Das sollten Sie als „Online-Banker“ unbedingt wissen ...

PHARMING

Dieses Kunstwort kommt natürlich aus dem Englischen und steht für „*password*“ (Passwort) und „*farming*“ (Landwirtschaft). Betrüger leiten Kunden unbemerkt auf falsche Webserver um. Sie ernten damit wie mit einem Schleppnetz Passwörter und Geheimzahlen, müssen dafür allerdings auch ganze Server-Farmen vorhalten. Als häufige Standorte wurden bisher gerne Südostasien und Osteuropa identifiziert.

PHISHING

Phishing setzt sich zusammen aus dem englischen „*password*“ und „*fishing*“ (Passwort und Fischen). Internetnutzer werden mit einer eMail auf fast perfekt gefälschte Seiten gelockt und aufgefordert, Passwörter, Geheimzahlen oder Transaktionsnummern preiszugeben.

SPOOFING

Beim Spoofing, englisch für Parodie, werden Internet-Adressen (URL) täuschend echt imitiert, indem einzelne Buchstaben ersetzt werden. So ist der Unterschied zwischen dem gewöhnlichen und dem kyrillischen „α“ selbst für geübte Augen praktisch nicht zu erkennen. Damit gilt die bisherige Regel nicht mehr, nach der man an Original-Internet-Adressen die Authentizität der Webseiten erkennen könnte. Am anfälligsten ist der Microsoft Internet Explorer. Der Link erscheint als authentisch, ist er aber nicht.

ETAN, ITAN, MTAN

Aufgrund der gravierenden Sicherheitsmängel modifizieren viele Kreditinstitute das bisherige PIN/TAN-Verfahren ein wenig. Die TANs werden entweder per Handy (mTAN) zugesandt, per eMail wird eine bestimmte indizierte TAN angefordert (iTAN) oder die elektronische TAN (eTAN) auf einem zusätzlichen externen Gerät generiert.

HBCI

Das **H**ome **B**anking **C**omputer **I**nterface (HBCI) ist ein nationaler, einheitlicher Standard, der als sehr sicher bei elektronischen Bankgeschäften gilt. Über ein spezielles Verfahren von Verschlüsselungen werden die Daten an die Bank mit einer elektronischen Signatur übermittelt. Hier werden sie entschlüsselt.
Der Kunde braucht eine elektronische Chipkarte und ein Kartenlesegerät. Alternativ können diese beiden Komponenten durch einen Datenträger (Speicherkarte, Diskette) ersetzt werden.
Bevor die Nachricht, z.B. eine Überweisung, im Internet zur Bank geschickt wird, werden die Daten mithilfe der Chipkarte oder des Datenträgers verschlüsselt. Die Kosten für den Kartenleser und die passende Software liegen einmalig bei ungefähr 35 Euro.

DAS PIN/TAN-VERFAHREN

Die meisten Banken setzen immer noch auf ein unsicheres PIN/TAN-Verfahren, dass den Kunden eindeutig identifizieren soll. Dieser erhält eine Geheimzahl, die persönliche Identifikationsnummer (PIN) und eine Liste mit Transaktionsnummern (TAN). Die PIN wird einmal pro Sitzung abgefragt und bleibt unverändert. Für jede Transaktion, etwa eine Überweisung, ist zusätzlich eine TAN anzugeben, die nur einmal verwendet werden kann, Geheimzahlen und Transaktionsnummer werden wie die übrigen Kundendaten vom Computer des Anwenders verschlüsselt und zum Bankrechner übertragen, dieser diese dann entschlüsselt.

DocRich EDV - Bremen
Düsseldorfer Str. 2
28327 Bremen
Tel.: 0421 / 68419 22
Fax: 0421 / 68419 23
eMail: info@docrich-edv.de
Web: www.docrich-edv.de
USt.IdNr.: DE239543375