Daniel Bachfeld

c't 17/08

# Zahl oder Karte

## Sicherer Zugriff aufs Online-Konto

Bankkunden sind Ziel Nummer eins der Kriminellen im Internet: Die Schäden durch das Ausspähen von privaten Kontodaten sind nach Angaben des Bundeskriminalamts im vergangenen Jahr drastisch gestiegen. 2007 habe man schon 4200 Phishing-Fälle offiziell registriert – 700 Fälle mehr als noch 2006. Die tatsächliche Zahl dürfte noch weit höher liegen, weil viele Einbrüche nicht an die Polizei gemeldet werden. Auch die Schäden sind laut BKA sprunghaft gestiegen. 2006 lag die Schadenshöhe im Durchschnitt noch bei 2500 Euro, 2007 sollen es schon 4000 bis 4500 Euro pro Phishing-Fall gewesen sein.

Dabei ist der klassische Klau von PIN und TAN über nachgemachte Webseiten immer mehr in den Hintergrund getreten, weil kaum noch eine Bank das herkömmliche PIN/TAN-Verfahren einsetzt. Nur zehn Prozent der Schäden sollen nach Angaben des Branchenverbandes BITKOM noch auf diese Weise zustande kommen. In den Vordergrund rücken Banking-Trojaner, die sich im PC einnisten und beobachten, wann ein Anwender Online-Banking startet, um dann loszuschlagen. Solche Trojaner bauen eigene Verbindungen zum Online-Banking des Kunden auf und nehmen mit einer abgeluchsten TAN eigene Überweisungen vor. Dabei präsentieren sie dem Anwender im Browser nachgemachte Banking-Seiten. Der Trojaner Win32.Banker.ohq soll beispielsweise laut dem Antiviren-Spezialisten Kaspersky 56 Bankenseiten imitieren können.

Um seinen Windows-PC mit einem Banking-Trojaner zu infizieren, muss man nicht zwangsläufig dubiose Webseiten aufrufen oder Anhänge in E-Mail öffnen. Mittlerweile reicht es, eine bekannte, vermeintlich sichere Webseite zu besuchen, um über eine Lücke im Browser einen Schädling untergeschoben zu bekommen. Auch die vielen neuen Möglichkeiten des Web 2.0 und das dabei eingesetzte JavaScript bieten Angreifern eine breite Palette von Möglichkeiten, um zumindest den Browser eines Bankkunden zu kontrollieren **[1|#literatur**].

Weil die Tricks immer fieser werden, ist es für die Kunden auch immer schwieriger, ihren PC zu schützen. Kommt es dann doch mal zum Schaden, zeigen sich viele Banken kulant, oft aber auch nicht – meist mit der Begründung, der Bankkunde habe seine Sorgfaltspflichten verletzt und beispielsweise keine aktuelle Antivirensoftware installiert. Nach einem Urteil des Amtsgerichts Wiesloch vom Juni dieses Jahres haften die Banken jedoch für Schäden, die durch das Abfangen vertraulicher Daten entstehen. „Das Fälschungsrisiko des Überweisungsauftrags trägt die Bank“, heißt es in der Gerichtsentscheidung. Im verhandelten Fall hatten sich trotz Virenscanner 14 Schädlinge in den PC eingeschlichen. Für den Kunden sei es nicht zumutbar, sich in der gleichen Geschwindigkeit, wie sich Viren ändern, die entsprechende Software zuzulegen. Für ihn dürfe keine höhere Sorgfaltspflicht gelten als für die Bank.

Keine Diskussion mit ihren Kunden um den Schadensersatz verspricht die Citibank beim Abschluss der kostenlosen Online-Sicherheitsgarantie. Sie ersetzt die durch Phishing, Pharming und Trojaner entstandenen Schäden. Voraussetzung ist laut Citibank lediglich, dass der Kunde die missbräuchliche Verwendung von Zugangsdaten beziehungsweise TANs unverzüglich meldet, eine Strafanzeige erstattet und die Citibank bei der Aufklärung unterstützt. Offenbar hat die Bank, die als eine der wenigen nur das alte TAN-Verfahren anbietet, damit auf Vorwürfe reagiert, kein sicheres Online-Banking anzubieten und dann auch noch die Haftung für das Risiko auf den Kunden abzuwälzen.

### Zahlenspiele

So gut wie alle deutschen Banken haben auf die Attacken reagiert und neue Verfahren zu Authentifizierung von Transaktionen eingeführt. Allerdings orientieren sich viele davon immer noch an den herkömmlichen Phishing-Angriffen. Ein sicheres Verfahren muss aber heutzutage das Leerräumen des Kontos verhindern können, auch wenn der PC infiziert ist.

Die meisten Banken sind nur vom normalen TAN- auf das iTAN-Verfahren umgestiegen, bei dem statt einer beliebigen Transaktionsnummer aus einer Liste eine bestimmte von der Bank angeforderte eingegeben werden muss. Allerdings sind Trojaner in der Lage, auch das iTAN-Verfahren auszuhebeln. Dazu präsentieren sie dem Opfer während einer Überweisung die Nachfrage nach der iTAN für eine parallel vom Trojaner abgeschickte Überweisung, die das Opfer arglos eingibt, im Glauben, die eigene Transaktion zu legitimieren.

Mit einer sogenannten Man-in-the-Middle-Attacke lässt sich auch die von wenigen deutschen Banken eingesetzte eTAN aushebeln, die nichts anderes als eine elektronische TAN-Liste darstellt. Mittels einer genauen und mit der Bank synchronisierten Uhr zeigt der TAN-Generator alle paar Sekunden eine andere Nummer an. Das Verfahren ist in den USA und in Asien weitverbreitet. Allein mit dem Einführen von Hardware ist es aber nicht getan. Fängt der Trojaner die eTAN ab, kann er damit innerhalb eines kurzen Zeitraums eigene Überweisungen vornehmen. Ähnlich angreifbar sind auch TAN-Generatoren auf Basis der GeldKarte, wenn sie nur das sogenannte Einschrittverfahren benutzen, also gleich beim Einstecken der Karte eine TAN auf dem Display anzeigen.

**Mehrschritt**

Um die Sicherheit zu erhöhen, schalten einige Volksbanken ab dem 30. 9. ihr altes Sm@rtTAN-Verfahren ab und stellen auf das sichere Zweischrittverfahren Sm@rtTAN plus um – die Auftragseinreichung und die TAN-Übermittlung sind zwei voneinander getrennte Prozesse. Dazu ist ein neuer Kartenleser mit Tastatur notwendig, über die man nach dem Einstecken der Bankkarte noch einen von der Bank übermittelten Überweisungszahlencode und die letzten sechs Ziffern des Zielkontos eingeben muss. Anschließend zeigt das Sm@rtTAN-plus-Gerät die zur Freigabe erforderliche TAN. Die TAN lässt sich nur für genau diese Transaktion benutzen. Das von einigen Sparkassen angebotene neue chipTAN-Verfahren ist ebenfalls ein Zweischrittverfahren.

Noch weiter geht das Zweischrittverfahren mit dem neu entwickelten Flickercode. Nach Eingabe seines Auftrags hält der Kunde einen Flickercode-TAN-Generator mit eingebauten Fototransistoren vor den Bildschirm, auf dem die Bank mittels mit Flash, JavaScript oder animiertem GIF über fünf Felder einen Schwarzweiß-Blinkcode sendet. Ein Feld gibt dabei den Takt vor. Der Code enthält die Überweisungsdaten sowie weitere zur Berechnung einer TAN benötigte Daten. Das Gerät zeigt nach dem Einlesen des Codes den Überweisungsbetrag und das Konto an – eine Manipulation der Transaktion durch einen Betrüger oder Trojaner fällt sofort auf. Nach dem Drücken der Bestätigungstaste erhält man die TAN. Bislang planen aber nur einige Volks- und Raiffeisenbanken, das System einzuführen.

Der Nachteil der sicheren TAN-Verfahren mit Chipkarte ist, dass der Anwender immer ein Zusatzgerät bei sich tragen muss, das zudem auch noch Geld kostet – zwar nur etwa 10 bis 15 Euro, aber immerhin. Bei der mobilen TAN (mTAN/smsTAN) machen sich die Banken den Umstand zunutze, dass in Deutschland so gut wie jeder Kunde ein eigenes Handy besitzt und meist auch immer dabei hat. So ist es möglich, die für eine Transaktion erforderliche Nummer auf einem vom PC unabhängigen Kanal zum Kunden zu schicken – nämlich per SMS. Darin stehen neben der TAN zur Kontrolle zusätzlich die Überweisungsdaten. Zudem ist die TAN sicherheitshalber nur wenige Minuten gültig. Bei vielen Instituten ist das Zusenden einer mTAN mittlerweile kostenlos. Um in den Genuss dieses flexiblen und sicheren Verfahrens zu kommen, muss man in der Regel nur einmalig seine Handy-Nummer registrieren und wie im Falle der Postbank sich per Telefon, Fax oder Post legitimieren. Anschließend kann man etwa bei den Sparkassen im Online-Überweisungsformular jedesmal zwischen iTAN und mTAN auswählen.

**Kartenspiele**

Neben den Chipkarten-basierten TAN-Generatoren gilt nach wie vor HBCI (seit 2002 auch FinTS genannt) mit Chipkarte als eine sichere Methode für Online-Banking. Insbesondere in Zusammenarbeit mit Homebanking-Software wie StarMoney bietet HBCI nicht nur Schutz vor Phishing und Pharming-Angriffen, sondern auch einen bequemen Zugang zum Konto – statt über das Web-Interface der Bank. Transaktionen werden nicht mehr mit einer TAN legitimiert. Vielmehr signiert der Anwender eine Prüfsumme seiner Transaktionsdaten mit seinem geheimen, auf der Karte gespeicherten Schlüssel und schickt das Ganze an die Bank. Da der Signaturvorgang in der Karte erfolgt und sich der Schlüssel nicht aus der Karte auslesen lässt, kann ein Angreifer mit ihm keine eigenen Transaktionen signieren. Zum Signieren muss der Kunde

zudem eine PIN eingeben, um den Vorgang freizuschalten. Anhand des bei der Bank hinterlegten Schlüssels kann die Bank die Gültigkeit der empfangenen Transaktionsdaten verifizieren.

Die Sache hat allerdings drei Haken. Erstens: Für HBCI mit Karte benötigt man einen kostenpflichtigen Kartenleser, der das Verfahren immobil macht. Zweitens: Es muss ein Lesegerät mit eigener Tastatur sein, weil sonst die Eingabe der Karten-PIN auf dem PC erfolgen muss. Dort könnte aber ein Trojaner mitlesen und damit eigene Überweisungen freischalten. Drittens: Zwar zeigt die Banking-Software die Daten einer Überweisung an, jedoch sieht der Anwender nicht, was er letztlich mit der Karte signiert, da selbst Kartenleser mit Display keine diesbezüglichen Daten anzeigen. Hier könnte ein Trojaner eingreifen, indem er die vom Kunden auf dem PC eingegebene Überweisung vor der Übermittlung an den Kartenleser ändert. Zwar sind solche Schädlinge noch nicht verbreitet, eine Vorstufe war aber mit dem StarMoney-Trojaner Anfang 2008 zu sehen, der TANs von Nutzern stahl.

Wie bei den TANs rüsten die Banken auch bei HBCI nach: Der Zentrale Kreditausschuss (ZKA) hat eine Spezifikation für eine neue Generation universeller Chipkartenleser unter dem Namen Secoder entwickelt und im Frühjahr vorgestellt. Mit Secoder soll Online-Banking mit digitaler Signatur noch sicherer werden, unter anderem weil für den Leser eine Tastatur und ein Display obligatorisch sind – und letzteres sogar die Transaktionsdaten zur Kontrolle anzeigt. Zudem muss die Eingabe der PIN zwingend auf dem Lesegerät erfolgen; unter HBCI ist dies selbst bei Klasse-3-Geräten eine Frage der Einstellung in der Finanzsoftware.

Darüber hinaus eignet sich Secoder zusammen mit der Geldkarte auch zum Bezahlen im Internet und für den Altersnachweis auf Webseiten. Die Geldkarte kann mittels Secoder sogar über das Internet aufgeladen werden. Und für alle, die Angst haben, im Internet Spuren zu hinterlassen: Durch die Geldkarten-Funktion soll sich im Internet sogar anonym einkaufen lassen. Bislang bieten allerdings nur einige vom IT-Dienstleister GAD betreute Volks- und Raiffeisenbanken im Norden und Westen Deutschlands Secoder an. Andere Institute wie die Deutsche Bank prüfen noch die Einführung oder planen den Start erst 2009. Einen Nachteil hat Secoder jedoch: Es läuft derzeit mit keiner Finanzsoftware zusammen, lediglich die Browser-Anwendung der GAD unterstützt ihn bereits.

**Was tun?**

Das einfache TAN-Verfahren ist nicht mehr zeitgemäß, iTAN hilft nicht gegen Trojaner und HBCI ist ob der Hardware immobil. Zudem ist es etwas betagt und für kommende Trojaner-Angriffe nicht gerüstet. Da selbst auf einem Kartenleser mit Display die Überweisungsdaten nicht angezeigt werden, hat der Anwender keine Kontrollmöglichkeit. Dies ändert sich mit dem neuen Standard Secoder, der viele andere nützliche Funktionen bietet, den bislang aber nur die Volks- und Raiffeisenbanken im Norden und Westen unterstützen. Viele Banken scheinen HBCI derzeit hauptsächlich als Mittel anzusehen, um Kunden per Finanzsoftware an ihr Konto zu binden – und nicht um für mehr Sicherheit zu sorgen. Dies gilt insbesondere für die Banken, die HBCI nur zusammen mit PIN und TAN statt mit Chipkarte anbieten und diesen sicherheitstechnischen Rückschritt irreführend auch noch als HBCI+ anpreisen.

Nichtsdestotrotz sollten Anwender, die nur die Wahl zwischen iTAN und HBCI mit Chip haben, HBCI wählen. Wie man dies am besten unter Windows und Linux zum Laufen bekommt, zeigt der Artikel auf den folgenden Seiten. Bei den Sparkassen und Volksbanken bieten die TAN-Generatoren eine hohe Sicherheit, aber auch sie wollen unterwegs verstaut sein. In einer mobilen Gesellschaft ist die mTAN am zeitgemäßesten: Sie kostet nichts, ist quasi immer dabei und sehr sicher – solange man sein Handy nicht aus der Hand gibt.

Wer nur vor die Wahl zwischen TAN und iTAN gestellt wird, sollte besondere Sicherheitsmaßnahmen ergreifen und sich überlegen, wie er seinen Rechner noch weiter sichern kann. Dazu gehört unter Windows neben einem Virenscanner, einer aktivierten Firewall, regelmäßigen Sicherheits-Updates und optimierten Sicherheitseinstellungen vielleicht auch die Überlegung, einen anderen Browser als den Internet Explorer einzusetzen.

Alternativ bietet sich das auf der Heft-CD beiliegende, speziell gehärtete Live-System c't Bankix auf Basis von Linux an, das vor Phishing-Angriffen schützt und gegen Banking-Trojaner immun ist. Wie man damit umgeht, beschreibt der Artikel auf Seite 104 in c't 17/08. (**dab[1]**)

**Literatur**

[1] **Daniel Bachfeld, Dunkle Flecken, Neuartige Angriffe überrumpeln Webanwender[2]**, c't 11/08, S. 82

***"Online-Banking sicher"***

*Artikel zum Thema "Online-Banking sicher" finden Sie in der c't 17/2008:*



---

**URL dieses Artikels:**
http://www.heise.de/ct/artikel/Zahl-oder-Karte-291676.html

**Links in diesem Artikel:**
[1] mailto:dab@ctmagazin.de
[2] http://www.heise.de/ct/08/11/082