Sicherheit

„Die Kunden suchen bequeme Lösungen“

Mobile Banking ist eines der meist diskutierten Themen der vergangenen Monate. Denn Smartphone und Tablet-PC haben die Kommunikation stark verändert. Kunden erwarten, dass sie ihre Bank rund um die Uhr und überall erreichen können. Was das für die Kreditinstitute bedeutet, diskutierten Experten aus Rechenzentren, Banken und Sicherheitsunternehmen gemeinsam mit Banken+Partner-Chefredakteurin Margaretha Hamm

Vor welche Herausforderungen stellen Smartphone und Tablet-PC die Kreditinstitute aktuell?

Mittelstädt: Ein zentrales Thema ist die Sicherheit. Denn es geht darum, die Wünsche der Kunden so einfach und so sicher wie möglich zu erfüllen. Wichtig ist dabei, dass man die Transaktion von der Legitimation vollständig trennt, dass man also Systeme implementiert, die voneinander unabhängig sind. Das ist die Herausforderung, der wir uns derzeit stellen müssen. Voraussetzung ist freilich, dass der Kunde die Sicherheitslösungen auch akzeptiert.

Garip: Ganz genau. Das Dilemma ist es, die höchste Sicherheit anzubieten und das bei höchstem Komfort. Die Kunden sind wie das Wasser, sie suchen immer den einfachsten Weg. Sie setzen voraus, dass die Bank ihnen Sicherheit bietet. Deshalb wollen sie selbst mit der Sicherheit nicht viel zu tun haben.

Tak: Aber auch die Banken haben ganz unterschiedliche Vorstellungen zum Thema Sicherheit. Unsere Aufgabe als Anbieter ist es daher, eine große Bandbreite von Lösungen bereitzustellen. Wir sehen, dass das Mobile Banking mit dem Tablet-PC immer mehr zum Ersatz des Online Bankings am Computer wird. Daneben gibt es beispielsweise in den USA sehr eindrucksvolle Konzepte, bei denen das Mobiltelefon zum Transaktionsterminal wird, an dem auch Privatpersonen Zahlungen entgegennehmen können. Auch für solche Dienste müssen wir Sicherheitslösungen schaffen.

Koch: Insgesamt haben sich die Mobile-Zugriffszahlen in den vergangenen zwei Jahren verzehnfacht und machen inzwischen zehn Prozent des gesamten Online-Aufkommens aus. Und man kann davon ausgehen, dass die Nutzung mittels mobiler Geräte weiter massiv wächst. Die Kunden wollen jederzeit und überall mit ihrer Bank kommunizieren. Dieses Bedürfnis gilt es zu befriedigen. Zudem verändern die vielfältigen Möglichkeiten der Geräte die Kommunikation. Alle verfügbaren Zugangswege, die die Bank anbietet und alle damit verbundenen Services, können wir nun in einem Gerät vereinen. Das Thema Sicherheit spielt dabei eine große Rolle. Es gilt aber vor allem Hürden abzubauen. Sicherheit muss für den Kunden vorhanden, aber nicht vordergründig sein.

Vollrath: Ganz richtig, Sicherheit kann man deshalb nicht dem Kunden überlassen. Man muss sich von der Seite der Bank aus darum kümmern. Wir versprechen beispielsweise unseren Kunden, dass wir Schäden übernehmen, die ihm beim Online- oder Mobile Banking entstehen. Unser Augenmerk gilt dem Kunden. Dabei ist das Gerät, über das der Zugriff erfolgt, nicht ausschlag-

gebend. Unsere Anwendungen müssen auf kleinen und großen Bildschirmen benutzerfreundlich und ohne Einschränkungen rund um die Uhr zur Verfügung stehen.

Kloha: Als Rechenzentrum bieten wir schon seit einiger Zeit Apps für Mobile Banking auf allen gängigen Plattformen an. Denn die Kunden erwarten heute rund um die Uhr Informationen über ihre Bank auch auf ihren mobilen Geräten. Zur Absicherung der Transaktionen möchten viele Bankkunden auf ein zweites Gerät zwar verzichten – wir sehen aber aktuell die Notwendigkeit, auf einem zweiten sicheren Kanal die Geschäftsvorfalldaten, zum Beispiel Kontonummer, Bankleitzahl und Betrag zu prüfen. Dafür müssen wir neue und smarte Lösungen finden.

Mergemeier: Auch wir bieten eine breite Palette an Apps für den Endkunden. Dabei haben wir uns in den vergangenen Jahren auf multibankenfähige Lösungen konzentriert. Die neuen Geräte haben allerdings auch zu einer veränderten Nutzung geführt. Früher gab es am Abend zeitliche Spitzen beim Online-Banking. Das hat sich geändert, die Kunden gehen jetzt auch während des Tages auf ihr Konto. Auch die Anzahl der Transaktionen ist rapide gestiegen, weil der Kunde nun über verschiedene Kanäle die Möglichkeit hat, online zu sein. Das muss man managen.

Putz: Für die Sparda-Banken haben wir das strategische Ziel der Plattformunabhängigkeit bei allen mobilen Endgeräten. Allerdings ist es dem Kunden völlig egal, ob er eine native App hat oder eine plattformunabhängige. Er will, dass das Mobile Banking funktioniert und dies einfach und ohne Erklärungen.

Güler: Eine weitere Herausforderung für die Banken sind doch sicherlich auch die neuen Anbieter, die in den Markt eindringen und Lösungen für den mobilen Zahlungsverkehr anbieten. Hier stellt sich die Frage, wie die Banken reagieren. Ob sie sich dem Wettbewerb stellen oder nicht. Denn es besteht die Gefahr, dass die Banken ein wichtiges Kundenbindungsinstrument verlieren, wenn der Zahlungsverkehr zu anderen Dienstleistern abwandert.

Die Gesprächsteilnehmer

Matthias Kloha
Produktmanagement eBanking und Portale, Fiducia

Sonja Vollrath
Ressortleiterin Internet Marketing, ING-Diba

Dr. Salim Güler
Vice President Corporate Communications, Kobil Systems

Norbert Mittelstädt
Bereichsleiter IT, Organisation und Verwaltung, 1822direkt

Oliver Putz
Abteilungsleiter Multikanalvertrieb, Sparda Datenverarbeitung

Adnan Garip
Vertriebsleiter Deutschland, Kobil Systems

Markus Tak
Chief Technology Officer Client Systems, Kobil Systems

Michael Koch
Leiter Online Business Plattform PBC, Deutsche Bank

Detlev Mergemeier
Portfoliomanagement / Produktfeld Vertriebswege, GAD

Koch: Das ist korrekt. Die Abwicklung von Transaktionen ist ein zentraler Service aller Banken. So bleiben sie mit ihren Kunden im Kontakt. Deshalb haben wir auch unbedingt Interesse daran, alle Zahlungsaufträge unserer Kunden selbst

Gesprächsteilnehmer:
Komfort und Sicherheit dürfen nicht im Widerspruch stehen.

auszuführen. Es besteht durch neue Anbieter tatsächlich die Möglichkeit, dass schleichend die Kundenbeziehung und -bindung abwandert. Diesem Szenario sollten sichere, einfache und standardisierte mobile Payment-Verfahren entgegengesetzt werden. Ich bin davon überzeugt, dass sich hier innerhalb der nächsten zwölf bis 24 Monate entsprechende Lösungen am Markt etablieren werden. Das bietet Vorteile für den Kunden wie Bequemlichkeit, Schnelligkeit und Transparenz, aber auch für die Bank in Form von weniger Bargeld-Logistik und einem besseren Einlagenmanagement.

Sie alle sagen, dass der Kunde einfache Sicherheitslösungen wünscht. Kann es tatsächlich eine Alternative sein, den Kunden von jeder Verantwortung zu entlasten?

Mergemeier: Nein, nicht jede Bank kann alle Schäden übernehmen, die beim Mobile oder Online Banking entstehen. Allerdings dürfen Komfort und Sicherheit nicht in einem Widerspruch stehen. Komfort für den Kunden bedeutet nicht, dass er von der Kontrolle befreit wird. Schließlich gibt er bei einer Transaktion eine Willenserklärung ab, die korrekt sein muss. Die Freigabe der Zahlung mit Hilfe einer wie auch immer gearteten Sicherheitslösung soll ja dazu führen, dass der Kunde sich sicher sein kann, dass er auch die Überweisung durchführt, die er angestoßen hat. Zudem ist es schwierig für den Kunden, ohne ein solches Legitimationsverfahren zu erkennen, ob die Internetseite der Bank manipuliert wurde.

Vollrath: Bei Transaktionen ist das auch für uns nicht die Frage. Unbequem für viele Kunden ist jedoch schon das Einloggen auf seiner Bankenseite. Die diversen Sicherheitsabfragen denen er dabei begegnet sind unbequem. Die Frage ist nicht, ob man sich sicher ist, dass man Geld überweisen will, sondern erst einmal dahin zu kommen, dass man es kann. Zahlungsverkehr ist nur eine Variante.

Koch: Doch gerade hier stellt sich noch eine weitere Frage: Weshalb können alternative Zahlungsverkehrsdienstleister eigentlich sehr viel einfachere Verfahren anbieten als Banken? Dort reicht häufig nur ein Passwort und schon ist die Zahlung beauftragt. Das ist natürlich für die Kunden sehr viel bequemer. Die Banken unterliegen allerdings zurzeit noch stärkeren regulatorischen Vorgaben und müssen daher komplexere Sicherheitsverfahren anwenden.

Wenn die Banken die Sicherheitsanforderungen reduzieren, öffen sie damit nicht kriminellen Angriffen Tür und Tor?

Koch: Nicht unbedingt. Die Frage ist ja, wo die Sicherheitslösungen überall verankert sind. Wenn man dem Kunden keine komplexen Lösungen zumuten will, dann kann man auch weitere Sicherheits-Systeme im Hintergrund einbauen. Solche Lösungen werden ja schon jetzt sehr erfolgreich bei Kartentransaktionen eingesetzt. Wir brauchen ein integriertes Sicherheitsmanagement über die komplette Prozesskette, die nicht überwiegend auf die Kundenseite verlagert wird. Sicherheit lässt sich nicht allein durch verschiedene komplizierte TAN-

Diskussionsrunde: *Eine Analyse der Kundenzahlungen schafft zusätzliche Sicherheit.*

Verfahren beim Kunden erreichen. Wer weiß, vielleicht ist es in Zukunft sogar möglich, ganz auf die TAN zu verzichten. Die TAN könnte in der Zukunft durch eine Kombination von entsprechenden Lösungen ersetzt werden, wie einer sehr guten Anti-Betrugs-Maschine sowie Software-Zertifikaten.

Kloha: Ganz so würde ich es nicht formulieren, allerdings sehen auch wir die Zukunft von Sicherheitslösungen noch mehr in den Back-End-Systemen der Banken. Beispielsweise könnte eine ungewöhnliche Kundenzahlung angehalten und überprüft werden. Damit die Banken auch den dadurch entstehenden manuellen Aufwand leisten können, ist es wichtig eine gut funktionierende Lösung bereitzustellen, die wirklich nur risikobehaftete Transaktionen herausfiltert. Denn wenn man nur zehn Prozent der Transaktionen nachtelefonieren müsste, dann wäre der zusätzliche Aufwand nicht leistbar.

Putz: Allerdings kann man schon heute Ausreißer sehr gut erkennen. Die Zahlungsströme eines Kunden lassen sich in der Regel recht gut analysieren. Da kann zwar immer noch etwas durchgehen, aber es ist nicht die Masse. Man muss ungewöhnliche Zahlungen erkennen können, den Kunden darüber informieren und sie mit ihm abstimmen. Der Kunde weiß dann, dass etwas auf seinem Konto passiert ist, was nicht gewöhnlich war und kann darauf reagieren.

Koch: Die Kunden reagieren auf einen solchen Anruf zur Verifizierung übrigens meist positiv. Sie finden es sehr gut, dass sich ihre Bank um ihre Sicherheit kümmert.

Tak: Es ist tatsächlich notwendig, eine Brücke zu schlagen zwischen dem mobilen Service und dem Risikomanagement. Beispielsweise, wenn man erkennt, dass ein Mobiltelefon gehackt wurde, oder weiß, dass der Kunde jetzt tatsächlich im Ausland ist und eine Überweisung anstößt. Für solche Lösungen, bei denen die Bank ganz individuelle Regeln festlegen kann, bekommen wir auch ein positives Feedback

Wenn die Kunden sich Einfachheit wünschen und es durch Back-Office-Systeme Möglichkeiten zur Vereinfachung gibt, weshalb gibt es dann noch immer unbequeme Sicherheitslösungen?

Güler: Weil die Banken ganz unterschiedliche Bedürfnisse und Anforderungen haben. Für uns als Hersteller von Sicherheitslösungen ist es eine Herausforderung, alle diese Bedürfnisse zu befriedigen. Wir müssen verschiedene Möglichkeiten entwickeln, um den Banken die Lösung bieten zu können, die für sie genau richtig ist. Dabei versuchen wir natürlich einfache Produkte zu schaffen

Tak: Ideal wäre ein Lösung, bei der der Kunde nur noch bestätigen muss, dass er eine Transaktion machen will. Ihm wird sozusagen die Transaktion nochmals zur Bestätigung vorgelegt. Er muss dann nur noch einen roten oder grünen Knopf drücken.

Vollrath: So etwas würden sich sicherlich die meisten Kunden wünschen. Wir müssen aber auch tatsächlich nachfragen, welche Bedürfnisse der Kunde hat, und nicht nur die Meinungen der Experten auf den Kunden projizieren. Denn

vieles was Experten für richtig finden ist dem Kunden nicht zu vermitteln. Wir fragen unsere Kunden beispielsweise einmal im Monat „Wie sicher fühlen Sie sich“. Dabei wurde Unsicherheit beispielsweise im Rahmen der Finanzkrise deutlich. Das hat uns gezeigt, dass die gefühlte Sicherheit nicht allein von Maßnahmen der Bank abhängt, sondern vom politischen, wirtschaftlichen und gesellschaftlichen Umfeld.

Koch: Ganz bestimmt ist es richtig auf den Kunden zu hören, aber häufig wissen die Kunden nicht was möglich ist und können sich deshalb keine ganz neuen Lösungen vorstellen. Deshalb muss man ihnen Möglichkeiten anbieten und sie dann fragen, was sie davon halten.

Solche Erkenntnisse sind sicherlich wichtig für die Entwicklung neuer Sicherheitslösungen. Wie aber werden diese in Zukunft aussehen?

Putz: Wir dürfen nicht vergessen auf den Kunden zu hören. Schauen was der Kunde braucht und welche Lösungen für ihn am besten und am einfachsten zu bedienen sind. Von der Technologie her wird sich noch vieles am Markt ergeben – dazu gehört vielleicht die Biometrie, aber mehr noch Lösungen wie eine sichere Mobile- oder Foto-TAN. Solche Lösungen können alle wie kleine Sprossen aus dem Boden kommen, und die weitere Entwicklung lässt sich deshalb nicht genau prognostizieren. Einen Marktstandard für Sicherheitslösungen im mobilen Bereich wird es aus meiner Sicht kurzfristig nicht geben.

Koch: Sicher ist allerdings, dass mobile Geräte ein mächtiger Innovationstreiber sind. Und das bezogen auf Prozesse, auf Design und auf Workflow. Man sieht schon heute, dass die mobile Nutzung auf den Desktop-Bereich abfärbt. Wir optimieren unsere Internet-Seiten auf Tablets, um sie dann auf dem Desktop ähnlich darzustellen.

Mergemeier: Was wir in der Zukunft leisten müssen, ist ein ausgewogenes Verhältnis herzustellen zwischen den Sicherheitsbedürfnissen der Bank und denen des Kunden, und zwar möglichst so, dass der Kunde mit den Medien, die er anwendet, auch zufrieden ist. Dadurch können wir eine Win-Win-Situation schaffen, so dass der Kunde dann ungefährdet seine Transaktion durchführen kann – gleichgültig auf welchem Gerät.

Kloha: Die aktuelle Ausbaustufe der Apps ist in Sachen Sicherheit sehr hoch. Neben den Sicherheitserfordernissen gilt es aber auch, die Hardware-Möglichkeiten der Devices optimal auszunutzen und in die Abwicklung der Prozesse der Bankkunden zu integrieren. Gleichgültig ob dafür die Kamera, das GPS oder das Mikrofon genutzt wird. Diese Möglichkeiten unterscheiden Apps von den herkömmlichen Desktop-Browser-Lösungen. Die nächste Technologie, die ebenfalls interessant wird, ist die Near Field Communication. Damit könnten per Funkübertragung Zahlungen angestoßen werden. Die Zukunftsvision wäre beispielsweise eine Bankcard, die bereits ein eigenes Display zur Verifizierung der Geschäftsvorfalldaten mitbringt.

Vollrath: Meine Vision ist, dass wir eine Lösung finden, die für alle Kanäle gleichzeitig taugt, kundenfreundlich ist, bezahlbar und sicher. Diese Lösung existiert noch nicht am Markt und wir müssen weiter nach ihr suchen. Bisher gibt es überwiegend Einzellösungen.

Mittelstädt: Tatsächlich müsste man ein Legitimationsmedium finden, das den Kunden eindeutig identifiziert, unabhängig von den benutzten Devices. Im Moment versuchen wir für die jeweiligen Geräte passende Sicherheitsmedien. Das ist das Problem. Wir sollten vielmehr ein Sicherheitsmedium entwickeln, das für alle Legitimationsbedürfnisse passt. Und wir sollten als Banken die Legitimationsstelle werden, und das Entwickeln andern überlassen können.

Güler: Eine Lösung werden wir aber immer nur in Zusammenarbeit mit den Banken erarbeiten können. Denn die Kreditinstitute haben tatsächlich einen sehr unterschiedlichen Blick auf das Thema.

Tak: Und nicht nur das. Wir sind als Hersteller mit sehr viel mehr Geräten und Betriebssystemen konfrontiert als früher. Deshalb ist es uns wichtig, generische Lösungen und verlässliche Sicherheitssysteme zu entwickeln, die einheitlich gemanagt werden können und mit den sich ständig weiterentwickelnden Bedrohungen Schritt halten können.

Garip: Da haben wir zwar bereits viel erreicht, doch die neuen Sicherheitslösungen müssen auch dem schnellen technologischen Wandel Rechnung tragen und adäquat auf die neuen Herausforderungen reagieren. *Margaretha Hamm*