FAQ

Christian Wölbert

Online-Banking und TANs

Antworten auf die häufigsten Fragen

Sichere TAN-Verfahren

Welche TAN-Verfahren sind sicher?

Es gibt mehrere Anforderungen an sichere Verfahren. Wichtig ist, dass die TANs aus den Überweisungsdaten erzeugt werden und deshalb nur zur gewünschten Kontonummer und zum gewünschten Betrag passen. Manipuliert jemand im Hintergrund diese Daten, passt die TAN nicht mehr.

Darüber hinaus dürfen TANs nur zeitlich begrenzt gültig sein und sie müssen auf einem separaten Gerät erstellt oder angezeigt werden – also nicht auf dem Smartphone, auf dem die Online-Banking-App läuft. Sehr wichtig ist auch, dass die beteiligten Geräte möglichst sicher vor Manipulationen sind.

Das Chip-TAN-Verfahren mit TAN-Generator erfüllt diese grundlegenden Anforderungen und gilt deshalb als sehr sicher. Der Generator wird nicht an den PC angeschlossen, er kann also kaum manipuliert werden. Er kostet nur 10 bis 15 Euro. Einziger Nachteil: Man muss ihn immer mitschleppen, wenn man unterwegs überweisen will.

Ebenfalls sehr hohe Sicherheit bieten die seltener genutzten Verfahren BestSign mit Seal-One-USB-Stick sowie HBCI mit spezieller Chipkarte und Secoder-zertifiziertem Kartenlesegerät. Bei diesen beiden Verfahren werden die Geräte zwar an den PC angeschlossen, sind aber vor Manipulation geschützt. Die Hardware kostet rund 30 Euro (BestSign) beziehungsweise 70 Euro (HBCI).

iTAN und mTAN

Sind andere gängige Methoden wie iTAN und mTAN unsicher?

Beim iTAN-Verfahren werden die Nummern nicht aus den Überweisungsdaten erzeugt, sondern lassen sich universell einsetzen. Deshalb werden sie massenhaft von Kriminellen missbraucht.

mTAN ist eine Stufe sicherer, aber Gauner haben sich schon in vielen Fällen mit Tricks eine zweite SIM-Karte für den Mobilfunkvertrag ihres Opfers besorgt, sodass sie dessen mTANs abfangen konnten. Weil sie sich mit einem Trojaner oder durch Phishing auch die Zugangsdaten beschafft hatten, konnten sie bequem das Konto leer räumen.

Das relativ junge App-TAN-Verfahren wird zum Beispiel von der ING Diba und den Sparkassen eingesetzt. Es hat den konzeptionellen Nachteil, dass die TAN auf dem Gerät angezeigt wird, das auch für das Online-Banking verwendet wird. Der Angreifer muss also nur ein Gerät unter seine Kontrolle bringen. Die Sparkassen-Lösung wurde von Sicherheitsforschern im Labor geknackt, aber noch nicht in der Praxis.

Chip-TAN

Wie funktioniert das Chip-TAN-Verfahren in der Praxis?

Das Chip-TAN-Verfahren wird vor allem von Sparkassen und Volksbanken angeboten, aber auch von der Postbank und einigen Direktbanken. Sie benötigen dafür einen TAN-Generator. Bei jeder Überweisung geben Sie die Transaktionsdaten in den Generator ein – entweder automatisch mithilfe einer animierten Grafik im Online-Banking-Portal (Flicker-Code) oder von Hand mit den Zifferntasten des Generators.

Besonders beim Flicker-Code müssen Sie kontrollieren, ob der Generator die korrekte Kontonummer und den korrekten Betrag anzeigt. Weichen diese Daten von Ihrer geplanten Überweisung ab, wurden sie vermutlich manipuliert. Falls aber alles stimmt, drücken Sie auf OK. Dann berechnet der Chip auf Ihrer Girocard, die im Generator steckt, die TAN. Der Generator zeigt die TAN nur an. Deshalb ist es auch kein Problem, wenn Sie den Generator verlieren.

TAN-Generator

Wie finde ich den richtigen TAN-Generator?

Wenn Sie den TAN-Generator bei Ihrer Bank kaufen, können Sie kaum etwas falsch machen. Die meisten Modelle kosten dort nur 10 bis 15 Euro inklusive Versand; im Online-Handel zahlt man oft mehr.

Falls Sie das Gerät trotzdem im Handel kaufen, sollten Sie darauf achten, dass es die Vorgaben Ihrer Bank einhält. Meist verweisen die Banken auf den Standard der Deutschen Kreditwirtschaft (HHD 1.3.2 oder 1.4).

Das Chip-TAN-Verfahren ist sehr sicher, wenn man die Transaktionsdaten auf dem Display des Generators kontrolliert.

Risiko und Haftung

Welches Risiko gehe ich eigentlich ein, wenn ich ein unsicheres TAN-Verfahren einsetze?

Egal welches TAN-Verfahren Sie nutzen, grundsätzlich ist die Bank für die Sicherheit verwantwortlich. Laut Gesetzeslage muss sie für alle nicht autorisierten Zahlungsvorgänge haften. Sie als Kunde gehen also kein finanzielles Risiko ein – es sei denn, Sie handeln grob fahrlässig. Was das genau bedeutet, hängt von den Gerichten ab, die im Einzelfall urteilen.

Aufgrund der bisher entschiedenen Fälle können Sie von folgenden Regeln ausgehen: Sie müssen ein aktuelles Antivirenprogramm nutzen, die Warnhinweise auf den Webseiten Ihrer Bank beachten und dürfen nicht auf offensichtliche Phishing-Attacken hereinfallen, die zur Eingabe von TANs auffordern.

Außerdem dürfen sie mTANs nicht auf dem Smartphone empfangen, auf dem Sie mit einer App oder im Browser Geld überweisen. Bei der App-TAN haben die Banken kein Problem damit, wenn man alles auf einem Gerät erledigt. Das „Prinzip der Kanaltrennung“ bleibe erhalten, weil ein „gesicherter zusätzlicher Kommunikationskanal“ und ein „zweites virtuelles Device“ geschaffen würden, erklärt die ING Diba.

Bei transaktionsgebundenen TAN-Verfahren (zum Beispiel mTAN, Chip-TAN, BestSign) müssen Sie prüfen, ob die angezeigten Überweisungsdaten korrekt sind.

Schadensfall

Was muss ich im Schadensfall tun?

Sie sollten Ihre Bank informieren und Strafanzeige erstatten. Außerdem empfiehlt es sich, den PC auf Viren zu scannen und den Scan-Bericht zu sichern, damit Sie im Notfall beweisen können, dass Sie einen Virenscanner installiert hatten. Oft verzichten die Banken jedoch auf diesen Nachweis.

(cwo@ct.de)