Die sieben wichtigsten Trends für die Zukunft der Finanzdienstleis-tungsbranche

Die Finanzdienstleistungsbranche erlebt weltweit einen nie dagewesenen Wandel. Zunehmende gesetzliche Auflagen zum Schutz der Verbraucherdaten, Forderungen der Verbraucher selbst nach Zugriff auf und Kontrolle über ihre Finanzdaten, verstärkter Wettbewerb in einem expandierenden Finanzdienstleistungsumfeld … Angesichts dieses Umfelds benötigen Sie eine IAM-Lösung (Identity and Access Management), die Folgendes ermöglicht:

- Einhaltung von Open Banking- und Verbraucherschutzbestimmungen
- Umsatzsteigerung und Sicherung des Wettbewerbsvorteils
- Vereinfachung von Kundengewinnung, Kundenbindung und Kundenschutz durch kompromisslose Zero-Trust-Sicherheit
- Bereitstellung nahtloser Omnichannel-Erlebnisse über alle Plattformen hinweg: Filiale, Internet und Mobilgeräte

Sieben Trends werden die Zukunft der Finanzdienstleistungsbranche maßgeblich beeinflussen. Wenn Sie diese Trends kennen, können Sie die richtige IAM-Lösung auswählen, um die Herausforderungen der Zukunft zu meistern.

TREND 1

Gesetzliche Bestimmungen und Datenschutz

Neue gesetzliche Bestimmungen beschleunigen die digitale Innovation und den Verbraucherschutz. Seit der Verabschiedung der Datenschutzgrundverordnung (DSGVO) durch die Europäische Union (EU) im Mai 2018 müssen Unternehmen aus aller Welt, die in der EU Geschäfte tätigen, strenge Datenschutzbestimmungen erfüllen, darunter das „Recht auf Vergessenwerden bzw. Löschung“. Sämtliche Unternehmen sind gesetzlich verpflichtet, die Verbraucher darüber zu informieren, wie ihre Daten verwendet werden. Zudem müssen sie ihnen die Möglichkeit zum Löschen ihrer Daten geben.

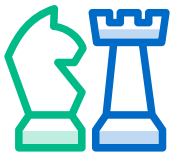
Vorschriften wie Open Banking in der EU und Großbritannien, die EU-Zahlungsdiensterichtlinie 2 (PSD2) und das kalifornische Gesetz zum Verbraucherdatenschutz (CCPA) verlangen von Banken, dass sie die Identitäten und Finanzdaten ihrer Kunden schützen und die Risiken für die persönlichen Daten ihrer Kunden minimieren. Risikomanagement-Experten sind deshalb auf der Suche nach kundenorientierten Technologien, die integrierte Sicherheit („Security by Design“) bieten und sich nahtlos in ihre Risikomanagement- und Compliance-Strategien einbinden lassen. Angesichts täglich neu aufkommender Bedrohungen für personenbezogene Daten muss Ihr Unternehmen zuverlässig in der Lage sein, Risiken zu erkennen und zu mindern sowie die Identifizierung und Verfolgung von Straftätern zu unterstützen.

Achten Sie bei der Auswahl von IAM-Produkten auf folgende Funktionen:

Identifizieren und Vermeiden von Betrug durch kontextuelle Authentifizierung und Autorisierung

Erkennen von Signalen in Verhalten und Umgebung, z. B. Jailbreak-Erkennung, IP-Adressen, Gerätezuordnungen, Geofencing, Standortbereiche usw.

Ihre IAM-Lösung sollte sich zudem problemlos in branchenführende Sicherheitslösungen, wie Betrugserkennung und Identitätsüberprüfung, integrieren lassen, um Ihre Kunden zu schützen, ohne Abstriche beim Benutzererlebnis zu machen.



TREND 2

Zunehmender Wettbewerb

Um angesichts der Verlagerung des Privatkundengeschäfts und anderer Bankdienstleistungen auf Onlinekanäle wettbewerbsfähig zu bleiben, reicht es nicht aus, die Prozesse und Kosten zu optimieren. Fintechs ebenso wie branchenfremde Markteinsteiger und rein digitale „Neobanken“ revolutionieren die Finanzdienstleistungsbranche, indem sie die digitale Innovation und den Wettbewerb anheizen. Die breite Akzeptanz von Digital Banking treibt das Wachstum etablierter und neuer Wettbewerber am digitalen Bankenmarkt voran, insbesondere in Südostasien und Lateinamerika. Viele Banken greifen diese neuen Trends auf und beschleunigen ihre Investitionen in die digitale Transformation, um Erträge für die Banken und Gewinne für die Aktionäre zu erzielen, während sie gleichzeitig ihre Kosten senken.

Damit Ihr Unternehmen in diesem neuen Umfeld bestehen kann, muss es agil handeln und über eine flexible IT-Architektur verfügen. Ohne Systeme und Plattformen für einen vollständig digitalen Service laufen Sie Gefahr, für das neue Kundenerlebnis an Relevanz zu verlieren. Achten Sie bei der Auswahl einer IAM-Lösung deshalb darauf, dass diese sowohl Ihre bestehenden als auch Ihre zukünftigen Bereitstellungspläne unterstützt – unabhängig davon, ob Sie Ihre Lösung vor Ort, in Public-, Private- oder Multi-Cloud-Umgebungen oder als Service bereitstellen.

TREND 3

Beschränkungen durch Altsysteme

Traditionelle Filialbanken bemühen sich, ihre digitale Transformation zu beschleunigen, werden jedoch durch veraltete Prozesse, Geräte und Software ausgebremst. Die Migration von Altsystemen ist naturgemäß mit Risiken verbunden. Sie kann dazu führen, dass Benutzer ihren Zugang verlieren, Compliance-Audits scheitern, Kosten überschritten werden und das Ansehen leidet. Digitale Transformation mit bestehender Infrastruktur erfordert eine sorgfältig geplante, zielgerichtete Migration mit den richtigen Tools und Systemen, um einen übermäßigen Zeit-, Kosten- und Arbeitsaufwand zu vermeiden.

Viele Banken nutzen für die Transaktionsabwicklung immer noch althergebrachte lokale Computersysteme und überholte Programmiersprachen.[1] Da jedoch viele Experten, die diese Systeme vormals betreut haben, mittlerweile im Ruhestand sind, klafft in der Belegschaft eine zunehmende Qualifikationslücke. Isolierte IAM-Altsysteme sind unflexibel und lassen sich nicht skalieren, um neue Anwendungsfälle, bessere Authentifizierungsmethoden und weitere Bereitstellungsmodelle zu unterstützen. Um diese Beschränkungen durch Altsysteme zu überwinden, benötigen Sie eine IAM-Lösung, die die Migration und Zentralisierung von Identitäten aus verschiedenen Identitätsmanagementsystemen auf einer einzigen IAM-Plattform unterstützt. Dadurch können Sie Ihre bestehenden Systeme schnell und einfach rationalisieren und auf früheren Investitionen aufbauen – ohne jegliche Beeinträchtigung für die Nutzer. Schon das Hinzufügen von modernen Authentifizierungstechnologien und Multi-Faktor-Authentifizierung zu bestehenden Anwendungen kann die Sicherheit und Benutzerfreundlichkeit Ihrer Anwendungen sofort erhöhen.

TREND 4

Open Banking und Open Finance

Open-Banking- und Open-Finance-Initiativen bewirken eine zunehmende Akzeptanz digitaler Kanäle und Technologien sowie robusterer offener Programmierschnittstellen (APIs). Open Banking soll den Datenaustausch erleichtern und es Banken und Drittanbietern ermöglichen, maßgeschneiderte Lösungen basierend auf neuen, einheitlichen Plattformen zu entwickeln. Mit der Umstellung von Banken und anderen Finanzdienstleistungsunternehmen auf Open Banking können Dritte deren Kundendaten für Dinge wie Cross-Selling und Direktmarketing nutzen. Finanzinstitute werden die Daten ihrer Kunden künftig vermehrt einsetzen, um Kredite, Kreditkarten, Hypotheken und andere Dienstleistungen anzubieten.

Finanzdienstleister weltweit wollen eine Art Open Banking Framework implementieren, das auf drei grundlegenden Technologien basiert:

- Eine Finanz-API (FAPI) von der OpenID Foundation
- Ein einheitliches Authentifizierungssystem mit OpenID Connect
- Eine Identitätsmanagementmethode, die Zustimmung und Delegation beinhaltet

Während Open Banking und Open Finance in einigen Regionen, wie z. B. Europa, durch gesetzliche Vorschriften reguliert werden, sind die USA weniger durch Vorschriften als vielmehr durch den Wettbewerb am Markt und die Forderung der Verbraucher nach mehr Kontrolle über ihre Finanzdaten motiviert. Financial Data Exchange (FDX) ist eine in den USA und Kanada ansässige Organisation für offene Standards mit dem Ziel, „den Finanzsektor auf einen gemeinsamen, interoperablen und gebührenfreien Standard für den sicheren und bequemen Zugang von Verbrauchern und Unternehmen zu ihren Finanzdaten zu verständigen“.[2] Die vorgeschlagene FDX-Standard-API unterstützt die sichere Authentifizierung und den sicheren Datenzugriff unter Berücksichtigung der bestehenden Authentifizierungs- und Autorisierungsprotokolle. Dies ermöglicht den Austausch von Verbraucherdaten ohne „Screen Scraping“ (gemeinsame Anmeldedaten). Die Einführung der FDX-API auf breiter Basis würde ein sichereres Vertrauensumfeld kreieren, das es innovativen Fintech-Unternehmen ermöglicht, neue Dienstleistungen anzubieten – ohne Kompromisse in puncto Sicherheit.

Um im Zeitalter von Open Banking und Open Finance relevant zu bleiben, benötigen Sie eine IAM-Lösung, die den neuesten Standards entspricht, die also ein sicheres Onboarding und Staging unterstützt und die Zustimmung von Drittanbietern (TPPs) erlaubt.

[1] American Banker, Why some banks still lean on mainframes

[2] Financial Data Exchange, Frequently Asked Questions about FDX US

TREND 5

Forderung der Verbraucher nach mehr Kontrolle und besserem Nutzererlebnis

Die DSGVO hat viele Datenschutzinitiativen auf lokaler, nationaler und internationaler Ebene ins Rollen gebracht. Sie hat außerdem unter Verbrauchern weltweit die Forderung nach mehr Kontrolle über ihre Daten entstehen lassen. Verbraucher sind zunehmend unzufrieden darüber, dass ihre persönlichen Daten ohne ihr Einverständnis gesammelt und für Marketingzwecke verwendet werden. In der Folge kam es in der Finanzdienstleistungsbranche zu einem drastischen Anstieg der Gerichtsverfahren im Zusammenhang mit der Erfassung von Daten. Die Verbraucher ergreifen die Initiative und verlangen die Kontrolle über ihre Daten.

Ob Sie Ihre Kunden nahtlos über Mobilgeräte oder Desktop-Plattformen, zu Hause oder im Büro erreichen wollen, Ihre IAM-Lösung muss eine Customer Experience (CX) bieten, die:

- strenge Datenschutzbestimmungen erfüllt;
- den Verbrauchern ein Höchstmaß an Sicherheit und Kontrolle über ihre persönlichen Daten erlaubt;
- ein gleichbleibendes Erlebnis über alle Touchpoints bietet.

TREND 6

Gesellschaftliche Veränderungen

Die Finanzdienstleistungsbranche ist seit langem ein Spiegelbild der Wirtschaft und gesellschaftlichen Trends im Allgemeinen. Man denke nur an die Veränderungen in der Dienstleistungsbranche seit den frühen 2000er Jahren. Berufe, die ein hohes Maß an „Digitalisierung“ erfordern, haben zwischen 2002 und 2016 um den Faktor 4,6 zugenommen – von der Brookings Institution als „Verbreitung digitaler Technologien in nahezu allen Unternehmen und Arbeitsplätzen“ bezeichnet. Berufe, die nur geringe oder gar keine digitalen Kompetenzen erfordern, sind hingegen um die Hälfte zurückgegangen.[3] Dieser Trend zur Digitalisierung wird weiter zunehmen, da Technologien wie künstliche Intelligenz (KI) und maschinelles Lernen (ML) die Art und Weise, wie wir arbeiten, leben und Geschäfte tätigen, verändern.

Die durch COVID-19 hervorgerufene plötzliche Veränderung des Verbraucherverhaltens hat die Nachfrage nach sicheren Online-Diensten bei Banken und anderen Finanzinstituten verstärkt, die ein persönliches Erscheinen in der Filiale oder im Büro unnötig machen. Laut Gartner erwarten die Leiter von Finanzdienstleistungsunternehmen nach der Pandemie einen durchschnittlichen Anstieg der IT-Budgets um 11 % mit einem Schwerpunkt auf dem Wachstum des direkten digitalen Umsatzes.[4]

Der Bankensektor befindet sich in der größten Umwälzung seit den frühen 1990er Jahren. Dabei ändern sich die Rollen

und Beziehungen zwischen Finanzinstituten, Kunden, Partnern und Mitarbeitern in rasantem Tempo. Da immer mehr Finanztransaktionen online stattfinden, muss Ihre IAM-Lösung skalierbar sein, um mehrere Millionen Benutzer unterstützen zu können, ohne dass die IT-Abteilung einen enormen Aufwand betreiben muss oder die bestehenden Benutzer beeinträchtigt werden.

[3] Mark Muro, Sifan Liu, Jacob Whiton und Siddharth Kulkarni, „Digitalization and the American Workforce“
[4] Weiss, Juergen und Iyengar, Partha, „Financial Services CIOs Must Realize IT Investments' Revenue Potential to Drive Digital Acceleration“, 17. Februar 2021. https://www.gartner.com

TREND 7

Cyberrisiken

Angesichts der Zunahme von Ausmaß, Umfang und Raffinesse von Cyberangriffen, wie z. B. Identitätsbetrug, haben Investitionen in die Cybersicherheit höchste Priorität. Ransomware-Angriffe sind zwischen 2019 und 2020 um 150 % angestiegen.[5] Um Angriffe mit dem Ziel der Kontoübernahme abzuwehren und Mitarbeiter, Verbraucher und Geräte, die mit dem Internet verbunden sind, zu schützen, benötigen Sie eine ganze Reihe von Sicherheitsmaßnahmen, wie das Zero-Trust-Modell und die CARTA-Strategie (Continuous Adaptive Risk and Trust Assessment).

Eine gefährliche Sicherheitslücke für die meisten Finanzinstitute ist die schleichende Ausweitung der Berechtigungen, d. h. dass Mitarbeiter, vertrauenswürdige Dritte und Partner Zugang zu mehr Systemen oder höheren Berechtigungsstufen erhalten, als für ihre jeweilige Funktion erforderlich ist. Wenn man davon ausgeht, dass jedes Unternehmen schon einmal Ziel irgendeines Angriffs war, wird deutlich, dass eine schleichende Ausweitung der Berechtigungen und ein Mangel an Identitätsmanagement dazu führen können, dass Benutzerrollen und Zugriffsrechte im gesamten Unternehmen offen zugänglich sind. Dies ermöglicht es Angreifern, Ihr Unternehmen zu unterwandern, sich ungestört in Ihren Netzwerken zu bewegen und Daten unbemerkt herauszuschleusen.

Jedes Unternehmen, das risikobehaftete Online-Transaktionen ausführt, muss alle seine Systeme mit Defense in Depth (DiD) ausstatten. Ihre IAM-Lösung sollte zudem Identity Governance mittels KI unterstützen und Folgendes ermöglichen:

- Identifizieren und Anwenden geeigneter Benutzerzugriffsebenen
- Automatisieren hochsicherer Zugriffsgenehmigungen
- Empfehlen einer Zertifizierung für Konten mit geringem Risiko
- Automatisches Entfernen von unnötigen Rollen

Ihre IAM-Lösung sollte Ihr Unternehmen außerdem befähigen:

- den Einfluss des Benutzerzugriff auf die Gefährdung des Unternehmens zu verstehen;
- durchgängige, kontextbezogene Informationen über alle Zugriffsrechte und Befugnisse bereitzustellen; und
- bei Bedarf unverzüglich Maßnahmen zu ergreifen.

Derartige Sicherheitslücken setzen Ihre Unternehmen der Gefahr aus, interne Audits zu verfehlen, Bußgelder aufgrund von Compliance-Verstößen zu zahlen, Ransomware-Angriffe zu erleiden und das Vertrauen der Kunden zu verlieren.

Fazit

Die folgenden wichtigen Trends und Entwicklungen bestimmen den Fortschritt in der Finanzdienstleistungsbranche:

1. Gesetzliche Bestimmungen und Datenschutz
2. Zunehmender Wettbewerb
3. Beschränkungen durch Altsysteme
4. Open Banking und Open Finance
5. Forderung der Verbraucher nach mehr Kontrolle und besserem Nutzererlebnis
6. Gesellschaftliche Veränderungen
7. Cyberrisiken

Basierend auf diesen Erkenntnissen können Sie eine erfolgreiche Strategie entwickeln, um von diesen Trends zu profitieren. Eine solche Strategie wird Ihnen helfen, sich in einem neuen Marktumfeld durchzusetzen und Veränderungen in Ihrem Kundenstamm zu antizipieren.

Der Trend zum digitalen und mobilen Verbraucher bedeutet, dass Ihr Unternehmen von einer produktorientierten Strategie zu einer kundenorientierten Strategie übergehen muss. Bieten Sie Ihren Kunden das nahtlose, sichere Benutzererlebnis, das sie sich wünschen, damit Ihr Unternehmen und die Finanzdienstleistungsbranche als Ganzes in diesem sich wandelnden Markt erfolgreich sein werden.

[5] Group IB, Get Ransomware Uncovered 2020/2021