

Sicherheit entscheidet

Die Akzeptanz für Online-Banking steigt – auch wegen neuer Lösungen



Optische TAN-Generatoren wie z.B. Ezio Optical TAN von Gemalto erhöhen den Nutzerkomfort beträchtlich.

24 Millionen Menschen in Deutschland nutzen heute schon Online-Banking-Angebote. Neben den Faktoren Leistungsumfang und Preis wird die Sicherheit der privaten Kontodaten zunehmend zum Entscheidungskriterium für die Bankenwahl. Viele Banken und Sparkassen verwenden immer noch PIN/TAN-Listen und/oder eine mobile TAN. In Anbetracht zunehmender Cybercrime-Attacken stellen diese Techniken jedoch ein Risiko dar, schließlich vertrauen die Kunden darauf, dass ihnen moderne und sichere Lösungen angeboten werden. Neue Lösungen wie z.B. optische TAN-Generatoren vereinen Sicherheit und Nutzerkomfort. Die ersten Kreditinstitute bereiten sich auf den Technologiewechsel vor. Mit den entsprechenden Kommunikationsmaßnahmen untermauert, kann sich der Umstieg für Banken und Sparkassen lohnen und als entscheidender Wettbewerbsvorteil erweisen.

Für die wachsende Akzeptanz von Online-Banking gibt es gute Gründe: Die Internetnutzung nimmt Generationen übergreifend zu. Schnelle Breitbandanschlüsse erreichen zunehmend auch ländliche Gebiete. Darüber hinaus ist die Bank im Internet rund um die Uhr geöffnet, so dass man Bankgeschäfte bequem nach Feierabend von der Couch aus erledigen kann. Auch finanziell lohnt sich Online-Banking, denn die Finanztransaktionen im Internet sind meist preiswerter als am Schalter. Die Kosten für Kreditinstitute liegen bei Online-Angeboten bei nur einem Fünftel der papiergebundenen Prozesse und diese Vorteile können sie weitergeben.

Kernkriterium Sicherheit

Dies sollte allein schon Anreiz genug sein, sich intensiver mit dem elektronischen Geschäftsbereich zu beschäftigen. Für eine

Vielzahl von Kunden ist das Online-Angebot schon ein entscheidender Faktor bei der Wahl „ihrer“ Bank. Stehen anfangs noch Kriterien wie Leistungsumfang und Kosten im Mittelpunkt, entwickelt sich mit zunehmender Internet-Erfahrung der Faktor Datensicherheit zu einem Kernkriterium.

Gerade in diesem Bereich haben die Banken allerdings noch Nachholbedarf: Wenn es um den Schutz bei der Übertragung persönlicher Kontodaten via Internet geht, vertrauen viele noch auf das herkömmliche PIN/TAN-System. Aktuelle Berichte zeigen jedoch, dass diese Methode nicht ausreicht, um organisiertes Cybercrime zu unterbinden. Der Markt ist lukrativ und Betrüger sind kreativ in der Entwicklung perfider Methoden des Datenklau wie Phishing, Pharming und Trojanern. Dem IT-Bundesverband Bitkom zufolge wurden im Jahr 2007 an die 4100 Fälle mit einem Gesamtschaden im zweistelligen Millionenbereich mit einer durchschnittlichen Schadenssumme von ca. 3700 € bekannt. Das Bundeskriminalamt (BKA) registrierte allein im Jahr 2008 1.800 erfolgreiche Versuche, das auf einer indizierten TAN-Liste basierende i-TAN Verfahren zu knacken. Mobile TAN kann Zwei-Faktoren-Authentifizierung nicht vollständig gewährleisten

Diese Zahlen geben Banken und Sparkassen zu denken, denn grundsätzlich trägt das Kreditinstitut das Risiko für den Missbrauch beim Online-Banking. Viele Institute haben deshalb bereits mit der Verbesserung ihrer Sicherheitsverfahren reagiert und mit der Ablösung der bisherigen TAN-Listen begonnen. Doch ob ein Ausweichen auf die mobile TAN zielführend ist, sei in Frage gestellt. Nach seiner Registrierung bei der Bank erhält der Kunde bei diesem Verfahren eine transaktionsbezogene TAN per SMS auf sein Mobiltelefon, d.h. zusätzliche Hardware ist nicht nötig. Da die Betrüger nicht gleichzeitig den Kunden-PC (Kunde an Bank) und das Mobilfunknetz (Bank an Kunden) abhören können, gilt das Verfahren mit mobilen TANs als relativ sicher.

Im Vergleich zur simplen TAN-Liste mag das auch gelten. Die Schwäche liegt jedoch darin, dass beide Kommunikationskanäle unterschiedlichen Sicherheitsrichtlinien unterliegen und die Banken keinerlei Einfluss auf die Infrastruktur des Mobil-

funknetzes haben. Der exakte Zeitpunkt des SMS-Versands der mobilen TAN ist nicht steuerbar und mit Kosten verbunden. Zudem ist die PIN-Eingabe zur Authentifizierung bei Smartphones nur optional, die Anforderung einer Ersatz-SIM-Karte (Träger der Mobilfunknummer) im Falle eines Verlusts beim Provider relativ einfach. Deshalb lässt sich anzweifeln, ob man in diesem Fall wirklich von einer Zwei-Faktoren-Authentifizierung durch Besitz (Mobilfunknummer) und Wissen (PIN) sprechen kann. Negative Erfahrungen im mobilen Online-Banking sind z.B. aus Südafrika belegt.

Eine gänzlich andere Alternative ist die Absicherung per Chipkarte über das HBCI (Homebanking Computer Interface)-Verfahren. Diese Methode gewährleistet einen sehr hohen Sicherheitsstandard – allerdings benötigt der Benutzer hierfür auch eine eigene Software und ein Chipkartenlesegerät. Diese Restriktionen sind dafür verantwortlich, dass dieses Verfahren auf nur wenig Resonanz im Markt stößt.

Eine dritte Methode für sicheres Online-Banking sind schließlich TAN-Generatoren. Auf Knopfdruck erzeugen diese eine TAN, die nur für eine kurze Zeitspanne gültig ist und auf dem Display des Geräts angezeigt wird. Das auch als „Smart TAN“ bezeichnete Verfahren erschwert das Abfangen und die missbräuchliche Verwendung von Nutzerdaten erheblich. Beim intelligenteren „Smart-TAN Plus“-Verfahren gibt der Kunde bestimmte Daten der Transaktion in einen speziellen Kartenleser ein, der zusammen mit der Bankkarte eine TAN erzeugt. Der Bankrechner rechnet dann die TAN nach und gibt bei Übereinstimmung die Transaktion frei. Da die errechnete TAN nur für diese Transaktion anwendbar ist und die TAN mit Hilfe der Bankkarte errechnet wird, ist dieses Verfahren als sehr sicher zu bewerten. Lediglich die Eingabe von Transaktionsdaten über die Tastatur des Lesers wird manchmal als umständlich empfunden und birgt die Möglichkeit von Fehleingaben.

Optische Technologie spart manuelles Eintippen

Optische TAN-Generatoren wie z.B. Ezio Optical TAN von Gemalto erhöhen hier den Nutzerkomfort beträchtlich, ohne Abstriche bei der Sicherheit zu machen. Das neue Verfahren, als „Smart TAN comfort“ bezeichnet, basiert auf dem ZKA Standard HHD 1.32. Der Nutzer muss die zur Berechnung erforderlichen Transaktionsdaten nicht mehr manuell eingeben. Diese Arbeit übernehmen optische Schnittstellen, die auf der Rückseite des Lesers integriert sind. Dazu muss der Anwender das Gerät nur kurz vor seinen Bildschirm halten, die über Flickercodes ausgelesenen Daten im Display bestätigen und per Knopfdruck eine TAN erzeugen, die nur für diese Transaktion gilt. Die Technologie erfordert keine Software auf Kundenseite und das Lesegerät passt mit seiner Scheckkartengröße sogar in die Brieftasche.

Sichere Technologien sind heute schon verfügbar. Wieso aber halten dann doch noch so viele Banken an ihren TAN-Listen

Wachstumsmarkt Online-Banking

Die Abwicklung von Bankgeschäften via Internet ist für viele deutsche Sparkassen- und Bankkunden selbstverständlich geworden. Einer aktuellen Umfrage der europäischen Statistikbehörde Eurostat zufolge erledigen 24 Millionen Menschen in Deutschland, d.h. 38% aller Bundesbürger im Alter von 16 bis 74 Jahren, ihre Bankgeschäfte über das Internet. Dies bedeutet eine Steigerung von 11 Millionen oder 85% in den letzten fünf Jahren. EU-weit reicht dies allerdings nur zu einem Platz im Mittelfeld. Im Vergleich zu Online-Banking-Raten im Bereich der 70% wie in Finnland oder den Niederlanden liegt im deutschen Markt noch jede Menge Wachstumspotenzial.

fest? Als Begründung werden hier immer wieder die Umstellungskosten auf das neue Verfahren (Server-Lösung auf Banken- und TAN-Generatoren auf Kundenseite) sowie Zweifel an der Akzeptanz der neuen Lösungen angeführt. Diese Sichtweise ist jedoch etwas kurz gegriffen. Schließlich vertraut der Kunde darauf, dass das Kreditinstitut seines Vertrauens ihm ausgefeilte Online-Banking-Lösungen bietet – und nicht nur beim Leistungsumfang, sondern gerade auch beim Thema Sicherheit stets auf dem aktuellen Stand bleibt.

Banken wie Barclays in Großbritannien und die Vietcombank in Vietnam haben mit modernen Sicherheitslösungen wie TAN-Generatoren bereits sehr positive Erfahrungen gemacht. Nicht nur dass die Kunden die neuen und sicheren Lösungen schnell adaptieren, die Institute konnten darüber hinaus eine überproportional steigende Nachfrage nach Online-Kontomodellen verzeichnen.

Kommunikationskonzepte gefragt

Dieses Resultat mag zuerst überraschen, schließlich scheuen sich viele Banken davor, mit kostenpflichtigen Extra-Angeboten an ihre Online-Kunden heranzutreten. Dass Datensicherheit ihren Preis hat, ist vielen Internet-Nutzern mittlerweile allerdings bewusst; die steigenden Absatzzahlen von Virenschutzprogrammen belegen dies. Vor dem virtuellen Bankschalter wird diese Investitionsbereitschaft nicht stoppen. Hier sind vielmehr tragfähige Kommunikationskonzepte gefordert, mit denen Banken ihre Kunden über die Vorteile der neuen Sicherheitstechnologien informieren. Dieser Aufwand lohnt sich, denn mit jeder neuen Cybercrime-Welle wird Sicherheit im Online-Banking zum entscheidenden Wettbewerbsfaktor.

Autor:

Eckardt Mohr, Area Sales Manager bei Gemalto