



Tipps zum sicheren Online-Banking

Meldung vom: 01.01.2008 - 10:43 Uhr

Mit iTAN, mTAN oder HBCI Bankgeschäfte über das Internet abwickeln

Online-Banking bietet für Internet-Betrüger drei zentrale Angriffspunkte: den Rechner der Bank, den des Bankkunden und die Verbindung zwischen den beiden Rechnern. Es besteht die Gefahr, dass zum Beispiel bei Überweisungen die Bankverbindung von Dritten mitgelesen wird. Damit könnten Betrüger sich dann ungehindert Geld vom Konto des Geschädigten überweisen. Damit Ihnen so etwas nicht passiert, werden im Folgenden Methoden vorgestellt, die das Abwickeln der eigenen Bankgeschäfte im Internet sicherer machen.

Drei Verfahren in der Übersicht

Die großen Banken bieten ihren Kunden Online-Banking über das PIN/TAN-Verfahren oder das HBCI-Verfahren per Chipkarte an. Beim indizierten TAN-Verfahren (iTAN) sind die Transaktionsnummern durchnummeriert. Die Liste aller zur Verfügung stehenden TAN-Nummern wird dem Kunden per Post zugeschickt. Die Liste kommt aus den gleichen Sicherheitsgründen per Post, wie der PIN-Code zu einer neuen EC-Karte dem Besitzer in einem getrennten Umschlag zugeschickt wird. Sollte die TAN-Liste also nicht beim Kunden ankommen, können potenzielle Betrüger damit nichts anfangen, solange ihnen die zugehörigen Bankverbindungsdaten fehlen. Auf Anfrage teilt die Bank dann dem Kunden den Listenplatz der TAN-Nummer, die für den beabsichtigten Vorgang funktioniert, online mit. Manche Kreditinstitute bieten an, nach ausgeführter Transaktion eine Bestätigungsnummer (BEN) zurückzuschicken, mit der die Bank die Auftragsannahme im Gegenzug quittiert. Der Kunde weiß dadurch, dass nur die gewünschte Aktion ausgeführt wurde.

Beim mobileTAN (mTAN) wird jeweils nur ein TAN-Code kurzfristig per SMS verschickt und ist dann auch nur für den konkreten Vorgang gültig. Bei einer Überweisung sind in dieser SMS nochmal der Betrag und die Empfängerdaten enthalten. Der Kunde kann diese Daten also noch einmal kontrollieren, bevor er den Auftrag abschließend freigibt. Da Manipulationen so direkt auffallen ist es laut der Internet-Sicherheitsfirma Symantec eine äußerst sichere Methode, das Handy als zweiten Authentifizierungskanal einzubinden. Um das mTAN-Verfahren zu nutzen zu können, ist eine Registrierung mit der Handy-Nummer bei der Bank erforderlich.

Online-Banking mit Chipkarte

Als sicherste Methode, eigene Bankgeschäfte online abzuwickeln, schlagen Sicherheitsexperten das HBCI-Verfahren vor. HBCI, Home Banking Computer Interface, erlaubt nur mit einer Chipkarte samt des dazugehörigen Kennworts den Zugriff auf die Online-Kontoinformationen. Für Online-Banking per HBCI, braucht man eine Homebanking-Software, in die man sich mit Passwort einlogged. Danach kann die gewünschte Transaktion, zum Beispiel ein Überweisungsauftrag, in der entsprechenden Eingabemaske ausgefüllt werden. Indem der Nutzer seine Chipkarte in das Lesegerät steckt, identifiziert er sich als Kunde und der Signier-Schlüssel "unterschreibt" und codiert die gewünschte Transaktion bevor

sie an die Bank verschickt wird. Diese beiden Schlüssel sollten für Dritte unsichtbar sein, da sie sich nur auf der Chipkarte und im gesicherten Bankrechner befinden. Sobald die Bank den Auftrag erhält, wird die Signatur dekodiert und die "Unterschrift" mit dem bankeigenen Signier-Schlüssel verglichen. Stimmen die Informationen überein, wird der Auftrag ausgeführt.

Die Kosten für das Chipkarten-Lesegerät und die dazugehörige Software muss der Kunde allerdings selber tragen. Die Software StarMoney 6.0 zum Beispiel wird zu zwei unterschiedlichen CyberJack-Chipkarten-Lesegeräten angeboten. Das Gerät der Sicherheitsklasse 2 besitzt eine eigene Tastatur, so dass eine PIN-Eingabe über den Computer, die von Betrügern ausgespäht werden könnte, hinfällig wird. Dieses Paket wird von vielen Groß- und Direktbanken ab rund 70 Euro angeboten. Lesegeräte der Sicherheitsklasse 3 haben zusätzlich ein eigenes Display, um die Daten vor der Signatur prüfen zu können, und kosten rund 30 Euro mehr.

Grundregeln für sicheres Online-Banking

Online-Banking mit Chipkarte ist zwar laut **Oliver Karow von Symantec** am sichersten, allerdings ist es auch nur von dem Computer aus möglich, wo das Lesegerät angeschlossen ist. Deshalb würden Kunden mit den iTAN und mTAN Verfahren praktikabler und, wenn der Kunde selbst einige Sicherheitsregeln beachtet, ebenso sicher ihre Online-Geschäfte abwickeln können.

Computer, die für Online-Banking genutzt werden, sollten wie alle Computer, mit denen im Internet gesurft wird, natürlich ausreichend vor Viren geschützt sein. Um eventuelle Sicherheitslücken zu schließen, gibt es für die meisten Browser auch zusätzlich frei verfügbare Erweiterungen, die zum Beispiel komfortabel die Verwendung von Java Script nur auf "vertrauenswürdigen" Seiten zulassen. Beim Browser Firefox zum Beispiel ist dafür das Add-on "NoScript" gedacht.

Nutzer von Homebanking-Software sollten vor der Installation sicherstellen, dass die Software aus vertrauenswürdiger Quelle stammt und nicht als Shareware bereits mit Viren verseucht ist. Die Online-Banking-Zugangsdaten sollte der Kunde natürlich geheim aufbewahren und nicht im Computer speichern. Solche wichtigen Informationen werden am besten, wie zum Beispiel auch der EC-Karten-PIN, mit dem man am Automaten Geld abheben kann, nur im Gedächtnis gespeichert. Darüber hinaus sollten Passwörter und Nutzernamen regelmäßig geändert werden. Seinen Kontostand sollte der Kunde regelmäßig überprüfen, damit Veränderungen direkt auffallen. Zusätzlich kann mit der Bank ein Limit für die tägliche Geldbewegung vereinbart werden. Generell gilt: Bei Verdacht auf Missbrauch der Kontodaten sollte der Online-Banking-Zugang umgehend gesperrt werden.

Die Zukunft des Online-Bankings

Ein Pressevertreter der Software-Firma Symantec rät, dass Online-Banking-Kunden schon bei der Wahl ihrer Bank darauf achten sollten, dass diese ein moderneres Sicherheitsverfahren anbietet. Die Banken ihrerseits hätten ein Interesse an einem umfassenden Sicherheitskonzept, da der Vertrauensverlust der Öffentlichkeit schwerer wiegt als der finanzielle Schaden. Eine von der Butler Group im Auftrag von Symantec durchgeführte Studie sieht für die Zukunft den Einsatz einer integrierten Software, die den PC des Kunden vor den typischen Gefahrenquellen wie Viren und Trojanischen Pferden schützt, als zentrales Element zur Verbesserung der Sicherheit. Darüber hinaus muss die Software den E-Mail-Verkehr überwachen und eventuell auftretende Phishing-Versuche wirksam abblocken. Auf diese Art und Weise würden einerseits die mit Abstand wichtigsten Gefahrenquellen für das Online-Banking beseitigt und andererseits E-Mail als wichtiges Kommunikationsmittel wieder zugänglich.

Autor: Anja Zimmermann - zimmermann@teltarif.de

URL dieses Artikels:

<http://www.teltarif.de/arch/2008/kw01/s28328.html>

Links in diesem Artikel:

Info-Seite: SMS - <http://www.teltarif.de/i/sms.html>

Extern: Symantec - <http://www.symantec.com/de/de/index.jsp>

Online-Banking - <http://www.teltarif.de/internet/sicherheit/online-banking.html>

Viren - <http://www.teltarif.de/internet/sicherheit/viren.html>