ANGRIFFSZIEL ONLINEBANKING

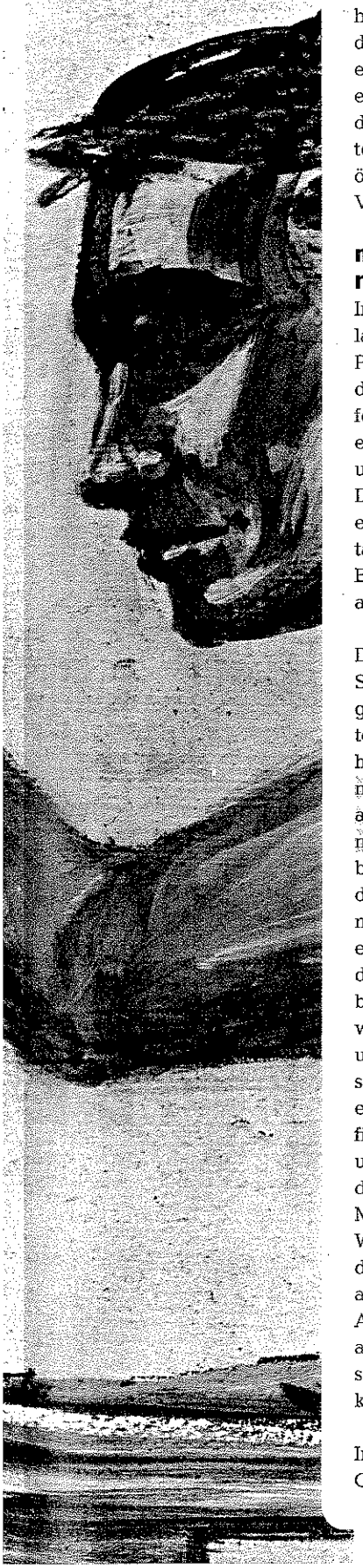
VERMEHRT PHISHING-ATTACKEN

Onlinebanking-

Wie sicher ist das m-TAN-Verfahren und wann haftet die Bank?

WANN haftet die Bank?

GRUNDSÄTZLICH HAFTET DIE BANK FÜR JEDE ÜBERWEISUNG, die nicht vom Bankkunden autorisiert wurde. Allerdings kann sie eventuell Schadenersatzansprüche gegen den Kunden geltend machen, wenn die Überweisung aufgrund verlorengegangener TAN-Nummern oder durch Missbrauch erfolgt ist. Bis zu 150 Euro Schadenersatz kann die Bank verlangen. Bei grober Fahrlässigkeit hat sie sogar Anspruch auf Ersatz des gesamten Schadens. Oft argumentieren Banken, dass diese grobe Fahrlässigkeit bereits dann vorliegt, wenn der Kunde keinen aktuellen Virenscanner installiert hat. Die Bank muss das Vorliegen der groben Fahrlässigkeit jedoch erst einmal nachweisen.



Beim Phishing werden Daten von Internetnutzern über gefälschte E-Mails, SMS oder Webseiten abgefangen. Viele Banken verschicken sogenannte mTANs und verweisen auf die hohe Sicherheit dieser Methode. Bei diesem Verfahren kann die finanzielle Transaktion nur durch die Eingabe einer TAN abgeschlossen werden, die der Anwender zuvor per SMS erhalten hatte. Leider finden Betrüger immer öfter Wege, das vermeintlich sichere Verfahren auszutricksen.

mTAN-Verfahren schützt nicht vor Phishing

In einem aktuellen Fall aus Süddeutschland haben Betrüger durch einen Phishing-Angriff Zugriff auf die Handynummer und Kontodaten der betroffenen Frau erhalten und anschließend eine neue SIM-Karte aktivieren lassen, um die Überweisung durchzuführen. Die Kundin hatte zuvor unwissentlich einen Trojaner auf ihrem Computer installiert, der ihre Tasteneingaben beim Einloggen auf der Onlinebankingseite ausspionierte.

Durch aktuelle und richtig eingestellte Sicherheitssoftware (aktiver Hintergrundwächter, aktive Firewall) sollten sich solche Manipulationen verhindern lassen. Jedoch denken viele nicht daran, dass Smartphones genau so anfällig für Schadprogramme sein können wie der heimische Computer. Das beweist der folgende Fall: Eine Kundin loggte sich über den Firmenrechner in ihren Onlinebanking-Account ein. Prompt erschien ein Fenster mit der Aufforderung, sich für das Onlinebanking neu zu zertifizieren. Abgefragt wurden ihre Handymarke, das Modell und ihre Handynummer. Daraufhin sollte sie eine SMS mit einem Link erhalten, unter dem sie das neue Zertifikat für ihr Mobiltelefon herunterladen und daraufhin installieren sollte. Mit der Installation des Zertifikats auf ihrem Mobiltelefon installierte die Kundin in Wirklichkeit eine Schadsoftware, mit der die eingehenden SMS unmittelbar an die Betrüger weitergeleitet wurden. Auf ihrem Handy wurden die SMS nicht angezeigt. In zwei Tagen wurden insgesamt rund 92.000 Euro von ihrem Girokonto auf fremde Konten überwiesen.

In beiden Fällen haben die Banken das Geld an ihre Kunden zurücküberwiesen. Doch nicht immer bekommt der Kunde sein Geld zurück (siehe Kasten).

Wie kann sich der Bankkunde gegen Phishing schützen?

Den besten Schutz vor jeder Art von Phishing bietet die Beachtung eines einfachen Grundsatzes: Niemals auf telefonische Anfrage (Ausnahme: Telefonbanking) oder auf eine E-Mail PIN oder TAN herausgeben. Selbst wenn die entsprechende Aufforderung noch so seriös wirkt, sollte im Zweifel bei der Bank nachgefragt werden. Dies gilt auch bei ungewohnten Browserfenstern. Schließlich sollte sich der Bankkunde nicht auf vermeintlich sichere Methoden wie das mTAN-Verfahren verlassen. Wer auf Nummer sicher gehen will, verwendet das mTAN-Verfahren mit einem alten Mobiltelefon, welches weder fähig ist, Drittprogramme zu installieren, noch generell auf das Internet zugreifen kann. Ein effektiver Schutz kann auch durch die Nutzung einer speziellen Bank-App erreicht werden. Eine solche App ist weit weniger anfällig für Schadsoftware. Allerdings sollte man nicht das gleiche Gerät für die Nutzung der App und zur Durchführung des m-TAN-Verfahrens nutzen.

Gefälschte Webseiten oder E-Mails sind zum Teil schwer als solche zu erkennen, doch mit ein wenig Misstrauen und gesundem Menschenverstand lassen sich viele Fallen umgehen. Wer als Bankkunde für die üblichen Sicherheitsvorkehrungen beim Onlinebanking gesorgt hat, hat im Verlustfalle zudem in der Regel gute Chancen, sein Geld zurückzubekommen.

CHRISTIAN SOLMECKE

Rechtsanwalt Christian Solmecke (39) von der Kölner Kanzlei Wilde Beuger Solmecke hat sich auf die Beratung der Onlinebranche spezialisiert. Insgesamt arbeiten in der Kanzlei 24 Anwälte. Solmecke hat in den vergangenen Jahren den Bereich Internetrecht/E-Commerce stetig ausgebaut. So betreut er zahlreiche Medienschaffende und Web-2.0-Plattformen. Er vertritt ebenfalls Tausende Filesharer, die von der Musikindustrie abgemahnt worden sind.