AIRLOCK®
SECURE ACCESS HUB

WHITEPAPER

Starke Authentifizierung. Einfach.

Airlock 2FA

Inhaltsverzeichnis

1 Grundlagen eines sicheren Logins

Warum eine Zwei-Faktor-Authentifizierung notwendig ist?

Eine Alltagsweisheit lautet: Doppelt hält besser. Und doppelte Sicherheit – das bietet die Zwei-Faktor-Authentifizierung (kurz 2FA, MFA oder SCA[1]) im Bereich IT-Security. Damit ist 2FA die optimale Lösung für die steigende Komplexität im Zugriffsmanagement. Der zweite Faktor bietet unumstritten mehr Sicherheit als die einfache Abfrage von Benutzernamen und Passwort. Er soll aber auch benutzerfreundlich und kosteneffizient sein und aktuellen gesetzlichen Anforderungen entsprechen.

Der Hauptgrund für starke Authentifizierung sind zumeist Schwachstellen der Passwörter:

- **90% der Passwörter sind innerhalb weniger als sechs Stunden geknackt.**
- **2/3 als Benutzer verwenden das gleiche Passwort für verschiedenen Webdienste.**
- **Passwörter suggerieren dem Benutzer bequeme Sicherheit, die aber nicht vorhanden ist.**

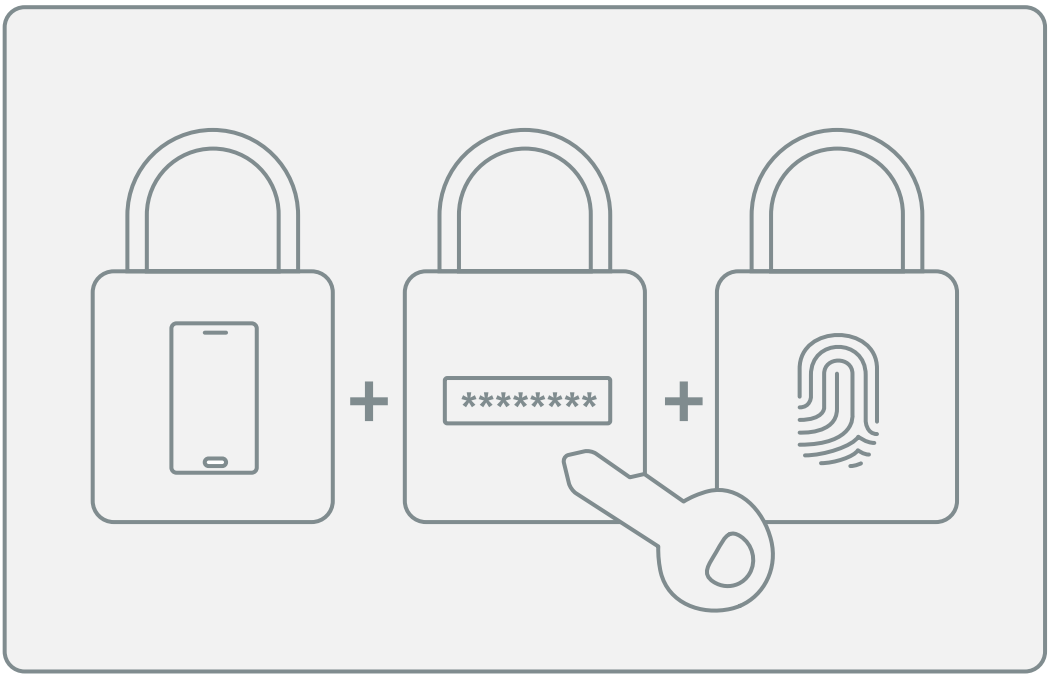
Durch gesetzliche Vorgaben, wie z.B. PSD2 ist die Komplexität deutlich gestiegen. Anforderungen an die Überprüfung der Identität haben sich stark verändert. Viele Regulatoren und Gesetze verlangen eine starke Authentifizierung.

Es gibt neben der Sicherheit und rechtlichen Anforderungen noch einen weiteren Punkt, der bei der Einführung einer 2FA-Lösung eine entscheidende Rolle spielt: die Benutzerfreundlichkeit. In Kombination mit einem leistungsstarken Customer Identity- & Access Management (cIAM) werden viele Prozesse wesentlich vereinfacht. Das erhöht zum einen die Benutzerfreundlichkeit über Self-Services, Benutzerströme oder Single Sign-on, zum anderen werden die internen Abläufe und Aufwände vereinfacht.

[1] MFA steht für Multifaktorauthentifizierung, SCA für «strong customer authentication» oder starke Authentifizierung.

Starke Authentifizierung – was ist das überhaupt?

«Wissen», «Haben», «Sein» – das sind die drei Prinzipien, auf denen die Multi-Faktor-Authentifizierung basiert. Wie diese im Detail umgesetzt werden, kann sehr unterschiedlich sein. Für eine starke Authentifizierung müssen zumindest zwei der drei Prinzipien erfüllt sein.



Etwas, dass nur der Nutzer besitzt:

z.B. eine Bank- oder Kreditkarte, Schlüssel, Smartphone oder Token[2].

Etwas, das nur der Nutzer weiss:

z.B. der Benutzername, Kennwörter, PINs oder Antworten auf Sicherheitsfragen

Etwas, dass der Nutzer ist:

z.B. seinen Fingerabdruck, sein Gesicht oder sein Iris-Muster.

[2] Ein Token ist eine Hardware- oder Softwarekomponente zur Identifizierung und Authentifizierung von Benutzern. Er ist eindeutig einer Identität zugeordnet und wird meist in Kombination mit einem Passwort oder Pin verwendet.

2 Auswahl des optimalen zweiten Faktors – die wichtigsten Überlegungen

Je nach Anwendungsfall kann der zweite Faktor ganz unterschiedlich umgesetzt werden. Der Markt bietet eine Vielzahl unterschiedlicher Varianten der Authentifizierung an: von Zertifikaten, über TAN-Listen, mTAN per SMS, eigene Hardware oder über das Smartphone. Eine Übersicht zu den derzeit üblichen Varianten kann unter folgendem Link nachgelesen werden: **https://www.airlock.com/secure-access-hub/komponenten/customer-identity-access-management-ciam/2-faktor-authentifizierung/authentifizierungsvarianten**

Daher ist eine sorgfältige Auswahl sinnvoll, die Aspekte des Anwenders, der IT-Security und des Unternehmens berücksichtigt. Folgende Überlegungen müssen angestellt werden:

Fokus auf Anwender

- **Die Zielgruppen**
  Von wem wird der zweite Faktor genutzt? Von Kunden im B2C- oder B2B-Umfeld, Partnern oder auch Mitarbeitenden? Von Digital Natives oder auch älteren Anwendern?
- **Der Kontext**
  Wie ist das Sicherheitsempfinden bei den Nutzern im konkreten Anwendungsfall? Wird von ihnen ein aufwendiger Authentifizierungsprozess positiv bewertet? Zum Beispiel bei hohen Finanztransaktionen. Oder soll es möglichst einfach sein – wie z.B. bei Zahlungen am Kiosk?
- **Das eingesetze Gerät**
  Akzeptiert der Nutzer eine App auf seinem Smartphone als zweiten Faktor? Oder ist ein zusätzlicher Hardware-Token erforderlich? Brauchen die Benutzer mehrere Geräte, mit denen sie sich authentifizieren?
- **Die Nutzungssituationen**
  In welchen Situationen authentisieren sich die Nutzer? Braucht es vielleicht sogar eine kontinuierliche Überprüfung? Kann der Benutzer immer online sein? Hat die Authentifizierung auch in Gebieten ohne Netzabdeckung zu funktionieren?

Fokus auf IT-Security und Compliance

- **Art der Autorisierungen**
  Wird der zweite Faktor nur für die Anmeldung zu einem Online-Service verwendet oder werden auch Transaktionen oder sensible Daten freigegeben?
- **Sicherheitsrelevante Szenarien**
  Wie hoch soll das Sicherheitsniveau sein? Genügen SMS bzw. mTAN oder ist eine modernere Authentifizierungslösung mit erhöhter Sicherheit und Benutzerfreundlichkeit erforderlich?
- **Rechtliche Anforderungen**
  Welche Applikationen brauchen aus regulatorischen Gründen eine starke Authentifizierung? Hat das Unternehmen z.B. dem Schweizer Bundesgesetz über das elektronische Patientendossier (EPDG) oder der europäischen Zahlungsrichtlinie (PSD2) zu entsprechen? Müssen Vorgaben gemäss PCI-DSS oder MAS erfüllt werden?
- **Kompetenzen der Applikationsentwickler**
  Laut einer Studie des NoSQL-Entwicklers MongoDB sagen weniger als ein Drittel der Entwickler, dass sie für die Security die Verantwortung tragen. Sollen die Entwickler nun bei jeder neuen Applikation selbst über die Authentifizierungsmethode und damit die Sicherheit entscheiden? Oder soll eine zentralisierte, allgemein verwendbare Gesamtlösung gewählt werden?

Fokus auf unternehmerische Aspekte

- **Einbindung von Partnern und digitalen Eco-Systemen**
  Sollen zusätzliche Services von Drittanbietern eingebunden werden und APIs für zukünftige externe Partner zur Verfügung stehen? Ist auch hier stark zu authentifizieren?
- **Marktsituationen**
  Ist Agilität und eine schnelle Time-to-Market wichtig? Bestehen bereits viele digitale Services? Wird die Anzahl durch die Digitalisierung steigen?
- **Marken-Kontext**
  Wie stark ist die Marke respektive die Corporte Identity und das Corporate Design zu berücksichtigen? Sollen nicht-gebrandete Lösungen eingesetzt werden?
- **App-Einbindung**
  Soll die 2FA-Technologie auch in Unternehmens-Apps eingebunden werden?

Für all diese Fragen müssen in der gewählten Zwei-Faktor-Authentifizierung Antworten gegeben werden können. Eine fundierte Evaluation schützt daher vor zukünftigen Problemen in der Umsetzung.

Die wichtigsten Vor- und Nachteile der gängigsten Methoden sind in der folgenden Tabelle auf einen Blick erfasst.

Methode	Sicherheit	Benutzerfreundlichkeit	Management	Kosten
Zertifikat	⊕⊕	⊖⊖	⊖	⊖
Streichlisten	⊖	⊖	⊖	≈
Matrixkarten	≈	⊖	⊖	≈
mTAN per SMS	⊖	≈	≈	≈
Hardware OTP	⊕	≈	⊖	⊖
Software OTP	⊕	≈	≈	⊕⊕
Push	⊕⊕	⊕⊕	≈	⊕
QR Code				
– mit OTP	⊕⊕	≈	≈	≈
– ohne OTP	⊕	⊕	⊖	⊖⊖
Biometrisch	≈	≈	≈	≈
– mit Hardware	⊕⊕	≈	⊖	⊖⊖
– mit Smartphone	⊕	⊕⊕	≈	≈
FIDO-2	⊕⊕	⊕	≈	≈
FIDO-1	⊕	≈	⊖	⊖⊖
OTP per E-Mail	≈	≈	≈	⊕

Die Begriffserklärungen sind im Glossar näher ausgeführt.

3 Sechs Erfolgskriterien für die erfolgreiche 2FA-Integration

Bei jeder Einführung einer starken Authentifizierung gibt es bestimmte Besonderheiten, die berücksichtigt werden müssen. Die wichtigsten werden im Folgende erörtert.

2FA in bestehende Systeme einbinden

Eine Zwei-Faktor-Authentifizierung bietet einzig die Möglichkeit, eine Identität stärker zu prüfen. Sie ist daher keine alleinstehende Lösung, sondern ist möglichst effizient in bestehende Systeme zu integrieren, die Identitäten verwalten und Zugriffe regeln. In welcher Form, in welchen Abläufen und mit welchen Zugriffrechten der zweite Faktor zum Einsatz kommt, ist davor zu definieren.

1. **Identitäten**
   An welche Benutzerverzeichnisse soll 2FA angebunden werden? An eine eigene Datenbank, an Microsoft Active Directory (AD), LDAP und/oder an ein Customer IAM (cIAM)?
2. **Zugriffe**
   Welche Anwendungen sollen konkret geschützt werden? Welche APIs, Web-Portale oder mobile Applikationen? Ist für gewisse Applikationen schon eine 2FA-Lösung im Einsatz?
3. **Authentifizierung**
   Welche Komponenten sind beim Anwender bereits vorhanden? Smartphones, Hardware-Tokens, etc.? Diese können als Träger des zweiten Faktors einbezogen werden, um Kostenersparnisse und einen höheren Nutzungskomfort zu erzielen.

Vorgelagerte Authentifizierung

Vorgelagerte Authentifizierung bedeutet: Es wird nicht mehr jede einzelne Applikation separat geschützt, sondern die gesamte Applikationslandschaft. Der erste Vorteil ist ein deutliches Plus an Sicherheit für die gesamte IT-Infrastruktur. Der zweite ist eine nachhaltige Steigerung der Effizienz. So wird bei einer vorgelagerten Authentifizierung jedes Sicherheits-Update, jede Compliance-Änderung und jede Implementation eines neuen Authentisierungsmittels zentral gesteuert und verwaltet – das spart viel Zeit und erhöht die Wirtschaftlichkeit. Die Entwicklungskosten und -zeit für neue Applikationen werden deutlich gesenkt.

Risikoszenarien entwickeln

Jede Kundengruppe ist anders. Und jedes unternehmensspezifische Risikoszenario ebenso. Darum ist eine fundierte Evaluation entscheidend. Im ersten Schritt geht es dabei um die Frage, ob und für welche Applikationen und Services eine starke Authentifizierung erforderlich ist. Danach sollte das gewünschte Sicherheitsniveau für jede Applikation – oder für die gesamte Applikationsarchitektur – definiert und die Art der Registrierung bestimmt werden. Schliesslich müssen auch die Benutzer genauer analysiert werden: Wie technikaffin sind diese und vertrauen sie digitalen Identitäten?

Eine durchgängige Customer Journey ermöglichen

Benutzerfreundliche Abläufe sind bei der Gewinnung von neuen Kunden essenziell. Die logische Konsequenz: Die Customer Journey muss gut durchdacht und logisch aufgebaut sein. Dabei sind die genutzten Geräte ebenso zu berücksichtigen wie die konkrete Ausgestaltung des Onboarding-Prozesses. Dieser kann stufenweise über Social-Registration und Social-Login für niedere Eintrittsbarrieren bis hin zum stark authentifizierten Benutzerkonto für hohe Sicherheit gestaltet werden. Auch Funktionalitäten, wie User Self-services oder Single Sign-on (SSO) optimieren die Benutzerfreundlichkeit weiter. Wenn der zweite Faktor selbst gewählt werden kann und im Notfall ein zuverlässiger Austausch zur Verfügung steht, dann sind das für Kunden wertvolle Mehrwerte, die zudem den Support deutlich entlasten.

Rollout- und Ersatz-Abläufe optimieren

Eine integrierte Security-Lösung mit cIAM und integrierter Zwei-Faktor-Authentifizierung minimiert unternehmerische Aufwände und erleichtert die Workflows. Das gilt nicht nur für den laufenden Betrieb, sondern auch für den Rollout. So übernehmen moderne cIAM-Systeme beim Einführen von neuen 2FA-Methoden automatisiert die gesamte Kundeninformation – dank durchdachter Kommunikation über verschiedene Kanäle. Gerade bei der Erstanmeldung entlasten intuitiv verständliche User-Self-services den Helpdesk nachhaltig, aber auch wenn dem Benutzer das Gerät für den zweiten Faktor verloren geht oder er es wechseln will.

Migrationen erleichtern

Alles Neue ist mit Aufwand verbunden – nicht nur für Unternehmen, sondern auch für Kunden. Darum gilt es, Migrationsprozesse von bestehenden Zwei-Faktor-Lösungen möglichst einfach und benutzerfreundlich zu gestalten. So sollte die neue Zwei-Faktor-Authentifizierung schrittweise eingeführt werden und einen Mischbetrieb in der Übergangsphase erlauben, bei dem sowohl die alten als auch die neuen Authentifizierungsmethoden genutzt werden.

4 cIAM und 2FA – Gemeinsam mehr Sicherheit

Die Zwei-Faktor-Authentifizierung ist eine singuläre Technologie, um Merkmale von Identitäten zu verifizieren. Doch wer Identitäten überprüft, muss diese und ihre Zugriffsberechtigungen auch verwalten. Hierfür ist das Customer Identity & Access Management (cIAM) zuständig.

Was im echten Leben gilt, das gilt auch für die IT-Security: Flughafenkontrollen sind hier die perfekte Analogie. Sie sind komplexer, als man denkt. Denn Grenzen müssen gezogen, Kontrollmechanismen bestimmt und Identitäten mit ihren Berechtigungen definiert werden. Aber auch die Inhalte müssen geprüft werden. Und genau hier liegt die eigentliche Herausforderung. Denn ein Passagier erscheint zuerst als Person ohne Identität und Bezug zu einem Flug. Erst die verschiedenen Kontrollen qualifizieren ihn dazu, in das für ihn bestimmte Flugzeug zu steigen und den richtigen Sitzplatz zu finden.

2FA entspricht in dieser Flughafenanalogie der Ausweiskontrolle. Wie werden aber die Ticket-Ausgabe und -Kontrolle oder das Gepäck-Scanning, Boarding etc. in der IT-Security abgedeckt? Auch die Web-Applikationen und APIs müssen umfassender geschützt werden. Zukunftssicher ist darum eine abgestimmte Orchestrierung von Identitätsverwaltung und -kontrolle in einer integrierten Gesamtlösung. Mit 2FA in Kombination mit cIAM, einer vorgelagerten Web Applikation Firewall und einem API Security Gateway.

Fünf Gründe, warum die Kombination wichtig ist:

- **Volle Integration**

  Ein modernes cIAM ist mit verschiedensten Authentifizierungsverfahren kompatibel und bietet eine leicht zu integrierende Möglichkeit der effizienten Benutzer- und Zugriffsverwaltung. Dadurch ist die Anbindung an einen zweiten Authentisierungsfaktor besonders einfach, speziell wenn dieser bereits voll integriert ist.

- **Optimale Authentisierungsabläufe**

  In Kombination mit 2FA kann ein cIAM den Benutzerzugriff unterschiedlich steuern und risiko- als auch nutzerbasiert verschiedene Zugriffsmöglichkeiten anbieten – z.B. unter Berücksichtigung der Zugriffshistorie oder des gerade verwendeten Gerätes. Für den Kunden bedutet das: Er erlebt einen durchgängigen Authentisierungsablauf, der seiner jeweiligen Situation optimal entspricht. So kann seine Identität zu Hause z.B. ohne zusätzliche Interaktion und einer risikobasierten Authentifizierung überprüft werden, während er unterwegs auf eine benutzerfreundliche Authentifizierung mit nur einer Berührung via Smartphone zurückgreift.

- **Praktisches Single Sign-on**

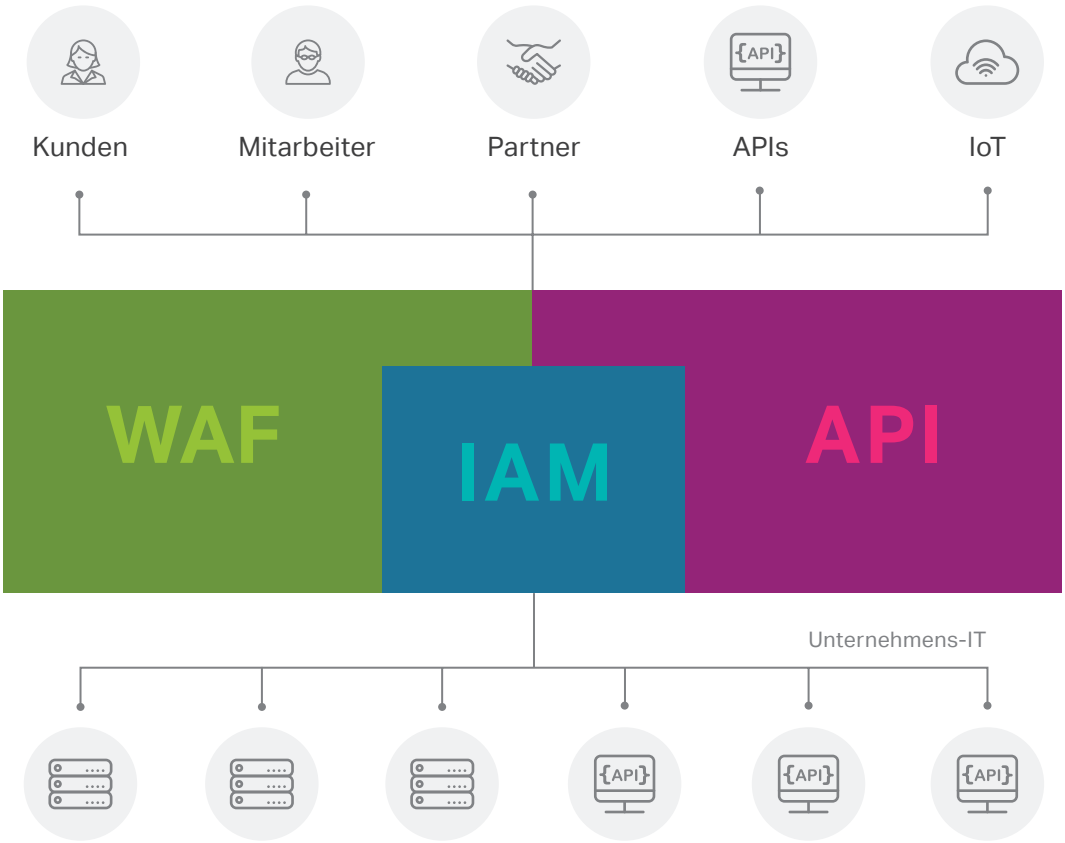
  Einzelne Zugriffe auf Applikationen werden entkoppelt und die Identität eines authentifizierten Benutzers mehrfach genutzt. Dadurch wird ein transparentes Single Sign-on möglich, das hohe Sicherheit mit hoher Benutzerakzeptanz verbindet.

- **Moderne User Self-services**

  Damit nicht nur die Anmeldung benutzerfreundlich ist, ist eine verständliche Benutzerselbstverwaltung wichtig – z.B. für das Verwalten der eigenen Daten, Zustimmungserklärungen (DSGVO), der Wahl des zweiten Faktors oder um neue Dienste zu nutzen. Zudem entlasten User Self-services, die über cIAM realisiert werden, den Helpdesk von Unternehmen und führen so zu massiven Kosteneinsparungen.

- **Effiziente Out-of-the-Box-Lösung**

  Schon bei der Auswahl einer 2FA-Lösung stellt sich die Frage: Soll ich eine integrierte Gesamtlösung wählen? Oder doch vorhandene Komponenten nutzen, dafür aber noch einen weiteren Server einrichten und alles einzeln an den Authentifizierungsprozess anpassen? Diese Frage stellt sich aber nicht nur bei der Systemauswahl, sondern auch beim Systemmanagement. Denn einzelne Komponenten bedeuten: Jedes Update und jede Änderung von Regularien ist an allen Stellen anzupassen. Daher lohnt es sich, hier die Vollkostenrechnung zu machen, die oft zugunsten einer ganzheitlichen Out-of-the-Box-Lösung ausfällt.



Web-Applikationen und APIs

Drei zentrale Vorteile für Unternehmen

Eine orchestrierte Security-Lösung bringt auch wirtschaftlich grosse Vorteile. Denn integrierte Gesamtlösungen überzeugen vor allem dort, wo es heute drauf ankommt: bei der Optimierung interner und externer Prozesse.

1. Vorteil: Benutzerfreundlichkeit erhöhen

Vieles spricht für folgende These: Die sehr hohe Benutzerfreundlichkeit und die intuitive Nutzerführung sind wesentliche Erfolgsfaktoren digitaler Champions wie Amazon, Apple, Google, Netflix oder Uber.

Für diese Feststellung sprechen zum einen die klaren Zahlen: So sind einer CEI-Umfrage[3] zufolge 86 Prozent der Käufer bereit, für eine bessere Benutzerfreundlichkeit mehr zu bezahlen. Das ist die gute Nachricht. Und die schlechte Nachricht: Nur 1 Prozent der Kunden hat den Eindruck, dass Anbieter ihre Erwartungen diesbezüglich konsequent erfüllen.

Laut einer weiteren Studie von PWC[4] ist für 73% der Käufer die Customer Experience ein entscheidendes Kaufkriterium. Die Kluft zwischen der gewünschten, positiven Benutzererfahrung und der erlebten User Experience ist allerdings abhängig von der Branche mit zwischen 33% und 10% immens.

Auf der anderen Seite zeigt allein schon unsere Alltagserfahrung, warum einfache Onboarding- und Authentifizierungsprozesse sinnvoll sind. Denn wenn der Kauf des Flugtickets per Fingerabdruck bestätigt, der Online-Einkauf über eine App getätigt oder die Anmeldung zum Online-Banking nur über Umgebungsgeräusche vollzogen werden kann, dann ist das nicht nur sicher, sondern macht auch richtig Spass.

2. Vorteil: Kosten senken

Sicherheit kostet. Das ist auch bei der Einführung von 2FA so. Allerdings lassen sich mit Sicherheit auch Kosten sparen – je nachdem, wie intelligent die gewählte Lösung ist. Dies betrifft sowohl die Aufwände bei der Implementierung als auch im laufenden Betrieb.

So wird von vielen Unternehmen noch immer SMS und mTAN als 2FA-Methode eingesetzt. Das ist nicht nur sicherheitstechnisch bedenklich. Auch in puncto Kosteneffizienz schneiden SMS schlecht ab. Unternehmen, die auf einen anderen zweiten Faktor wechseln, sparen allein schon bei den Telekommunikationskosten schnell fünf- bis sechsstellige Beträge ein.

[3] Quelle Forbes / Rightnow Customer Experience Impact Report.

[4] https://www.pwc.com/us/en/advisory-services/publications/consumer-intelligence-series/pwc-consumer-intelligence-series-customer-experience.pdf

Ein anderer Kostentreiber sind Anfragen beim Helpdesk eines Unternehmens. So zeigen Recherchen, dass bei einem Schweizer Finanzdienstleister pro Jahr durchschnittlich 40% aller Support-Anrufe auf Probleme mit dem Login und dem Onboarding beruhen. Die Folge: Immenser finanzieller Aufwand für etwas, das über 2FA und durchdachte User Self-services auch vom Anwender selbst umgesetzt werden kann – User Self-services, die schneller und angenehmer für die Kunden sind.

Und bei der Implementierung von 2FA? Hier kann die Kombination von 2FA und cIAM seine Stärken voll ausspielen, da durch einen hohen Standardisierungsgrad fast keine Initialaufwände anfallen. Weiteres Plus: In Kombination mit cIAM erfolgt die Kommunikation mit den Kunden vollständig automatisiert, so dass die technischen Aufwände bei der Migration und dem Ausrollen neuer zweiten Faktoren gegen Null tendiert.

3. Vorteil: Sicherheit steigern

Was doppelt überprüft wird, ist auch doppelt sicher, so die grundlegende Logik von 2FA. Doch neben diesem wesentlichen Vorteil sprechen noch weitere Sicherheitsvorteile für den Einsatz einer Multi-Faktor-Authentifizierung, wie oben in der Flughafenanalogie ausgeführt.

Grundsätzlich lässt sich feststellen, dass heute ein Faktor für die sichere Authentifizierung von Benutzern und Identitäten einfach nicht mehr reicht. Auch der Rückgriff auf SMS und mTAN als zweiten Faktor gilt als überholt. So ist Smishing (Phishing-Versuche per SMS) zu einem echten Problem geworden und viele Mobilfunkanbieter gehen dazu über, den SMS-Versand ins Ausland zu blockieren. Daher sind mobile Apps mit persönlichem Schlüssel auf dem eigenen Smartphone die bessere Alternative.

Zudem bietet 2FA in Kombination mit cIAM Mehrwerte, die heute immer wichtiger werden. Ein Beispiel hierfür sind Transaktionsfreigabe (Transaction Approvals oder auch Transaction Signing). Hierbei wird durch eine eigene Interaktion mit dem Kunden die Genehmigung für eine Transaktion einfordert.

5 Airlock 2FA

Wie ist nun ein optimaler Mix zwischen Nutzerfreundlichkeit, Kostensenkung und höherer Sicherheit zu erreichen? Diese Frage ist zentral bei der Wahl des zweiten Faktors. Heute stehen dynamische Lösungen zur Verfügung, um risikobasiert auf unterschiedliche Anwendungsfälle zu reagieren.
Der Vorteil einer risikobasierten Authentifizierung: ein nahtloser Ablauf der Authentifizierung, der beiden Anforderungen gerecht wird – dem nach Sicherheit und dem nach Benutzerfreundlichkeit.

Zero-Touch

Einfacher geht es nicht: Eine einzigartige 2FA-Variante, die ein sicheres Login ohne jegliche Benutzerinteraktion erlaubt. Zero-Touch verwendet Umgebungsinformationen und macht die Anmeldung so einfach wie noch nie.

UX: ⊕⊕⊕ Sicherheit: ⊕⊕ Kosten: ⊕⊕⊕ Online

One-Touch

Mit Hilfe von **Push-Benachrichtigungen** über Airlock 2FA bestätigen Benutzer mit einer einzigen Berührung des Displays eine Anmeldung oder geben eine Transaktion frei. Auch zusätzlich abgesichert durch Fingerabdruck oder Gesichtserkennung.

UX: ⊕⊕ Sicherheit: ⊕⊕⊕ Kosten: ⊕⊕⊕ Online

(Offline) QR-Code

Durch das Scannen eines QR-Codes mit Airlock 2FA melden sich die Benutzer innerhalb von Sekunden sicher an oder autorisieren eine Transaktion, auch offline.

UX: ⊕ Sicherheit: ⊕⊕⊕ Kosten: ⊕⊕⊕ Online

Passcode

Alle 30 Sekunden wird in Airlock 2FA automatisch ein neues Einmalkennwort (One-time Password, kurz OTP) generiert. So geben die Nutzer ihre Aktionen auch ohne Internetzugang frei.

UX: ⊖ Sicherheit: ⊕⊕⊕ Kosten: ⊕⊕⊕ Online

Airlock Secure Access Hub: Alles aus einer Hand!

Klar, je integrierter ein System ist, desto besser ist es auch. Darum ist die optimale Lösung ein Secure Access Hub, der WAF, API Gateway, cIAM und 2FA beinhaltet und miteinander verbindet. Die zentralen Vorteile dieser Lösung sind: höchste Sicherheit zu niedrigen Kosten, in einer Gesamtlösung, die eine effiziente Applikationsentwicklung und schnelle Time-to-Market ermöglicht, ohne einzelne Komponenten unterschiedlicher Hersteller mühsam aufeinander abstimmen zu müssen.

Variante	Benutzer-freundlichkeit	Sicherheit	Desktop	Single Device Authentifizierung („Mobile Only“)	Offline
2-Faktor-Authentifzierung					
Zero-Touch	⊕⊕⊕	⊕⊕	●	●	
One-Touch	⊕⊕	⊕⊕⊕	●	●	
Offline QR-Code	⊕	⊕⊕⊕	●		●
Passcode	⊕	⊕	●	●	●
Transaktions-genehmigung					
One-Touch	⊕⊕	⊕⊕⊕	●	●	
Offline QR-Code	⊕	⊕⊕⊕	●		●
Passwortfreie Authentifizierung					
One-Touch	⊕⊕	⊕⊕⊕	●	●	
Offline QR-Code	⊕	⊕⊕⊕	●	●	●

⊕⊕⊕ hervorragend ⊕⊕ sehr gut ⊕ gut ● Airlock 2FA

6 Glossar

- **Zwei-Faktor-Authentifizierung (2FA):** bezeichnet den Identitätsnachweis eines Nutzersmittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten aus den Varianten Wissen, Besitz und Sein.

- **Multi-Faktor-Authentifizierung (MFA):** bezeichnet eine Verallgemeinerung der Zwei-Faktor-Authentifizierung, bei der die Zugangsberechtigung durch mehrere unabhängigen Merkmale (Faktoren) überprüft wird.

- **Strong Customer Authentication (SCA):** ist eine andere Bezeichnung für Zwei-Faktor-Authentifizierung.

- **3-D Secure-Protokoll**: auch 3DS genannt wird speziell beim Onlineshopping eingesetzt. Käufer müssen sich als rechtmässiger Karteninhaber gegenüber ihrer Bank authentifizieren. Um den Bestellvorgang abzuschliessen, wird bei 3-D Secure beispielsweise ein Code verlangt oder eine Push-Nachricht an den Kunden geschickt.

- **One-Touch:** bezeichnet eine Authentifizierungsvariante von Airlock 2FA, die mit minimaler Benutzerinteraktion auskommt.

- **Zero-Touch:** bezeichnet eine Authentifizierungsvariante von Airlock 2FA, die ohne Benutzerinterkation auskommt.

- **Zertifikatsauthentifizierung:** Starke Authentifizierungsmethode basierend auf elektronischen Zertifikaten (typischerweise nach X.509 Standard). Das Zertifikat, resp. dessen private Schlüssel, ist dabei auf einem USB-Token, einer Smartcard oder einem Soft-Token gespeichert. Je nach Anwendung ist dazu eine PKI (public key infrastruktur) notwendig.

- **TAN-Listen:** Der Benutzer erhält einen Brief mit einer Liste an Codes (Streichliste), die jeweils nur einmal gültig sind. Durch die Eingabe des Codes wird der zweite Faktor erbracht.

- **Token:** eine Hardware- oder Softwarekomponente zur Identifikation und Authentifizierung von Benutzern. Es wird meist in Kombination mit einem Passwort oder Pin verwendet.

- **mTAN:** Um dieses Verfahren zu nutzen, benötigt der Nutzer ein Mobiltelefon mit SMS-Funktion und muss die Mobiltelefonnummer beim Anbieter hinterlegen. Es wird ein einmal gültiger Sicherheitscode per SMS verschickt und durch den Benutzer abgetippt.

- **OTP:** steht für "One-Time Password" und findet in unterschiedlichen Authentifizierungsvarianten wie z.B. auch mTAN Anwendung. OTPs werden häufig auch zeitabhängig in Hardwaretokens oder Apps generiert.

- **Push:** Der Nutzer erhält per Push an eine spezielle Smartphone-App entweder eine Nachricht, die er bestätigen oder ablehnen kann, oder er erhält einen Transaktionscode, auch pushTAN genannt, den er abtippt. Das Verfahren wird häufig auch zur Bestätigung von Transaktionen (Transaction Approval oder Transaction Signing) verwendet, da man einfach Transaktionsdaten übermitteln und anzeigen kann.

- **QR-CodeAuthentifizierung:** Mit einer Smarphone App oder einem Hardwaretoken wird ein QR-Code (zweidimensionaler Barcode) abgescannt und daraus unter Einbezug von kryptographischem Schlüsselmaterial ein OTP berechnet. Dieser wird dann vom Benutzer eingegeben, um den Identitätsnachweis oder eine Transaktion zu bestätigen.

- **Challenge Response:** Unter den Begriff «Challenge Response» fallen alle Verfahren, in denen eine «Challenge» – häufig ein zufälliger Wert – vom Server zum Authentisierungstoken geschickt, dort mit geheimem Schlüsselmaterial verrechnet und wieder an den Server zurückgeschickt wird («Response»). Viele Authentifizierungsverfahren basieren auf diesem Prinzip. Beispiele: Zertifikatsauthentifizierung, QR-Code Login, Matrixkarten, Push.

- **Authentisierung:** ist der Vorgang, mit dem der Benutzer sich an einem Dienst anmeldet. (z.B. Eingabe von Benutzername und Kennwort). Es geht also um den Loginvorgang aus Benutzersicht.

- **Authentifizierung:** ist die Verifikation der Anmeldung einer Identität. Es geht also um den Loginvorgang aus Serversicht.