Kontroll- und Vertrauensverlust erfordert mehr **Schulterschluss**

Von Sebastian Litschke

Noch genießen Kreditinstitute und Kartenorganisationen im Zahlungsverkehr einen starken Vertrauensbonus der Verbraucher. Mit der Öffnung der Kontoschnittstelle für neue Anbieter durch die PSD II drohen Banken die Kontrolle zu verlieren, riskieren aber gleichzeitig Imageschäden im Missbrauchsfall. SecuRe Pay würde dieses Ungleichgewicht wieder aushebeln. Doch auch dann könnte der Vertrauensbonus der etablierten Player rasch abnehmen, warnt Sebastian Litschke. Denn auch die Zahlungsanbieter arbeiten an einer Verbesserung der Sicherheit – ohne Einbußen bei der Bequemlichkeit. Wenn Banken das „Cockpit" des Zahlungsverkehrs zurückerobern wollen, so Litschke, kann das nur gemeinsam gelingen. Die bisherigen Initiativen überzeugen dagegen nicht. Red.

Branchenfremde Internet-Bezahldienste schieben sich verstärkt zwischen Banken und Kartenunternehmen auf der einen und die Kunden auf der anderen Seite. Damit kontrollieren die etablierten Geldinstitute nicht mehr die komplette Zahlungskette. Eine riskante Entwicklung. Denn im Falle von Betrügereien durch Hacker, verursacht durch Sicherheitslücken der Online-Payment-Anbieter, fallen Imageschäden und Haftungsansprüche auch auf die kontoführende Bank zurück. Nach dem Kontrollverlust droht das Vertrauen verloren zu gehen.

Das Vertrauen der Kunden ist das Kapital der Banken und Kartenanbieter. Gegenüber reinen Zahlungsausführern besitzen sie einen Vorsprung. Aus der Erfahrung vieler Überweisungen und Lastschriften haben die Kunden gelernt, dass sie sich auf ihre Hausbank verlassen können. Zahlungen mit Girocard und Kreditkarte werden nahezu immer zuverlässig und sicher ausgeführt – auch im Internet und in der mobilen Bezahlwelt. 57 Prozent der deutschen Smartphone-Besitzer wären bereit, Einkäufe auch mobil zu begleichen, wenn sie das direkt über eine App ihrer Bank erledigen könnten, so das Ergebnis einer Studie des britischen Payment-Dienstleisters Monitise. Verbraucherfreundliche Haftungsregelungen sind ein zusätzliches Sicherheitspolster, das Vertrauen schafft. Dieses haben sich Banken und Kartenunternehmen vor allem durch sichere Bezahlprozesse erarbeitet.

Authentifizierungsmethoden über eine persönliche Identifikationsnummer (PIN) und eine Transaktionsnummer (TAN) erschweren Betrügereien erheblich. Zwar bieten auch diese Maßnahmen keinen 100-Prozent-Schutz. Sicherheitslöcher konnten die Institute allerdings bislang schnell stopfen, denn sie kontrollierten die gesamte Zahlungskette.

Zum Autor

Sebastian Litschke, PPI AG, Hamburg.

Weniger Kontrolle durch PSD II

Payment-Angebote beliebter Internetmarken wie Google, Apple und Amazon besitzen diesen Vertrauensbonus nicht. Noch nicht. Doch sie erhalten Unterstützung aus Brüssel. Die Neuauflage der europäischen Payment Services Directive (PSD II) definiert das Geschäftsmodell sogenannter dritter Zahlungsdienstleister zwischen Kunde und Bank. Bisher nicht regulierte Dienste werden damit erstmals einbezogen. Kunden können Dritte beauftragen, Zahlungen in ihrem Namen gegenüber einem Kreditinstitut auszulösen.

Umstritten ist dabei die geplante Öffnung der Schnittstelle zwischen Bank und Kunde für die neuen Anbieter. Unklar ist, welche Partei für die Schnittstelle organisatorisch zuständig ist. Die Mehrheit der Banken hat Bedenken, dass die Kommunikation über mehrere Anbieter hinweg anfällig sein könnte. Sie befürchten neue Einfallstore für Betrügereien. Derzeit legitimiert sich der Kunde mit Kontodaten und PIN bei seiner Bank. Zahlungen löst er zusätzlich mit einer TAN aus. Diese bilaterale Schnittstelle ist rechtlich geregelt und genügt hohen Sicherheitsstandards. Zudem haben die Kunden gelernt, dass sie ihre

Zugangsdaten tunlichst nur bei ihrer Bank verwenden sollten – und nirgends sonst. Eine unkontrollierte Öffnung der Kunde-Bank-Schnittstelle für dritte Zahlungsdienstleister dürfte also das Risiko erhöhen, dass Zahlungen nicht mit der gewohnten Zuverlässigkeit der Banken ausgeführt werden. Darüber hinaus leide die Sicherheit, so die Sorge der Kreditwirtschaft.

Banken tragen einseitiges Risiko bei fehlenden Sicherheitsstandards

Einhergehend mit der PSD II sieht das European Forum on the Security of Retail Payments (SecuRe Pay) eine strengere Kundenauthentifizierung vor, um internetbasierte und mobile Zahlungen sicherer zu machen. Geplant ist eine Zwei-Faktor-Prüfung. Das bedeutet: Kunden müssen zur Freigabe einer Zahlung mindestens zwei von drei Sicherheitselementen eingeben, die sie kennen oder besitzen müssen. Dies kann beispielweise ein Passwort in Verbindung mit dem Besitz einer bestimmten Hardware oder eines biometrischen Merkmals sein. Die drei Merkmale müssen voneinander unabhängig sein, sodass der Diebstahl eines Merkmals nicht die Sicherungsmaßnahme aushebeln kann. PSD II verpflichtet allerdings nicht alle Marktteilnehmer gleichermaßen, sichere Authentifizierungsmethoden einzuführen.

Die primäre Haftung, wenn Zahlungsdienste derartige Login-Prozeduren von ihren Kunden nicht verlangen, übernimmt das kontoführende Institut. Das sind in der Regel die etablierten Banken und die Kreditkartenunternehmen. Sie tragen das Risiko auch dann, wenn ein dritter Anbieter die Zahlung ausgelöst hat oder für einen Schaden herangezogen werden könnte. Die Banken haften damit für Zahlungsvorgänge, die sie nicht selbst zu hundert Prozent steuern können.

Hinzu kommt der drohende Imageschaden. Denn die Bank ist – egal bei welchem Problem – nahezu immer der erste Ansprechpartner des Kunden. Sie muss also die Kundenbetreuungskosten alleine schultern und übernimmt für Dritte die Problemlösung.

Bezahlanbieter im Wettbewerb begünstigt

Bezahlanbieter wie Paypal würden von dieser Regelung, wenn sie so bleibt, massiv profitieren. Sie können weiter ihre benutzerfreundlichen Ein-Klick-Bezahlprozesse anbieten. Die Kunden lösen Zahlungen lediglich mit Eingabe von Benutzernamen und Passwort aus. Den Schwarzen Peter sperriger und teurer Authentifizierungen behalten die Banken und Kartenanbieter.

Unter den neuen Dienstleistern im Bereich Payment zählt Paypal zu den ärgsten Wettbewerbern der Institute. Größe und Erfolg haben die Finanzbranche aufgeschreckt. Aktuellen Medienberichten zufolge arbeiten einige deutsche Banken bereits an einer eigenen Alternative zu Paypal. Sie setzen darauf, dass die meisten Bundesbürger beim Bezahlen im Internet lieber einen Service ihrer Bank nutzen als das Angebot eines Internetkonzerns aus Kalifornien. Doch die Ebay-Tochter genießt bei den Deutschen mittlerweile ein ähnlich großes Vertrauen wie die Banken. Mit Instrumenten wie dem Verkäufer- und Käuferschutz positioniert sich Paypal seit dem Markteintritt in Deutschland gezielt als Vertrauensstifter zwischen anonymen Vertragspartnern. Unter der Berücksichtigung der hohen Dynamik im Bereich Mobile Payment kann der Vertrauensvorsprung der Banken möglicherweise schon in zwei Jahren aufgebraucht sein.

SecuRe Pay spielt Banken in die Karten

Die Banken setzen deshalb auf „SecuRe Pay". Geplant sind verpflichtende Mindestsicherheitsstandards, die sämtliche Dienstleister betreffen, die Online-Zahlungen verarbeiten, also auch die dritten Zahlungsanbieter. Damit wären die Kreditinstitute ihren neuen Wetterbewerbern wieder einen Schritt voraus. Denn die Mehrheit der Institute bietet bereits die vorgesehene Zwei-Faktor-Authentifizierung beim Online-Banking. Ihr SecuRe-Pay-konformes m-TAN-Verfahren wird durch die Standardisierung aufgewertet.

Commerzbank, Raiffeisenbanken und weitere Institute bieten Kunden zudem mit einem Foto-TAN-Verfahren ein System, das ebenfalls auf die Zwei-Wege-Authentifizierung setzt und mehr Komfort als das m-TAN-Verfahren bieten soll. Der Kunde erhält beim Bezahlen einen QR-Code oder ein sogenanntes Flicker-Bild angezeigt. Das entschlüsselt er via Smartphone-App und gibt die Zahlung frei. Wird die Regel verbindlich für alle Bezahldienstanbieter, sind Dienstleister wie Paypal, i-Zettle und Klarna gezwungen, in Sachen Sicherheit nachzurüsten. Sie müssen die Sicherheitsstandards in ihre Verfahren integrieren.

Doch der Vorsprung in Sachen Sicherheit ist schnell verspielt. Einige Zahlungsdienstleister arbeiten seit geraumer Zeit daran, die Sicherheit ihrer Bezahlsysteme Schritt für Schritt zu erhöhen. Paypal entwickelt bereits Alternativen zur Zahlungsbestätigung per E-Mail-Adresse und Passwort. Im Hintergrund werden Gesichtserkennungsverfahren getestet. Parallel sollen Anti-Betrugssysteme Hacker- und Phishing-Attacken abwehren. Die eingesetzte IT erkennt zum Beispiel Muster beim Eintippen der Login-Daten.

Initiativen der Kreditwirtschaft nicht E-Shopping-tauglich

Banken und Kreditkartenfirmen sollten also schnell aktiv werden. Beim aktuellen Ansatz der deutschen Kreditwirtschaft bleibt abzuwarten, ob dieser zum Erfolg führt. Die Beteiligten möchten die Girocard, früher ec-Karte, auch als Zahlungsmittel für Online-Shops und E-Commerce-Dienstleistungen etablieren. Als Authentifizierungsverfahren sind drei Alternativen im Gespräch. Ein Lesegerät zur PIN-Eingabe, eine Authentifizierung

über Bankleitzahl, Passwort und Benutzername sowie eine optische Kopplung mit dem jeweiligen Internetzugang über Flicker-Verfahren. Die Authentifizierung des Karteninhabers mit Hilfe der beiden hardwaregestützten Verfahren gilt bei Banken als wahrscheinlichste Variante.

Die geplanten Prozesse sind zwar deutlich sicherer als die von Paypal und Co. Allerdings rümpfen die Online-Händler bei dem Vorhaben bereits die Nase. Für sie wirken hardwarebasierte Verfahren eher abschreckend. In der „Online-Payment-Studie 2014" des EHI Retail Instituts bevorzugen fast alle Händler softwarebasierte Authentifizierungsmöglichkeiten. Zwei Drittel favorisieren diese auch für das Einkaufen und Bezahlen über mobile Geräte. Hardware- und biometrische Verfahren lehnen die Händler mehrheitlich als nicht alltagstauglich ab. Zudem darf bezweifelt werden, dass der Kunde im Internetzeitalter immer noch seine Girokarte in der Tasche haben möchte.

Mehrwerte sind Trumpf

Die Kunden wollen Mehrwerte. Alle Zahlungsvorgänge an einer Stelle zu verwalten, kann bereits als Mehrwert betrachtet werden. Eine wirksame Antwort auf den Kontrollverlust ist deshalb, das Cockpit für das Bezahlen zurückzuerobern. Die Banken und Kartendienstleister sollten wieder zur Kommandozentrale der Kunden werden, über die sie all ihre Finanzen steuern.

Einen kleinen Schritt in diese Richtung unternimmt zum Beispiel die DKB Bank. Das Institut bietet seinen Kunden den Service, ihr Paypal- mit dem DKB-Konto zu verknüpfen. Die Nutzer können damit ihre Zahlungen über die Ebay-Tochter in ihrer gewohnten Online-Banking-Umgebung steuern. Das Institut holt sich mit dieser Maßnahme den Kontakt zu seinen Kunden ein Stück weit zurück. Abzuwarten bleibt, inwieweit die Bank Einfluss auf die Sicherheitsprozesse bei Paypal nimmt.

Der Nachteil derartiger Maßnahmen wie bei der DKB Bank liegt darin, dass sie nicht innovativ und weit genug gedacht sind, um die Kunden nachhaltig auf der eigenen Plattform zu halten und damit wieder die Kontrolle über die gesamte Bezahlstrecke zu bekommen. Die neuen Wettbewerber sind da einfallsreicher. Paypal hat im September 2013 seine Wallet-App kräftig verbessert. Mit den Neuerungen bietet die App unter anderem die Möglichkeit, Geschäfte und aktuelle Angebote in der Umgebung zu lokalisieren. Zudem gibt es eine Funktion, um in Schnellrestaurants über das Smartphone Vorabbestellungen durchzuführen und so Warteschlangen zu vermeiden.

Banken und Kartenunternehmen bieten einen ähnlichen Service. Bestellung und Bezahlung sind allerdings nur an einem stationären Terminal möglich, nicht über ein Smartphone. Eine dritte Neuerung der Wallet App ist die Möglichkeit zur Sofortfinanzierung des Einkaufs.

Das Beispiel zeigt: Bankkunden werden Mehrwerte nicht nur im reinen Zahlungsdienst erkennen, sondern in der Summe der angebotenen Dienste. Sichere Zahlungen in Verbindung mit einem persönlichen Finanzmanagement über ein mobiles Online-Banking können entscheidende Schlüsselservices sein, um Kunden zu halten – oder neue zu gewinnen

Bei den Banken fehlen bisher derartige Ideen für das Bezahlen von morgen. Die brauchen sie aber, um das Vertrauen ihrer Kunden zu behalten. Ideal wäre ein Schulterschluss verschiedener Bankenverbände und Kartenanbieter. Eine übergreifende Lösung hat größere Chancen, dass sich bei den Kunden eine Marke für das Bezahlen im Kopf verfestigt und ähnlich wie bei der ec-Karte als allgemein akzeptierter Standard durchsetzt.

Die Institute sollten federführend Kooperationen mit Internetunternehmen und Online-Händlern vorantreiben. Denkbar ist zum Beispiel eine von Banken, Händlern und anderen Dienstleistern gemeinsam entwickelte virtuelle Identität für das Bezahlen im Internet. Diese kann der Kunde bei jedem Dienstleister- und Bankwechsel mitnehmen. Über derartige Ideen können sich Banken und Kartendienste ihren Vertrauensbonus langfristig sichern und auch wirtschaftlich stärker von ihren sicheren Bezahlprozessen profitieren.