heise Business Services

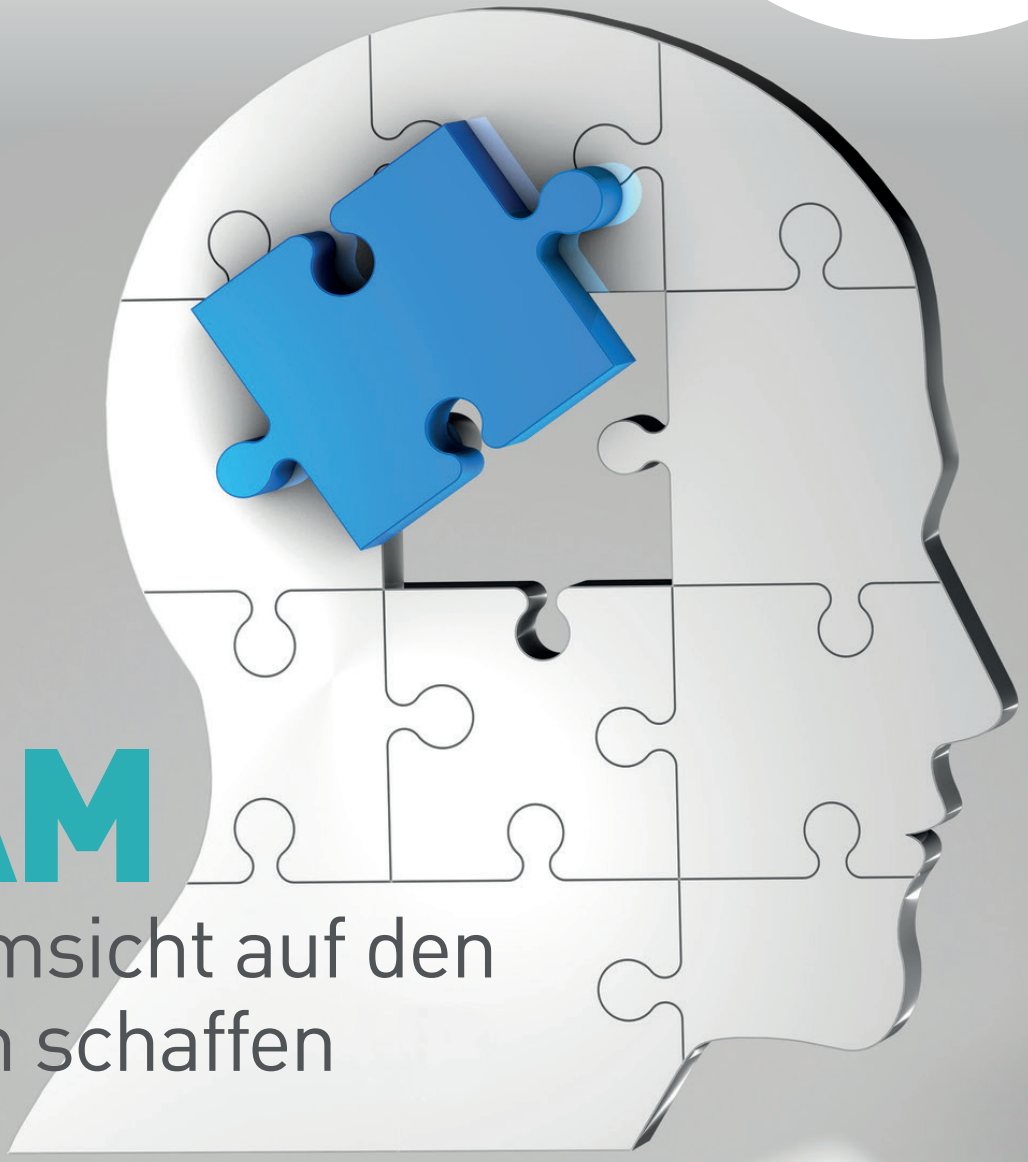
Ein eBook von

Mit Exklusiv-Inhalten von

AIRLOCK by ergon

PROMON

VASCO THE AUTHENTICATION COMPANY



CIAM

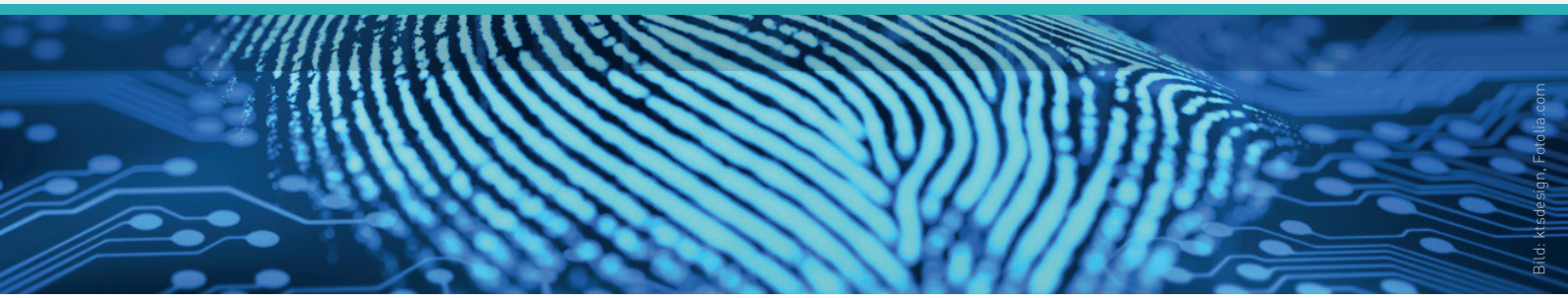
Rundumsicht auf den Kunden schaffen

Die Identität des Konsumenten: Consumer IAM im Blickfeld

Compliance – Herausforderung oder Chance?

Sicherheitsanforderungen für B2C-Plattformen

Titelbild: vege, Fotolia.com



Editorial

Katharina Friedmann,
Manager Solutions & Services, Heise Medien

Im Zuge des digitalen Wandels verändern sich auch die klassischen Geschäftsmodelle. Sie entwickeln sich weg vom Absatz physischer Produkte hin zum Handel mit digitalen Mehrwertdiensten. Voraussetzung dafür, dass Kunden Zugang zu diesen Services erhalten, ist deren Identitäten zu kennen. Das traditionelle, nach innen gerichtete Identity and Access Management (IAM) mit Fokus auf der internen Zugriffsregelung greift hier zu kurz. Deutlich weiter gefasst ist das aufkommende Consumer oder Customer IAM (CIAM): Neben der Verwaltung von Kunden- und Konsumentenidentitäten und deren Authentifizierung geht es hier darum, die gewonnenen Informationen auch dafür zu nutzen, um den Kunden optimal zu bedienen beziehungsweise automatisiert gezieltes Marketing zu betreiben. Ziel des CIAM ist, durch die Integration der wichtigsten Aspekte und häufig auf unterschiedliche Lösungen im Unternehmen verteilten Funktionen des Managements von Kundenidentitäten eine Rundumsicht auf den Kunden oder Konsumenten zu ermöglichen.

In diesem eBook erfahren Sie, ...
... wie das Identity und Access Management für Konsumenten mit der Digitalen Transformation zusammenhängt,
... welche Aspekte das CIAM umfasst - und welche (technischen) Voraussetzungen dafür gegeben sein müssen,
... was der Umgang mit Konsumenten- und Kundendaten für Unternehmen an Pflichten durch Compliance-Vorgaben mit sich bringt, und
... warum und in welchen Bereichen CIAM besondere Anforderungen an die Sicherheit stellt.

Ich wünsche Ihnen eine interessante Lektüre!

Katharina Friedmann
Manager Solutions & Services, Heise Medien

Heise Medien GmbH & Co.KG
Abt. Heise Business Services
Hans-Pinsel-Straße 10a
85540 Haar bei München

Registergericht:
Amtsgericht Hannover HRA 26709

Persönlich haftende Gesellschafterin:
Heise Medien Geschäftsführung GmbH

Registergericht:
Amtsgericht Hannover, HRB 60405

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

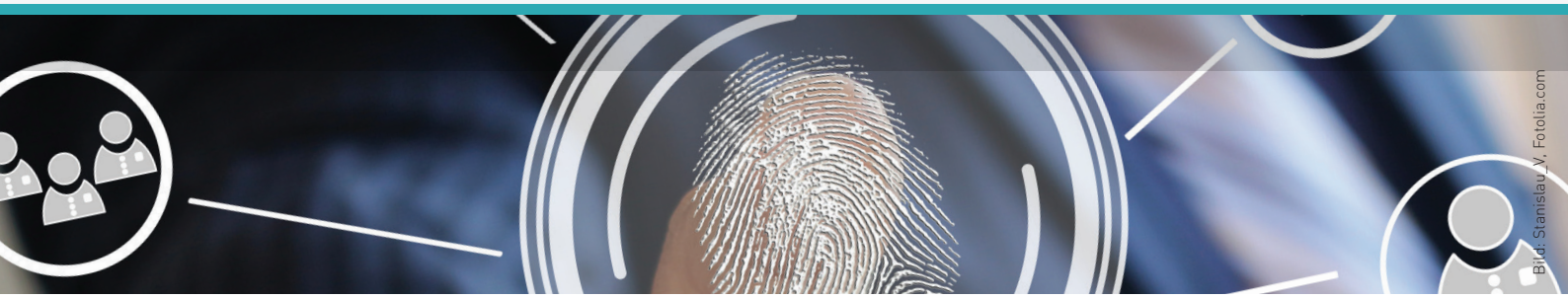
Verantwortlich für den Inhalt:
Heise Business Services
Frank Klinkenberg, fkl@heise.de

Haben Sie Fragen zu diesem eBook oder haben Sie Interesse an einer eigenen Produktion, dann schicken Sie bitte eine E-Mail mit dem Betreff **„HBS-eBook“** an hbs@heise.de

Inhalt

ÜBER DEN AUTOR

Martin Kuppinger ist Gründer und Principal Analyst von KuppingerCole



Die Identität des Konsumenten: Consumer IAM im Blickfeld

Die Welt der IT verändert sich. Längst geht es nicht mehr nur darum, Mitarbeitern Zugriff auf interne Systeme zu geben. Dienste für die Konsumenten und Kunden stehen im Blickfeld. Unternehmen müssen ihre Konsumenten kennen, um sie an sich binden und optimal bedienen zu können. Aber selbst wenn die Funktion im Mittelpunkt steht: Die Dienste müssen auch sicher sein.

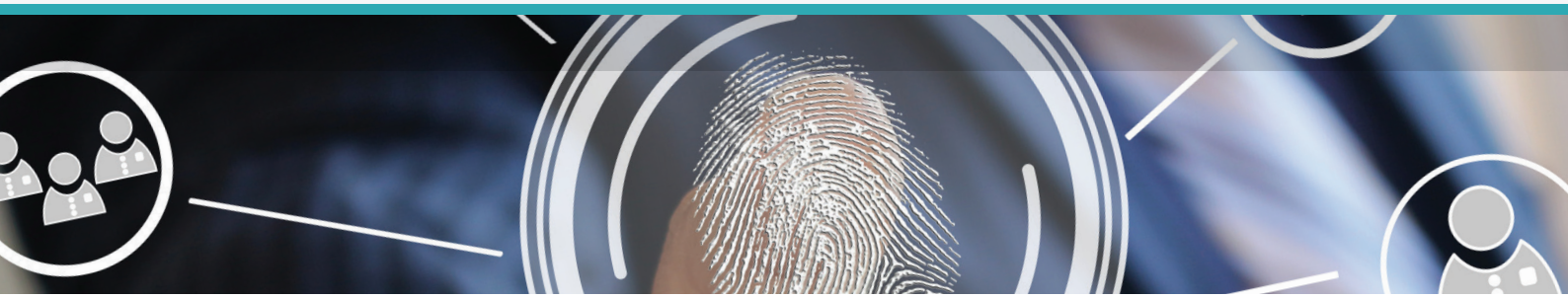
von Martin Kuppinger

In diesem Spannungsfeld zwischen Business und IT entwickelt sich das Consumer IAM, das Identity und Access Management für Konsumenten. Dabei handelt es sich nicht um eine geschlossene technische Lösung, sondern um das Zusammenspiel verschiedener Technologien. Es geht um die Verwaltung der Identitäten von Konsumenten und Kunden, es geht um deren Authentifizierung, es geht aber auch um das Nutzbarmachen dieser Informationen für die optimale Versorgung der Kunden mit Marketinginformationen.

Doch ohne ein technisches Fundament wird CIAM nie funktionieren. Hierzu gehören Web Application Firewalls (WAFs), Ansätze für die starke Authentifizierung und die Sicherheit am Endgerät, um beispielsweise Apps so zu entwickeln und zu härten, dass sie nicht zum Einfallstor für Angriffe gegen die Business-Anwendungen im Backend werden.

Digitale Transformation: die treibende Kraft

Die treibende Kraft hinter dieser Entwicklung ist das, was heute oft als „Digitale Transformation" der Unternehmen bezeichnet wird: die Veränderung von Geschäftsmodellen hin zu digitalen Mehrwertdiensten, weg von der klassischen Erstellung und dem Verkauf physischer Produkte.



Dazu gehören beispielsweise Informationsdienste im Auto oder Überwachungs- und Wartungsdienste im Maschinenbau oder schon fast traditionell das Streaming von Musik im Abonnement statt des Verkaufs von Tonträgern. Auch in der Finanzindustrie gibt es einen massiven Wandel, bei dem die traditionellen Banken durch sogenannte FinTechs, innovative Anbieter von Finanzdienstleistungen, unter Druck geraten.

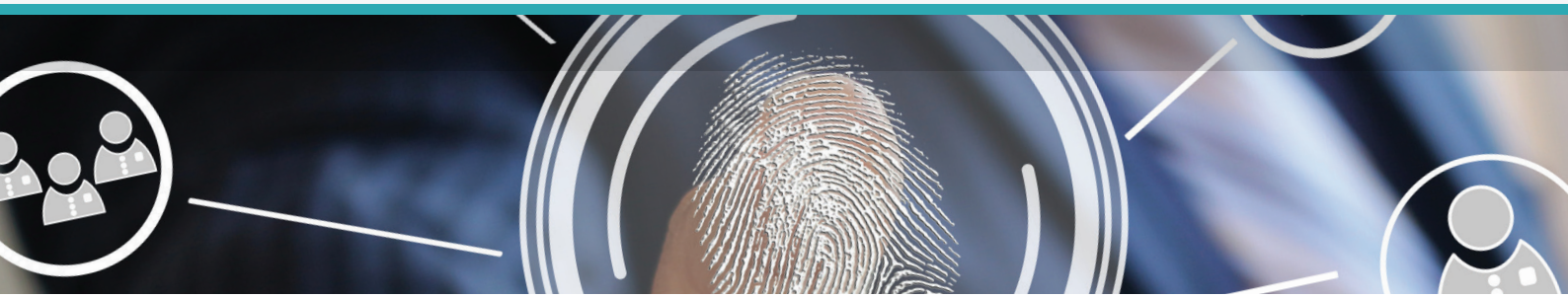
Ein gemeinsames Merkmal all dieser Entwicklungen ist, dass hierzu die Kunden und Konsumenten Zugang zu diesen Diensten erhalten müssen. Viele Unternehmen kannten ihre Konsumenten bisher nicht, ob es nun der Hörer des Tonträgers oder der Käufer eines Konsumgutes war.

Ein weiterer zentraler Aspekt ist die Verflechtung mit dem Internet of Things (IoT). Es geht nicht nur um Kundenidentitäten, sondern auch um die Identitäten von „Dingen" und Geräten und darum, die Kunden ihren Dingen und Geräten zuzuordnen. Zudem wandert der Zugriff in den „mobile space": Der Zugriff von mobilen Endgeräten über Apps – die entsprechend sicher sein müssen – ist längst die Regel und nicht mehr die Ausnahme.

CIAM: mehr als IAM, mehr als Marketing-Automatisierung

Um dem Kunden und Konsumenten Zugang zu Diensten geben zu können, muss man ihn kennen. Die „Identität" ist eine Grundvoraussetzung dafür, Mehrwertdienste anbieten zu können. Gleichzeitig rückt damit aber auch das Thema Sicherheit ins Blickfeld, also die Frage, wie man den Zugang zu neuen digitalen Diensten absichern kann. Es geht aber um viel mehr: Es geht auch darum, wie sich die Daten, die aus der Interaktion mit Konsumenten und Kunden gesammelt werden, nutzbar machen und einsetzen lassen.

Wie so oft bei neuen Entwicklungen hat sich auch hier schnell ein Schlagwort etabliert: CIAM steht für Consumer Identity and Access Management oder Customer Identity and Access Management. Der Konsument ist dabei der Überbegriff, weil dieser auch diejenigen erfasst, die nicht direkt Kunden sind. So ist der Konsument eines Pharmaherstellers derjenige, der die Arzneimittel einnimmt, der direkte Kunde aber vielleicht der Pharma-Großhändler. Der Fokus auf die breite Schar der Konsumenten und nicht nur auf die bestehenden Kundenbeziehungen ist das, was die



Entwicklung treibt. Daher sollte die Konzentration auf Consumer IAM liegen und sich nicht auf Customer IAM beschränken.

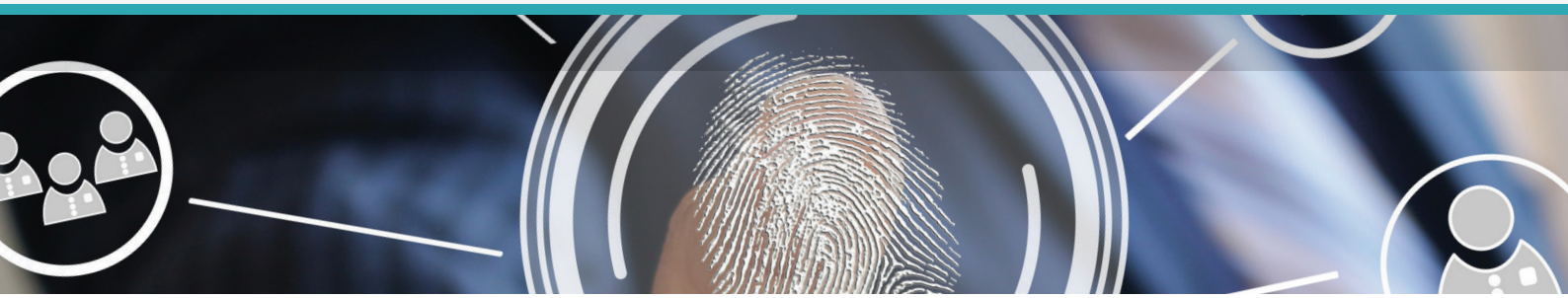
Dieser Begriff deckt wiederum das breite Feld des Identity Management und das eher technisch geprägte Access Management ab. Das Identity Management umfasst Aspekte wie die Registrierungsprozesse der Konsumenten, das Sammeln und Nutzen von Daten über diese und damit auch die Schnittstelle hin zu Marketingdiensten – hier insbesondere dem Feld der Marketing Automation mit dem Ziel, den Konsumenten optimal mit Informationen zu bedienen.

Ebenso gibt es Schnittstellen zu CRM-Systemen, in denen bestehende Kunden verwaltet werden, zu analytischen Anwendungen rund um die vielen über Kunden gesammelten Daten (Big Data) und zu KYC-Lösungen („Know Your Customer") etwa im Bankenbereich, die unter anderem die initiale Identifikation von Kunden umfassen.

Herausforderung Access und Sicherheit

Der andere wichtige Aspekt des Begriffs ist der Access, also der Zugriff. Wie kann sich der Kunde authentifizieren? Wer hat Zugriff auf seine Daten? Auf welche Anwendungen darf der Kunde in welcher Form zugreifen? Ist der Zugriffsweg sicher, von der App bis zum Backend? Solche Fragestellungen sowie Fragen zum Management von Identitäten müssen gelöst werden – und stehen hier im Blickpunkt.

Traditionelles IAM reicht für die neuen Anforderungen von CIAM nicht mehr aus. Bei CIAM geht es in der Regel um sehr viel mehr Identitäten, da es in den meisten Unternehmen viel mehr Konsumenten als Mitarbeiter gibt. Es geht um andere Prozesse - beispielsweise die Selbstregistrierung statt eines „Onboardings" von Mitarbeitern über das HR-System. Es geht um sichere Apps, eine flexible, aber dennoch sichere und den Vorgaben entsprechende Authentifizierung und vor allem auch um Skalierbarkeit und hohe Verfügbarkeit. Der Konsument erwartet, dass Systeme immer verfügbar sind. Und es geht um eine durchdachte Architektur, bei der zentrale Aufgaben wie das Management von Benutzern sowie die Authentifizierung zentral erfolgen. Ebenso müssen die Rollen der Apps und Web-Schnittstellen, der Backend-Systeme und der zentralen CIAM-Lösungen sowie der ergänzenden Sicherheitssysteme wie Web Application Firewalls (WAFs) klar und verbindlich definiert sein.

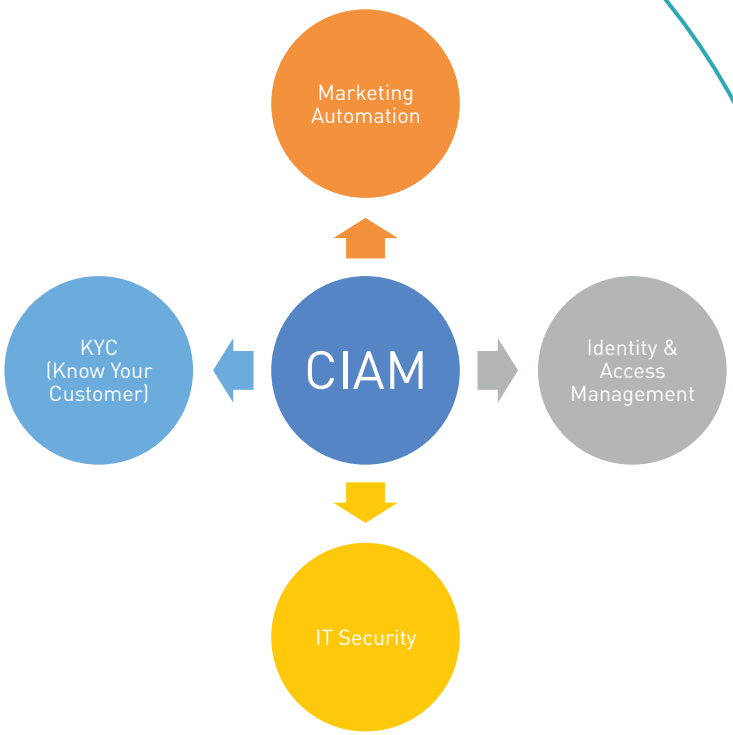


Die technische Basis für sicheres CIAM

Für den Erfolg neuer Geschäftsmodelle ist es wichtig, den Konsumenten zu erreichen und optimal zu bedienen. Die Grundlage dafür muss aber ebenso geschaffen werden – von der einfachen Selbstregistrierung bis hin zum einfachen, aber sicheren Zugang. Die Digitale Transformation ohne Sicherheit wird scheitern.

Sicherheit beginnt hier ganz vorne, bei der App und bei den Web-basierten Diensten, auf die die Konsumenten zugreifen. Sie umfasst aber viele weitere Aspekte - von der Verwaltung der Authentifizierungsmechanismen und dem Angebot einer flexiblen, adaptiven Authentifizierung bis hin zur Frage, wie man den Zugriff einer ungleich höheren Anzahl von Benutzern auf Backend-Dienste ermöglicht und absichert, die bisher lediglich von internen Nutzern oder einer überschaubaren Menge von Kunden genutzt wurden.

Consumer IAM ist vielschichtig und hat sowohl eine IT- als auch eine Marketing-Ebene ▼



CIAM verändert das IAM. Anpassungsfähige Workflows, eine flexible Authentifizierung, hohe Skalierbarkeit und Verfügbarkeit, aber ausgeprägte Sicherheit und die Erfüllung regulatorischer Vorgaben müssen gegeben sein. Dieses technische Fundament muss stehen, um den Konsumenten optimal bedienen und das Marketing automatisieren zu können. Denn das beste Marketing bringt nichts, wenn auf einmal sensitive Kundendaten verloren gehen und das Image dadurch angeschlagen ist. ■

Bild: Jakub Jirsák, Fotolia.com

Compliance – Herausforderung oder Chance?

Die Vielzahl neuer Regulierungen rund um Sicherheit und Datenschutz wie EU GDPR, PSD2 oder ITSiG erhöht den Druck auf Unternehmen – insbesondere wenn es um den Umgang mit Konsumenten- und Kundendaten geht. Doch bergen diese Regulierungen auch Chancen.

von Martin Kuppinger

Es vergeht kaum ein Jahr ohne eine neue Regulierung im Bereich Sicherheit und Datenschutz mit weitreichender Wirkung. Während sich manche wie PSD2 (Revised Payment Services Directive) nur auf bestimmte Branchen beziehen und einige wie das ITSiG (IT-Sicherheitsgesetz, Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme) nur auf ein Land, in diesem Fall Deutschland, haben andere Regulierungen wie die EU GDPR (General Data Protection Regulation) globale Auswirkungen auf alle Branchen.

Compliance als Chance

All diese Regulierungen bringen es mit sich, dass sich Unternehmen anpassen müssen. So haben diese die Authentifizierung ihrer Kunden zu verbessern und Schnittstellen für andere Finanzdienstleister bereitzustellen (PSD2). Starke Authentifizierung von Kunden (SCA, Strong Customer Authentication) ist eines der Kernelemente von PSD2, das viele betroffene Unternehmen vor große Herausforderungen stellt. Unternehmen haben generell dem „Stand der Technik" in puncto IT-Sicherheit zu entsprechen und müssen bei Angriffen staatliche Stellen informieren (ITSiG) oder die Zustimmung von Nutzern für die Verwendung von Daten modifizieren (EU GDPR). Gerade für den Umgang mit Kunden und Kundendaten führen die neuen Regulierungen zu deutlich höheren Anforderungen.

Doch bergen diese erzwungenen Änderungen auch Chancen – und zwar auf zwei Ebenen: Die eine betrifft die Differenzierung von den Wettbewerbern, die

andere die Option, die Änderungen so zu gestalten, dass sie gleichzeitig das Zusammenspiel mit Konsumenten und Kunden verbessern.

Bei der Differenzierung von den Wettbewerbern geht es darum, auch die Chancen zu erkennen, die mit einem sicheren Umgang mit Nutzerdaten, mit differenzierten Regelungen für den Datenschutz sowie Kontroll- und Steuerungsmöglichkeiten durch den Nutzer einhergehen. Je besser sich der Nutzer bedient und in seinen in Bezug auf den Datenschutz bestehenden Ängsten ernst genommen fühlt, desto loyaler wird er sein. Es geht also nicht nur darum, Imageschäden und Strafen bei erfolgreichen Angriffen auf solche Daten vorzubeugen, sondern parallel dazu die Chance zu nutzen, das Vertrauensverhältnis zum Konsumenten zu verbessern.

Das steht im engen Zusammenhang mit der zweiten Ebene: Wenn etwa die Authentifizierung verändert werden soll, warum dann nicht gleich so, dass der Nutzer – soweit im Rahmen der gesetzlichen Vorgaben zulässig – die Authentifizierungsmechanismen seiner Wahl verwenden kann? Warum bei der Anpassung der Zustimmungsregeln zur Datennutzung (Consent Management) nicht gleich auch die Selbstregistrierungsprozesse vereinfachen und flexibler gestalten? Das bringt Sicherheit für den Kunden und den Anbieter, vereinfacht Prozesse und reduziert Kosten – und erleichtert Anpassungen durch mehr Flexibilität. Vor allem aber erhöht es die Kundenzufriedenheit.

Rechtliche Anforderungen: Was man können muss

Ohne ins Detail aller relevanten gesetzlichen Vorgaben gehen zu wollen: Bereits in den drei aufgeführten Regulierungen und Gesetzen gibt es einige interessante Aspekte, die beeinflussen, wie CIAM gestaltet werden kann und muss – beispielsweise durch die Unterstützung zweckgebundener Zustimmungen (consent per purpose) und des Rechts auf Einsicht und Veränderung gespeicherter Daten. Hinzu kommen weitere branchenspezifische Anforderungen – etwa in der Finanzindustrie das regulatorische Themenfeld KYC (Know Your Customer), das ursprünglich durch Regelungen zur Verhinderung von Geldwäsche getrieben war, oder die Anforderungen an den Umgang mit Patientendaten in Krankenhäusern.

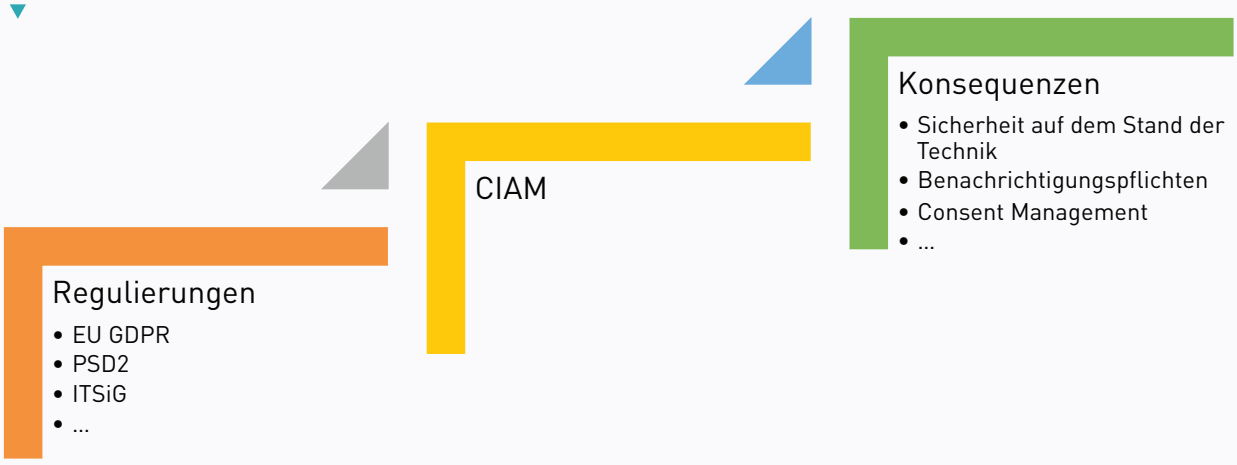
Bei der EU GDPR stehen vor allem die Regelungen für das Zustimmungsmanagement im Fokus. Hier wird beispielsweise eine Zustimmung pro Verwendungszweck – mit verständlicher Information über diesen Zweck – statt der bisherigen, oft sehr allgemein gehaltenen Zustimmung gefordert. Benutzer

dürfen die Zustimmung entsprechend auch für einzelne Zwecke zurückziehen, ihre Daten anfordern und vieles mehr. Hinzu kommt eine sehr kurze Benachrichtigungsfrist bei Datenlecks, die personenbezogene Daten betreffen. Das bedeutet, dass CIAM-Lösungen einerseits die generelle Sicherheit dieser Daten erhöhen müssen, andererseits aber auch flexible Lösungen für das Zustimmungsmanagement als Teil von Registrierungsprozessen sowie für spätere Änderungen erforderlich werden.

Bei PSD2 stehen die veränderten Anforderungen an die starke Kundenauthentifizierung im Blickfeld, die nun sehr häufig eine Zwei-Faktor-Authentifizierung (SCA) erzwingen, aber auch die geforderte Öffnung von Schnittstellen für die Initiierung von Zahlungsvorgängen (Payment Initiation) und für den Kontenzugriff (Account Information) für TPPs (Third Party Provider), also externe Finanzdienstleister. Hier geht es also einerseits um die Authentifizierung, andererseits um die Absicherung von Schnittstellen.

PSD2 schreibt darüber hinaus einen Manipulationsschutz für Authentifizierungsverfahren und einen besonders hohen Schutz für Single-Device-Umgebungen vor. Sichere Apps werden damit noch wichtiger als bisher.

Die neuen Regulierungen haben unterschiedliche, aber oft auch überlappende Wirkungsbereiche.



Das ITSiG bewegt sich dagegen eher im vagen Bereich mit seiner Forderung nach der Einhaltung des „Standes der Technik", die aber an anderer Stelle wie dem IT-Grundschutz oder durch die ISO 270xx ausgefüllt wird. Allerdings definiert beispielsweise PSD2 für betroffene Unternehmen deutlich konkretere Anforderungen, aus denen sich der Stand der Technik ableiten lässt.

Geschäftliche Anforderungen: Was man können sollte

Wie bereits ausgeführt, reicht es nicht aus, die Anforderungen „mal eben so" zu erfüllen. Die nächste Verschärfung der Regulierungen kommt bestimmt – und man muss dann wieder investieren –, und Chancen nutzt man damit auch nicht.

Folgende Aspekte stehen aus geschäftlicher Sicht im Mittelpunkt: die flexible (adaptive) Authentifizierung, einfach anpassbare Workflows für die Kundenregistrierung und das Zustimmungsmanagement, sichere und auf allen Geräten nutzbare Schnittstellen sowie eine einheitliche Sicht auf die Identität des Konsumenten und Kunden. Adaptive Authentifizierung bezeichnet hier Ansätze, bei denen die Authentifizierungsmechanismen austauschbar sind, aber unterschiedliche Verfahren auch in Kombination eingesetzt werden können. So lässt sich beispielsweise bei einem höheren Risiko eine stärkere Authentifizierung fordern oder bei Zahlungsprozessen auf das von PSD2 geforderte Niveau erhöhen, während der Zugang zu anderen Informationen einfacher möglich ist.

Flexibilität und Konsumentenorientierung als Ziel

Dabei gilt es, immer die sich verändernden Interessen der Konsumenten im Blick zu behalten. Der Nutzer möchte mit dem Gerät seiner Wahl arbeiten – und das kann morgen schon ein ganz anderes sein. Er möchte einfache, intuitive Registrierungs- und Zustimmungsprozesse – und dennoch das Gefühl haben, dass seine Daten nicht missbraucht werden können. Er möchte unterschiedliche Schnittstellen nutzen können. CIAM – richtig angegangen – hilft, die Kundenzufriedenheit zu erhöhen und die Balance zwischen Marketingwünschen, Sicherheitsanforderungen und dem regulatorischen Rahmen zu finden. ■

Bild: Myst, Fotolia.com

Sicherheitsanforderungen für B2C-Plattformen

Wer Systeme öffnet, macht sie auch angreifbar. Mehr Zugriffe von mehr Nutzern auf bestehende Systeme und neue Anwendungen, die für die bessere Bedienung der Kunden als Teil der Digitalen Transformation geschaffen werden, erhöhen die Sicherheitsrisiken und erzwingen geeignete Gegenmaßnahmen.

von Martin Kuppinger

Dabei geht es um eine Sicherheit von Ende zu Ende, von der App oder der Web-Schnittstelle, aber auch vom externen System, das ein TPP (Third Party Provider) etwa im Finanzbereich einsetzt, bis hin zu den Backend-Systemen, gleich wo diese stehen – ob on premises oder in der Cloud.

Neue Backends, alte Backends

Die Digitale Transformation erfolgt nicht auf der grünen Wiese. Während Start-ups ihre Lösungen von Grund auf neu entwickeln können, laufen die Kernsysteme von Banken und Versicherungen heute oft noch auf dem Mainframe. Und wenn der Kunde in Zeiten von „Industrie 4.0" die Möglichkeit haben soll, noch kurzfristig Farbe oder Ausstattung seines längst bestellten Neuwagens zu verändern, müssen dazu auch die bestehenden Steuerungssysteme für die Produktion vernetzt werden. Das ist die eine Seite.

Auf der anderen Seite werden zunehmend mehr Funktionen auf neue Systeme in der Cloud verlagert. Das resultiert häufig in mehr Systemen und in einer tendenziell höheren Komplexität der nun hybriden IT-Infrastruktur. Kunden können dabei direkt oder indirekt Funktionen unterschiedlichster Systeme nutzen – in der Cloud und on premises. In beiden Welten, in der Cloud und der internen IT, führen die mit der Nutzung neuer und der Öffnung bestehender Systeme einhergehenden Veränderungen zu neuen Herausforderungen. Für bestehende Systeme liegen diese in der Bereitstellung und Verwaltung von Schnittstellen, der Sicherheit und der Skalierbarkeit.

Das Konzept der IT mit zwei Geschwindigkeiten oder der „bi-modalen IT" trifft hier zu: Bestehende Kernsysteme werden um neue Anwendungen und konsumentenorientierte Apps ergänzt, um neue Funktionen wie den direkten Zugriff von Kunden auf ihre Versicherungsverträge oder Zugriffe von Drittanbietern im Kontext von PSD2 abzubilden. Stabile Kernsysteme werden so von den sich dynamisch entwickelnden neuen Anwendungen abgegrenzt. Das setzt allerdings voraus, dass die Schnittstellen sauber definiert, verwaltet und abgesichert sind und die Skalierbarkeit für die potenziell ungleich höhere Zahl von Zugriffen gegeben ist.

Benutzer verwalten und Schnittstellen sichern

Als besondere Herausforderung für das Management von Identitäten und Zugriffen kommt hinzu, dass die Backend-Systeme oft nicht alle Nutzer kennen und auch nicht in der Lage sind, die Identitäten aller denkbaren Konsumenten und deren Zugriffsberechtigungen individuell zu verwalten. Der Zugriff erfolgt daher häufig über technische Benutzer. CIAM muss diesen Spagat schaffen: Auf der einen Seite müssen sich die Konsumenten einfach registrieren und authentifizieren können, auf der anderen Seite ist die kritische Backend-Infrastruktur zu schützen und der Schutz der Daten auch bei technischen Benutzern zu gewährleisten. Gleichzeitig gilt es, die (neu) exponierten Schnittstellen abzusichern. Der Zugriff erfolgt sowohl bei der App-Nutzung als auch bei Zugriffen, die über Anwendungen von Dritten erfolgen – nicht über die Authentifizierung des Benutzers direkt an der Anwendung, sondern über eine System-zu-System-Kommunikation.

Web Application Firewalls (WAF), die sowohl die Authentifizierung von Benutzern und die Zugriffssteuerung auf Anwendungen unter Verwendung technischer Benutzerkonten als auch die exponierten APIs schützen können, stellen ein wichtiges Element in den Sicherheitskonzepten für moderne, konsumentenorientierte Anwendungen dar. Sie schotten den inneren Kreis der geschäftskritischen Kernsysteme ab und kontrollieren den Datenfluss zwischen der Außenwelt und den internen Systemen.

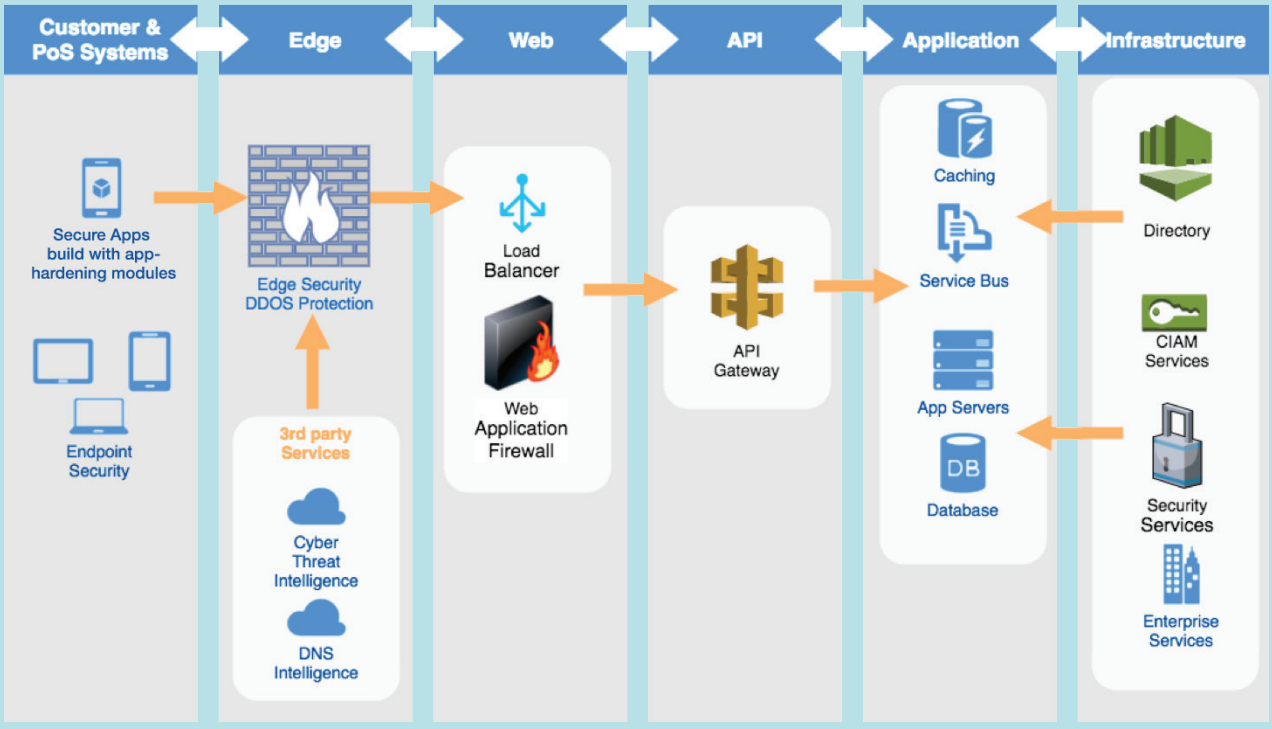
Adaptive Authentifizierung

Neben Aspekten wie hoher Skalierbarkeit spielt die flexible Unterstützung von Authentifizierungsanforderungen eine zentrale Rolle. Hier geht es nicht nur um die Balance zwischen Nutzerfreundlichkeit – die Unterstützung

einer einfach nutzbaren Authentifizierung von dem Gerät der Wahl – und Sicherheit respektive Compliance, sondern auch darum, unterschiedliche Zugriffswege wie direkte Zugriffe auf Web-Anwendungen oder indirekte Zugriffe via Apps zu unterstützen.

Hohe Flexibilität in diesem Bereich ist ein Schlüsselkriterium für den Erfolg auf dem Weg zu Anwendungen, die den Konsumenten einbinden – und damit für den Erfolg von CIAM. Die adaptive Authentifizierung und die Bereitstellung einer Auswahl sicherer, aber einfach nutzbarer Authentifizierungsmethoden hilft, die Einstiegshürde für den Konsumenten zu senken und insbesondere den Übergang vom Konsumenten zum Kunden zu erleichtern, bei dem beispielsweise für Bestellprozesse eine stärkere Authentifizierung erforderlich wird.

Mehrschichtige Sicherheitsarchitektur für CIAM



Sicherheit im Umgang mit Konsumenten und Kunden erfordert mehrschichtige Architekturen.

Die App: der Einstiegspunkt

Die App stellt einen Einstiegspunkt dar. Damit ist sie eine Schnittstelle, die dem Benutzer den Zugang zu neuen Diensten ermöglicht, gleichzeitig aber auch eine Schnittstelle für Angreifer. Sicherheit muss sich von der „gehärteten" App mit einem hohen Schutzniveau lokaler Daten über die Schnittstellen wie WAF-Systeme bis hin zu den Backend-Systemen erstrecken. Sichere Apps zu liefern ist eine Aufgabe des Anbieters.

CIAM beginnt, wie der Name schon sagt, beim Kunden und reicht bis hin zur Steuerung der Zugriffe auf die Backend-Systeme. Dabei ist der CIAM-Bereich, der sich mit der Verwaltung der Identitäten, ihrer Registrierung, dem Zustimmungsmanagement, der Authentifizierung und der Sicherung von Zugriffen von der sicheren App bis zum Backend-System erstreckt, ebenso wichtig wie die Unterstützung von Marketingautomatisierung. Die damit einhergehenden Anforderungen sind ungleich höher als bei traditionellen B2C-Systemen: Mehr Nutzer, mehr Endgeräte, komplexere und vor allem auch variablere Anforderungen an die Authentifizierung, die vermehrte Öffnung von APIs und die viel höheren Anforderungen an die Registrierungs- und Zustimmungsprozesse von Konsumenten erfordern neue Lösungen – sowohl solche, die das Marketing optimal unterstützen, als auch solche, die die Sicherheit gewährleisten. ■

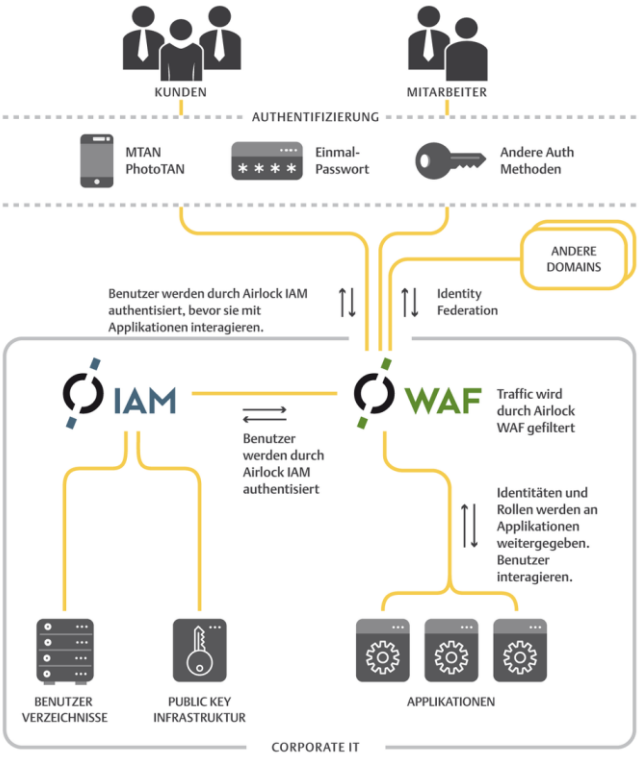
Was ist App-Härtung und warum ist sie wichtig?

Digitale Transformation bedeutet, den Nutzer so zu bedienen, wie er es möchte - das umfasst auch das Gerät seiner Wahl und damit eine Mobilitätsstrategie. Diese erfordert die Nutzung von Apps, in denen sensible Daten bereitgestellt werden. Die Ausführung findet dabei auf dem Privateigentum des Kunden statt, dem Smartphone. Der Sicherheitszustand privater Smartphones lässt sich jedoch nicht einschätzen. Das Risiko, dass das Smartphone und seine Apps zum Einfallstor für Cyber-Angriffe werden, ist demnach nicht abschätzbar. Unternehmen müssen ihre Apps daher als „Security-Endpoint" verstehen und diese absichern. Hier kommen Lösungen zur App-Härtung ins Spiel.

Dabei handelt es sich um Softwaremodule, die von den App-Entwicklern in die App eingebaut werden und eine Vielzahl von Sicherheitsfunktionen bereitstellen. So geschützte Apps können sich selbstständig „verteidigen" und schützen sich proaktiv vor Malware, Trojanern und Hacker- Angriffen. Damit lassen sich die Daten der Kunden und Unternehmen mit viel höherer Sicherheit in der App verarbeiten und lagern und können nicht von Dritten abgezogen oder manipuliert werden. Der Einsatz von App-Härtung ist daher ein wichtiger Baustein in einem Sicherheits-Gesamtkonzept, um eine vollständige „360 Grad-Sicherheit" zu ermöglichen. Ziel sind sichere Apps, die den Best-Practice Empfehlungen der Behörden und Sicherheitsexperten folgen.

Customer IAM in der Praxis - Praxisbeispiel eines Versicherungskonzerns

Auf die verschiedenen Brokersysteme eines großen internationalen Versicherungskonzerns greifen insgesamt 7.000 externe und interne Mitarbeiter zu. Beide Nutzergruppen erstellen dort Offerten, managen ihre Portfolios und fragen Informationen über Schulungen und Provisionen ab. Der Zugriff der Externen auf die firmeninternen Applikationen ist jedoch kompliziert – das IAM-System basiert auf fünf verschiedenen Produkten von mehreren Anbietern. Ein neues System soll mit Single Sign-on die Komplexität reduzieren und allen Nutzern erweiterte User Self-Services ermöglichen. Der Konzern wurde mit einer Lösung fündig, die sehr schnell einsatzbereit war und ihm zusätzlich 50 Prozent der laufenden Kosten einsparte.



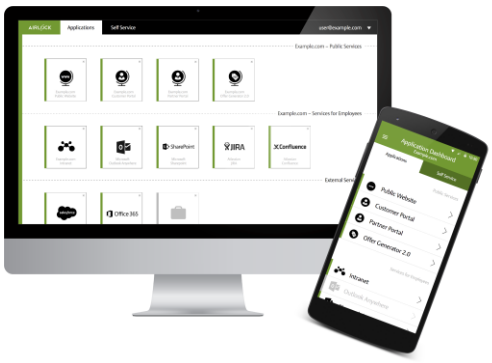
Die Prüfung der Investitionskosten und der Amortisationszeit einer neuen Lösung machte bald klar, dass der Wechsel zu einem neuen, einheitlichen System sinnvoll war. Denn neben dem einfachen Zugang für Broker wurde auch die Ausbaufähigkeit zunehmend wichtig: die Skalierbarkeit für künftige Anwendungen, zum Beispiel ein Kundenportal, musste durch die neue Lösung gegeben sein. Man wollte unterschiedliche Benutzerrollen für Mitarbeiter, Partner und Kunden definieren können. Durch den Zugriff von extern wurde die Applikation zudem exponierter, was zu erhöhten Sicherheitsanforderungen führte.

Auf der Suche nach einer umfassenden und gleichzeitig flexiblen Lösung für all diese Anforderungen wurde der Konzern mit der Airlock Suite fündig. Die Kombination der Web Application Firewall **Airlock WAF** mit dem Authentisierungsserver **Airlock IAM** bot die gesuchte passgenaue Lösung aus einer Hand. Brokerportale und Authentifizierungslösung konnten entflochten werden; die Partner der Versicherung erhielten einen einfachen und sicheren Zugang zu den internen Applikationen.

Das CIAM zusätzlich schützen

Ein Vorteil der Kombination einer Customer IAM Lösung mit einer Web Application Firewall ist, dass der Ablauf der Kundeninteraktionen mit der IAM-Lösung gesichert wird und das IAM-System sowie die Applikationen umfänglich vor bekannten OWASP Top 10 Schwachstellen, wie z.B. Script-Angriffen geschützt werden. Die Schweizer Lösung aus einer Hand ersetzte das bisherige System des Versicherungskonzerns dank ihrer Flexibilität in Rekordzeit: in fünf Monaten war die Airlock Suite in Betrieb.

Flexibilität der Airlock Suite



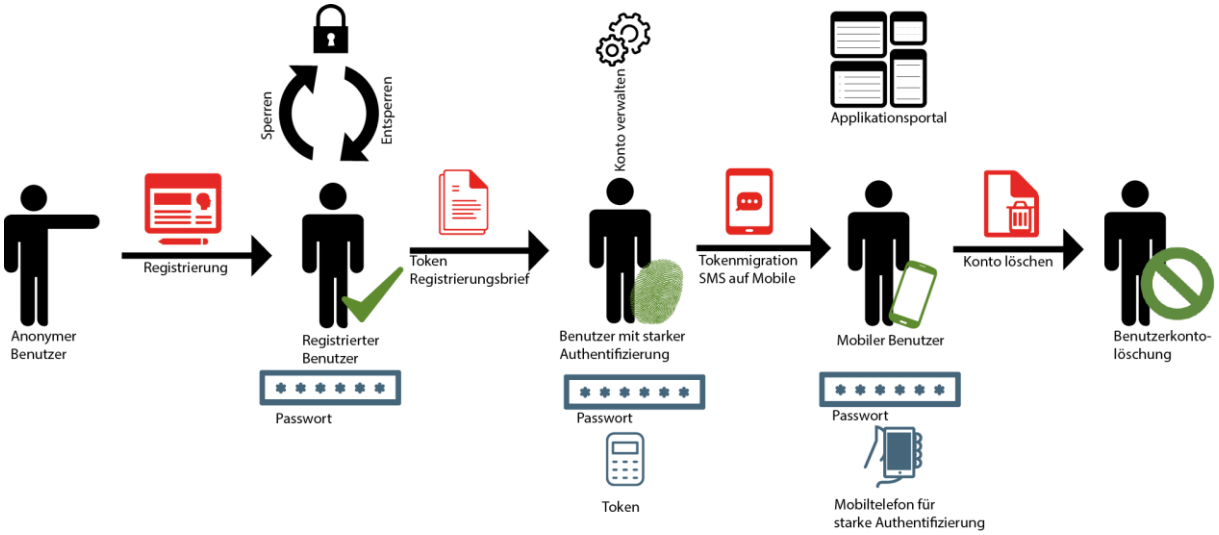
Eine besondere Herausforderung im Migrationsprojekt war die große Zahl an Applikationen. Die sehr heterogenen Mechanismen zur Übergabe der Benutzerdaten hielten sich zum Teil nicht an gängige Standards. Mit einer kleinen spezifischen Erweiterung im Airlock IAM konnten die Experten von Airlock eine Vielzahl an Backends zusätzlich unterstützen. Sie ermöglicht die Verarbeitung und Weitergabe einiger herstellerspezifischer, nicht-standardisierter Identitätsträger. Während der Umsetzung wurde zudem klar, dass nicht alle Nutzer einer externen Benutzergruppe zu einer bestimmten Applikation umfassenden Zugriff haben durften. Auch diese neue Anforderung wurde innerhalb eines Tages erfolgreich umgesetzt: Mit einer Erweiterung der Airlock WAF-Konfiguration und einigen Anpassungen innerhalb der Airlock IAM-Konfiguration wurden verschiedene Zugrifflevels auf dieselbe Applikation möglich.

Für die Anwender erhöhte sich mit der neuen Lösung vor allem die Benutzerfreundlichkeit. Eine einzige Anmeldung genügt nun für den Zugriff auf alle Applikationen - egal ob intern oder in der Cloud. Aber auch die Kosten gingen zurück. Zuvor war insbesondere der Support ein wichtiger und großer Kostenfaktor, denn Benutzerselbstverwaltung gab es nicht. So mussten die Nutzer zum Beispiel einen Passwort-Reset via Helpdesk veranlassen. Im Airlock CIAM kann jeder Kunde sein Passwort, wie auch alle anderen Tätigkeiten zur Verwaltung des Kontos selbst verwalten. Der Versicherungskonzern konnte dadurch die Anrufe beim Support um 30 Prozent reduzieren. Insgesamt konnte das Unternehmen durch die neue, zentralisierte CIAM-Lösung über 50 Prozent der laufenden Betriebskosten einsparen.

Das Unternehmen konnte sich dank der neuen Lösung an den Marktstandard anpassen, die laufenden Kosten massiv senken, die Nutzerakzeptanz erhöhen und die Plattform weiter skalieren.

Die CIAM-Lösung – die Vorteile auf einen Blick:

- Für große Anzahl an Nutzern geeignet
- User Self-Services für den gesamten Lebenszyklus
- Hohe Performance
- Hohe Sicherheit und Schutz der Privatsphäre
- Web- und Mobile-Zugriff möglich
- Kosteneffizient
- Digital Onboarding
- Social Media-Login
- Anpassbare Zugriffskontrolle
- API-Integration
- Hohe Flexibilität
- Skalierbarkeit
- Delegierte Administration für Helpdesks
- Synchronisation von Directory Services
- Flexibilität bei der Authentisierung
- Risikobasierte und adaptive Authentisierung
- Schutz der Identitäten
- Fraud Detection



Self-Service- und Sicherheitsfunktionen erleichtern das Management digitaler Identitäten über deren gesamten Lebenszyklus hinweg. Bild: Ergon Informatik

User Self-Services als Teil des CIAM-Systems

Bei traditionellen IAM-Lösungen übernehmen Helpdesks einen Großteil der Verwaltungsaufgaben für die Nutzer, so dass diese kaum Aufwand haben. Allerdings ist eine solche Lösung nicht skalierbar und wird für ein Unternehmen bei vielen Kunden nicht nur unübersichtlich, sondern vor allem sehr kostenintensiv. Laut Gartner vergisst jeder Nutzer im Durchschnitt 1,8 Mal im Jahr sein Passwort. Dieser muss das Kennwort dann vom Support zurücksetzen lassen, um wieder Zugriff zu erhalten. Die Kosten für einen Anruf beim Helpdesk schätzt Gartner auf durchschnittlich ca. 50 Euro. Anrufe vieler Kunden lassen diese Kosten rapide in die Höhe schnellen.

Gerade bei wiederkehrenden Aufgaben können Helpdesks durch ein CIAM-System einfach entlastet werden. Die Lösung heißt „User Self-Services“. Sie automatisieren Abläufe und übertragen einfache Aufgaben an die Nutzer. Diese können sich selbst registrieren, ihr Passwort zurücksetzen oder ihr Profil selbst pflegen. Auch Adress- oder Bankdatenänderungen können selbstständig in eine Maske eintragen werden. Dieser Service ist nicht nur im Sinne der Benutzer, die so besser Kontrolle über ihre Daten haben, sondern auch kosteneffizient. Selbst wenn das Unternehmen oder der Kunde sich entscheidet, ein neues Authentisierungsmittel einzuführen, können die Nutzer den Wechsel prozessgestützt selbst vornehmen.

Für weitere Fragen stehen wir Ihnen jederzeit gerne zur Verfügung:
+41 44 268 87 00
info@airlock.com
https://www.airlock.com/

VERTRAUEN in die digitale Welt bringen

Einführung

Die meisten Menschen sind heutzutage täglich, wenn nicht sogar ständig online. Unser Leben wird immer digitaler. Fragen Sie sich: Nehmen Sie Ihr Smartphone sofort nach dem Aufwachen am Morgen in die Hand? Wie viele Laptops und Tablets haben Sie zu Hause? Wir erledigen unsere Bankgeschäfte online, interagieren online, machen Arzttermine online, lesen Bücher und treffen sogar neue Freunde online.

In der digitalen Welt sind persönlich identifizierbare Informationen (PII), wie z.B. Finanzkonten, Kreditkartennummern oder sogar IP-Adressen, eine hoch geschätzte Ware. Die Sicherung dieser Informationen sollte daher oberste Priorität haben.

Dennoch gibt es überall Betrug. Infolgedessen braucht das Leben in einer digitalen Welt Vertrauen. Vertrauen in die Benutzer, Plattformen, Anwendungen und Geräte. Doch in diesem immer komplexer werdenden Umfeld ist eines der größten Probleme der IT-Sicherheitsexperten, dass das traditionelle Modell für Vertrauen brüchig geworden ist.

Was bedeutet Vertrauen?

Also, wie definieren Sie Vertrauen? Laut dem Wörterbuch, "Vertrauen ist ein fester Glaube an die Zuverlässigkeit, Wahrheit, Fähigkeit oder Stärke von jemandem oder etwas."

Im Rahmen von Sicherheit und Technologie besteht jedoch das Vertrauen zwischen:

- Benutzer und Client-Anwendungen
- Client-Anwendungen und Server-Anwendungen
- Server-Anwendungen und Benutzer

Wenn Vertrauen zwischen diesen Komponenten besteht, kann Benutzer erlaubt werden mehr tun. Zum Beispiel können vertrauenswürdige Benutzer auf weitere Funktionen in mobilen Apps zuzugreifen, die ihnen aus Sicherheitsgründen nicht anderweitig zur Verfügung stehen würden (z. B. Unterzeichnen von Verträgen, Senden einer Überweisung oder Eröffnung eines Bankkontos)

Mobile Geräte und der Faktor Vertrauen

Heute werden immer häufiger mobile Geräte als Mittel zur Bezahlung von Waren und Dienstleistungen eingesetzt. Das mobile Gerät wird immer mehr zum zentralen Punkt des Benutzerökosystems und Nutzer wollen immer mehr damit tun. Doch in den meisten Fällen sind diese Geräte nicht vertrauenswürdig, denn:

In einem kürzlich veröffentlichten Bericht[1] waren 95% der getesteten mobilen Anwendungen anfällig gegen Angriffe. Das beinhaltet:

- Durchschnittlich 6.5 Schwachstellen pro mobiler Anwendung
- 35% hatten kritische Probleme
- 45% hatten Probleme mit hohem Risiko

[1] Trustwave Global Security Report 2015: https://www2.trustwave.com/GSR2015.html

Für 90% dieser Anwendungen konnten die Tester sensible Informationen offenlegen, einschließlich Karteninhaberdaten, Benutzernamen und / oder Passwörter, persönlich identifizierbare Informationen (PII) und sogar Quellcode – eben die Informationen, die zu hoch geschätzten Waren von Cyberkriminellen geworden sind.

Es ist keine Überraschung, dass das Smartphone neue Anforderungen wie einen Bedarf an Plattformsicherheit und an einem Server-basierten Risikomanagement bringt.

Die Trends für Benutzer- und Anwendungssicherheit für mobile Geräte zeigen, der Markt sucht nach reibungsloser und passwortloser Authentifizierung und Transaktionsdatenerfassung. In einigen Kreisen gewinnt die Biometrie an Bedeutung, doch in einigen Ländern besteht weiterhin große Sorge um die Privatsphäre. Zudem wachsen die Märkte für Systeme zur Online-Betrug Erkennung und Systemen zur Authentifizierung und Betrugsprävention immer stärker zusammen.

Bezeichnend dafür ist, dass Regulierungen weiterentwickelt werden, um diese neue Märkte zu adressieren:

- E-Banking: Lokale Vorschriften, EBA, FFIEC
- E-Government: eIDAS
- Gesundheitswesen: EPCS, eIDAS
- E-Commerce: PSD2, XS2A, eIDAS

Letztlich muss eine passende und reaktionsfähige mobile Sicherheitslösung sowohl Ende-zu-Ende Vertrauen und Sicherheit bieten als auch benutzerfreundlich sein.

Wo wird Vertrauen benötigt?

Um eine Vertrauensstellung zu erreichen ist es nicht ausreichend initial und einmalig das Vertrauen zu erhalten. Es muss während der gesamten Transaktionskette aufrecht erhalten bleiben:

1. Sie müssen darauf vertrauen, dass Sie Ihren Benutzer kennen
2. Sie müssen Vertrauen haben, im bekannte Benutzer mit starken Zugangsdaten zu versehen, die dennoch eine einfache Authentifizierung ermöglichen
3. Sie müssen darauf vertrauen, dass die Geräte sicher sind
4. Sie müssen auf die Sicherheit der Anwendung vertrauen
5. Sie müssen dem Kommunikationskanal zu / von Ihren vertrauenswürdigen Identitäten, Geräten und Anwendungen vertrauen
6. Sie müssen der Absicht des Nutzers vertrauen, wenn Informationen ausgetauscht werden
7. Sie müssen dem Verhalten des Benutzers auf allen seinen Geräten über alle Ihre Kanäle vertrauen

Mit Vertrauen zwischen diesen Komponenten kann Benutzern erlaubt werden, mehr zu tun und vertrauenswürdig auf weitere zusätzliche Funktionen zuzugreifen. In technischer Hinsicht wird das Vertrauen über Identitätsnachweis, Multifaktor-Authentifizierung, mobile Anwendungssicherheit, Betrugsprävention und digitale Signatur aufgebaut. Brauchen Sie einen weiteren Anreiz zum Schutz mobiler Transaktionen?

Betrachten Sie diese Binsenweisheit: Es dauert Jahre Vertrauen aufzubauen, aber nur Sekunden es zu brechen und für immer es zu reparieren.

Was sind die fünf Technologien hinter Online-Vertrauen?

In der physischen Welt muss man sich Vertrauen verdienen Das gilt auch in der Online-Welt, in der das Vertrauen in jedem Transaktionsschritt einer Transaktion schrittweise verdient werden muss. Das beinhaltet:

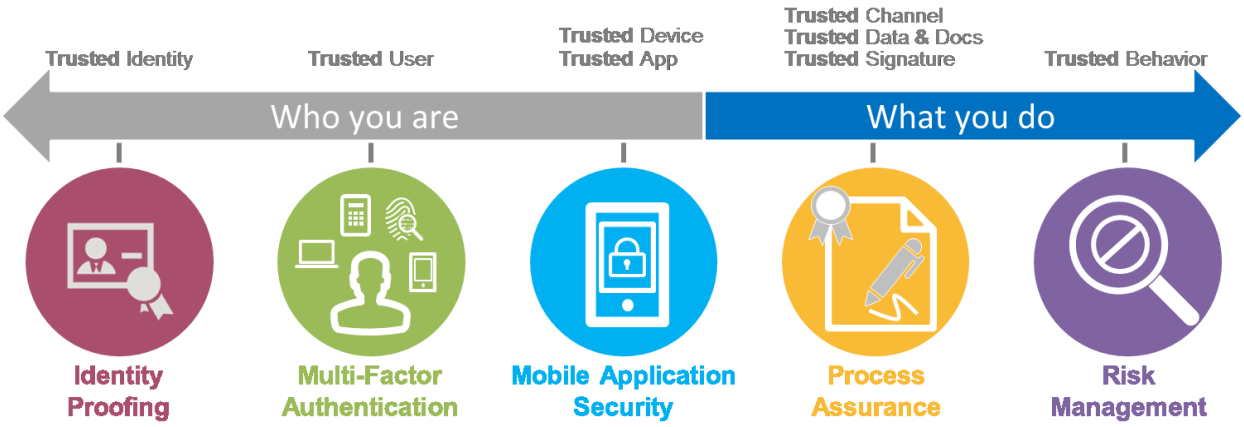
1. Identitätsüberprüfung (sind Sie wirklich derjenige, der Sie vorgeben zu sein)
2. Multifaktor-Authentifizierung (kann der Benutzer, als den Sie sich

ausgegeben haben, durch verfügbare Authentifizierungsmethoden bestätigt und validiert werden)
3. Mobile Anwendungssicherheit (ist der Plattform [Gerät und Anwendung] zu vertrauen, die Sie verwenden, um die Transaktion auszuführen,)
4. Transaktionssicherheit (ist der Austausch von Daten und der Prozess des Datenaustauschs zwischen Ihnen und dem Empfänger vertrauenswürdig)
5. Verhalten (ist Ihr Online-Verhalten zuverlässig und konsistent oder abweichend und verdächtig).

Vertrauenswürdige Plattform

VASCO ist ein anerkannter Marktführer für Mobile Application Security, Multi-Faktor-Authentifizierung, elektronische Signaturen und Risikomanagement-Lösungen für Unternehmen und öffentliche Verwaltungen in über 100 Ländern weltweit.

Die Abbildung unten zeigt den ganzheitlichen Ansatz von VASCO, digitales Vertrauen in der mobilen und Online-Interaktion eines Kunden zu schaffen und aufrecht zu erhalten.



Schlussfolgerung

Die in diesem Dokument beschriebenen Elemente ermöglichen eine sichere digitale Plattform, die der digitalen Welt viel nötiges Vertrauen schafften: Ihren Mitarbeitern, Ihren Kunden und Ihren Partnern. So können sie dieses digitale Vertrauen bei der Arbeit, zu Hause und unterwegs genießen, egal was sie tun, Bankgeschäfte, ein Haus kaufen, eine Versicherungspolice abschließen, Bilder mit Freunden austauschen oder neue Leute treffen. Eine vertrauenswürdige digitale Identität, die durch die Vielzahl neuer technologischer Fortschritte geschaffen und gefördert wird, wird bald das Medium sein, mit dem Sicherheit einfach und die Verbesserung der Nutzererfahrung möglich wird. Ausgestattet mit vertrauenswürdigen digitalen Identitäten, kann Mitarbeitern und Verbrauchern erlaubt werden, mehr zu tun, und das viel schneller. VASCO hilft Ihnen dabei sicherzustellen, wer Sie sind und was Sie tun.

PROMON

CUSTOMER-IAM UND APPS: MOBIL ABER UNSICHER?

Smartphones in jeder Hand

Smartphones erobern die Geschäftswelt. Immer mehr Unternehmen nutzen Apps, um mit ihren Kunden in Kontakt zu treten. Dieser Kontakt bietet Chancen und birgt Risiken zugleich: Eine digitale Kundenbeziehung erleichtert es den Unternehmen mit den Kunden zu interagieren, erfordert aber auch eine Absicherung der von beiden Seiten zur Verfügung gestellten Daten. Dieser Themenkomplex wird mit Lösungen aus dem Bereich Customer IAM (CIAM) adressiert.

Diese Lösungen erfordern eine besonders hohe Flexibilität und Sicherheit bei der Authentisierung und dem Management von Identitäten. Ein ideales Customer IAM verbessert die Customer-Experience, verringert dabei die Sicherheitsrisiken und reduziert die Kosten.

Eine der größten Herausforderungen hierbei ist, dass der Kontaktpunkt zwischen Kunde und Unternehmen eine App ist. Die App wird auf dem Privateigentum des Kunden – dem Smartphone – ausgeführt. Der Sicherheitszustand der privaten Smartphones kann nicht eingeschätzt werden und liegt außerhalb der Kontrolle des App-Anbieters. Sicherheit muss also dort ansetzen, wo die Daten der Unternehmen und der Kunden verarbeitet werden.

Die etablierten Sicherheitskonzepte und -Strategien der Unternehmen greifen hier nicht mehr, die Geräte der Endkonsumenten lassen sich nicht managen oder kontrollieren. Die Sicherheit muss folglich dort abgebildet werden, wo die Verantwortung des Unternehmens liegt – **in der App**.

Die Bedrohungslandschaft für Apps ist größer als gewöhnlich bekannt. Das bedeutet, dass Angreifer mit Hilfe von Malware, Keyloggern, Spyware oder anderen Schadprogrammen, Zugriff auf Daten der Benutzer und der Unternehmen in der App erhalten können.

Promon ist Pionier auf dem Gebiet proaktiver, „whitelist-basierter“ Runtime-Application-Self-Protection und bietet mit SHIELD™ die führende Technologie zur App Härtung an.

Die App als Security-Endpoint

Sicherheitsrisiken auf mobilen Systemen

Schadsoftware auf mobilen Systemen agiert als „Man-In-The-App“ („MITA“) - auf Windows auch als „Man-In-The-Browser“ („MITB“) bekannt. Als MITA übernehmen Trojaner gezielt Apps und führen ihren Schadcode in der Laufzeit der App aus, um diese „von Innen“ zu kontrollieren und zu übernehmen. Effektiv erhalten Angreifer so die Kontrolle über die angegriffene Applikation und die darin eingegebenen, gespeicherten und verarbeiteten Daten. Auch in den Apps liegende Zertifikate oder Schlüsselmaterial sind durch dieses Szenario bedroht und können von Angreifen abgezogen und für skalierende Malware-Modelle wiederverwendet werden.

Um MITA Angriffe zu konzipieren, nutzen Angreifer Reverse-Engineering. Apps, die sich in Emulatoren ausführen lassen oder von Debuggern analysiert werden können, sind einfache Angriffsziele. Angreifer nutzen diese Umgebungen, um Apps zu analysieren und sensible Daten wie Schlüsselmaterial und Zertifikate zu entwenden. In diesen Umgebungen kann auch gezielt Malware entwickelt werden und beispielsweise direkt in den App Code integriert werden, ohne dass dies vom App-Anbieter oder Nutzer bemerkt wird. „Repackaging“ nennt man diesen Vorgang und die dadurch entstandenen Apps werden über Third-Party App-Stores oder Phising Mails und Webseiten verbreitet.

Abgesehen von gezielten Angriffen auf die App finden sich heute in den App Stores Programme, die sich als gewöhnliche Apps tarnen. Für die Nutzer können sich diese Malware Apps als Spiele oder Funktions-Apps darstellen, ihre Hauptfunktion ist aber die Eingaben von User-Credentials zu entwenden. Solche Programme können Screenshots der Keyboard-Highlights (iOS und Android) erstellen oder werden direkt als Drittanbieter Keyboards und Screen-Reader (Android) angeboten.

Eine hochentwickelte Rooting- und Jailbreak Erkennung ist unerlässlich für ein mobiles Sicherheitskonzept. Je nach Sicherheitsbedarf sollte entweder vollständig ausgeschlossen werden, dass Apps in solchen Umgebungen ausgeführt werden oder zumindest sichergestellt sein, dass Apps auch in solchen Umgebungen wehrhaft sind.

Um sich nachhaltig vor diesen Risiken zu schützen, muss ein Sicherheits-Modul in die App eingebunden werden, welches die App proaktiv gegen die hier beschriebenen Angriffe schützt.

Alte Konzepte und moderne Lösungsansätze

Herkömmliche Antimalware-Lösungen gelten inzwischen als nicht ausreichend, aufgrund ihres „Blacklist-Ansatzes“, sie können die Sicherheit der mobilen Betriebssysteme Android und iOS nicht gewährleisten. Durch die vorhandene Sandbox-Struktur dieser Betriebssysteme wird die Ausführung für Sicherheitssoftware erschwert (Android) oder gar verhindert (iOS). Promon SHIELD™ ist eine Technologie für Apps, die proaktiv Sicherheitsbedrohungen erkennt und abwehrt. SHIELD™ kann durch seinen „Whitelist-basierten“ Ansatz auch auf unsicheren oder ungeschützten Geräten ein hohes Schutzniveau für Applikationen und Daten ermöglichen. App-Anbietern wird so ermöglicht, sich selbst verteidigende Apps anzubieten.

Transparenz ist der Schlüssel

Teil moderner CIAM Lösungen ist oft eine App, welche der Endkonsument zur Identifikation / Authentifizierung nutzt. Um für Endkonsumenten attraktiv zu sein, muss eine App heute einfach und angenehm nutzbar sein. Das bedeutet auch, dass Sicherheits-Mechanismen keinen Einfluss auf die Nutzbarkeit haben dürfen. Dies ist eine Chance für alle App-Anbieter auf moderne Sicherheits-Technologien umzusteigen, wie es etwa Banken vormachen: die Sicherheitsmechanismen werden in die App integriert, transparent für die Kunden.
Promon SHIELD™ ist Bestandteil der App und wird vom App Entwicklungsteam mit geringem Aufwand integriert und ist für den Nutzer nicht sichtbar. Damit ermöglicht Promon den App-Anbietern Anwendungen mit Fokus auf die Nutzbarkeit zu entwickeln und trotzdem ein höchstes Maß an Sicherheit für den Konsumenten und den Anbieter zu erreichen, ohne die Wahrnehmung des Endnutzers zu stören. Die mit SHIELD™ gehärtete App wird aktiv und transparent zur Laufzeit kontrolliert und vor auf dem Gerät befindlicher Schadsoftware geschützt.

Promon SHIELD™ wird in allen Bereichen eingesetzt, in der Apps mit sensiblen und sicherheitskritischen Daten oder Business-Logik arbeiten. Beispiele sind Banking- und Payment Apps, Authentisierungs-Apps, sowie Apps aus den Einsatzbereichen Automotive, IOT, Smartlock, eHealth und Remote Employee Access.

Promon SHIELD™ wird als SDK (Software Development Kit) bereitgestellt, plattformspezifisch in die zu schützende App implementiert und für Windows, iOS und Android ausgeliefert.

Mehrwert durch App-Härtung mit Promon SHIELD™

- Bestehende Apps können einfach geschützt und über die offiziellen Stores ausgerollt werden
- Endbenutzer sind nicht involviert – keine zusätzlichen Downloads oder Eingaben durch die User
- SHIELD™ beeinflusst weder die Usability noch das Aussehen Ihrer App
- Einschleusen von Schadcode in die App wird unterbunden: höchster Schutz der in der App verarbeiteten Daten, Schlüssel und Zertifikate
- Wirkungsvolle Erkennung und Reporting von Jailbreak und Rooting: SHIELD™ erhöht die Sicherheit der App auch auf „gebrochenen“ Geräten oder ermöglicht dem App-Anbieter die Ausführung der App in solchen Umgebungen zu verhindern
- Anti-Reverse-Engineering: Die Ausführung der App in Emulatoren und das Anhängen von Debuggern wird unterbunden
- Code Asset Protection / Secure Storage of Keys / Whitebox Cryptography: SHIELD™ verteilt Schlüsselmaterial sicher zwischen Server und App oder legt es sicher in der App ab
- Repackaging-Schutz: Die Nutzung von verfälschten Apps wird verhindert
- Schutz vor „Data Leakage“: SHIELD™ verhindert Keylogging, Screenshots, Screen-Reader und externe Monitore (Screen-Mirroring) während die App ausgeführt wird. Ein Secure Text Field - z. B. für Passwortfelder - nutzt ein neutrales sicheres „In-App-Keyboard“.
- Binding und Obfuscation: Die SHIELD™-Sicherheitsbibliothek wird an die App gebunden und verschleiert den App-Code
- Reporting: SHIELD™ kann sicherheitsrelevante Erkenntnisse an den App-Anbieter weiterleiten
- Overlay-Detection-API: Eine API wird angeboten, um zu erkennen wann und wie die App in die Hintergrund-Benutzung geraten ist; z. B. durch Android-Trojaner.

Über Promon

Die Technologie von Promon stammt aus den international anerkannten Forschungsstätten der SINTEF und der Technischen Universität Oslo. Die patentierte Sicherheits-Technologie von Promon schützt weltweit eingesetzte Banking-Applikationen seit 2009. Die Firma Promon AS ist eine 2006 gegründete norwegische private Aktiengesellschaft. Die Hauptniederlassung befindet sich in Oslo.