AIRLOCK®
SECURE ACCESS HUB

WHITEPAPER

IT-SICHERHEITSLÖSUNGEN

Vom Spielverderber zum Beschleuniger der Digitalisierung

www.airlock.com

Inhaltsverzeichnis

1 • Executive Summary

Kohärente Gesamtlösungen – sowohl für Business als auch für IT.

Die Digitalisierung stellt Unternehmen vor neue Herausforderungen, die weit über die Informationstechnologie hinausgehen. Das betrifft vor allem einen Aspekt, der heute immer wichtiger wird: Die IT-Sicherheit.

Moderne IT-Security ist daher mehr als nur Security. Denn wer Anmeldeprozesse sagt, sagt auch Kundenerlebnisse. Und wer das Daten-Management optimiert, der optimiert oft auch ganze Prozesslandschaften. Die Konsequenz: Business- und IT-Logik müssen heute zusammengedacht werden und gerade bei der Sicherheit sind kohärente Gesamtlösungen gefragt.

Die sechs zentralen Anforderungen an integrierte Sicherheitslösungen:

1. **Überzeugende User Experience**
   Mit intelligenten Prozessen, die eine hohe Benutzerfreundlichkeit garantieren.
2. **Hohe Kosteneffizienz**
   Mit einer konsolidierten Sicherheitsarchitektur, welche die Kosten deutlich reduziert.
3. **Schnelles Time-To-Market:**
   Mit kohärenten Frameworks, die eine effiziente Applikationsentwicklung ermöglichen.
4. **Umfassendes Compliance-Management:**
   Mit einem zentralen Daten-Handling, das allen gängigen internationalen Standards entspricht.
5. **Optimale Applikations- und Datensicherheit**
   Mit vorgelagerten Sicherheitslösungen, die Applikationen zuverlässig schützen.
6. **Hohe Verfügbarkeit:**
   Mit einer hohen Ausfallsicherheit, die bei Angriffen eine lange Downtime vermeidet.

Resümee:

Für ein zukunftssicheres Access Management ist eine zentrale Sicherheitsdrehscheibe notwendig, die auf drei Komponenten basiert: auf einem IAM für das zentrale Access-Management, einer WAF für den Schutz vor externen Angriffen und einem API Gateway für den Schutz von Schnittstellen.

2 • «Disrupt or be disrupted» [1]:

Willkommen in der digitalen Transformation.

Der mechanische Webstuhl, das Fliessband, elektronische Steuerungssysteme und die Anfänge der IT – der technologische Wandel war schon immer der wichtigste Treiber der modernen Wirtschaft. Doch nun steht die nächste radikale Transformation an, die in ihrer Tiefe, Dynamik und Reichweite alle Unternehmen und jede Branche vor grosse Herausforderungen stellt: Die digitale Transformation.

Das Radikale an der digitalen Transformation: Sie ist strukturell. Und sie ist systemisch. Das sind natürlich grosse Begriffe und für manche läuten hier schon die Buzz-Words-Alarmglocken. Doch es genügt schon ein kurzer Blick in unseren Alltag, um zu erkennen, was sich in den letzten Jahren grundlegend geändert hat: Uber statt Taxi, Zalando statt Einkaufszentrum, Mobile-Banking statt Schalter und der YouTube Influencer anstatt Thomas Gottschalk und «Wetten, dass.. ?». Unser Leben ist heute schon in vielen Bereichen digital geworden – ein Trend, der sich morgen noch deutlich verstärken wird.

«Alles, was digitalisiert werden kann, wird digitalisiert.» [2]

Wie durchgreifend diese Transformation ist, zeigt eine aktuelle Studie von McKinsey. [3] So gehen nur acht Prozent der befragten Führungskräfte davon aus, dass ihr Geschäftsmodell die digitale Transformation übersteht. Eine radikale Feststellung, die den systemischen Charakter des digitalen Wandels klar unterstreicht. Denn wenn sich Geschäftsmodelle ändern, dann ändern sich nicht nur Technologien und operative Prozesse. Dann ändern sich auch das Konsumverhalten, die Wertschöpfungsketten, die Innovationsprozesse und – punkto Agilität, Dynamik und Mitarbeiterführung – die grundlegende Kultur von Unternehmen. Die wichtigsten Eckpunkte des Wandels lassen sich daher wie folgt skizzieren:

Wie Digitalisierung den Wettbewerb transformiert:

- **Markteintrittsbarrieren fallen** – und ganze Branchen werden von innovativen Geschäftsmodellen angegriffen, siehe Airbnb und Uber
- **Steigende Preis- und Angebots-Transparenz** – denn der nächste Anbieter ist nur einen Klick entfernt, siehe Amazon, Zalando und Google Shopping
- **Weltweite Verdrängungsmärkte** – und Entstehung von marktbeherrschenden Monopolen, siehe Google, Facebook und Netflix

[1] John Chambers, CEO Cisco Systems

[2] Carly Fiorina, Ex-CEO Hewlett-Packard

[3] Siehe: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/why-digital-strategies-fail

Wie Digitalisierung das Kundeverhalten transformiert:

- **Maximale Kundenorientierung** – Kunden erwarten eine hohe Servicequalität über den gesamten Kundendialog hinweg
- **Optimale User Experience** – Kunden fordern einfache und schnelle Prozesse und eine durchgängige Customer Journey
- **Individualisierung** – Kunden wünschen personalisierte Angebote, die auf individuelle Bedürfnisse zugeschnitten sind
- **7x24h** Self-Service Möglichkeiten

5 DOMÄNEN DER DIGITALEN TRANSFORMATION

Gross denken und konkret Handeln: Erfolgsfaktoren der Digitalisierung.

So interessant die abstrakten Erklärungen auch sind: Die eigentliche Herausforderung für Unternehmen ist die Umsetzung der Digitalisierung im konkreten Geschäftsalltag. Es geht also nicht mehr um das «Warum» der Digitalisierung, sondern vielmehr um das «Wie» und damit um die operationelle Umsetzung. Diese Umsetzungen sind natürlich so spezifisch, wie das betreffende Unternehmen selbst und eine «One-Size-Fits-All»-Lösung ist leider noch nicht erfunden worden. Dennoch gibt es drei grundlegende Erfolgsfaktoren, die für alle Unternehmen gültig sind.

- **Eigene Kernkompetenzen intern ausbauen** – und Routineaufgaben extern auslagern
- **Individualisierung wo nötig** – und Standardisierung wo möglich
- **Experimentieren und schnelles Prototyping** – und dadurch digitale Kompetenz aufbauen

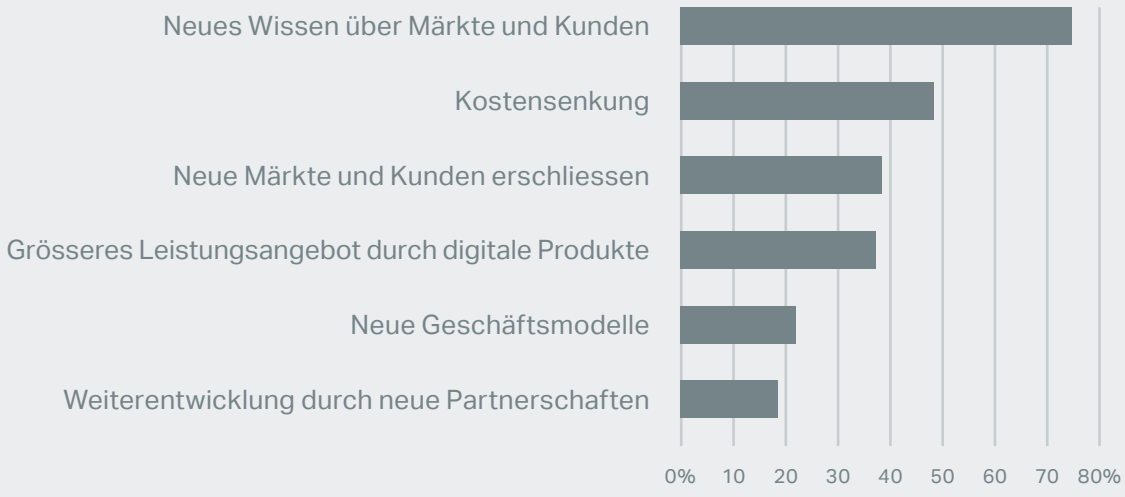
Wo Veränderungen sind, sind auch Chancen: Der Stand der Digitalisierung.

Die digitale Transformation ist nicht nur in aller Munde, sondern scheint auch in den Köpfen europäischer Führungskräfte angekommen zu sein. So zeigt eine Studie des deutschen Bundesministeriums für Wirtschaft und Energie[4], dass 68 Prozent der Unternehmen in der gewerblichen Wirtschaft neues Wissen durch die Digitalisierung generieren konnten, 47 Prozent der Unternehmen haben dank der Digitalisierung die Kosten gesenkt und 38 Prozent ermöglichte sie die Erschliessung neuer Märkte und Kundengruppen.

Diese Zahlen belegen, dass besonders die mittelständischen Unternehmen die Herausforderungen angenommen haben und Digitalisierung nicht nur im Silicon-Valley stattfindet, sondern auch Europa erreicht hat. Kein Wunder, denn auch das ist ein Spezifikum der vierten industriellen Revolution: Sie kann unabhängig von Raum und Zeit genutzt werden und erlaubt auch kleinen Playern, in kurzer Zeit ein beachtliches Wachstum zu erzielen. Ein weiteres Spezifikum: Sie eröffnet nicht nur einzelnen Unternehmen neue Chancen, sondern auch den europäischen Volkswirtschaften im Ganzen.

So meint McKinsey: «Eine konsequente Digitalisierung des deutschen Mittelstands erhöht das deutsche Wirtschaftswachstum bis 2025 um 0,3 Prozentpunkte pro Jahr. Dies entspricht einem zusätzlichen Wertschöpfungspotenzial von 126 Milliarden Euro.»[5] Und wir meinen: Diese Zahlen belegen eindrücklich die vorhandenen Potenziale. Potenziale, die es nun energisch und engagiert zu nutzen gilt.

Durch Digitalisierung erreichte Ziele.



[4] "Monitoring-Report, Kompakt Wirtschaft DIGITAL des BMWI 2017"

[5] Siehe https://www.mckinsey.com/de/news/presse/digitalisierung-im-mittelstand-erhoht-wachstum-in-deutschland-um-03-prozentpunkte-pro-jahr

Digitalisierung in der Finanzbranche

Ob Robo-Advisors, die Automatisierung aller Kundenprozesse oder PSD2 und innovative Fintech-Anbieter: Die Finanzbranche ist von der Digitalisierung nicht nur stark betroffen, sondern auch mit besonderen Anforderungen hinsichtlich Compliance und Regulatorik konfrontiert.

Digitalisierung in der Industrie

Globale Logistikketten, eine durchgängige Automatisierung und das Internet der Dinge: Was heute als Industrie 4.0 die Schlagzeilen bestimmt, wird morgen die Produktion prägen und zu Kostensenkungen und steigender Flexibilität führen. Die besondere Herausforderung dabei: Investitionsgüter sind auf Langfristigkeit ausgelegt – im Gegensatz zu den sich rasant beschleunigenden Innovationszyklen.

Digitalisierung im Versicherungssektor

Von User-Self-Services und der papierlosen Kommunikation, über neue Peer-to-Peer-Plattformen bis hin zu Wearables und digitalem Monitoring: Wie Banken arbeiten auch Versicherungen mit Zahlen und sind daher für Big-Data prädestiniert. Allerdings: Big-Data heisst auch Big-Datenschutz – und in diesem Spagat von Durchlässigkeit und Sicherheit liegt die spezifische Herausforderung für die Versicherungsbranche.

Digitalisierung in der öffentlichen Verwaltung

E-Government ist das, wovon viele Bürger träumen – beim Ausfüllen der Steuerunterlagen, beim digitalen Identitätsnachweis und einem 7x24h Kundenservice. Allerdings: So sehr offene Zugänge gewünscht werden, so stark werden auch Datenmissbrauch und staatliche Kontrolle gefürchtet, weshalb Identity-Management ein zentrales Thema für Behörden ist.

3 • IT-Sicherheit - der Spielverderber?

Intelligente IT-Sicherheit: Risiken managen und Chancen erfolgreich nutzen.

IT-Projekte bewegen sich in einem anspruchsvollen Spannungsfeld. Denn Agilität und schnelle Time-to-Market, welche vom Business Development gefordert werden, widersprechen scheinbar den Anforderungen der IT-Security, die auf Kontrolle und Absicherung setzt. Doch wer das Denken in getrennten Silos verlässt und eine unternehmerische Sicht auf IT-Herausforderungen einnimmt, erkennt: Digitalisierung ist erst dann erfolgreich, wenn Chancen und Risiken, Stärken und Schwächen systemisch zusammengedacht werden.

Plakativ formuliert: Digitalisierung kann in den Economies of Scales zu einem exponentiellen Wachstum führen. Es kann aber auch das genaue Gegenteil bewirken, da nicht nur die digitalen Chancen auf Skaleneffekten basieren, sondern auch die Risiken. Denn wenn Datensätze gestohlen, Betriebssysteme zerstört, die Anwälte im Haus und die Integrität und das Vertrauen weg sind – dann kann das Fortbestehen des eigenen Unternehmens substantiell gefährdet sein. Zugegeben: Das hier skizzierte Szenario ist ein Worst-Case-Szenario. Doch wie hoch die Eintrittswahrscheinlichkeit von substantiellen Sicherheitsproblemen ist, können die folgenden Zahlen belegen.

IT-Sicherheit in Zahlen [6]

- Laut Bitkom waren 2017 53% der Industrieunternehmen in Deutschland Opfer von Datendiebstahl, Spionage und Sabotage. Es entstand ein Schaden von rund 55 Milliarden Euro. Prominentestes Opfer eines Daten-Leaks war 2018 der Hotelkonzern Marriott, dem 500 Millionen Kundenidentitäten entwendet wurden.
- Laut VDMA sind 70 Prozent der Unternehmen von Produktpiraterie betroffen.
- Täglich werden rund 390.000 neue Schadprogramm-Varianten entdeckt.
- Gezielte Cyber-Spionage (Advanced Persistent Threats) wird im Schnitt erst nach 243 Tagen entdeckt.

Eine Burg bauen und wertvolle Assets wie Kundendaten, Patente und die Betriebssoftware nachhaltig schützen ist aber nur ein Aspekt einer zuverlässigen Sicherheitsarchitektur. Die zwei anderen Aspekte, die moderne, intelligente Sicherlösungen heute auszeichnen: Sie sind kundenzentriert. Und sie sind businessfokussiert.

[6] https://www.bitkom.org/Presse/Presseinformation/Spionage-Sabotage-Datendiebstahl-Deutscher-Wirtschaft-entsteht-jaehrlich-ein-Schaden-von-55-Milliarden-Euro.html

Von der technologischen Sicherheit zur Zukunftssicherheit.

Businessfokussiert heisst: Moderne IT-Security ist heute integraler Bestandteil in der Applikations-Entwicklung und bei IT-Projekten. Denn Fragen bezüglich Modularisierung, Identity-Management oder der zukünftigen Erweiterbarkeit von Anwendungen – z.B. dank der Integration von Drittanbietern – sind beides zugleich: Sicherheitsfragen und Businessfragen. Wer heute also von Sicherheit spricht, spricht daher vor allem von Investitions- und Zukunftssicherheit, die sich intelligent verschiedenen Anforderungen anpasst.

Vom Gatekeeper zur Concierge.

Dass Sicherheit intelligent geworden ist, zeigt sich im neuen Rollenverständnis der IT-Securitymanager: War früher der grimmige Gatekeeper das Vorbild für die digitalen Sicherheitswächter, so ist es heute die freundliche Concierge und der höfliche Welcome-Officer. Dieses veränderte Aufgabenverständnis mag auf den ersten Blick banal erscheinen, hat aber konkrete Konsequenzen wie das Beispiel der Online-Portale verdeutlicht.

User Experience ist Security Experience.

Wie Kunden das Onboarding und den Check-Out-Prozess erleben, ist in vielen Branchen geschäftskritisch für den wirtschaftlichen Erfolg. Denn ob die Konversion gelingt und der Kunde die gewünschte Aktion wirklich vornimmt – das liegt nicht nur an der Farbe der Buttons und der Attraktivität der Corporate-Bildwelt. Sondern in erster Linie am User-Erlebnis, das den Kunden im Authentisierungsprozess erwartet.

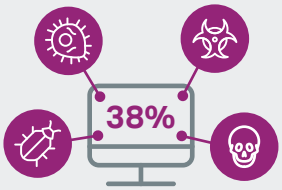
Konkret heisst das: Wenn sich Käufer beim digitalen Spontankauf einfach über Social Logins anmelden können – dann ist das Sicherheit, die zum User-Erlebnis wird. Und wenn Single Sign-On Versicherungskunden ermöglicht, verschiedene Anwendungen unkompliziert zu nutzen – dann ist das ein Identity Management, das von den Kunden als guter Service wahrgenommen wird. So bringen intelligente Sicherheitsprozesse zusammen, was zusammen gehört: Ein kohärentes Markenerlebnis, eine kosteneffiziente Abwicklung, eine bessere Konvertierungsrate und eine clevere Userführung.

Reine Verteidigung ist schlicht zu wenig.

Nun fragt sich natürlich, wie viele Ressourcen in die IT-Sicherheit investiert werden sollen – eine Frage, die wiederum auf den anvisierten Zielen basiert. Wir meinen: Dass IT nicht nur sicher sein soll, sondern sicher sein muss, ist nicht mehr der entscheidende Punkt. Der entscheidende Punkt ist vielmehr: Wie intelligent kann und muss Sicherheit heute sein, um im Internet up-to-date zu sein – bei der Hochverfügbarkeit, beim Compliance-Management, bei Cloud-Lösungen, bei der User-Führung und der Sicherheit von Collaboration-Umgebungen? Diese Frage muss jedes Unternehmen letztendlich für sich selbst beantworten, doch wer Digitalisierung ernst nimmt, wird schnell erkennen, dass reine Verteidigung heute schlicht zu wenig ist. Darum sollten auch die Innovationsfähigkeit, die Agilität, die Usability und die Multifunktionalität der gewünschten Lösung zentraler Entscheidungsfaktor sein.

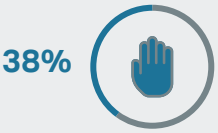
IT-Sicherheit:
Die wichtigsten Fakten auf einen Blick.

Die Key Findings im Überblick



Gefahr von außen
38 Prozent der Unternehmen sehen die externe Bedrohungslage als größte Herausforderung für ihre IT-Security, gefolgt von einem zu geringen(IT-)Security-Budget.

Partnerwahl
42 Prozent der Unternehmen achten bei der Wahl eines externen (IT-Security-)Dienstleisters auf Firmensitz und Rechenzentrum in Deutschland.



Nachholbedarf
Derzeit setzen nur 38 Prozent der befragten Firmen eine Softwarelösung für Identity- & Access-Management (IAM) ein. Vorreiter sind die großen Unternehmen.

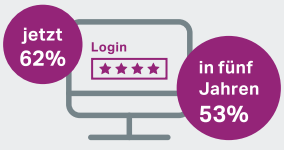
Compliance-Herausforderung Nummer 1
Die EU-Datenschutz-Grundverordnung trat am 25. Mai 2018 in Kraft. 40 Prozent der Firmen sehen sich davon (sehr) stark betroffen.

Mangelware
Nur rund ein Drittel der Unternehmen setzt Lösungen für Single Sign-On (SSO), Mobile Device Management (MDM) der Security Information und Event Management (SIEM) ein.

Externe IAM-Dienstleister sind gefragt
Das Gros der Unternehmen arbeitet beim Thema IAM mit einem oder mehreren externen Dienstleistern zusammen.

Klar definiert
69 Prozent der Unternehmen haben durch die genaue Definition der Rollen der Mitarbeiter bereits die Basis für effizientes IAM geschaffen.

Unsicherer Zugang
21 Prozent der Unternehmen sichern ihre Zugänge zum Netzwerk NICHT über eine Multi-Faktor-Authentifizierung mit Token (Hardware, Software, oder Push) ab.



Ohne Passwort läuft nichts
Das Passwort ist und bleibt mit Abstand die wichtigste Methode im Rahmen der Multi-Faktor-Authentifizierung.

Federführend
In mittleren und großen Unternehmen ist vor allem die IT-Abteilung für IAM verantwortlich; in kleinen Firmen bis zu 100 Mitarbeitern dominiert hingegen die Geschäftsführung.

Quelle: https://www.airlock.com/fileadmin/content/07_Airlock-PDFs/Studie_Identity-_und_Access_Management_2017.pdf

Integrierte IT-Sicherheitslösung

Integrierte Sicherheit: Kohärente Systeme statt singuläre Lösungen.

Der digitale Wandel wird immer schneller und komplexer. Und auf diese Komplexität müssen Unternehmen auch punkto Sicherheit adäquat reagieren. Dabei geht der Trend klar in Richtung vorgelagerter Security Layer, die einen eindeutigen Vorteil bieten: die Konvergenz von Application Security, API Protection und Access Management.

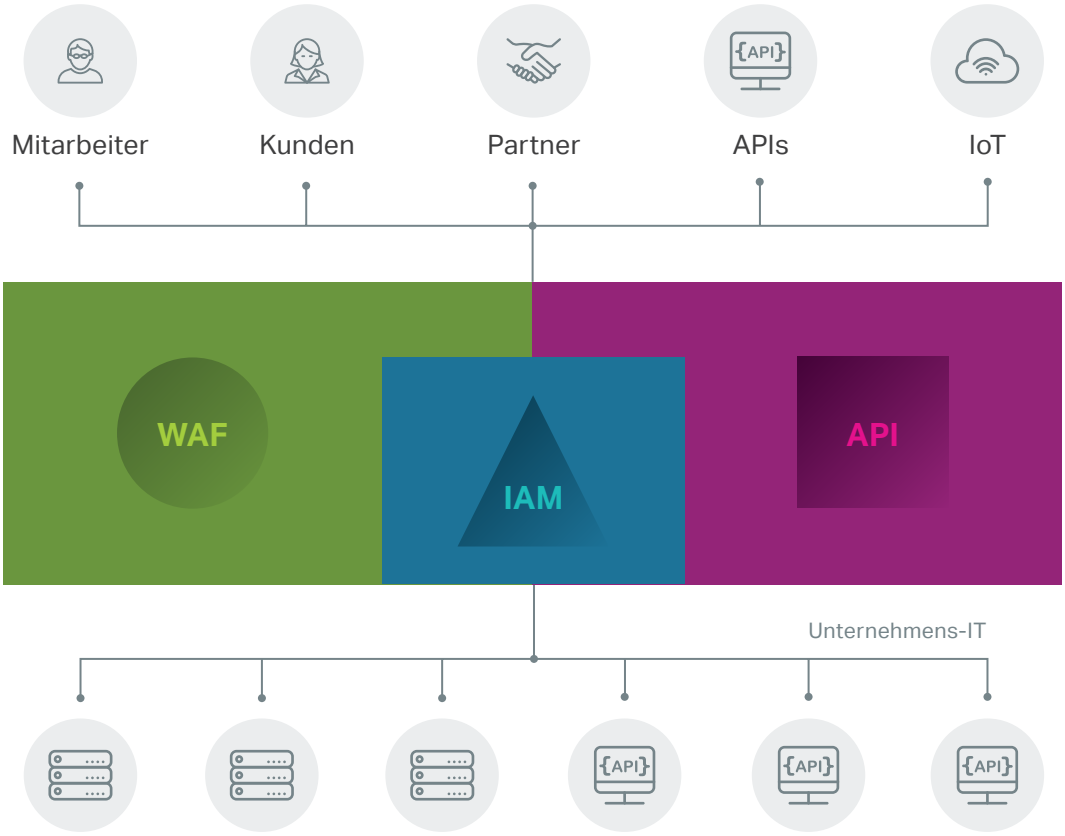
In Zeiten der Digitalisierung werden mehr und mehr Applikationen, APIs, Daten und Identitäten über die Grenzen der Unternehmens-IT hinaus exponiert. Waren es früher nur Webseiten, die mit der internen IT kommunizierten, so sind es heute Web-Applikationen, mobile Applikationen, eigene oder fremde APIs mit externen Identitäten von Kunden, Partnern oder Dingen (IoT), die in eine konvergente Sicherheitslösung integriert werden müssen. Die logische Folge gemäss Gartner: «Bis 2021 werden 65 Prozent der neuen Anwendungen als System aus mehrkanaligen Anwendungen und mehrschichtigen Backend-Diensten aufgebaut sein, die über APIs kommunizieren.»[7]

Die Herausforderung lautet also: WAFs müssen APIs schützen, API Gateways müssen Web Security lernen, APIs brauchen Access Control und die Benutzer lassen sich nur noch schlecht mit herkömmlichen Enterprise IAM-Systemen verwalten. Doch wenn «Spot Solutions», die viele Lücken an den Übergängen offen lassen, nicht mehr die Lösung sind, was ist es dann?

Die einfache Antwort: Es braucht integrierte Systeme mit intelligenten Schnittstellen, bei denen einzelne Komponenten kohärent aufeinander abgestimmt und vormals lose Enden zuverlässig miteinander verknüpft sind. Und die technische Antwort: Für ein sicheres Access Management braucht es eine konvergente Lösung, bestehend aus einer WAF, einem API Gateway und einem Customer IAM System. Dieses kurze Statement soll im Folgenden etwas detaillierter ausgeführt werden – mit einem kurzen Schlaglicht auf vier technische und einen unternehmerischen Aspekt.

[7] Critical Capabilities for Full Life Cycle API Management, Gartner, 2018 (Übersetzung RB)

Mit konvergierenden Technologien ein kohärentes Sicherheits-Ökosystem aufbauen.



Web-Applikationen und APIs

Herausforderung 1: Web Application Firewalls müssen dazu lernen

Während vor zehn Jahren Kunden noch von einer Web Application Firewall (WAF) überzeugt werden mussten, ist heute der WAF-Markt milliardenschwer und hochkompetitiv. Doch steigende Anforderungen an die User Experience sowie eine zunehmende Vernetzung von Services lassen herkömmliche Webapplikationen aussterben. Moderne Applikationen sind daher Rich-Clients, die im Browser laufen und meist hauseigene Services sowie Angebote von Drittanbietern integrieren. Diese Services – oder APIs – werden meist als RESTful-Webservices entwickelt und benutzen andere Datenformate als herkömmliche Webapplikationen. Die Konsequenz: Für den Schutz von APIs braucht es neue Technologien, da sich das Interaktionsparadigma zwischen Client und «Server» grundlegend geändert hat.

Herausforderung 2:
API Security heisst auch Web Security

Traditionelle XML Gateways sind nur bedingt geeignet, um den neuen Typus von Web-Services abzusichern. Diese sind meist auf SOAP-Webservices ausgelegt, die vor allem unter ihresgleichen kommunizieren, Enterprise Service Busse benötigen und im Korsett hochkomplexer Standards gefangen sind. Dies passt schlecht zur neuen REST-Welt, die durch Agilität geprägt ist. Zudem werden moderne APIs von ganz unterschiedlichen Clients genutzt – von herkömmlichen Webapplikationen, Browser-basierten Rich-Clients, Smartphone Apps, «Things» und anderen Softwaresystemen. Das hat zur Folge, dass interne APIs plötzlich im Internet exponiert sind. Damit stellen sich an den API-Gateway Anforderungen, die ähnlich denen einer WAF sind, und Web-Security-Themen wie die OWASP Top 10 werden ebenfalls relevant.

Herausforderung 3:
APIs brauchen Access Management

Content Filtering ist für den Schutz von APIs sehr wichtig. Der wichtigste Grund für den Einsatz von API Gateways ist allerdings Access Control. Der Zugriff auf APIs muss mittels Standards wie OAuth 2.0, OpenID Connect und SAML abgesichert werden können. Dazu gehört nicht nur die technische Autorisierung von «Clients», sondern auch die Benutzer-Authentifizierung. Dies erfordert wiederum eine Integration von Web Single Sign-On und Identity und Access Management (IAM).

Herausforderung 4:
IAM und die Kunden

Die angesprochenen Identitäten sind sehr heterogen und umfassen eine Vielzahl «externer» Identitäten, wie beispielsweise Kunden oder Partner. Diese Identitäten müssen gemanagt werden und unterliegen strengen Vorschriften wie z.B. der europaweiten Zahlungs-dienstrichtlinie PSD2 und der DSGVO. Diese Richtlinien verlangen von Banken, APIs für Kontoeinsicht und Zahlungen zur Verfügung zu stellen, die von hunderten sogenannter Payment Provider genutzt werden dürfen. Der Zugriff muss dabei stark authentisiert erfolgen. Die Lösung für diese komplexe Herausforderung: Sogenannte Customer IAM (cIAM), die im Unterschied zu Enterprise-IAM-Systemen besser auf die Verwaltung von externen Benutzern ausgelegt sind, da sie sich einfach skalieren lassen und eine nahtlose User Experience durch integrierte UIs für Onboarding und Self-Services garantieren.

Herausforderung 5: Verkrustete Organisationsstrukturen aufbrechen

Eine weitere zentrale Herausforderung ist allerdings weniger technischer, sondern vielmehr organisatorischer Natur – nämlich das Silo-Denken in vielen Unternehmen. Denn wenn diverse Technologien zu einem grossen Ganzen konvergieren: Wer ist dann der Ansprechpartner und Entscheider? Ist es der CISO, weil Security-Themen die IT-Infrastruktur und den Netzwerkbetrieb betreffen? Oder ist es das Business, weil integrierte Lösungen einen tieferen TCO und ein schnelles Time-to-Market sicherstellen? Oder muss das Marketing im Lead sein, denn eine intuitive Userführung und geringere Absprungraten sind schliesslich die Domäne von Kommunikation und Marketing?

Wie auch immer die Antwort lautet – was Aristoteles schon zu Zeiten von Papyrus und Tonscherben formulierte, gilt auch im Zeitalter von Bits und Bytes: Die Summe ist mehr als ihre Teile! Dieses holistische Denken ist heute auch beim Thema IT-Security gefragt – und nicht nur dort. Denn die digitale Transformation ist nicht nur ein technologischer Wandel, sondern verändert auch Business-Prozesse, Organisationsstrukturen und das Verhalten von Kunden, Partnern und Mitarbeitern. Und weil sich so viel ändert, muss sich auch das Denken ändern: in Unternehmen, bei der IT und vor allem beim Thema Sicherheit.

4 • IT Sicherheit - der Beschleuniger

Integrierte IT-Security: Die wichtigsten Vorteile auf einen Blick.

Zwei Fliegen mit einer Klappe schlagen: Das ist nun auch beim Thema IT-Security möglich. Denn ein vorgelagerter Security Layer garantiert nicht nur eine optimale IT-Sicherheit, sondern ermöglicht auch die Agilität, Effizienz und Benutzerfreundlichkeit, auf die es heute ankommt.

Vorteil 1: Optimale Applikations- und Datensicherheit

2018 haben sich die Angriffe auf Applikationsebene (OWASP Top 10) mehr als verdoppelt. Darum ist ein umfassender Schutz von Webapplikationen und APIs eine businesskritische Aufgabe, um den Ausfall von Services, den Datenverlust und einen Reputationsschaden bei Kunden und Partnern zu verhindern. Zudem drohen seit Einführung der DSGVO hohe Strafen von bis zu 4% des Jahresumsatzes, weshalb Datenschutz auch Investitionsschutz ist.

Die Vorteile im Detail:

- Eine vorgelagerte Sicherheitslösung mit WAF, API Gateway und Customer IAM (cIAM)-System schützt Applikationen, APIs und Daten zuverlässig vor Identitätsdiebstahl, den häufigsten Angriffen auf Web-Applikationen und den OWASP Top 10 wie zum Beispiel SQL Injections oder Cross-Site-Scripting (XSS).

- WAF und API Gateway analysieren dabei den gesamten Datenfluss der geschützten Applikationen und APIs. Angriffe werden sofort blockiert, bevor sie beim Ziel Schaden anrichten können.

- cIAM schützt mit starker Authentisierung und einem zentralen Access Management vor unberechtigten Zugriffen auf Applikationen und APIs. Zudem stellen sichere Prozesse beim Onboarding und bei den User Self Services sicher, dass heikle Informationen nicht in falsche Hände gelangen.

Laut einer Studie von Whitehat Security bleiben kritische Sicherheitslücken durchschnittlich 129 Tage offen– auch, weil internen IT-Sicherheitsteams oftmals die nötigen Ressourcen fehlen. Daher bietet der Secure Access Hub mit seinen integrierten und automatisierten Interaktionen die richtige Antwort zur Verbesserung dieser unternehmenskritischen Situation.

Vorteil 2: User Experience

Bei integrierten Security-Lösungen sind Sicherheit und Benutzerfreundlichkeit optimal aufeinander abgestimmt. So basieren sämtliche User Interfaces zwar auf dem Prinzip «Security First» – dank umfangreicher Benutzerkontakte und vielfachen Usability-Iterationen sind die Nutzerschnittstellen jedoch so gestaltet, dass sie eine hervorragende User Experience garantieren.

Die Vorteile im Detail:

- Einfache Registrierung: Die Registrierung sollte möglichst unkompliziert sein. Darum bieten intelligente Sicherheitslösungen Wizards an, die leicht verständlich durch die Selbstregistrierung führen, wobei der User verschiedene Self-Services nutzen kann. Um die Eintrittsbarrieren niedrig zu halten, können bestehende Identitäten, z.B. via Social Logins, eingebunden werden. Mit dem integrierten Consent Management entscheidet der Kunde zudem, welche Applikationen Zugriff auf seine Daten erhalten.

- Benutzerfreundliche Nutzung: Auch nach der Registrierung soll die Sicherheitssoftware mit einer hohen Convenience überzeugen. So können Kunden dank Single-Sign On verschiedene Dienste nutzen, ohne sich neu authentisieren zu müssen. Als Authentisierungsmittel werden verschiedene Lösungen angeboten, wobei unterschiedliche Kundengruppen auch unterschiedliche Authentisierungsmittel einsetzen können.
  Mit der risikobasierten oder adaptiven Authentisierung wird immer nur so viel Authentifizierung durchgeführt, wie gerade notwendig ist. Beispielsweise kann bei einem Log-in vom internen Arbeitsplatz auf einen zweiten Faktor verzichtet werden.

Vorteil 3: Hohe Kosteneffizienz

Prozesse vereinfachen und Kosten reduzieren – was die Digitalisierung antreibt, ist auch einer der zentralen Benefits eines vorgelagerten Security Hubs. So basieren integrierte Sicherheitslösungen auf einer kohärenten Systemarchitektur und garantierten einen attraktiven TCO.

Die Vorteile im Detail:

- Standardisierung: Ein Secure Access Hub beruht auf standardisierten Security Services, die auch von neuen Applikationen genutzt werden können. Diese Entkopplung von Authentisierungs- und Businesslogik sorgt für ein Maximum an Flexibilität und eine schnelle Time-to-Market.

- Konsolidierung: Eine konsolidierte Sicherheitsarchitektur stellt sicher, dass mit einer einzigen Softwarelösung unterschiedliche Sicherheitsmassnahmen gemanagt werden. Aktionen wie Authentifizierung, Access Management und der Schutz vor Angriffen können so an einer einzigen Stelle überwacht werden. Dadurch lassen sich Infrastrukturen vereinfachen und die Kosten deutlich reduzieren.

- Compliance: Mit einer integrierten Lösung lassen sich Compliance-Anforderungen effektiv umzusetzen, so dass nicht jede Applikation einzeln angepasst werden muss. Konkret heisst das: Zustimmungserklärungen und Consents werden zentral verwaltet und branchenspezifische Regularien, z.B. PSD2 für die Finanzindustrie, lassen sich mühelos umsetzen, da entsprechende Audits effizient durchgeführt werden können.

- Kundenservice: Intelligente Sicherheitslösungen senken nicht nur die IT-Kosten, sondern auch den Aufwand im Kundendienst. So können mit der Verlagerung vom Inbound-Callcenter zum digitalen User Self-Service grosse Einsparungen erzielt werden, wobei die Kunden zudem von einen deutlichen Komfortgewinn profitieren.

> ***Benutzer vergessen 1,8 Mal pro Jahr ihr Passwort und ein Support-Anruf kostet im Schnitt 50 Euro.***
>
> Gartner

Vorteil 4: Time-to-Market

Unternehmen müssen heute in immer kürzeren Zyklen innovative Services lancieren. Doch so wichtig Schnelligkeit auch ist: Neue Softwarelösungen müssen auch sicher sein. Dieses Dilemma zwischen Sicherheit und Schnelligkeit lösen integrierte Security Services, indem sie auf erprobten sowie standardisierten Lösungen beruhen und das Sicherheitsthema schon in den agilen DevOps-Prozess integrieren.

Die Vorteile im Detail:

- Ein Secure Access Hub reduziert den Time-to-Market-Prozess, da Sicherheitsfunktionen auf einer durchgängigen All-in-One-Lösung basieren - z.B. für Authentisierung, Registrierung, die Anbindung von Directories, das Login sowie Single Sign-on, User Self-Services und Social-Login.

- Ein Secure Access Hub schützt Software-Entwicklungen vor den grössten Bedrohungen für Webanwendungen (OWASP Top 10) und Applikationsentwickler können Businessfunktionen in kürzester Zeit umsetzen. Zudem werden Compliance-Aktivitäten zentral verwaltet und regelmässig an neue Anforderungen angepasst.

- Intelligente Sicherheitslösungen ermöglichen eine agile und flexible Softwareentwicklung. So wird dank der DevSecOps-Methode (Development, Security, Operations) der Security-Prozess schon in der Applikationsentwicklung integriert, um eine kohärente Framework-Strategie zu etablieren und eine einheitliche Sicherheitsinfrastruktur aufzubauen.

- Ganzheitliche Sicherheitslösungen setzten meistens auf APIs, Automatisierbarkeit und innovative Technologien wie z.B. Let's Encrypt. Dadurch werden wiederkehrende Aufgaben überflüssig und menschliche Fehler minimiert. Mit den Staging-Funktionen lassen sich zudem die Konfigurationsbasis automatisch aktualisieren und neue Applikationen entsprechend den höchsten Sicherheitsanforderungen einführen.

> ***In the new world it is not the big fish which eats the small fish, it`s the fast fish which eats the slow fish.***
>
> Klaus Schwab

Vorteil 5: Compliance

Ob Finanzdienstleister, Krankenhäuser, Versandhäuser oder die Tourismusbranche – unterschiedliche Branchen unterliegen unterschiedlichen Regularien. Darum erfüllen integrierte Sicherheitslösungen standardmässig eine Vielzahl von Compliance-Richtlinien.

Die Vorteile im Detail:

- Datenschutz-Grundverordnung (DSGVO / GDPR): Gemäss DSGVO muss der Kunde der Datennutzung zweckgebunden zustimmen und das Unternehmen den Zustimmungsprozess nachvollziehbar gestalten. Das Management dieser Benutzer-Consents erfolgt bei einer integrierten Security Software zentral und vorgelagert, ohne dass Applikationen angepasst werden müssen. Zudem können Benutzer mittels Self-Services jederzeit die erteilten Consents einsehen und der Zugriff auf eine Applikation wird nur erteilt, wenn ein Benutzer allen notwendigen Consents zugestimmt hat.

- Schutz kritischer Infrastrukturen (ITSiG): Zeitgemässe Sicherlösungen unterstützen sowohl die revisionssichere Speicherung als auch die Umsetzung hoher Sicherheitsanforderungen bei der Datenspeicherung. Da gemäss ITSiG staatliche Stellen bei Cyberattacken unverzüglich informiert werden müssen, wird darüber hinaus ein zentrales und interaktives Real-time-Reporting garantiert.

- Payment Service Directive (PSD2): PSD2 betrifft Banken und fordert die Bereitstellung von Schnittstellen für externe Finanzdienstleister. Zugriffe auf diese Schnittstellen müssen stark authentisiert erfolgen und Unternehmen haben dem «Stand der Technik» in puncto IT-Sicherheit zu entsprechen. Hier bieten intelligente Sicherheitslösungen mit umfangreichen Access-Management-Funktionalitäten, den unterstützten Federation-Standards und integriertem API-Schutz beste Voraussetzungen für einfache und zuverlässige PSD2 Compliances.

- Payment Card Industry Data Security Standard (PCI DSS): Unternehmen, die Kreditkarten-Transaktionen abwickeln, müssen sich zwingend an die Datenschutzrichtlinien der Kreditkartenindustrie halten. Grosse E-Commerce-Firmen sollten die Sicherheit ihrer Netzwerke zudem alle drei Monate extern überprüfen lassen. Mit einem Secure Access Hub lassen sich diese Massnahmen effizient realisieren, da der Schutz stets auf höchstem Niveau bleibt und Applikationen nicht dauernd aufgrund neuer Bedrohungen angepasst werden müssen.

- Compliance-Standards von spezifischen Zielmärkten: Ein Secure Access Hub berücksichtig zahlreiche weitere Normen, die in bestimmten Regionen von Bedeutung sind – zum Beispiel die deutsche Richtlinie der Bundesaufsicht für Finanzdienstleistungen (BaFin) oder die Datenschutzrichtlinien der Monetary Authority of Singapore (MAS). Durch den zentralisierten Ansatz des Secure Access Hubs sind Umsetzungen von Compliance-Anforderungen effizient möglich, da sie kontrolliert an einem Ort erfolgen, ohne die gesamte Applikationslandschaft zu tangieren.

Vorteil 6: Höhe Verfügbarkeit

Zahlungsanbindungen, Kundenkonten, Lagerbewirtschaftung: wenn digitale Services ausfallen, fallen oft zentrale Unternehmensaktivitäten aus. Darum ist Hochverfügbarkeit und eine Ausfallsicherheit von mindestens 99.99% ein wichtiges Sicherheits-Feature, um selbst bei schweren Angriffen eine lange Downtime zu vermeiden.

Die Vorteile im Detail:

- Intelligente Sicherheitslösungen stellen ein aktives Loadbalancing der geschützten Services sicher. Falls ein System nicht zur Verfügung steht, wird daher ein Failover auf ein weiteres verfügbares System erstellt. So bleibt die User Experience erhalten, selbst wenn ein System ausfällt bzw. Maintenance-Arbeiten ausgeführt werden.

- Angriffe wie Denial-of-Service-Attacken (DoS), Scanning, Brute forcing oder die Ausnutzung von Sicherheitslücken können die Verfügbarkeit einschränken oder sogar zum Totalausfall führen. Der Secure Access Hub hilft mit seinen integrierten mehrstufigen und individuell konfigurierbaren Möglichkeiten, gegen diese Arten von Angriffen, um vor unautorisierten Zugriffen zu schützen.

- Wer genauer schaut, sieht mehr. Darum beobachten Security-Spezialisten des Herstellers aufmersam die Entwicklungen in der Hackerszene und stellen schnell Regelwerke zur Verfügungen, damit Applikationen beim nächsten «Heartbleed» nicht vom Netz genommen werden müssen.

5 • Case-Study Raiffeisen

Best-Practice: Warum Raiffeisen auf eine zentrale Sicherheitsstruktur setzt.

Sie ist die drittgrösste Bankengruppe der Schweiz und konnte in den letzten Jahren stolze Wachstumszahlen aufweisen: Die Raiffeisen Gruppe aus Sankt Gallen. Eine der wichtigsten Gründe für diesen Erfolg ist ihre Kundennähe – nicht nur offline, sondern auch online

Raiffeisen gilt als nahbar, vertrauenswürdig und sympathisch. Diese Werte scheinen zu überzeugen und die Bank konnte bis heute 3.8 Millionen Kunden für sich gewinnen. Da die Raiffeisen-Werte ein zentraler Erfolgsfaktor sind, sollten sie natürlich auch im E-Banking zum Ausdruck kommen – doch hier stiess das bisherige IT-System leider an seine Grenzen.

User mit Usability überzeugen

Im digitalen Zeitalter heisst Kundenfreundlichkeit Benutzerfreundlichkeit – mit einer intuitiven User-Führung und einfachen, schlanken Prozessen. Allerdings war die bisherige Softwarelösung diesen Anforderungen nicht gewachsen und jede Implementierung neuer Webapplikationen erforderte eine extra Login-Seite. Die Folge: Die Kunden mussten viele Zugangsdaten mit verschiedenen Benutzernamen und komplexen Passwörtern kreieren und sich diese merken.

Zentralisierte Sicherheit und das Rad-Modell

Raiffeisen setzte sich daher zum Ziel, eine zentrale Sicherheitsinfrastruktur zu realisieren: mit einer Authentisierungsplattform, die den Kunden nach einmaliger Anmeldung den Zugang zu allen Daten, Anwendungen und Internetdiensten ermöglicht. Die Logik der Infrastruktur wurde dabei mit einem einfachen Modell visualisiert, das Stevan Dronjak, Team Lead Web Application Security Raiffeisen Schweiz, wie folgt darstellt: «Für unsere Sicherheitsarchitektur wählten wir das Bild des Rad-Modells. So ist jede Applikation wie eine Fahrradspeiche in deren Mitte die sichere Radnabe liegt. Die Radnabe ist also die zentrale Authentifizierungsplattform, über welche jede Authentisierung, der Applikationsschutz und die Fraud-Detection läuft. Der Vorteil: Dank der Sicherheitsfunktionalität in der Mitte können wir nun weitere Anwendungen hinzufügen, ohne uns um alle Sicherheitsaspekte kümmern zu müssen.»

Ganzheitlicher Schutz dank einem Secure Access Hub

Das Bild des Rad-Modells galt es nun in konkrete Security-Technik zu transformieren. Die Lösung war ein vorgelagerter Secure Access Hub, der sich aus einem IAM-System und einer Web Application Firewall (WAF) zusammensetzt.

Das IAM-System liefert dabei die nötigen Technologien, um die Zugriffsberechtigungen der Nutzer zu verwalten. Ein solches System ist im Gegensatz zu einer klassischen IAM-Lösung nicht nach innen, sondern nach aussen gerichtet und auf eine grössere Anzahl digitaler Identitäten ausgelegt. Ein weiteres wichtiges Element ist zudem die Web Application Firewall (WAF), denn klassische Netzwerk-Firewalls schützen nicht gegen Angriffe auf der Applikationsebene. Um hier möglichen Angreifern den Wind aus den Segeln zu nehmen und Anwendungen vor den bekannten OWASP Top 10 Bedrohungen zu schützen, entschied man sich für die vorgelagerte Kombination aus WAF und einer Authentisierungsplattform, dem sogenannte Secure Access Hub.

Einfacher Zugriff auf alle Services

Ein Anbieter einer solchen zentralen und vorgelagerten Authentifizierungsplattform ist Airlock. «Wir hatten die WAF von Airlock schon im Einsatz und kannten Ergon Informatik AG schon von früheren Projekten», berichtet Dronjak. «So hatten wir mit den Airlock-Experten schon gute Erfahrungen gemacht und schätzen ihr Know-how hinsichtlich Qualitätsstandard und Geschwindigkeit. Nach einer Pitchphase haben wir uns sehr schnell für den Airlock Secure Access Hub entschieden.»

Die Anforderungen für die neue zentrale Authentisierungsplattform waren dabei klar formuliert: Höchste Sicherheit. Und eine überzeugende Nutzerfreundlichkeit. So sollten Kunden via Single Sign-on einfachen Zugriff auf alle Services erhalten und somit unkompliziert zwischen den verschiedenen digitalen Angeboten von Raiffeisen hin und her wechseln können, ohne sich jeweils neu authentisieren müssen.

«Nachdem die Konfigurationseinstellungen fertiggestellt waren und erste Tests erfolgreich liefen, konnten wir den Airlock Secure Access Haub sehr schnell live schalten. Wenn jetzt ein digitales Projekt ansteht und ein neuer Service in die Plattform integriert werden muss – d.h. eine neue Speiche dazu gehängt werden soll – sprechen wir nur noch von einer Implementationszeit von ca. zwei Wochen,» berichtet Dronjak begeistert.

Neben Single Sign-on war auch die Realisierung der Authentisierungshierarchie besonders wichtig. Je nach Anforderung sind nun verschiedene Authentisierungsstärken möglich. Hat sich ein Nutzer in einer Session mit einem starken Authentisierungsmechanismus erfolgreich angemeldet, ist für alle Anwendungen, die eine gleich starke oder schwächere Authentisierung verlangen, kein Login mehr nötig.
Auch in puncto Verfügbarkeit und Skalierbarkeit zeigen sich erste Erfolge: So wurde die Plattform kontinuierlich ausgebaut und neue Applikationen implementiert, während die Nutzerzahlen und –anfragen stetig gestiegen sind.

Die Lösung von Airlock ermöglicht Raiffeisen ein durchdachtes Rechtemanagement: Administratoren können die Berechtigungen für den Zugriff der Nutzer transparent verwalten, was eine optimale Balance zwischen Compliance, Nutzereinwilligungen, IT-Sicherheit und einer ansprechenden Customer Experience ermöglicht. Die User werden durch das IAM-System sicher authentifiziert, bevor sie mit den Finanzapplikationen interagieren.

> ***Mit der hohen Benutzerfreundlichkeit und neuen, zentralen Sicherheitsinfrastruktur haben wir für unsere Kunden eine eindeutige Raiffeisen-Identität geschaffen. Kundennähe und Vertrauenswürdigkeit haben bei unserer E-Banking-Lösung oberste Priorität. Mit dem Airlock Secure Access Hub können wir diese hohen Anforderungen erfüllen.***

Stevan Dronjak,
Team Lead Web Application Security,
Raiffeisen Schweiz

Digitale Raffeisen-Identität

Die Anwendung ist dabei für Nutzer sehr intuitiv. Gerade bei Online-Angeboten für Finanztransaktionen, die höchste Sicherheitsstandards erfüllen müssen, ist dies nicht selbstverständlich, für den Erfolg aber massgeblich: Ist das Vertrauen des Kunden in das Unternehmen vorhanden und die Handhabung der App unkompliziert und schnell, wirkt sich das positiv auf die Nutzung und damit Attraktivität der Applikation aus.

«Durch die hohe Benutzerfreundlichkeit mit der neuen zentralen Sicherheitsinfrastruktur haben wir für unsere Kunden eine eindeutige digitale Raiffeisen-Identität geschaffen. Kundennähe und Vertrauenswürdigkeit haben bei unserer E-Banking-Lösung oberste Priorität. Mit dem Airlock Secure Access Hub konnten wir diese hohen Anforderungen erfüllen», fasst Dronjak den Erfolg zusammen.