accenture

Strategy | Consulting | Digital | Technology | Operations

Accenture Payment Services und Accenture Technology Advisory

PSD2 und Open Banking

Auswirkungen auf Sicherheit und Betrug bei Banken

Sind Sie bereit?

High performance. Delivered.

Inhaltsverzeichnis

HAFTUNGSHINWEIS

Accenture ist ein weltweiter Anbieter professioneller IT-Lösungen und -Dienstleistungen. Die in diesem Dokument geäußerten Ansichten und Meinungen basieren auf der Kenntnis und dem Wissen über das Geschäftsfeld, die Märkte und die Technologie, die Accenture sich angeeignet hat. Die in diesem Dokument enthaltenen Informationen erheben nicht den Anspruch, die genauen Anforderungen der Zahlungsdiensterichtlinie II (engl. „Payment Services Directive 2", PSD2), des Entwurfs zu den technischen Regulierungsstandards (RTS), der Europäischen Datenschutz-Grundverordnung (engl. „General Data Protection Regulation", GDPR) oder sonstiger gesetzlicher oder regulatorischer Bestimmungen darzulegen, und sind nicht als Rechtsauskunft oder rechtliche Auslegung derartiger Bestimmungen zu verstehen. Zur Auslegung der unten stehenden Informationen sowie der besagten Anforderungen, Regeln des Zugangs zu regulierten Zahlungssystemen und zugrunde liegenden Betriebsfunktionen sowie der genauen Art des Zugangs müssen die Leser sich an ihre Rechts- und Finanzberater wenden.

Die PSD2-Richtlinie wurde am 12.01.2016 im Amtsblatt der EU veröffentlicht. Ab diesem Zeitpunkt haben die EU Mitgliedsstaaten zwei Jahre – bis zum 13.01.2018 – Zeit für die Umsetzung in nationales Recht. Bei Erstellung dieses Dokuments stand die förmliche Annahme des am 23.02.2017 von der Europäischen Bankenaufsichtsbehörde (EBA) veröffentlichten finalen Entwurfs der technischen Regulierungsstandards zur starken Kundenauthentifizierung und sicheren Kommunikation durch die EU Kommission noch aus. Nach der Verabschiedung der RTS voraussichtlich bis Ende des 2. Quartals 2017 müssen ab diesem Zeitpunkt u.a. Banken innerhalb die technischen Anforderderungen innerhalb von 18 Monaten umsetzen. Die RTS zur starken Kundenauthentifizierung und sicheren Kommunikation ist der Schlüssel zur Erreichung der Ziele der PSD2: Stärkung des Verbraucherschutzes, Förderung von Innovation und Verbesserung der Sicherheit von Zahlungsdiensten in der gesamten Europäischen Union. Die Datenschutz-Grundverordnung (GDPR) soll im Mai 2018 rechtskräftig werden.


TOUCH TO UNLOCK

Einleitung

Die überarbeitete EU-Zahlungsdiensterichtlinie II (PSD2) wird den Weg für ein neues Zeitalter im europäischen Zahlungsverkehr ebnen. Zu den Kernzielen der PSD2 gehören der bessere Schutz der Verbraucher vor Betrug und die Klärung der Haftungsfrage im Zahlungsverkehrsökosystem. Eine starke Kundenauthentifizierung ist neben einer sicheren Kommunikation der Schlüssel zum Ziel.

Die PSD2 gestattet den Zugriff auf Kundenkonten über Schnittstellen (APIs) und ermöglicht somit ganz neue Arten von Zahlungsdiensten – nämlich die Zahlungsinitiierung durch Dritte, sogenannte Zahlungsauslösedienste oder engl. „Payment Initiation Service Provider" (PISP), und den Kontozugriff über Dritte, sogenannte Kontoinformationsdienste oder engl. Account Information Service Provider" (AISP).

Im Februar 2017 veröffentlichte die Europäische Bankenaufsichtsbehörde (EBA) nach der Konsultationsphase im August 2016 den finalen Entwurf der technischen Regulierungsstandards (RTS), einer Reihe von Mindestanforderungen, die Zahlungsdienstleister (ZDL) oder engl. „Payment Service Provider" (PSP) – einschließlich Banken, die als kontoführende Zahlungsdienstleister (kontoführende PSP) agieren – einhalten müssen.

„Die Sicherheit elektronischer Zahlungen ist von grundlegender Bedeutung für die Gewährleistung des Schutzes der Nutzer und die Entwicklung eines soliden Umfelds für den elektronischen Geschäftsverkehr.

Alle elektronisch angebotenen Zahlungsdienste sollten sicher abgewickelt werden, wobei Technologien einzusetzen sind, die eine sichere Authentifizierung des Nutzers gewährleisten und das Betrugsrisiko möglichst weitgehend einschränken können."

Zahlungsdiensterichtlinie (PSD2), Art. 95

Aus dem finalen RTS-Entwurf der EBA

- Die Authentifizierung erfolgt anhand von mindestens zwei von drei Elementen – Wissen (z. B. Benutzername und Passwort), Besitz (z. B. Smartphone, TAN-Generator), Inhärenz (z. B. Fingerabdruck, Stimme, Iris, Verhaltensmuster).
- „Dynamische Verknüpfung": Der generierte Authentifizierungscode muss mit dem Bezahlbetrag und dem Zahlungsempfänger spezifisch verknüpft im gesamten Authentifizierungsprozess dem Bezahler angezeigt werden.
- „Unabhängigkeit der Känale" oder „Kanaltrennung": Der Authentifizierungscode darf nicht über den gleichen Kanal empfangen werden, der für die Initiierung der Transaktion verwendet wurde (z. B. Nutzung einer separaten mobilen Anwendung in einer sicheren Laufzeitumgebung innerhalb des gleichen Geräts oder eines komplett anderen Geräts).
- Zwei-Faktor-Authentifizierungsmechanismus zwischen autorisiertem Drittanbieter (PISP, AISP) und kontoführender Bank: Die EBA schlägt die Nutzung von Websitezertifikaten (eSeals) vor, die auf Grundlage des eIDAS-Rahmenwerts von qualifizierten Trust-Service-Anbietern (TSP) ausgestellt werden. Laut EBA wird voraussichtlich vor Oktober 2018 noch kein nach eIDAS qualifizierter TSP zur Verfügung stehen.
- In den technischen Regulierungsstandards (RTS) sind Ausnahmen für die Durchführung einer starken Kundenauthentifizierung festgelegt, sodass nicht bei jeder Transaktion Authentifizierungscodes vom Nutzer gefordert werden: Für PISP sind diese u.a. Transaktionsrisikoanalyse, Kleinstbeträge und Tickets und für AISP der Zugang auf Kontodaten für 90 Tage nach einmaliger starken Authentifizierung. Durch diese Ausnahmen für PISP, AISP und kontoführenden Banken steigt die Benutzerfreundlichkeit.
- Banken müssen autorisierten Drittanbietern ihre Zahlungs- und Kernbankensysteme unter Nutzung des ISO 20022 Datenformat für Finanznachrichten in Form von APIs öffnen.
- Bankenspezifische technische Spezifikationen, Arbeitsabläufe, Tools und Beispiele sind auf der Webseite der Bank kostenlos für autorisierte Drittanbieter zum Download bereitzustellen.
- Die APIs mit den zugrundeliegenden Dienstleistungen der Bank (Zahlungsinstrumente, Kontoinformation) müssen für die autorisierten Drittparteien gemäß denselben Service Level Agreements bereitgestellt werden, wie dies bei den eigenen Diensten der Bank, z. B. beim Onlinebanking, der Fall ist.

Starke Kunden-authentifizierung – Was versteht man darunter?

Laut RTS basiert eine starke Kundenauthentifizierung auf zwei oder drei Elementen, die unabhängig voneinander sind. Zusätzlich zu dieser Authentifizierung fordert die PSD2 von PSP die Einrichtung von Sicherheitsmaßnahmen, durch die die Vertraulichkeit und die Integrität der persönlichen Anmeldedaten der Zahlungsdienstnutzer (ZDN) sichergestellt wird, wenn der Zahlende:

Als starke Kundenauthentifizierung gilt eine Authentifizierung, die anhand von zwei oder mehr Elementen erfolgt:

a) online auf sein Zahlungskonto zugreift,

b) einen elektronischen Zahlungsvorgang initiiert,

c) über einen Remotekanal irgendeine Aktion ausführt, die mit dem Risiko eines Zahlungsbetrugs oder sonstigen Missbrauchs einhergeht.

Bei Initiierung von elektronischen Remote-Zahlungsvorgängen fordert die PSD2 u.a. von Banken erneut die Anwendung einer starken Kundenauthentifizierung. Zur Authentifizierung sind Elemente zu nutzen, die die Transaktion dynamisch mit einem bestimmten Betrag und einem bestimmten Zahlungsempfänger verknüpfen.

Ausnahmen von einer starken Kunden-authentifizierung

In Ausnahmefällen erlaubt die RTS, auf eine starke Kundenauthentifizierung zu verzichten. Ausschlaggebend sind dabei folgende Kriterien:

a) Risiko, das mit dem Dienst einhergeht (z.B. Transaktionsriskoanalyse)

b) Betrag und/oder Wiederholung der Transaktion (Bagatellgrenzen für kontaktlose Bezahlung oder Kleinstbeträge)

c) Zahlungskanal, über den die Transaktion ausgeführt wird (z.B. Fahrkarten und Parktickets am Automaten, E-Commerce-Zahlungen oder kontaktlosem Terminal)

Die PSD2 verlagert auch die Haftung: Dienstleister, die keine angemessene Authentifizierung anbieten, haften nun für sämtliche daraus resultierenden Verstöße.

In Fällen, in denen der PSP (z.B. die kontoführende Bank), den der Zahlende nutzt, keine starke Kundenauthentifizierung fordert, werden finanzielle Verluste dem Zahlenden nur dann aufgebürdet, wenn er in betrügerischer Absicht gehandelt hat.

In Fällen, in denen der Zahlungsempfänger – oder der PSP des Zahlungsempfängers – eine starke Authentifizierung nicht akzeptiert, hat er für die finanziellen Verluste, die dem PSP des Zahlenden entstehen, aufzukommen.

Des Weiteren gibt die RTS den Verzicht auf starke Kundenauthentifizierung bei Kontoinformationsdiensten für einen bestimmten Zeitraum vor.

Demzufolge erhalten AISP-Drittanbieter nach einmaliger starken Kundenauthentifizierung und Kundenzustimmung Zugang auf die Transaktionshistorie für 90 Tage. Diese Öffnung für einen relativ langen Zeitraum kann bei unzureichenden Schutzmaßnahmen zu Daten- und Identitätsdiebstahl und schnell zum Verstoß gegen die GDPR führen.

Schlüsselfrage

Die Kundenauthentifizierung muss über mindestens zwei von drei verschiedenen Elementen erfolgen. Haben Sie bereits entschieden, welche Elemente Sie wie nutzen werden?

Digitale Identität

Kundenauthentifizierung

Selbst nach Veröffentlichung des finalen RTS-Entwurfs der EBA bleibt unklar, wie die Authentifizierungstechnologien letztendlich aussehen werden. Accenture erwartet jedoch, dass sich eine standardisierte, einfache und benutzerorientierte Authentifizierungsmethode wie OAuth 2.0 und ihre Erweiterung OpenID Connect durchsetzen werden. Diese ermöglichen die Authentifizierung und Autorisierung, ohne dem PSP dabei die Anmeldedaten des Nutzers preiszugeben.

Praktisch umsetzen werden dies die meisten Banken wahrscheinlich, indem sie sich als ersten Faktor auf ein Wissenselement, z.B. eine PIN oder ein Passwort, verlassen und dann zwischen „Besitz" und „Inhärenz" oder eine Kombination aus beidem als zweitem Faktor wählen.

Der RTS-Entwurf hat zur Verunsicherung über das zweite Element "Besitz" geführt. Die Unabhängigkeit der Kanäle spielt in einer Multikanalumgebung eine entscheidende Rolle, vor allem in einem mobilen Ökosystem mit Desktopcomputern, mobilen Geräten und mobilen Anwendungen. Der Authentifizierungscode darf nicht über den Kanal übermittelt werden, über den der Kunde das Authentifizierungsverfahren ausgelöst hat.

Banken werden den Schwerpunkt auf besitzbasierte Lösungen legen, bei denen die Initiierung des Authentifizierungsvorgangs und der Empfang des Authentifizierungscodes über dasselbe Gerät erfolgen. Die technische Trennung der unterschiedlichen Authentifizierungselemente auf diesem Gerät wird dabei eine wichtige Rolle spielen. Banken sollten sie deshalb bei der Umstrukturierung ihrer Authentifizierungsmethoden berücksichtigen.

Die besitzbasierte Lösung wäre zwar – unabhängig von den damit einhergehenden Herausforderungen – technologisch stark, bietet aber evtl. nicht das erforderliche Maß an Präzision. Deshalb prüfen viele Banken die Möglichkeit, Inhärenz als zweiten Authentifizierungsfaktor zu nutzen.

Schlüsselfrage

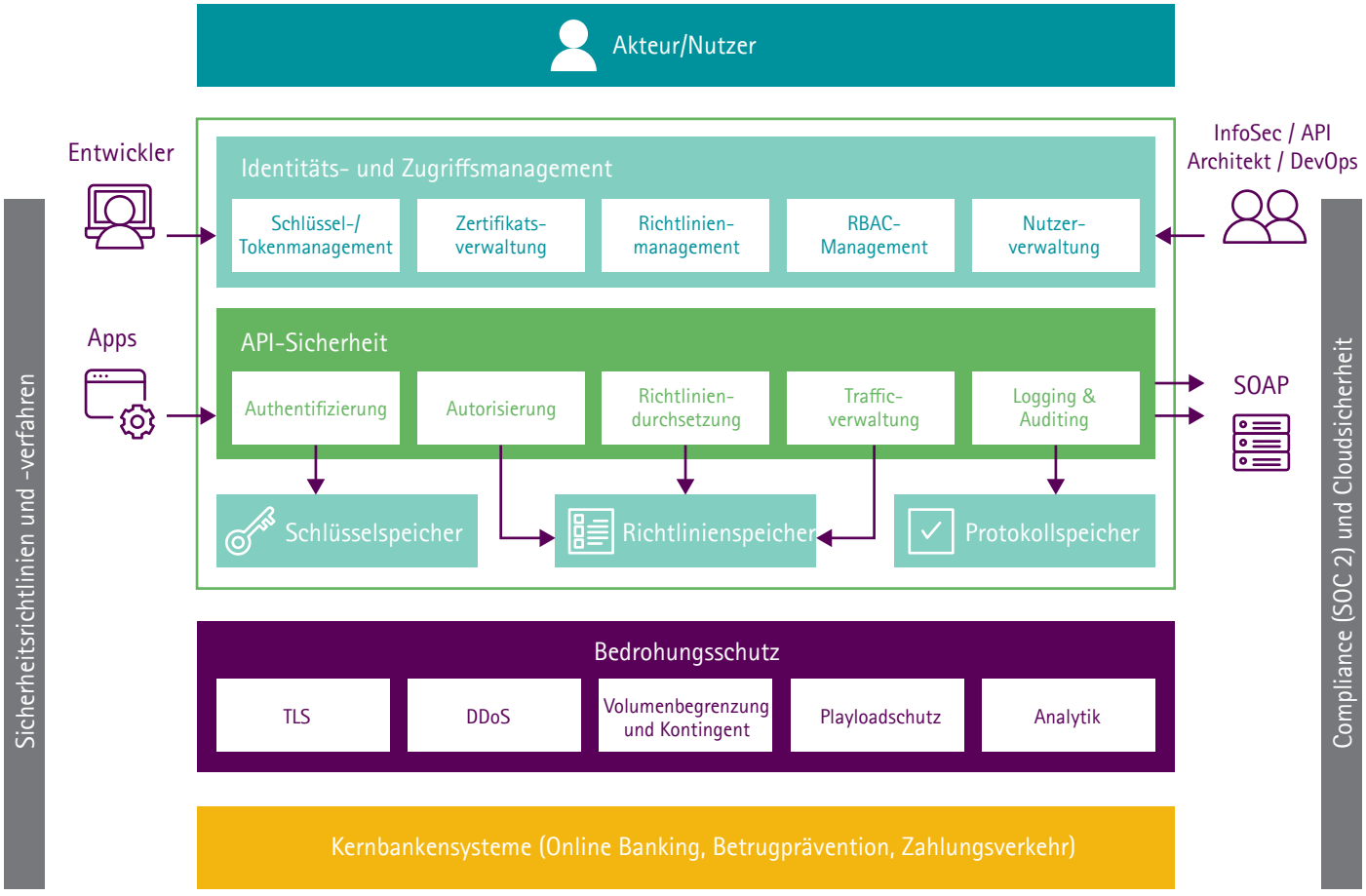
Ausgehend vom finalen RTS-Entwurf ist es wahrscheinlich, dass OAuth 2.0/OpenID Connect das bevorzugte Authentifizierungsprotokoll wird. Die Anforderungen an besitzbasierte Authentifizierungsmethoden sind strenger geworden. Ist Ihre Organisation vor diesem Hintergrund für eine OAuth-basierte Kunden-/Drittanbieter-Authentifizierung und besitzbasierte Authentifizierungsmethoden, die eine technische Trennung ermöglichen, gewappnet?


Off
On

Cybersicherheit

Banken stellen Drittanbietern ihre APIs zur Verfügung und bieten somit für potentielle Cyberkriminelle eine wesentlich größere Angriffsfläche an. Sie können kritische Anwendungen somit nicht länger hinter Perimeter-Firewalls verstecken. Banken, deren Architektur auf einem soliden Ansatz basiert, können dieses Risiko bewältigen, indem sie Sicherheitsvorkehrungen in grundlegende Geschäftsfaktoren und -szenarien integrieren.

Damit kann gewährleistet werden, dass die Sicherheitsprozesse anpassbar sind und so entsprechend auf Bedrohungen reagiert werden kann. Gleichzeitig werden die Sicherheitsprozesse auf diese Weise eng mit den Geschäftsauswirkungen verknüpft.
Im Folgenden ist eine solide Referenzarchitektur dargestellt für die APIs einer Bank:



API-Sicherheit und -Management

Die API-Sicherheit sollte ein integraler Bestandteil der API-Implementierung sein. Dazu muss die API-Architektur aus einem anderen Blickwinkel als bisher betrachtet werden. APIs galten ursprünglich als „vertrauenswürdige" bilateral vereinbarte B2B-Kommunikationsschnittstellen. Das heißt, man setzte einen geringeren Fokus auf starke Sicherheitsmechanismen als in den Bereichen mit direktem Kundenkontakt – wie z. B. dem Onlinebanking. Die Devise sollte stattdessen jedoch lauten: Misstrauen statt Vertrauen. In diesem Sinne sollten bei APIs ähnliche Sicherheitskontrollen vorgesehen werden wie beim digitalen Banking. Mit einer derart soliden und robusten Architektur sind APIs für die Zukunft gewappnet. Diese verstärkte Sicherheit sollte folgende Aufgaben wahrnehmen:

- Zugriffskontrolle
- Bedrohungserkennung
- Datenschutz
- Wahrung der Integrität

Innerhalb dieser Architektur ist bei der Entwicklung von APIs der Schutz vor Distributed-Denial-of-Service-Attacken (DDoS) zu berücksichtigen. Diese Bedrohung stellt glücklicherweise jedoch auch eine Chance dar.

Da die Entwicklung von Systemen mit offenen Schnittstellen für viele Organisationen praktisch „auf der grünen Wiese" stattfindet, bietet sie eine einmalige Chance, gleich von Anfang an alles richtig zu machen. Angriffe sollten direkt auf einer hohen Ebene abgewehrt und so die Informationen geschützt werden, die sich auf einer niedrigeren Ebene befinden.

Authentifizierung und Autorisierung	Nutzen Sie zur App-Authentifizierung möglichst wenige API-Keys und beschränken Sie den Zugriff der Apps lediglich auf die notwendigen und erlaubten Ressourcen. Nehmen Sie die Standardauthentifizierung ggf. über einen Autorisierungsheader für die Nutzerauthentifizierung vor.
Contentbasierte Angriffe	Schützen Sie sich vor verschiedenen Arten von contentbasierten Angriffen wie z. B. vor Bedrohungen in Form von schadhaften XML-Dateien, schadhaften JSON-Dateien und schadhaften „Injection"-Skripten.
Datenverschlüsselung	Verwenden Sie eine Transportschichtverschlüsselung wie TLS, um eine sichere Kommunikation zu gewährleisten. Sämtliche sensiblen Nachrichten in der API sind durch Verschlüsselung auf Nachrichten-/Feldebene zu schützen.
Identitätstracking	Die Nutzerinformationen und/oder die App-IDs sollten für das Identitätstracking anhand von Richtlinien innerhalb des Datenflusses protokolliert werden.
Nachrichten-validierung	Nutzen Sie Datenmaskierungsrichtlinien, um sensible Daten beim Protokollieren zu anonymisieren. Zum Schutz der APIs sollte das Prinzip „Validierung vor Nutzung" verfolgt werden.
Traffic-Verwaltung	Nutzen Sie Richtlinien zur Traffic-Verwaltung, um zu verhindern, dass die Infrastruktur überlastet wird. Implementieren Sie eine Drosselung sowie die Limitierung des Traffics auf die für eine App in einem bestimmten Zeitraum erlaubten Anfragen.

Anpassung an die Europäische Datenschutz-Grundverordnung (GDPR)

Mit Einführung der neuen Datenschutz-Grundverordnung (GDPR) der EU wird sich die Risikolandschaft nachhaltig verändern. Dieser Wandel wird mit neuen Anforderungen rund um Haftung, Dokumentation, Datenschutzüberprüfung und -konzepte sowie der Verhängung sehr hoher Strafen im Falle der Nichteinhaltung einhergehen.

Diese Änderungen kommen zu einem Zeitpunkt, zu dem viele Banken bereits vor Herausforderungen wie dem mangelnden Verständnis der Daten in ihren Organisationen, dem Anstieg des Volumens und des Ausmaßes von Cyberangriffen sowie öffentlichen Bedenken hinsichtlich des Themas Datenschutz stehen. Ab Mitte 2018 findet nun die GDPR Anwendung. Darüber hinaus wurden im Kontext des EU-US-Datenschutzschilds Initiativen zur Vereinheitlichung der Datenschutzregelungen in der EU und dem EWR angestoßen. All dies wirkt sich auf die genannten Herausforderungen aus, die in einigen Fällen dadurch noch wachsen dürften.

Der deutsche Gesetzgeber hat nach den ersten Lesungen des GDPR-Referentenentwurfs die Umsetzung in nationales Recht in die Wege geleitet. Aktuell wird mit dem deutschen Umsetzungsgesetz nach Konsultationen im Bundesrat mit der Veröffentlichung im Bundesgesetzblatt im Mai 2017 gerechnet.

Diese Regulierungswelle stellt – gepaart mit dem Übergang zu offenen Bankenschnittstellen unter der PSD2 – eine weitere große Chance dar, APIs von Grund auf so zu entwickeln, dass Datenschutz und Sicherheit maximiert werden. Bei der Entwicklung von APIs sollten Banken eine Reihe von Prinzipien berücksichtigen. Dazu gehören folgende:

Datenschutz ins Design integrieren
Datenschutz nicht als Add-on, sondern als fester Bestandteil eines jeden IT-Systems.

Proaktiv statt reaktiv
Versuchen Sie Ereignisse vorherzusehen, die die Privatsphäre gefährden, und beugen Sie diesen vor, statt im Nachhinein Schadensbegrenzung zu betreiben.

Maximale Privatsphäre als Standardeinstellung
Schützen Sie sämtliche personenbezogenen Daten.

Volle Funktionalität: Gewinn anstelle von Nullsummenspiel
Vermeiden Sie unnötige Kompromisse zwischen Privatsphäre und Sicherheit.

Sichtbarkeit und Transparenz
Die Transparenz der Komponenten, der Prozesse und des Betriebs in jedem IT-System sollten wie vereinbart gewährleistet sein.

Respekt vor der Privatsphäre der Nutzer
Integrieren Sie einen starken Datenschutz und einen entsprechenden Datenschutzhinweis.

Zustimmungsbasierte Verfügbarkeit
Zeigen Sie Informationen nur an, wenn der Nutzer seine Zustimmung zu einer bestimmten Aktion gegeben hat.

Geordnete Abschwächung statt Kollaps
Ein System sollte auch dann noch bestmöglich laufen, wenn einzelne Funktionen nicht mehr nutzbar sind.

Prinzip der Minimierung
Es sollte nicht möglich sein, auf mehr Informationen als absolut notwendig oder als der Nutzer gestattet hat, zuzugreifen.

Betrug und Finanzkriminalität

Unter PSD2 implementieren Banken APIs und öffnen ihre Infrastruktur für Drittanbieter. Dies könnte Betrügern jede Menge Angriffsfläche bieten – und das zu einem Zeitpunkt, zu dem Banken aufgrund von Betrug bereits beträchtliche Summen verloren haben und sich in einem Wettrüsten mit immer raffinierteren Cyberkriminellen befinden.

Mit PSD2 ändern sich die Regeln des Sicherheitsspiels deutlich. Die aktuellen Systeme der Banken gehen davon aus, dass Kunden direkt mit ihnen interagieren. Das bedeutet, dass der Bank selbst alle Informationen vorliegen, die notwendig sind, um festzustellen, ob eine Transaktion mit betrügerischer Absicht erfolgt. Unter PSD2 loggen sich viele Verbraucher nicht länger beim Onlinebanking ihrer Banken ein. Dadurch reduziert sich die Menge der relevanten Daten, die den Banken zur Verfügung stehen.

Drittanbietern eine sichere Infrastruktur zu bieten, stellt für Banken vor diesem Hintergrund eine enorme Herausforderung dar. Um Betrug in Echtzeit vorzubeugen, nutzen die meisten Banken Softwarepakete, deren Scoringmodelle über einen Zeitraum von 18 bis 24 Monaten trainiert werden. Nachdem mit der PSD2 neue Transaktionen über Drittanbieter eingeführt werden, wird es rund zwei Jahre dauern, bis die Banken Scores generieren können, die aussagekräftige Informationen über das Transaktionsrisiko liefern.

In der Zwischenzeit werden die Betrugsanalyseabteilungen von Banken die Transaktionen proaktiv im Auge behalten und ihre eigenen Regeln entwickeln müssen, um Betrug vorzubeugen. Gemäß der PSD2 können Banken Drittanbietern den Zugriff auf Konten verwehren, wenn es Hinweise darauf gibt, dass die Aktivität unautorisiert oder mit betrügerischer Absicht erfolgt. Es könnte gut sein, dass sie von dieser Möglichkeit Gebrauch machen müssen, wenn die PSD2 Anwendung findet.

Schlüsselfrage

Leidet Ihr Unternehmen unter Silos in der Betrugsprävention? Haben Sie überlegt, welche Auswirkungen auf Betrugspräventionsengines es in der neuen Umgebung haben könnte, dass E-Commerce-Transaktionen zum Risikoscoring in digitale Kanäle ohne E-Commerce-Erfahrung fließen? Ziehen Sie es in Erwägung, eine Schicht zur Betrugsbekämpfung direkt zu integrieren?

Inhärenzoptionen: Profiling anhand biometrischer Daten und des Verhaltens

Mit Inhärenz als zweitem Authentifizierungsfaktor wird gleich zwei Prioritäten der PSP entsprochen – Sicherheit und Nutzererfahrung. Eine bereits weit verbreitete Form der Inhärenz ist die biometrische Authentifizierung. Diese ist verbraucherfreundlich in Echtzeit möglich, kann einfach implementiert werden und wird den Forderungen der PSP nach einer präziseren Validierung gerecht.

Durch all dies sinkt das Risiko eines Identitätsbetrugs. Dies erklärt, warum biometrische Technologien, üblicherweise in Kombination mit Passwörtern, Einzug in mobile Endnutzergeräte halten.

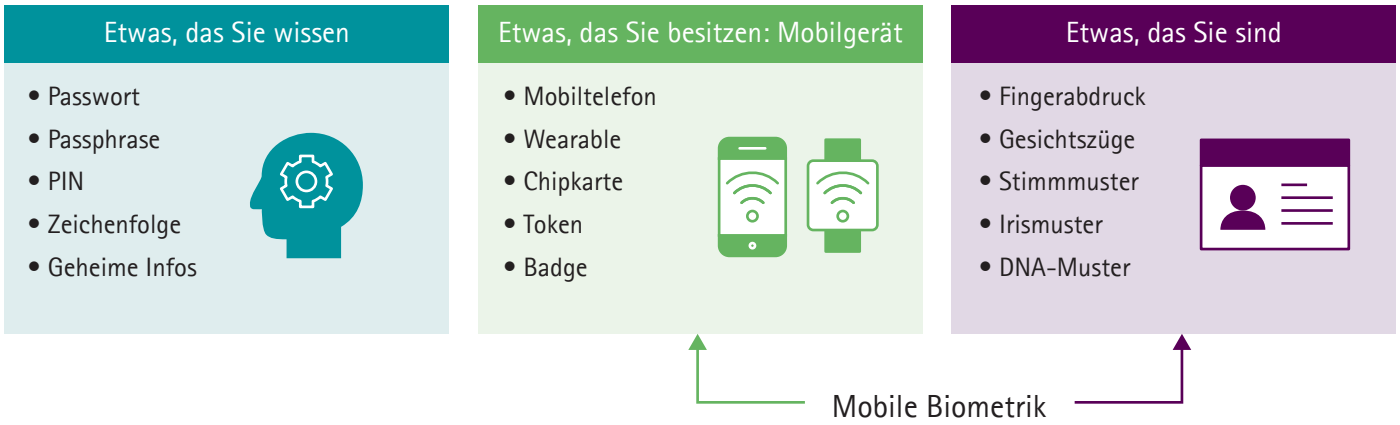
Die Verhaltensprofilierung stellt eine weitere wichtige Art der Authentifizierung über Inhärenz dar. Banken können sich ein besseres Bild vom Risiko und dem erforderlichen Authentifizierungsgrad machen, indem sie den Aufenthaltsort und das Verhalten des Kunden mit dessen üblichen Mustern abgleichen.

Und da die Verhaltensprofilierung im Hintergrund läuft, ist sie für die Nutzer nicht sichtbar und behindert daher die Customer Journey nicht.

Verhaltensprofilierung ist ein vergleichsweise neuer Mechanismus, der sich aktuell noch im Reifungsprozess befindet. Zum gegebenen Zeitpunkt eignet sie sich eher als Ergänzung zur Verstärkung der Betrugskontrollen denn als eigenständiger Authentifizierungsmechanismus.

Schlüsselfrage

Lässt sich die Authentifizierungsarchitektur Ihrer Organisation ergänzen und erweitern, sodass sie auch zukünftige Innovationen im Bereich der Authentifizierungstechnologien und -techniken unterstützen kann?



Schlussfolgerung

Angesichts der anstehenden Einführung der PSD2 und der Implementierung der RTS-Anforderungen ist es für alle Akteure im sich wandelnden Zahlungsökosystem – nicht zuletzt für Banken – unerlässlich, über eine spezifische PSD2-Sicherheitsstrategie zu verfügen.

Die gute Nachricht ist: Die PSD2 bietet Organisationen die einmalige Gelegenheit, Sicherheit von Grund auf in neue Systeme und APIs zu integrieren. Sicherheit wird damit zu einem Asset für die Organisation.

Wer die Chancen nutzen will, muss einen Mentalitätswandel vollziehen – von der compliancefokussierten Einstellung zum Thema Sicherheit hin zu einer echten Strategie für Cybersicherheit. Sicherheit ermöglicht Banken sich im Zentrum des Alltagslebens ihrer Kunden zu positionieren. Dies wird sich in den drei zentralen Rollen widerspiegeln, die Banken einnehmen, nämlich der des Vermittlers, der des Beraters und der des Wertschöpfers.

Damit diese Reise ein Erfolg wird, müssen die Sicherheitsteams der Banken sich kontinuierlich anpassen, um mit den sich weiterentwickelnden Geschäftszielen Schritt halten zu können. Das PSD2-Zeitalter rückt näher – es ist Zeit, sich an die Arbeit zu machen.

Bank als Berater

Geben Sie Ihren Kunden ausgehend von Ihrer fundierten Kundenkenntnis und Kaufalgorithmen Kaufempfehlungen

Sicherheit als Motor

Sichere und digitale Identitäten ermöglichen eine genaue, vertrauenswürdige und kontinuierliche Analyse und die Erstellung eines 360°-Überblicks über den Kunden

Bank als Zugriffsvermittler

Unterstützen Sie den Kunden bei der Kaufabwicklung im Alltag – überall (Einkauf, Zugriff auf alltägliche Dienste)

Sicherheit als Motor

Durch Reduzierung des Betrugs- und Bedrohungsrisikos bei gleichzeitigem Anstieg des Compliancevertrauens wächst das Vertrauen des Kunden; dank Kundenbindung und -treue werden kundenorientierte Geschäftsabläufe effektiver

Bank als Wertschöpfer

Stellen Sie verschiedene Komponenten (finanzielle und nichtfinanzielle, eigene und Drittparteiangebote) so zusammen, dass eine integrierte Lösung entsteht, die den echten Bedürfnissen der Kunden gerecht wird

Sicherheit als Motor

Sicheres Verhaltensprofiling ermöglicht Echtzeitmanagement und Präzision der Kundeninteraktion


Password

QUELLEN

1. https://iconewsblog.wordpress.com/2016/10/31/how-the-ico-will-be-supporting-the-implementation-of-the-gdpr/

KONTAKT

Dr. Martin Bentele
Managing Director, Acenture
Leitung des Bereichs Payments
martin.bentele@accenture.com

Hakan Eroglu
Senior Manager, Accenture
Leitung des Bereichs Digital Payments, PSD2/API Banking
hakan.eroglu@accenture.com

ÜBER ACCENTURE PAYMENTS

Accenture Payments unterstützt Banken sowie Zahlungsdienstleister und -abwickler aus Nichtbankensektoren dabei, ihre Geschäftsstrategie, Technologie und betriebliche Effizienz in puncto Kleinbetragszahlungen, geschäftlicher Zahlungsverkehr und Transaktionsbanking, Kartenzahlungen, digitaler Zahlungsverkehr und Innovation, Compliance und operative Prozesse zu optimieren. Accenture verfügt über 4.500 Experten, die Zahlungsdienstleistern und -abwicklern dabei helfen, eine Strategie zu entwickeln, sich in der digitalen Wirtschaft neu zu positionieren (inkl. Einsatz offener APIs, von Clouddiensten, Echtzeit- und Blockchaintechnologie sowie Finanztechnologie), neue mobile und digitale Dienste zu entwickeln, Zahungen als Umsatzgenerator zu nutzen, Kosten zu senken und ihre Produktivität zu steigern, neue gesetzliche Vorschriften einzuhalten sowie ihre Zahlungssysteme und -abläufe zu integrieren. Accenture hat bereits einige führende Zahlungsdienstleister und -abwickler dabei unterstützt, aus Zahlungsabwicklung ein effizientes Geschäft zu machen. Besuchen Sie uns unter **www.accenture.de/payments**, um mehr zu erfahren.

FINANCIAL SERVICES TECHNOLOGY ADVISORY – BERATUNG FÜR FINANZDIENSTLEISTER

Wir beraten unsere Kunden zum aktuellen Technologiewandel in der Finanzbranche und unterstützen sie dabei, sich an diesen anzupassen – vom Cognitive Computing bis hin zu Cybersicherheit, von der Anwendungsrationalisierung bis hin zu Kryptowährungen, vom Software-defined Networking bis hin zum DevOps-Einsatz. Wie auch andere Accenture-Sparten bietet Technologie Advisory den kompletten Delivery-Lifecycle – von der Beratung zu Strategien und Trends im Finanzdienstleistungssektor bis hin zur Umsetzung großer Transformationsprojekte. Mit ihren Fachkompetenzen und ihrer umfassenden Erfahrung helfen unsere Berater unseren Kunden dabei, Herausforderungen zu meistern. Wir regen Finanzdienstleister dazu an, bei den neusten Technologietrends einen Blick über Branchengrenzen zu werfen, und sind für CIOs, CTOs und CDOs der richtige Ansprechpartner, wenn sie auf der Suche nach den neusten Erkenntnissen sind.

ÜBER ACCENTURE

Accenture ist ein weltweit führendes Dienstleistungsunternehmen, das ein breites Portfolio von Services und Lösungen in den Bereichen Strategie, Consulting, Digital, Technologie und Operations anbietet. Mit umfassender Erfahrung und spezialisierten Fähigkeiten über mehr als 40 Branchen und alle Unternehmensfunktionen hinweg – gestützt auf das weltweit größte Delivery-Netzwerk – arbeitet Accenture an der Schnittstelle von Business und Technologie, um Kunden dabei zu unterstützen, ihre Leistungsfähigkeit zu verbessern und nachhaltigen Wert für ihre Stakeholder zu schaffen. Mit rund 401.000 Mitarbeitern, die für Kunden in über 120 Ländern tätig sind, treibt Accenture Innovationen voran, um die Art und Weise, wie die Welt lebt und arbeitet, zu verbessern. Besuchen Sie uns unter www.accenture.de.

TRETEN SIE MIT UNS IN DEN DIALOG

Accenture Banken Blog
bit.ly/Banken DACH

Accenture Finanzdienstleistungen DACH – Twitter
bit.ly/TweetFS

Accenture Finanzdienstleistungen DACH – LinkedIn
bit.ly/Link-FS

Accenture Finanzdienstleistungen DACH – XING
bit.ly/XING-FS

LESEN SIE UNSERE AKTUELLEN STUDIEN

Accenture.de/banken