nevis®

Nevis für Versicherungen

Digitale Sicherheitsinfrastruktur für Versicherungsportale

Making Security an experience.

Die Herausforderungen für Versicherungen

1

Credential Stuffing als reelle Bedrohung

Sensible personenbezogene Daten, die von Versicherungsunternehmen verarbeitet werden, sind für Cyberkriminelle von besonderem Interesse und können bei unzureichendem Schutz leicht erbeutet werden. Eine Datenschutzverletzung kann nicht nur für die betroffenen Kunden, sondern auch für das Unternehmen katastrophale Folgen haben.

2

Technisch herausfordernd

Versicherungsportale müssen die Bedürfnisse unterschiedlicher Gruppen – Privatkunden, Geschäftskunden, Broker und Versicherungsberater sowie Geschäftspartner und interne Mitarbeiter – in einer einheitlichen Sicherheitsinfrastruktur koordinieren. Gleichzeitig haben Versicherungsunternehmen sehr spezifische Sicherheitsanforderungen und müssen neben Kundendaten auch Online-Tarifrechner vor Wirtschaftsspionage geschützt werden.

3 Konformität garantieren

Versicherungsinformationen sind hochsensibel und müssen gemäss den geltenden Datenschutz- und Sicherheitsvorschriften - wie z.B. der DSGVO, BDSG und FADP - des jeweiligen Landes vertraulich und sicher behandelt werden. Die Implementierung einer CIAM-Lösung, die diesen Vorschriften entspricht, unterliegt einigen Herausforderungen.

4 Customer Journey

Versicherungsanbieter decken verschiedene Bedürfnisse wie z.B. Fragen zu Versicherungsdienstleistungen, Vertragsanpassungen, Schadensfallmeldungen und das Abschliessen neuer Verträge ab. Alles beginnt mit dem Onboarding, das auf die spezifischen Bedürfnisse des Benutzers abgestimmt ist. Schon alleine ein komplizierter Portalzugang kann jedoch die Kaufmotivation des Kunden senken und dazu bringen, ein Konkurrenzangebot einzuholen.

5 Verstärkter Wettbewerb

Kunden erwarten zunehmend eine personalisierte und nahtlose Kundenerfahrung, die von den digitalen Technologien, die sie täglich nutzen, geprägt ist. Versicherungen müssen in der Lage sein, mit den Kundenerwartungen Schritt zu halten und sich schnell an diese Entwicklungen anzupassen, um wettbewerbsfähig zu bleiben. Negative Nutzererfahrungen lassen Versicherte zu anderen Anbieter wechseln.

6 Bedarf an einfachen und sicheren Authentifizierungslösungen

Neue Authentifizierungslösungen können für Kunden verwirrend sein, was zu Frustration oder Ablehnung führen kann. Versicherer müssen sowohl ihre Kunden über die neuen Lösungen informieren und sie bei der Einführung begleiten, als auch sicherstellen, dass ihre Lösungen sicher und robust sind, um Cyberangriffe oder Missbrauch zu verhindern.

7 Kundenwunsch nach Datensouveränität

Kunden und Partner erwarten, dass sie ihre Daten sicher und vertraulich behandeln und gleichzeitig den Zugriff auf ihre Daten erleichtern. Versicherer müssen daher Wege finden, um Kunden die Kontrolle über ihre Daten zu geben, indem sie transparente Datenschutzpraktiken implementieren und die Kunden darüber informieren, wie ihre Daten gesammelt, gespeichert und verwendet werden.

8 Personalisierung

Kunden ein nahtloses Erlebnis zu bieten, wenn sie sich registrieren und Angebote anfordern stellt eine grosse Herausforderung dar. Sammeln Sie Daten sicher, um Kundenmeilensteine wie Hochzeiten und Geburten im Auge zu behalten und Möglichkeiten für neue Versicherungsbedürfnisse zu identifizieren.

So unterstützt Nevis die Versicherungsbranche

Vom sicheren Onboarding bis hin zur lebenslangen Kundenbeziehung

Erkennen Sie Betrug rasch und zuverlässig

Garantieren Sie mit einem zertifizierten Identitätsmanagement-Tool den sicheren Zugang zu Benutzerkonten. Verhindern Sie, dass sich Unbefugte unter Vorspiegelung falscher Tatsachen Zugang zu Kundendaten verschaffen.

- Account-Aktivierung/Selbstregistrierung
- Bestellung neuer Services und Berechtigungen
- Linken von Identitäten und Credentials
- Delegierte Administration: Berechtigungsverwaltung durch Kunden

Sichern Sie erhöhten Datenschutz und garantierte Konformität

Schützen Sie personenbezogene Kundendaten nachweislich bei der Erhebung, Speicherung und Weiterverarbeitung in allen verwendeten Systemen und Ihr Unternehmen vor Reputationsschäden und Sanktionen.

- Klare und sofortige Kundenidentifikation mit ID Verifikation
- Sekundenschneller Login durch MFA und Biometrie
- Login ersetzt unsichere, schwer zu merkende Kombinationen aus Benutzernamen und Passwort.
- Know your Customer Legitimationsprüfung (KYC)

Schaffen Sie Verbindungen mit Identity Federation

Binden Sie verschiedene Versicherungsbroker mittels Identity Federation ein und verknüpfen eine Identität in mehreren Identity Providern (z.B. IG B2B in der Schweiz, EasyLogin in Deutschland).

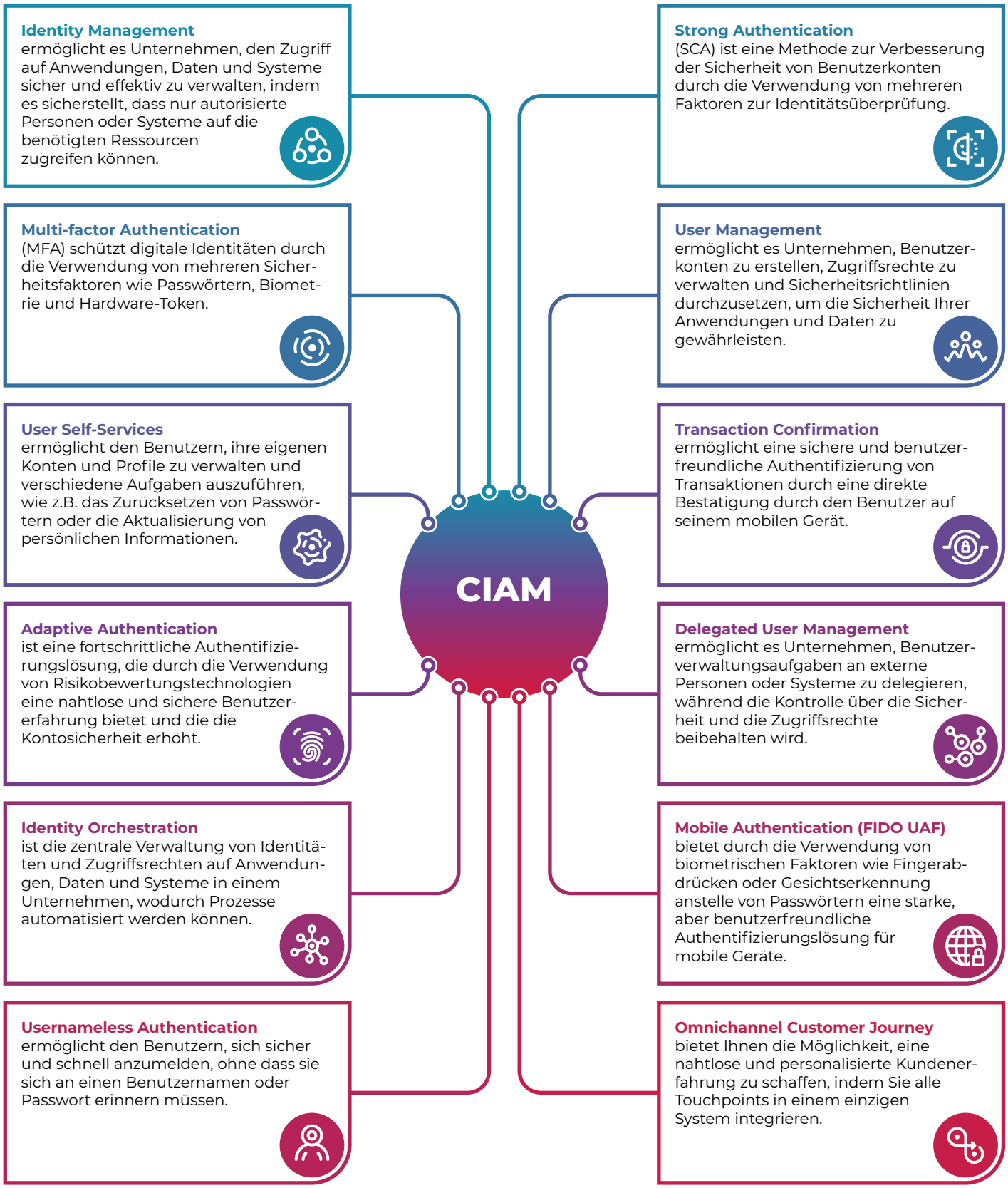
- Effiziente Verwaltung von Kunden-Accounts dank umfassender Self-Services, optional auch Social Logins (Facebook, Google etc.)
- Unterstützung verschiedener Authentisierungsmittel und Authentisierungsstärken
- Schnelle und automatisierte Bereitstellung der bestmöglichen Sicherheitsinfrastruktur

Garantieren Sie im Online-Vertriebskanal einen schnellen Zugriff auf Neuerungen, Aktualisierungen und Angebotsübersichten. Während Kundendaten und Beratungen früher am ehesten persönlich, telefonisch oder per Brief dokumentiert und durchgeführt wurden, bevorzugen heute die meisten Kunden, ihre Versicherungsverträge online abzuschliessen. Hierbei erwarten die Kunden, dass der Prozess kummerfrei ist und die Daten sicher verarbeitet werden.

Die Kundenidentitäts- und Zugriffsverwaltung (Customer Identity and Access Management, CIAM) bietet genau das und trägt gleichzeitig dazu bei, die Kundenbindung zu festigen. Mit CIAM sind Versicherer in der Lage, Identitäts- und Profildaten von Kunden zu erfassen und zu organisieren und den Kundenzugriff auf Anwendungen, Dienste und Online-Profile zu verwalten und sichern.

CIAM verbindet Sicherheit und Kundenerfahrung zu einer perfekten Lösung für das Daten- und Zugriffsmanagement.

Die wichtigsten CIAM Funktionen für Versicherungen



Identity Management
ermöglicht es Unternehmen, den Zugriff auf Anwendungen, Daten und Systeme sicher und effektiv zu verwalten, indem es sicherstellt, dass nur autorisierte Personen oder Systeme auf die benötigten Ressourcen zugreifen können.

Multi-factor Authentication
(MFA) schützt digitale Identitäten durch die Verwendung von mehreren Sicherheitsfaktoren wie Passwörtern, Biometrie und Hardware-Token.

User Self-Services
ermöglicht den Benutzern, ihre eigenen Konten und Profile zu verwalten und verschiedene Aufgaben auszuführen, wie z.B. das Zurücksetzen von Passwörtern oder die Aktualisierung von persönlichen Informationen.

Adaptive Authentication
ist eine fortschrittliche Authentifizierungslösung, die durch die Verwendung von Risikobewertungstechnologien eine nahtlose und sichere Benutzererfahrung bietet und die die Kontosicherheit erhöht.

Identity Orchestration
ist die zentrale Verwaltung von Identitäten und Zugriffsrechten auf Anwendungen, Daten und Systeme in einem Unternehmen, wodurch Prozesse automatisiert werden können.

Usernameless Authentication
ermöglicht den Benutzern, sich sicher und schnell anzumelden, ohne dass sie sich an einen Benutzernamen oder Passwort erinnern müssen.

Strong Authentication
(SCA) ist eine Methode zur Verbesserung der Sicherheit von Benutzerkonten durch die Verwendung von mehreren Faktoren zur Identitätsüberprüfung.

User Management
ermöglicht es Unternehmen, Benutzerkonten zu erstellen, Zugriffsrechte zu verwalten und Sicherheitsrichtlinien durchzusetzen, um die Sicherheit Ihrer Anwendungen und Daten zu gewährleisten.

Transaction Confirmation
ermöglicht eine sichere und benutzerfreundliche Authentifizierung von Transaktionen durch eine direkte Bestätigung durch den Benutzer auf seinem mobilen Gerät.

Delegated User Management
ermöglicht es Unternehmen, Benutzerverwaltungsaufgaben an externe Personen oder Systeme zu delegieren, während die Kontrolle über die Sicherheit und die Zugriffsrechte beibehalten wird.

Mobile Authentication (FIDO UAF)
bietet durch die Verwendung von biometrischen Faktoren wie Fingerabdrücken oder Gesichtserkennung anstelle von Passwörtern eine starke, aber benutzerfreundliche Authentifizierungslösung für mobile Geräte.

Omnichannel Customer Journey
bietet Ihnen die Möglichkeit, eine nahtlose und personalisierte Kundenerfahrung zu schaffen, indem Sie alle Touchpoints in einem einzigen System integrieren.

Nevis – Ihr Partner für Sicherheit und Compliance

Nevis bietet Ihnen die Lösung: Ihre Kunden erhalten einen passwortlosen und sicheren Zugang zu ihren Konten, um versicherungstechnische Angelegenheiten in Sekundenschnelle zu verwalten – nutzerfreundlich und absolut sicher.

Bequemes Login ohne Sicherheitsverlust

Die heutigen Nutzer von Versicherungsdiensten haben nicht nur hohe Erwartungen an die Benutzerfreundlichkeit, sondern legen auch mehr denn je Wert auf einen angemessenen Schutz ihrer persönlichen Daten. Eine Einschränkung der Benutzerfreundlichkeit um der Sicherheit willen oder umgekehrt ist daher keine Option. Das Online-Portal muss daher die Nutzung eines neuen Login-Verfahrens ermöglichen und ausbauen.

Adaptive Authentication

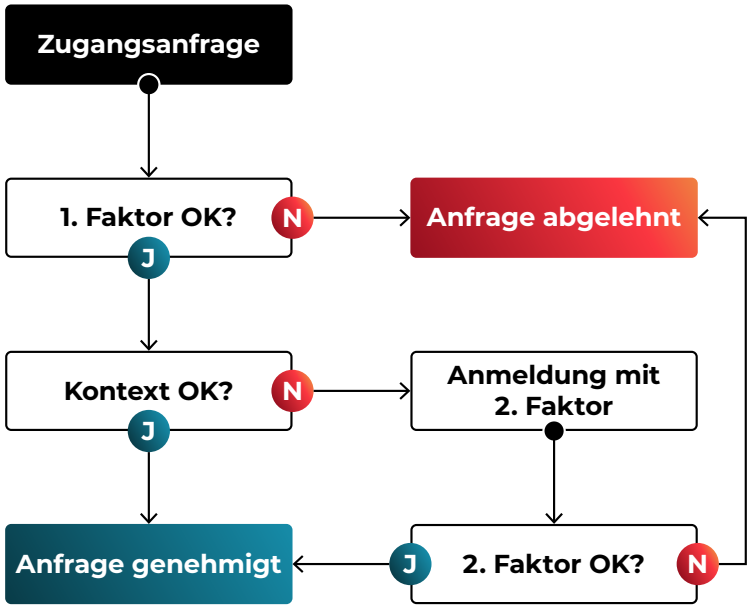
Adaptive Authentication ermöglicht es Versicherungen, die Authentifizierungsstärke an das jeweilige Risiko anzupassen und so eine sichere Umgebung für Kundendaten gewährleisten.

Wie es funktioniert:

Risikobewertung: Wenn ein Benutzer auf Patientendaten zugreifen möchte, bewertet das System das mit der Anfrage verbundene Risiko anhand von Kriterien wie dem Standort des Benutzers, dem Gerät und dem Zeitpunkt des Zugriffs.

Authentifizierungsstärke: Basierend auf der Risikobewertung entscheidet das System über die erforderliche Authentifizierungsstärke. Sollte die Bewertung als risikoreich ausfallen, werden zusätzliche Authentifizierungsmassnahmen verlangt.

Zugriffskontrolle: Sobald der Benutzer die erforderliche Authentifizierung bereitgestellt hat, gewährt oder verweigert das System anhand der Risikobewertung und der Stärke der Authentifizierung den Zugriff auf die Daten des Versicherten.



Der Versicherungssektor vertraut auf Nevis

«Wir haben es als besonders positiv empfunden, dass bei der Entwicklung der Lösung unser Feedback stets willkommen war und unsere Wünsche nach entsprechender Analyse direkt umgesetzt wurden.»

Kenneth Nydegger
Product Owner aller Gateway Services
die Mobiliar

Erfolgsstories

GENERALI

Generali – IAM für sichere digitale Geschäftsprozesse

die Mobiliar

Die Mobiliar – Access Infrastructure

helvetia

Helvetia Versicherungen – Web Application Firewall

Kontaktieren Sie uns für ein Beratungsgespräch.

Schweiz (HQ)	+41 43 508 06 81
Deutschland	+49 89 3803 8684
Grossbritannien	+44 20 4579 0404

oder via Kontaktformular:

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