

„Ein zweiter Kommunikationskanal zur Übermittlung der TAN ist sicherer“

Fragen an das Referat Cybercrime, Bundeskriminalamt, Wiesbaden

Sowohl beim Banking über mobile Endgeräte als auch über den heimischen Computer ist ein gesundes Maß an Misstrauen angebracht, so das Referat Cybercrime des Bundeskriminalamtes. Einen hundertprozentigen Schutz vor einer Infektion gebe es nicht. Red.

bm Die simpelste Anwendung, mit der mobile Endgeräte ins Bankgeschäft einbezogen werden, sind Alert-Funktionen per SMS – beispielsweise die Information über sämtliche Kreditkartentransaktionen, Bargeldabhebungen oder Überweisungen vom Girokonto. Was bringen solche Warnhinweise? Ist dann der Schaden nicht schon geschehen? Und wird eine solche Informationsflut vom Kunden überhaupt gelesen?

Auch wenn die Transaktion schon erfolgt ist und eine Ware gegebenenfalls auch schon herausgegeben oder versandt wurde, bewahrt sich die Bank durch solche Warnhinweise vor Schäden und auch vor wiederholter missbräuchlicher Nutzung.

Inwieweit diese Nachrichten vom Kunden gelesen werden, kann durch das BKA nicht beurteilt werden. Wichtig in diesem Zusammenhang ist insofern eine umfassende „Awareness-Kampagne“, um den Karteninhaber über die Risiken aufzuklären.

bm Lassen sich auch solche Warnhinweise von Hackern manipulieren oder unterdrücken?

Aktuelle Schadsoftware greift heutzutage nicht mehr nur den heimischen PC, sondern auch vermehrt mobile Endgeräte an. Entsprechende Manipulationen des Endgerätes sind möglich. Auch hier ist aber von Bedeutung, dass der Nutzer nicht sorglos Software auf sein mobiles Endgerät herunterlädt. Dahinter könnte sich auch durch gut eingesetztes Social Engineering eine Schadsoftware verbergen.

bm Derzeit gehen Banken verstärkt dazu über, die i-TAN durch die Chip-TAN mit separatem Chipkartenleser oder die mobile TAN zu ersetzen. Welches Verfahren ist sicherer?

Hierzu kann das BKA keine Stellung beziehen. Grundsätzlich kann jedoch festgehalten werden, dass ein zweiter Kommunikationskanal zur Übermittlung beziehungsweise dem Empfang einer TAN sicherer ist.

bm Wie lang schätzen Sie die „Halbwertszeit“ der mobilen TAN?

Es existiert bereits Schadsoftware, welche in der Lage ist, das m-TAN-Verfahren anzugreifen.

bm Sehen Sie Möglichkeiten, die Sicherheit bei der mobilen TAN zu verbessern? Oder eignet sich das Mobiltelefon grundsätzlich nicht zur Absicherung elektronischer Finanztransaktionen?

Grundsätzlich eignet sich das m-TAN Verfahren besser als das i-TAN Verfahren.

bm Ist das Mobile Banking genauso (un)sicher wie das Onlinebanking am PC oder sind die Sicherheitslücken noch höher?

Grundsätzlich lässt sich dazu nur sagen, dass es auch bei mobilen Endgeräten von Bedeutung ist, welche Software der Nutzer herunterlädt. Dahinter kann sich Schadsoftware verbergen.

Eine Infektion des heimischen PC kann heutzutage ohne weiteres Zutun des Internetnutzers, zum Beispiel durch eine sogenannte Drive-By-Infektion, erfolgen. Hundertprozentigen Schutz vor einer Infektion des PC gibt es nicht mehr.

bm Rät das BKA vom Mobile Banking ab?

Wichtig ist, dass der Bankkunde ein hohes Maß an Sensibilität bei der Durchführung des Online- und des Mobile-Bankings aufbringt sowie Unregelmäßigkeiten erkennt und entsprechend bewertet. Deutsche Strafverfolgungsbehörden, das Bundesamt für Sicherheit in der Informationstechnik sowie Banken sind ständig bemüht durch umfangreiche „Awareness-Kampagnen“ auf die Gefahren des Online- und des Mobile-Bankings hinzuweisen. Ein gesundes Misstrauen bietet bereits ein hohes Maß an Schutz.