mit Selbstregistrierung für den Benutzer und seine Geräte

Die Funktionalitäten des Nevis Öko-Systems im Überblick:



Das Nevis System dient als Vermittler und ermöglicht stellvertretend den sicheren und geprüften Zugriff auf Daten, Anwendungen und Bereiche des Unternehmens, die dem Nutzer nicht direkt zugänglich sind.

Die Nevis-Lösung ist skalierbar und kann jederzeit um weitere Funktionsbausteine erweitert werden. Diese Modularität und Ausbaubarkeit von Nevis garantieren einen maximalen Investitionsschutz.

Identity Management

Das Identitätsmanagement (IDM) ist in einem System, das Ressourcen zur Verfügung stellt, für die Identifizierung von Individuen zuständig, die auf diese Ressourcen zugreifen wollen. Es kontrolliert den gewünschten Zugriff auf die Ressourcen durch den Abgleich von festgelegten Identitäten mit Benutzerrechten und Einschränkungen und erstellt verschiedene Benutzerrollen, Gruppen und Richtlinien. So wird zum Beispiel der Zugriff blockiert, wenn ein Benutzer auf Ressourcen zugreifen will, für die er gemäss den Richtlinien keine Rechte hat. Solche und andere Vorkommnisse werden protokolliert und stehen als Bericht zur Verfügung.

Mithilfe des Identitätsmanagements lässt sich festlegen,

- was ein Nutzer tun darf
- mit welchen Geräten er Zugriff auf bestimmte Ressourcen hat und
- unter welchen Umständen ihm der Zugriff erteilt wird.

Richtlinien, die bestimmen, was ein Anwender abhängig von Faktoren wie seinem Gerätetyp oder Standort tun darf, bilden die Grundlage für das Identity-Management. Entsprechend liefert das System Berichte und Sicherheitswarnungen und bedient weitere Betriebs- und Verwaltungsanforderungen.

Die technische Architektur der Nevis Identitätsmanagement-Komponente ermöglicht folgende Funktionalitäten

User Management – beinhaltet die globale Verwaltung aller Benutzer und ihrer Berechtigungen. Nevis verwaltet Identitäten, Credentials, Rollen und Attribute von Benutzern zentral und stellt diese Anwendungen, Diensten und Systemen über eine sichere Kommunikationsinfrastruktur zur Verfügung. Weiterhin werden gemäss einem Regel- und Rollenmodell Benutzerkonten und Berechtigungen automatisiert bereitgestellt. Self-Administration, Delegated Administration und Identity-Management-Workflows ermöglichen eine effiziente Benutzerverwaltung.

User Self-Service – Die Selbstregistrierung von Benutzern gehört zu den gängigsten Mechanismen auf Online-Portalen. Dem Anwender wird ermöglicht, den Prozess der Kontoerstellung einzuleiten und seine Identitätsdaten anzugeben. Es ist möglich, sowohl vorgefertigte (mit Anpassungsmöglichkeit) Registrierungsabläufe zur Verfügung zu stellen als auch eigene Registrierungsprozesse zu generieren.

Delegated Administration – Der Benutzer registriert sich nicht selbst, sondern über einen Delegierten. Nevis bietet hier eine administrative Schnittstelle, die es Delegierten, wie z.B. Kundenbetreuern, ermöglicht, Benutzerkonten und Passwörter im Namen des Kunden zu erstellen, zu verwalten und zu löschen. Delegated Administration kann auch verhindern, dass z.B. unberechtigte Minderjährige auf ein Benutzerkonto zugreifen. Hierfür definiert man Regeln, nach denen nur die Eltern die Konten ihrer Kinder verwalten können.

Extensible Data Model / Erweiterbares Datenmodell – Das Identitätsmanagement von Nevis wird mit einem Kern-Datenmodell geliefert. Das Datenmodell besteht aus fixen Enti-ties (Kerneinheiten), wie z.B. Benutzer, Abteilungen/Units, Anwendungen und Rollen sowie Attributen. Zudem gibt es flexibel anpassbare Eigenschaften/Properties. Das Datenmodell umfasst auch die Beziehungen zwischen diesen Entities. Die fixen Entities (Benutzer, Units, etc.) und deren Attribute (allgemeine Eigenschaften oder Merkmale der Entities) sind vorgegeben. Die Auswahl der Attribute beruht auf den Best Practices unserer Kunden.
Immer wieder gibt es aber auch Geschäftsanforderungen und Anwendungsfälle, die sehr spezifisch sind und möglicherweise nicht durch das vorgegebene Datenmodell abgedeckt werden. Für diese Fälle enthält das Datenmodell zusätzlich die sogenannten „Properties“. Eine Property ist vergleichbar mit einem Attribut einer Entität, z.B. das Attribut „Vorname“ der Entität „Benutzer“. Dank der Verwendung der Properties kann das Datenmodell leicht an ganz spezifische Anforderungen angepasst und verändert werden.

History-Aware Data Model – Der History Viewer zeigt, wie sich Daten im Lauf der Zeit verändert haben und fasst diese Ereignisse zusammen. Nevis speichert Ereignisse wie Einfügen, Aktualisieren oder Löschen innerhalb von Versionierungstabellen, zusammen mit dem Zeitstempel und dem Akteur des Ereignisses (d.h. dem Benutzer, der die Aktion durchgeführt hat).

Multi-Tenant Support (Mandantenfähigkeit) – Es ist möglich, mehrere Mandanten zu bedienen, ohne dass diese gegenseitig Einblick in ihre Daten, Benutzerverwaltung und Ähnliches erhalten.

Real-Time Provisioning / Echtzeit-Verbreitung – Das Provisioning-Modul ist dafür zuständig, Informationen über Änderungen im Nevis Identitätsmanagement zu verbreiten. Solche Änderungen können z.B. das Anlegen eines neuen Benutzers oder die Zuweisung einer Rolle sein. Die durch solche Änderungen ausgelösten Provisionierungs-Ereignisse werden in Nachrichtenwarteschlangen geschrieben und können so von anderen Systemen konsumiert werden. Ein Beispiel wäre die Eröffnung eines neuen Kundeneintrags in Salesforce, nachdem sich jemand auf dem Firmenportal zum ersten Mal registriert hat.

Web-based Interface – Die Web-Benutzeroberfläche (Web-GUI) von Nevis bietet eine Administrationsschnittstelle für das Identitätsmanagement. Folgende Elemente können Sie über das Web-GUI verwalten:

- Benutzer
- Organisatorische Einheiten
- Anwendungen
- Benutzer-Credentials (Authentifizierungsinformationen)
- Rollen und Eigenschaften (Berechtigungsinformationen)
- Unternehmensrollen
- Mandanten
- Berechtigungsrichtlinien und Mail-Vorlagen

Der Zugriff auf diese Elemente wird über Administrationsrollen verwaltet. Das Web-GUI kann durch Ändern der Farben oder Ersetzen des Logos angepasst werden, um dem Corporate Design der Organisation zu entsprechen.

Kundenkommunikation mittels SMS, E-Mail und Briefen – Das Output-Management von Nevis unterstützt mehrsprachige Templates und alle gängigen Kanäle zur Kundenkommunikation. Nebst E-Mails für Passwort-Resets oder SMS-Notifikationen erstellt Nevis auch direkt PDF-Dateien, um z. B. Registrierungscodes per Briefpost an Kunden zu übermitteln.

Nicht alle diese Eigenschaften sind für den Endbenutzer direkt sichtbar, aber alle sind wichtig für ein effizientes und regelkonformes Identity Management.

Access Management

Access Management (AM) oder Zugriffsverwaltung ist ein Prozess der Informationssicherheit und Datenverwaltung und stellt die Umsetzung von Sicherheitsrichtlinien in Zugriffskontrollsystemen sicher. Greift das Access Management, sind Applikationen geschützt (Application Protection). AM kontrolliert den Zugriff von Benutzern auf digitale Daten, Dienste und Anwendungen basierend auf den im Identity Management (IDM) aufgestellten Regeln. Um Zugriff zu erhalten, muss ein Benutzer sich authentifizieren und vom IT-System autorisiert werden. Das AM gewährleistet, dass die im IDM festgelegten Rollen und Richtlinien eingehalten werden und nutzt sie als Grundlage, um Zugriffsanfragen zu verarbeiten.

Nevis bietet eine starke Benutzer- und Systemauthentifizierung (Strong Customer Authentication, SCA) im Zusammenspiel mit dem Identitäts- und Zugriffsmanagement. Nevis deckt so den gesamten Prozess der Identifizierung, Authentifizierung und Autorisierung ab. Einstiegs-Gateway und Web-Anwendung/Application Firewall (WAF) kommen ergänzend dazu. Während diese zusätzlichen Anwendungen den Inhalt von Benutzeranfragen filtern, um die Online-Anwendungen Ihres Unternehmens vor internen und externen Bedrohungen zu schützen, konzentriert sich Nevis bei der Authentifizierung auf die Identität des Benutzers. Die wichtigste Aufgabe dabei ist es, zu überprüfen, ob der Benutzer derjenige ist, der er vorgibt zu sein, um zu verhindern, dass unberechtigte Benutzer auf Ihre Anwendungen zugreifen.

Mit dem Identity- und Access-Management von Nevis werden On- und Offboarding-Prozesse vereinfacht, Berechtigungen für Teams gebündelt verwaltet und hierarchieabhängige Zugriffe ermöglicht. Diese und weitere Funktionen erhöhen in Unternehmen die Sicherheit und Produktivität. Gleichzeitig lassen sich damit interne Kosten und Sicherheitsaufwand reduzieren.

Die sichere Authentifizierung wird durch verschiedene Authentifizierungs-Backends sowie zusätzliche Funktionen, wie Multifaktor-Authentifizierung, Strong Customer Authentication (SCA), Identity Federation und API-Autorisierung, gewährleistet. Details dazu weiter unten.

Federation

Federation verbindet elektronische Identitäten und Attribute einer Person über verschiedene Identitätsmanagementsysteme hinweg. Dadurch können Identitäts- und Access-Management-Prozesse ausgelagert werden.

Die Federation-Standards, wie SAML, OpenID Connect, Web Services Federation (WS-Federation) oder OAuth 2, basieren auf dem Vertrauen in den verbundenen Identitätsanbieter (Identity Provider, IdP) und werden durch digitale Signaturen und Verschlüsselung gesichert. Neben diesen Standards für Federated Identities kann auch das Identitätsmanagement von Nevis als lokales Authentifizierungs-Backend verwendet werden.

Die Nevis ID Plattform unterstützt Identity Federation mit externen Netzwerken oder Sicherheitsdomänen. Single Sign-on und Social Login sind ebenfalls möglich.

Single Sign-on

Viele Unternehmen integrieren Single Sign-on (SSO), um für ihre Kunden und Kundinnen die Registrierung und Anmeldung für all ihre Online-Dienstleistungen zu vereinheitlichen. Statt sich also für diverse Dienstleistungen eines Unternehmens jedes Mal separat registrieren und anmelden zu müssen, genügt dank SSO eine zentrale Anmeldung und Registrierung.

Single Sign-on für Benutzer bewirkt, dass nach einer einmaligen, zentralen Anmeldung alle weiteren Anmeldungen automatisch ablaufen, um auf mehrere Web-Anwendungen im Backend zugreifen zu können.

Nevis kann:

- Zusammenführung in eine zentrale Identität für die Benutzer
- Nevis kümmert sich um das Identity Mapping
- Minimale Anwendungsanpassungen
- Zentralisierung der IAM-Prozesse

Vorteile:

- Verbesserte Usability
- Verbesserte geschäftliche Flexibilität
- Erhöhter Schutz der Anwendungen

Social Login

Das Social Login (eine Form von SSO und Federation) ermöglicht es Benutzern, sich bei einer Website oder App über einen Anbieter eines sozialen Netzwerks anzumelden. Social Login ist also eine Form von Single Sign-on für mehrere Systeme. Vorhandene Informationen aus einem sozialen Netzwerk werden dabei zur Anmeldung bei der Website eines Drittanbieters benutzt. Das Social Login vereinfacht den Anmeldeprozess, reduziert Abbruchraten, sorgt für genauere und validierte Daten und bringt Komfort für den Endbenutzer.

Bring Your Own Identity (BYOI)

Lösungen mit anerkannten elektronischen Identitäten, wie zum Beispiel SwissID in der Schweiz oder Verimi in Deutschland, funktionieren ähnlich wie Social Logins. Die Kunden verwenden ihre persönliche, geprüfte und anerkannte elektronische Identität.

Unternehmen, die davon profitieren wollen, müssen „Bring Your Own Identity“ (BYOI) integrieren. Auf diese Weise gelingt es, das Vertrauen in Kundenidentitäten zu steigern. Gartner empfiehlt: „Implementieren Sie ‚Bring your own identity´ (BYOI), aber stellen Sie sicher, dass das vom Identitätsanbieter bereitgestellte Vertrauensniveau dem Risikoniveau entspricht.“[1]

Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung (MFA) ist ein Sicherheitsmechanismus, bei dem Personen durch mehr als ein erforderliches Sicherheits- und Validierungsverfahren authentifiziert werden. Denn die Authentisierung nur mit Usernamen und Passwort als Identifikationsmittel ist unsicher und anfällig für Hackerangriffe.

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 (Mobiltelefon, 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

1: Gartner Innovation Insight for Bring Your Own Identity, 2018

Je ausgeklügelter die MFA gestaltet wird, desto sicherer ist das System. Die Benutzerfreundlichkeit darf dabei aber nicht vernachlässigt werden. Nicht jeder Online-Vorgang erfordert das gleiche Mass an Sicherheit. Deshalb lässt sich Nevis so konfigurieren, dass das System die Authentifizierungsstärke risikobasiert wählt und somit jederzeit maximale Benutzerfreundlichkeit gewährleistet.

Multi-Faktor-Authentifizierung ermöglicht maximale Benutzerfreundlichkeit, weil biometrische Verfahren wie die Gesichtserkennung oder die Analyse des Tippverhaltens den Anwender weder Zeit noch Mühe kosten. Dies steigert gleichzeitig den Schutz vor unbefugten Zugriffen, weil aufwändigere manuelle Sicherheitsmassnahmen von den Benutzern gerne umgangen werden. Die Kombination von mehreren Identifikationsfaktoren erschwert folglich sehr effektiv den Identitätsdiebstahl. Das ist besonders wichtig, wenn es um sensible Vorgänge wie Zahlungen oder den Zugriff auf schützenswerte Dokumente geht.

Die Vorteile von MFA

- Verbesserte Sicherheit durch Kombination verschiedener Authentisierungsverfahren
- Erhöhte Benutzerfreundlichkeit mit biometrischen Verfahren
- Erschwerter Identitätsdiebstahl
- Mehr Flexibilität beim Schutz von Ressourcen

Passwordless

Die passwortfreie Authentifizierung verifiziert, ob ein Anwender tatsächlich derjenige ist, für den er sich ausgibt. Anders als in herkömmlichen Systemen muss der Anwender dazu keine Zeichenfolge (das Passwort) manuell eingeben. Statt des Passworts werden andere Authentisierungsverfahren verwendet. Nevis nutzt für die passwortfreie Authentifizierung biometrische Verfahren wie Gesichtserkennung (z.B. FaceID von Apple) oder Fingerabdruck. Dies erhöht sowohl Sicherheit als auch Benutzerfreundlichkeit.

Das Besondere an dieser Lösung ist die **Verbindung aus maximaler Sicherheit und Benutzerfreundlichkeit**: Ihre Kunden geben ihren Benutzernamen auf der Anmeldeseite ein und tippen auf ihrem Mobiltelefon auf die Schaltfläche „Anmelden". Nevis 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.

Die passwortfreie Authentifizierung ist eine Angelegenheit von wenigen Sekunden. Die Eingabe des Benutzernamens oder einer E-Mail-Adresse nimmt dabei die meiste Zeit in Anspruch. Wenn der Browser ab der zweiten Anmeldung die E-Mail-Adresse automatisch ergänzt, geht es noch schneller.

Mit der passwortfreien Authentifizierung verbessern Sie das Kundenerlebnis und steigern die Akzeptanz von mobilen Lösungen. Sie erhöhen signifikant die Sicherheit bei der Authentifizierung, reduzieren Betrugsfälle bis zu 99%, sparen Kosten durch wegfallende Support-Anfragen und entlasten IT-Mitarbeiter bei der Wartung von Passwörtern. Die passwortfreie Lösung von Nevis kommt zudem ohne kostspielige SMS-Transaktionsgebühren aus.

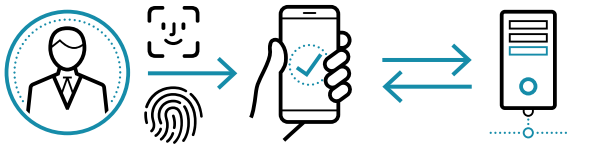
- Schneller, praktischer und sicherer als mit Passwort
- Verbesserung des Kundenerlebnisses
- Erhöhte Akzeptanz von mobilen Lösungen
- Reduktion von Betrugsfällen bis 99%
- Kostenersparnis durch wegfallende Support-Anfragen
- Entlastung von IT-Mitarbeitern bei der Wartung von Passwörtern
- Keine SMS-Transaktionsgebühren

Biometrische Verfahren

Dank der Kombination von Besitz („something I have“: das Smartphone) und Biometrie („something I am“: Gesicht oder Fingerabdruck) erfüllt das biometrische Verfahren die Anforderungen an die starke 2-Faktor-Authentifizierung. Sie ist ähnlich sicher wie Passwort plus zweiter Faktor.

Mehr Sicherheit durch 2-Faktor-Authentifizierung

Bei der starken Authentifizierung werden mindestens zwei von drei möglichen Identifikationskategorien eingesetzt.



Das Zusammenspiel zwischen Biometrie, Gerät und Server-Infrastruktur funktioniert bei der biometrischen Authentifizierung wie folgt: Zuerst installiert der Benutzer eine sogenannte **Access App** via App Store. Dann verknüpft er sein Gerät mit seinem Account. Dabei wird ein **Schlüsselpaar** generiert: Der **private Schlüssel** bleibt immer auf dem Smartphone und wird dort in einem speziell dafür vorgesehenen Chip-Set gespeichert (**Secure Enclave** oder **Trusted Execution Environment**). Solche Chip-Sets werden schon lange verwendet (erstmals z.B. beim Apple iPhone 5S bzw. Samsung Galaxy S5).

Bei jeder Authentisierung oder Transaktionsbestätigung wird eine Signatur-Operation mit dem privaten Schlüssel auf dem Smartphone ausgeführt. Die Biometrie dient dabei lediglich zur Freischaltung des privaten Schlüssels. Deshalb verlassen die biometrischen Informationen auch nie das Smartphone.
Der Austausch des Schlüssels (Registrierung des Gerätes) sowie die Use Cases Login, Transaktionsbestätigung und Deregistrierung des Geräts erfolgen nach dem standardisierten FIDO-UAF-Protokoll.
Die Lösung ist einfach erweiterbar: Falls zukünftige Smartphones weitere biometrische Verfahren zur Verfügung stellen, können diese durch ein Update der App integriert werden, ohne dass sich serverseitig und an den Prozessen grosse Änderungen ergeben.

Mobile Authentifizierung

Die mobile Authentifizierung erfolgt sicher und reibungslos, indem Benutzer ihre Identität mithilfe ihres Mobiltelefons verifizieren. Mit der mobilen Authentifizierung können Endbenutzer durch die Verwendung mehrerer Identifikationsfaktoren ihre Identität nachweisen und Transaktionen bestätigen. Jeder Faktor basiert auf etwas, das der Endbenutzer weiss, hat oder ist, etwa ein Geheimnis, ein bestimmtes Gerät oder ein Fingerabdruck.

Die Kombination aus starker Kryptografie und standardisierten Authentifizierungsschemata macht die mobile Authentifizierung für den Benutzer einfach und sicher. Die schützenswerten Zugangsdaten werden nur auf dem Gerät des Benutzers gespeichert. Dies schützt sowohl die Privatsphäre der Benutzer als auch Unternehmen vor potenziell geschäftsgefährdenden Sicherheitsverletzungen während der Anmeldung.

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 sowie PIN, und zwar basierend auf dem FIDO-Standard.

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

Während der Registrierung des Mobilgeräts als Authentisierungsfaktor generiert das System ein Schlüsselpaar, das aus einem privaten und einem öffentlichen Teil besteht. Die private Schlüsselkomponente wird – mittels Biometrie oder PIN geschützt – im erwähnten, sicheren Chip des Mobilgeräts abgelegt. Die öffentliche Schlüsselkomponente wird zu Nevis gesendet. Beim Login bzw. der Authentifizierung des Benutzers kann Nevis mithilfe der öffentlichen Schlüsselkomponente überprüfen, ob die Antwort auf die Authentisierungsanfrage tatsächlich mit dem privaten Schlüssel unterzeichnet wurde, der nur dem berechtigten Nutzer zugänglich ist.

Die Übermittlung der Authentisierungsanfrage für den passwortfreien Zugriff an das Mobilgerät erfolgt je nach Anwendung über einen QR-Code, einen Deep Link oder eine Push-Benachrichtigung.

Die Benutzeridentität wird von Nevis während der mobilen Authentifizierung DSGVO-konform gespeichert.

Transaction Confirmation

Die Transaktionsbestätigung (englisch: Transaction Confirmation) ist eine zusätzliche Sicherheitsmassnahme, die für bestimmte Finanztransaktionen und andere besonders sensitive Tätigkeiten erforderlich ist. Diese kommt dann zum Einsatz, wenn der Benutzer zusätzlich zur Authentisierung bestimmte Informationen prüfen und bestätigen muss. Die Transaktionsbestätigung ermöglicht, sowohl finanzielle als auch betriebliche Transaktionen mit nur einem Klick 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 lässt sich die Transaktion ganz einfach durch Scannen des Fingerabdrucks, des Gesichts oder durch die Eingabe eines PINs bestätigen oder ablehnen.

Mit der Transaktionsbestätigung wird nicht nur das Betrugsrisiko minimiert, sondern auch menschlichen Fehlern oder einem Vertippen vorgebeugt.

Sogenannter **Friendly Fraud**, bei welchem Kunden unberechtigte 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.

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 im Hinblick auf einzuhaltende Compliance- und Wirtschaftsprüfungsrichtlinien.

Offen bleibt noch die Frage, wie man beweisen kann, dass die Person, die die Transaktion initiiert hat, die richtige Person ist. Dieses Problem kann entweder durch eine biometrische Verifikation des Benutzers gelöst werden oder durch einen PIN, ganz ähnlich wie bei der Authentifizierung beim Login. Die Funktionalität der Transaktionsbestätigung 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 vielfältig:

- Bestätigung von Zahlungen
- E-Commerce-Transaktionen
- Erteilung von DSGVO-Einwilligungen[1]

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

Consent and Privacy Management

Verbraucher sind für Fragen des Datenschutzes sensibler geworden. Deshalb wurden weltweit mehr Vorschriften zum Schutz von Benutzerdaten im Internet eingeführt. Die EU-Datenschutz-Grundverordnung (DSGVO bzw. GDPR) schreibt vor, eine Einwilligung zur Datennutzung (etwa bei Cookies) einzuholen, diese zu dokumentieren und zu verwalten. Zusätzlich sollen die Besucher verständlich informiert werden, welche Daten erhoben und wie diese verarbeitet werden. **Unternehmen müssen die lokalen Richtlinien zur Datenaufbewahrung und Datenspeicherung einhalten**. Deshalb gilt es, Sicherheitsfunktionen zu implementieren, die den Schutz der Benutzerdaten gewährleisten.

Consent- und Privacy-Management ermöglicht es Unternehmen, diese Vorgaben zu erfüllen und das Einverständnis der Nutzer zu sammeln. Kommunikationspräferenzen und die Zustimmung zu rechtsverbindlichen Vereinbarungen können jederzeit bearbeitet werden.

Nevis bietet eine sofort einsatzbereite und schnell zu integrierende Lösung, in der die Benutzer die jeweiligen Allgemeinen Geschäftsbedingungen einfach durch Klicken auf eine Schaltfläche akzeptieren oder ablehnen können. Das System speichert und prüft dabei, wann der Anwender welche Version akzeptiert hat. Darüber hinaus lassen sich Präferenzen für Newsletter, Marketingkampagnen, Verkaufs- und Produkt-Update-E-Mails usw. verwalten.

User Behaviour Analytics (Adaptive Authentication): Betrugs- und Verdachtsfallerkennung

Über User Behaviour Analytics lassen sich Anomalien im Nutzerverhalten aufspüren, um unbefugte Datenzugriffe zu unterbinden und abzuwehren. Es ist möglich, bestimmte Muster im Nutzerverhalten zu erkennen, die entweder auf normales oder fremdartiges Verhalten hinweisen.

Um das Nutzerverhalten zu analysieren, müssen Anwenderdaten rückverfolgt, gesammelt und ausgewertet werden. Diese Daten fallen bei der Nutzung von digitalen Diensten an und können von Monitoring-Systemen verarbeitet werden.

Erfasst und analysiert werden Informationen wie Standort, Gerätinformationen und die aktuelle Zeit, aber auch typische Eigenarten der Benutzer wie das Tippverhalten, die Dynamik von Tastenanschlägen, Berührungen und Mausbewegungen. Diese dynamischen Aspekte einer Benutzeridentität können mit früheren Interaktionen verglichen werden, um das Risiko zu beurteilen. Die Effektivität der Komponente basiert auf der Tatsache, dass die Korrelation mehrerer Attribute wie Verhaltensbiometrie, Geostandort oder Geräteinformationen sehr eindeutige digitale Benutzer-Fussabdrücke erzeugt. Die Analyse beginnt bereits auf der Login-Seite und wird bis zur Beendigung der Session fortgeführt.

Anormales Benutzerverhalten könnte einen Angriff signalisieren. Daraufhin erhalten die Security-Teams die nötigen Informationen, um gegebenenfalls aktiv zu werden. Dabei wird zunächst ein Risikoschwellenwert, der sich aufgrund des anormalen Verhaltens ergibt, an das Risiko-Management-System übermittelt. Das System kann diese verdächtige Transaktion dann unterbinden oder deren Legitimität durch eine zusätzliche Authentifizierung (Step-up) überprüfen.

Nevis erlaubt, führende Technologien zur Anomalie-Erkennung auf einer Plattform zu vereinen und als zentralen Service für alle Anwendungen bereitzustellen.

Administrationskonsole/Management Konsole

Nevis stellt eine Konfigurations-, Bereitstellungs- und Überwachungslösung zur Verfügung, die moderne DevOps-Praktiken unterstützt. Somit können die Organisationen neue Funktionen schneller bereitstellen und gleichzeitig höhere Anforderungen an die Sicherheit erfüllen. Wiederverwendbare Konfigurationsvorlagen enthalten Best Practices für gängige Anwendungsfälle. Dies reduziert die Kosten und verbessert die Produktivität. Die umfassende Validierung von Konfigurationsänderungen ermöglicht zudem die kontinuierliche Einhaltung der Sicherheitsrichtlinien und -verfahren Ihres Unternehmens. Die Plattform wurde mit Blick auf Skalierbarkeit und Sicherheit für Unternehmen entwickelt. Die modulare Architektur unterstützt verschiedene Bereitstellungsprozesse, um den Anforderungen von anspruchsvollen IT-Umgebungen gerecht zu werden. Die Funktionen zur Zugriffskontrolle umfassen fein abgestufte Berechtigungen für Projekte und Benutzer.
Nevis bietet somit eine „Configuration Generation Engine", die Konfigurationen ohne menschliche Interaktion validiert und bereitstellt.

Unternehmen mit einzigartigen Infrastrukturen und Integrationsherausforderungen können die Grundvorlagen erweitern, um alle Geschäftsanforderungen zu erfüllen. Das reduziert die Komplexität und deckt häufige Anwendungsfälle ab, welche auch einfach angepasst werden können.

Vorteile:

- Schnelle Konfiguration und Implementierung von Best Practices für die Sicherheit mithilfe von wiederverwendbaren Konfigurationsvorlagen
- Dank der vollständigen Trennung von Konfigurations- und Infrastrukturdaten können neue Konfigurationen und Infrastrukturoptionen separat getestet werden
- Bearbeiten, Teilen und Überprüfen von deklarativen Konfigurationsdateien mit Unterstützung für das „Git Version Control System"
- Validierung von Konfigurationsänderungen und Überprüfung von Ausführungsplänen vor der Bereitstellung vermeiden unangenehme Überraschungen in der Produktion
- Passt sich an die Arbeitsweise Ihres Unternehmens an
- Die modulare Architektur ermöglicht flexible Bereitstellungsprozesse
- Integration mittels bereits von Ihnen verwendeten Tools über die „Configuration Generation Engine"

Wie Nevis dem Unternehmen hilft

Customer Identity and Access Management mit Nevis gewährleistet die gewünschte Sicherheit und erhöht den Wettbewerbsvorteil. Sowohl browser-basierte als auch app-basierte Login-Prozesse werden unterstützt. Somit bieten Sie Ihren Kunden auf jedem Endgerätetyp den gleichen Komfort bei maximaler Sicherheit.

→ Modular, flexibel, stabil, sicher.

Worin besteht der Nutzen für den Endkunden?

Kunden wollen mit minimalem Aufwand und maximaler Sicherheit auf Online-Angebote zugreifen. Sie erwarten innovative und durchgängig reibungslose 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 hinweg
- 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

Wie profitieren Unternehmen?

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 Nevis ID gewinnen Sie viele Vorteile. Einige Highlights:

- Deutlich bessere Usability durch Eliminierung unnötiger Schritte
  - Steigert Kunden-Loyalität
  - Steigert Bereitschaft, Premium-Preise zu bezahlen
- Verfügbar mit einer App mit unternehmenseigenem Branding
- Integriert sich nahtlos in bestehende Infrastrukturen und ist zukunftssicher
- Verkürzte Markteinführungszeit für digitale Angebote
- Keine laufenden SMS-Transaktionsgebühren dank passwortfreiem Zugang
- Weniger abgebrochene Konvertierungen mit sicherer und einfacher Transaktionsbestätigung (FIDO)
- Ein umfassendes Identitäts- und Zugriffsmanagement hilft Ihnen, Ihre Kunden besser kennenzulernen, und unterstützt gleichzeitig die Umsetzung der gesetzlichen Anforderungen für sensible Benutzerdaten (DSGVO, PSD2, GKV-SV usw.)
- 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

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 Nevis ID Plattform bietet maximale Unterstützung bei der Erreichung dieser Ziele. Sie spart Kosten und bietet gleichzeitig Rechtssicherheit:

- In wenigen Schritten in Ihre IT-Umgebung integriert
- Out-of-the-Box-Integration für Azure AD B2C und grosse E-Commerce-Shops
- Automatisierte Standardprozesse reduzieren den Helpdesk-Aufwand
- Verfügbar mit individuell gebrandeter App 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
- Investitionsschutz: Die FIDO-basierte Implementierung ermöglicht eine schnelle Anpassung an die zukünftigen Fähigkeiten mobiler Geräte
- Die offene Architektur unterstützt eine breite Auswahl von Standards
- Nevis wächst mit, egal ob grössere Volumen zu bewältigen oder neue Technologien einzubinden sind

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 diese schnell zur Konkurrenz.

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

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

Das breite Funktionsspektrum und die Skalierbarkeit der Nevis ID Plattform ermöglichen die Umsetzung unterschiedlichster Anforderungen. Alle Branchen profitieren zum Beispiel von Identity- und Access-Management-Lösungen für ihre Portale und den vielfältigen Self-Service-Prozessen.

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

Branche	Problem	Lösung	Vorteil
Financial Services und Banking	Komplizierter Konto-Zugriff via externes Tool	Passwortfreie Authentifizierung	Steigerung der Benutzerinteraktionen
	Identitätsdiebstahl	Transaktionen biometrisch genehmigen	Vertrauen der Kunden bleibt Gute Reputation
	Einhalten von Regulatorien	2FA mit passwortloser Transaktionsbestätigung (FIDO-Standard)	PSD2- und DSGVO-Konformität
	Fraud-Prevention und -Detection ist nicht benutzerfreundlich, aufwändig und kostspielig	Kontinuierliche, risikobasierte Benutzerauthentisierung mittels Kombination von Anomalie-Erkennungstechnologien	Kundenfreundlicher, weil nur bei Bedarf Zusatzauthentisierung (Step-up) verlangt wird Manueller Aufwand der Betrugsabteilung wird reduziert Kosten und Verluste sinken
	Konto-Administration ist aufwändig	Umfassende Self-Services	Kunden sind fähig, Passwörter selbst zurückzusetzen, Helpdesk wird entlastet
	Aufwändige Administration für Geschäftskunden	Delegierte Identity-Administration für Geschäftskunden	Geschäftskunden werden befähigt, wiederkehrende Operationen selbständig durchzuführen Reduktion von Leerläufen und Supportaufwand

Branche	Problem	Lösung	Vorteil
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
	Dokumente müssen per Einschreiben versandt oder persönlich übergeben werden	Einbindung der SwissID oder anderen anerkannten elektronischen Identitäten als Authentifizierungsmittel	Dokumente können online, verschlüsselt und rechtsgültig übermittelt werden Einsparung von Zeit und Geld für Bürger und Behörden Umweltschonend
	Die Abwicklung behördenübergreifender Geschäfte ist kompliziert	Multi-mandantenfähige Sicherheitsplattform für den Betrieb auf nationaler Ebene	Sicherer Austausch von Informationen über Behördengrenzen und -stufen hinweg
	Aufwändige Administration für Geschäftskunden	Delegierte Identity-Administration für E-Government-Services im Firmenumfeld	Geschäftskunden werden befähigt, wiederkehrende Operationen selbständig durchzuführen Reduktion von Leerläufen und Supportaufwand
	Risiko, dass normale Sicherheitsmassnahmen nicht genügen	Hochsichere IAM-Lösungen für Einsatzgebiete mit erhöhten Sicherheitsanforderungen (z.B. Justiz- und Polizeiwesen)	Substanzielle Reduktion von Cyber-Security-Risiko auf technischer Ebene

Branche	Problem	Lösung	Vorteil
Versicherungen	Komplizierter Zugriff auf das Versicherungsportal	Passwortfreie Authentifizierung	Steigerung der Benutzerinteraktionen
	Verwalten von Kunden-Accounts ist aufwändig	Effiziente Verwaltung von Kunden-Accounts dank umfassender Self-Services, optional auch Social Logins (Facebook, Google etc.)	Reduktion von Helpdesk- und Support-Kosten Erhöhte Kundenzufriedenheit dank besserer User Experience
	Hochladen von sensitiven Informationen ist heikel	Passwortfreie, biometrische 2FA	Compliance/Datenschutz
	Risiko, dass normale Sicherheitsmassnahmen nicht genügen	Adaptive Schutzmechanismen für Applikationen und Tarifrechner	Substanzielle Reduktion von Cyber-Security-Risiko auf technischer Ebene Bessere User Experience, weil nur bei Bedarf Zusatzauthentisierung (Step-up) verlangt wird
	Kommunikation und Datenaustausch mit Versicherungsbrokern ist kompliziert und unsicher	Einbindung von Versicherungsbrokern mittels Identity Federation (z.B. IG B2B in der Schweiz, EasyLogin in Deutschland)	Steigerung von Effizienz, Sicherheit und User Experience im Umgang mit Versicherungsbrokern
	Aufwändige Administration für Geschäftskunden	Delegierte Identity-Administration für Geschäftskunden	Geschäftskunden werden befähigt, wiederkehrende Operationen selbständig durchzuführen Reduktion von Leerläufen und Supportaufwand

Branche	Problem	Lösung	Vorteil
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
	Konto-Administration ist aufwändig	Self-Services für Endbenutzer (z.B. Selbstregistrierung, „Passwort vergessen”-Funktion)	Kunden sind fähig, Passwörter selbst zurückzusetzen, Helpdesk wird entlastet
	Risiko, dass normale Sicherheitsmassnahmen nicht genügen und erweiterte Massnahmen die Kundenerfahrung beeinträchtigen	Unterstützung verschiedener Authentisierungsmechanismen, abgestimmt auf Sicherheitsanforderungen	Angepasste Sicherheit und maximale Kundenerfahrung, weil nur bei Bedarf Zusatzauthentisierung (Step-up) verlangt wird
	Aufwändige Administration für Geschäftspartner und Fachbereiche	Delegierte Benutzer-Administration für Geschäftspartner und Fachbereiche	Geschäftspartner und Fachbereiche werden befähigt, wiederkehrende Operationen selbständig durchzuführen. Reduktion von Leerläufen und Supportaufwand
	Verschiedene Datensilos erschweren Abgleich und Berechtigungsmanagement	Anbindung an das ERP-System, bidirektionaler Abgleich von Stammdaten und Berechtigungsinformationen	Effizienter Abgleich von Stammdaten und Berechtigungsinformationen
	Kunden und Mitarbeiter verlieren Zeit mit separater Anmeldung für verschiedene Systeme	Organisationsübergreifendes Single Sign-on über verschiedene Anwendungen und Shop-Systeme mittels Identity Federation	Einmal angemeldet, haben Kunden und Mitarbeiter Zugriff auf alle Anwendungen und Systeme Effiziente Implementierung der Lösung
	Bestellprozesse sind zu wenig automatisiert	Einbindung spezieller Geräte (z.B. Barcode-Scanner) für automatische Bestellprozesse	Effizientere Bestellprozesse mit entsprechender Aufwandreduktion
	IoT kann schlecht integriert werden	IoT-Integration	Einfache IoT-Integration

Branche	Problem	Lösung	Vorteil
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
	Sicherheitslevel von Authentisierung mittels Benutzernamen und Passwort ist ungenügend	Unterstützung verschiedener Authentisierungsmittel: mTAN, SuisseID, HPC Card, Soft Certs etc.	Sensible Daten sind besser geschützt Einfache Integration verschiedener Authentisierungsmittel ins bestehende System
	Patienten, Kunden und Mitarbeiter verlieren Zeit mit separater Anmeldung für verschiedene Systeme	Single-Sign-on für Webapplikationen und weitere Services für den sicheren Datenaustausch	Einmal angemeldet, haben Patienten, Kunden und Mitarbeiter Zugriff auf alle Anwendungen und Systeme
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.

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

Ihr Nevis Partner: