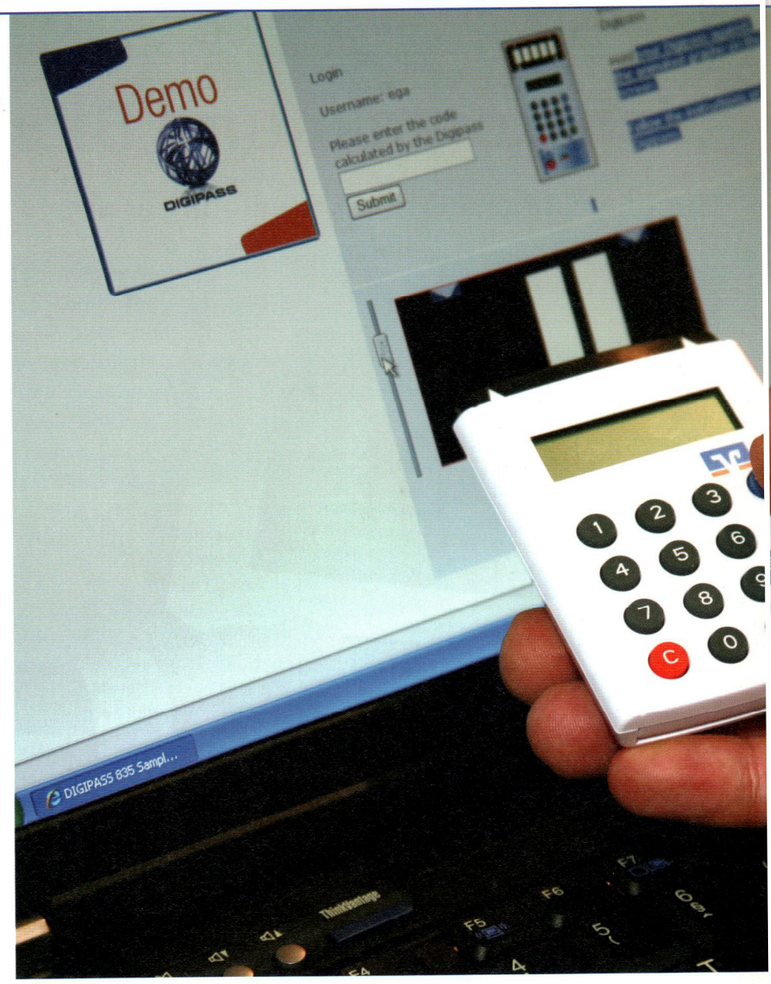
Sicheres Online-Banking

Mit smarten TANs gegen raffinierte Hacker

Nach wie vor sichern viele Online-Banking-Nutzer ihre Transaktionen mit einer indizierten TAN-Liste, obwohl dieses Verfahren längst als nicht mehr zeitgemäß gilt. Bei den meisten Volksbanken und Raiffeisenbanken in Nord-West-Deutschland ist das sichere Smart-TAN plus-Verfahren verfügbar – inzwischen mit zusätzlicher optischer Schnittstelle.



Internet-Betrüger haben auch in der Krise Hochkonjunktur: Das Ausspähen sensibler Daten hat im letzten Jahr um 60 Prozent zugenommen, meldet die Kriminalstatistik. Gegen die Flut von Hackerangriffen hatten die Banken und ihre Online-Kunden aber meist nur Schutzwälle aus Papier – nämlich die gute alte TAN-Liste (Transaktionsnummer). Auch wenn diese den Kunden nach einer Transaktion zur Eingabe einer bestimmten, also indizierten TAN auffordert, gilt sie unter Fachleuten inzwischen als nicht mehr sicher. „Das iTAN-Verfahren stelle für Kriminelle kein Problem mehr dar", erklärte Mirko Manske, Kriminalhauptkommissar im Bundeskriminalamt (BKA) auf dem 11. IT-Sicherheitskongress des Bundesamts für Sicherheit in der Informationstechnik in Bonn.

iTANs von Trojanern ausgehebelt

Zum Problem wird das iTAN-Verfahren immer dann, wenn es einem Kriminellen gelingt, ein Schadprogramm in den Computer eines Online-Banking-Kunden einzuschleusen. Diese so genannten Trojaner können sich nämlich unbemerkt in die Kommunikation mit der Bank einschleusen und eine Transaktion verfälschen. Aus einer Spende an Unicef wird dann unversehens eine saftige Abgabe an die Schattenwirtschaft – die der ahnungslose Online-Banker dann brav per iTAN bestätigt.

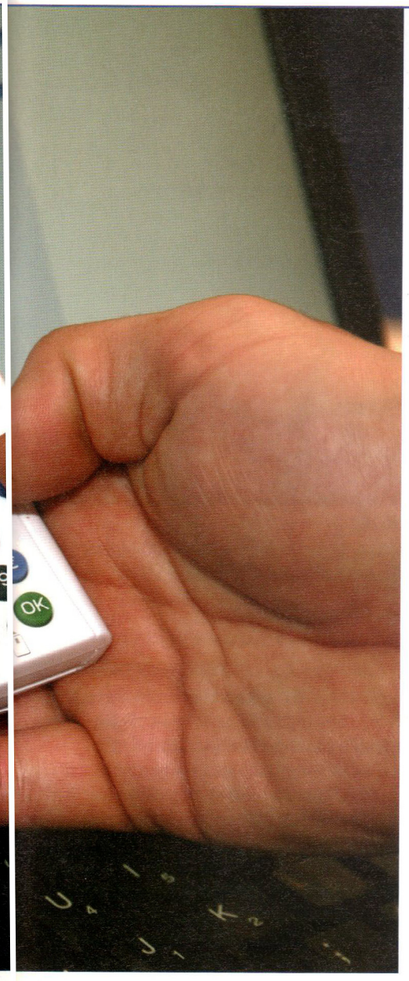
Dieser so genannte „Man-in-the-Middle"-Angriff nutzt prinzipielle Schwächen des etablierten TAN-Systems. Der Anwender weiß nicht, ob die Rückmeldung, die er da signiert, auch wirklich von seiner Bank stammt. Auch die Bank kann nicht mit Sicherheit sagen, ob eine Transaktionsanforderung wirklich von einem Kunden stammt – und nicht von einem Ganoven, der sich unbemerkt in die Übertragung eingeklinkt hat.

Rechtsfrage: Banken in der Pflicht

Dem Kunden die Schuld in die Schuhe zu schieben, ist einfach, aber nicht zielführend. Die Praxis zeigt immer wieder, dass Schadprogramme trotz der üblichen Sicherheitsmaßnahmen wie Virenscanner oder Firewall in den PC gelangen können. Dann kann man dem Kunden keine Verletzung seiner Sorgfaltspflicht nachweisen. Und dann haftet nicht selten die Bank für den entstandenen Schaden. Aber auch wenn die Bank keine Rechtsfolge trifft: Erfolgreiche Hacker-Attacken bringen das gesamte System Online-Banking in Misskredit und damit auch die Geldinstitute – wahrlich keine vertrauensbildende Maßnahme, gerade in Zeiten der Finanzkrise.

↓ AUTOR

***Jan Valcke** ist Präsident und Chief Operating Officer bei Vasco Data Security, Wemmel/Belgien.*
Tel.: +32 2 456891-0
E-Mail: jvalcke@vasco.com
www.vasco.com



Datenübertragung per Bildschirm: Mit Vasco Digipass 835A brauchen die Transaktionsdaten nicht mehr von Hand eingegeben zu werden. Bild: DG-Verlag

Dabei gibt es längst sichere Alternativen zur antiquierten iTAN: Bei verschiedenen Volksbanken Raiffeisenbanken ist das so genannte Smart-TAN-plus-Verfahren im Einsatz. Hierbei wird die Transaktionsnummer nicht mehr von einer Liste abgelesen, sondern von einem externen Zusatzgerät in Verbindung mit dem Chip der VR-Bankcard errechnet. Das Besondere dabei: Der Kunde tippt die Transaktionsdaten, zum Beispiel Betrag und Empfänger, in sein Gerät ein. Diese Daten werden dann intern verrechnet und fließen in die dynamische TAN ein. Eine Verfälschung der Transaktion durch einen zwischengeschalteten Hacker führt zu einer ungültigen TAN und damit zum Abbruch. Die externe Hardware ist für Betrüger unerreichbar. Es ist keine Verbindung der Zusatz-Hardware zum PC erforderlich, damit ist das System überall einsetzbar.

Mehr Sicherheit, das bedeutet aber in den meisten Fällen auch mehr Aufwand. So müssen bei Smart-TAN plus eben viele Daten von Hand in das Zusatzgerät eingetippt werden – was die Akzeptanz beim Endkunden nicht unbedingt steigert. Hier galt es, eine anwenderfreundlichere Lösung zu finden.

Benutzerfreundliche Lösung

Das Smart-TAN-plus-Verfahren mit optischer Schnittstelle erspart den Anwendern dabei den zusätzlichen Eingabeaufwand. Authentisierungsgeräte wie Vasco Digipass 835A bieten hier für Banken und ihre Kunden ganz neue Möglichkeiten.

Für die Eingabe der Transaktionsdaten nutzt der Smart-TAN-plus-Leser Digipass 835A nicht die „Biomechanische Schnittstelle Mensch", sondern den Bildschirm des Home-Banking-Rechners. Dort erscheinen die Transaktionsdaten, codiert als Blinksignale. Der Kunde hält einfach seinen Leser an den Bildschirm. Dessen Hardware verfügt über eine Leiste mit Fotozellen, die die Blinksignale wieder in Daten umsetzt. Dann werden die übermittelten Daten im Display des Lesers angezeigt und nach Überprüfung und Vergleich mit den Originaldaten vom Kunden bestätigt. Danach errechnet das Gerät eine dynamische TAN, die die Transaktion bestätigt. Diese gibt der Kunde dann wie gewohnt an seinem PC ein.

Die Idee eines Optokopplers ist zwar nicht neu, sie bietet aber gerade beim Online-Banking viele Vorteile. Man braucht nichts einzutippen, Fehleingaben sind ausgeschlossen. Der Leser braucht keine Kabel-, Infrarot- oder Funkverbindung zum Rechner und damit auch keine Treiber. Das System funktioniert auf jedem Rechner mit Internetanschluss. Sogar die Leser sind untereinander austauschbar. Die Individualisierung und Authentisierung erfolgt über die Banking-Karte des Kunden. Da alle sicherheitsrelevanten Berechnungen im externen Gerät erfolgen, sind Manipulationen ausgeschlossen, auch wenn man an einen mit Malware infizierten Rechner gerät.

Der Bankkunde kann auf dem Display den Transaktionsinhalt prüfen. Dann erst gibt er seine Freigabe. In die errechnete TAN fließen sowohl die Transaktionsdaten ein als auch Daten aus der Chipkarte des Kunden. Die TAN gilt also nur für einen bestimmten Transaktionsinhalt – und auch nur für einen bestimmten Zeitraum. Wird einer diese Werte während der Übertragung verfälscht, erfolgt sofort ein Abbruch.

Optische Schnittstelle

Seit Mai 2009 können Genossenschaftsbanken und deren Kunden im Einzugsbereich des Rechenzentrums GAD Smart-TAN plus mit optischer Schnittstelle nutzen. Seit der Einführung wurden bereits um die 50.000 Digipass 835A an die Kunden ausgeliefert. Diese Geräte sind abwärtskompatibel, also auch für Dateieingabe von Hand geeignet. Der DG Verlag testet die Geräte in der Entwicklungsphase auf Funktionsfähigkeit und Spezifikationskonformität. Er stellt die Lieferfähigkeit verschiedener Modelle sicher. Auch die Individualisierung der Leser ist möglich.

Mit eigenem Logo versehen, setzen Volksbanken Raiffeisenbanken die Leser auch als Werbegeschenk mit hohem Zusatznutzen ein. Der DG Verlag kümmert sich dabei um das Branding der Geräte, bei größeren Stückzahlen werden die jeweiligen Logos während der Herstellung von Vasco auf das Gehäuse aufgedruckt. Der DG Verlag übernimmt auf Wunsch auch den kompletten Rollout inklusive Geräte-Auslieferung an die Bankkunden und unterstützt die Banken in der Kundenkommunikation.

Mehr als 2.000.000 Privatkunden können Smart-TAN plus mit optischer Schnittstelle zurzeit nutzen, und noch in diesem Jahr wird das System flächendeckend für Volksbanken Raiffeisenbanken in Deutschland verfügbar sein. Das ist eine Weltneuheit und das System könnte zum Modell auch für andere Länder werden. Sicherheit ist eben ein globales Thema. □