Link: https://www.cio.de/a/banken-lagern-identitaetspruefung-in-die-videocloud-aus,2974965

Credentials as a Service

Banken lagern Identitätsprüfung in die Videocloud aus

Datum: 24.10.2014
Autor(en): Lothar Lochmaier

Warum nicht das neue Giro- oder Tagesgeldkonto mit ein paar Mausklicks eröffnen? Credential Service-Provider helfen als externe Dienstleister per Videochat und kümmern sich für die Banken um Authentifizierung und Passwortverwaltung der Nutzer.

Warum nicht das Mobiltelefon als Drehscheibe für die persönliche Neuanmeldung eines Bankkontos einsetzen? Dafür gibt es neuerdings Credential Service Provider. Zum Hintergrund: Der englische Begriff "credentials" beschreibt die sichere und datenschutzkonforme Authentifizierung des Nutzers anhand seiner individuellen Zugangsdaten. Schließlich liegt es längst im Trend, die Bankgeschäfte auch bequem von unterwegs aus mit dem Smartphone zu erledigen.

All dies ist keine Zukunftsmusik mehr: Denn die neue Bankverbindung einzurichten, das dauert nur wenige Minuten. Gerade für Technologie affine Nutzer dürfte das umständliche Postident-Verfahren zur Legitimation ausgedient haben. Die Direktbank ING-DiBa bietet jedenfalls seit kurzem die Eröffnung eines neuen Bankkontos - und die damit verbundene Authentifizierung für das Online-Banking - auch per Video-Chat an.

Der ganze Vorgang läuft bequem und direkt über das Smartphone. Den Prüfjob zum Ausweisdokument einschließlich der dazu gehörigen biometrischen Gesichtsmerkmale übernimmt dabei ein externer Dienstleister komplett in Eigenregie, übrigens auch an den Wochenenden, wenn die Postfiliale geschlossen hat.

Das funktioniert wie folgt: Um sich zu identifizieren, wird der Kunde über die Bankapplikation im Netz zunächst aufgefordert, einen gültigen Personalausweis oder Reisepass mit Vorder- und Rückseite vor die Webkamera zu halten.

Danach heißt es, den Ausweis vor der Webkamera mehrfach zu kippen und so zu bewegen, dass sich die relevanten Sicherheitsmerkmale wie ein Hologramm überprüfen lassen. Zudem erfasst der externe Dienstleister die Ausweisnummer und fertigt Fotos vom Kunden an.

Danach erhält der Antragsteller per E-Mail oder SMS eine Transaktionsnummer (TAN), um im Netz die Legitimation für das neue Konto zu bestätigen. Und los kann es mit dem bequem eingerichteten Online-Banking gehen.

Ausweis oder Reisepass

Derzeit ist die Video-Legitimation zwar nur für Kunden mit deutschem Ausweis oder Reisepass möglich. Die ING-DiBa möchte diesen Dienst aber nach und nach auch auf das Ausland ausweiten. Insbesondere Neukunden möchte die mit rund acht Millionen Kunden größte deutsche Direktbank so ansprechen. Darüber hinaus soll die Video-Legitimation künftig auch für andere Produkte möglich sein.

Einen ähnlichen Weg geht auch Deutschlands bekanntestes Finanzinstitut für die (Online-)Honorarberatung namens Quirion. Dort ist die Depoteröffnung mit Hilfe der Videolegitimation in Echtzeit möglich, in diesem Fall über den Videodienst Skype. Auch hier fungiert wie bei der ING-DiBa der Münchner Lösungsspezialist WebID Solutions als externer Dienstleister, sprich Credential Service Provider.

"Quirion zeigt mit dieser Weiterentwicklung, dass es die Bedürfnisse seiner Kunden verstanden hat", argumentiert Karl Matthäus Schmidt, Vorstandsvorsitzender der Online-Honoraranlageplattform. Durch den zeitgemäßen Ansatz hofft das Institut, neben seinen Produkten auch mit Hilfe von innovativen und bequem handhabbaren Sicherheitslösungen bei seiner aufgeschlossenen Kundenklientel zu punkten.

Ein weiteres Beispiel, wie sich dieses Prinzip auch für weitere Bankdienstleistungen nutzen lässt, stellt Western Union dar, einer der führenden, global operierenden Spezialisten für Geldtransfer-Dienstleistungen. Dort können die Nutzer sich direkt mit ihrer Kreditkarte über die Web- oder Handykamera für einen Bezahlvorgang authentifizieren, anstatt die Daten händisch einzugeben.

Bequeme und sichere Lösungen

Doch wie ist es um die Risiken bestellt, über eine Drittpartei zum Einfallstor von Computerhackern zu werden? "Ein sicheres Passwortmanagement bei der Nutzung von cloud-basierten Diensten bleibt gerade für die durch kriminelle Akteure besonders im Visier stehende Bankenbranche absolut unverzichtbar", betont Volker Fischer, Leiter Geschäftsentwicklung Financial Services bei HP Deutschland.

Angefacht durch den weiter grassierenden Diebstahl von Passwörtern sind auch in Europa die rechtlichen Vorgaben beim mobilen Bezahlen in jüngster Zeit erheblich verschärft worden. Gefragt sind neben ausgereiften technischen Lösungen vor allem Gesetzes konforme Konzepte, etwa zu europäischen Vorgaben wie SecuRePay, der Zahlungsdiensterichtlinie und der EU-Datenschutzrichtlinie. Zusammengefasst: Ausgeschlossen sind insbesondere Zahlungen, bei denen lediglich ein Internetbrowser oder eine Applikation zum Online-Banking über das mobile Endgerät aufgerufen wird.

"Um den Vertrauensvorsprung der Banken gegenüber den Anbietern von E-Commerce-Dienstleistungen zu wahren, genießt deshalb vor dem Hintergrund der digitalen Wachstumsagenda die Weiterentwicklung von zentralen Sicherheitsmechanismen hohe Priorität", gibt IT-Experte Volker Fischer von HP zu bedenken.

Als praxisnahe Referenz, welche Dynamik eine neue Bankeninitiative entwickeln kann, nennt der Experte den lokalen de-facto-Branchenstandard für das Mobile Payment in Polen, auf den bereits über 20 Banken und Payment Service Provider setzen. Eine neue Bankeninitiative www.polskistandardplatnosci.pl soll nun bereits zum Jahresende rund 1,5 Millionen Nutzer aufweisen.

Was Credential Service Provider leisten

Parallel dazu wächst die Zahl der IT-Dienstleister weltweit, die sich auf das Passwortmanagement und die Identitätsverwaltung in der Cloud spezialisiert haben. Gefragt sind verlässliche "Credential Service Provider", sowohl beim Privatkunden als auch professionellen Anwendern in den Unternehmen.

Die Lösungsspezialisten wie Passwordsafe, LastPass, KeePass, Roboform oder Open Source Safe ermöglichen dabei nicht nur das sichere Verwalten der unterschiedlichen Benutzerlogins. Die externen Dienste sorgen auch dafür, dass der Anwender in der Lage ist, sichere Passwörter zu generieren und letztlich auch richtig einzusetzen.

Darüber hinaus offerieren einige IT-Sicherheitsspezialisten wie F-Secure neuerdings, angetrieben durch die jüngsten Datenschutzskandale, cloud-basierte Speicherdienste für die sichere Passwortumgebung. Der Clou: Der Zugang für die professionell geschützten Anwender erfolgt in diesem Fall verschlüsselt über einen Masterkey. Dadurch seien alle Daten ausschließlich auf Servern innerhalb der Europäischen Union gespeichert, betont der Anbieter.

Welchen Standards sollte der externe Dienstleister genügen? "Der Credential Service Provider stellt im Idealfall ein zertifizierter, sprich von den Aufsichtsbehörden kontrollierter und unabhängiger Systemspezialist dar, insbesondere mit Blick auf spezifische gesetzliche Rahmenwerke in der Bankenbranche wie die PCI Compliance", regt Volker Fischer von HP Deutschland an.

Um den hohen Sicherheitsvorgaben im Finanzsektor Stand zu halten, benötigten die Banken außerdem generell ein konzeptionell schlüssiges System, um technische Backendfunktionen und alle relevanten Transaktionskanäle verlässlich miteinander zu verbinden, gibt der Experte zu bedenken.

Wasserdichte Sicherheitsarchitektur minimiert Einfallstore

Um generell die Sicherheit bei Transaktionen über mobile Kanäle zu erhöhen, benötigen aber sowohl die Banken als auch die am Wertschöpfungsprozess beteiligten externen Dienstleister mittel- bis langfristig eine technisch ausgereifte Sicherheitsarchitektur. Schließlich gibt es in der weit verzweigten Finanzbranche eine fast unübersichtliche Zahl an Applikationen und Dateninseln, die es zu schützen gilt.

"Das von Hewlett Packard entwickelte moderne Ökosystem 'Technologies for Payment' bildet die zentrale Schnittstelle für alle Aktivitäten, konform zu einer bereits existierenden Infrastruktur für mobile Endgeräte, und zwar auf der Grundlage eines zentralisierten Authorisierungsprozesses gegenüber allen Datenressourcen, einschließlich der vorhandenen Back-Office-Umgebung", betont Volker Fischer.

Unabhängig von komplexeren betriebswirtschaftlichen Anwendungen macht der Trend am Frontend, beim privaten Nutzer, weiter Schule. Bei Deutschlands größter Direktbank ist man zuversichtlich, was den Schwenk der Identitätsprüfung unter anderem in die Videocloud angeht. Die technischen Voraussetzungen zur Durchführung seien vorhanden.

Der Nutzer benötige dazu lediglich eine stabile Internet-Verbindung, eine Webkamera und einen aktuellen Browser, bekräftigt Zeljko Kaurin, Generalbevollmächtigter der ING-DiBa. "Die im Hintergrund benutzte Technik ist eine sichere und schnelle WebRTC-Funktionalität, die bei den genannten Browsern automatisch integriert ist", beruhigt der Experte.

Fazit: Letztlich verbleibt auch im Zeitalter von (mobilem) Cloud Computing via "Credentials as a Service" die Verantwortung beim beauftragenden Unternehmen, sprich dem IT-Management bzw. der bankinternen Revision. "Sobald ein externer Administrator eine Verbindung mit und zu den internen Banksystemen und -applikationen aufbaut, sollte die Bank jederzeit in der Lage sein, sowohl den Urheber als auch inhaltliche Zielstellung dieses Vorgangs in Echtzeit zu kontrollieren", empfiehlt Fischer. Denn nur so ließe sich das unternehmensweite Management von Zugriffsberechtigungen stets in einem verlässlichen regulatorischen Rahmen halten.