Bequem, aber unsicher

Online-Banking mit TAN-Apps

Viele Online-Banking-Apps sind verwundbar und Angreifer könnten etwa Überweisungen manipulieren. Eine derartige Attacke ist jedoch komplex. Sicherheitsforscher demonstrieren erfolgreiche Übergriffe und zeigen abermals die Gefahren das TAN-App-Ansatzes auf.

Von Dennis Schirrmacher

Transaktionsnummern, kurz TAN, sind beim Online-Banking unabdingbar. Man kann sie als einmaliges Passwort betrachten, das etwa die Ausführung einer Überweisung autorisiert. Anfangs las man die Transaktionsnummer von einem Zettel ab und gab diese auf dem Computer in das Formularfeld ein. Das ist quasi der Klassiker der Zwei-Faktor-Authentifizierung, bei dem das Bankgeschäft strikt getrennt mit zwei Medien abläuft. Selbst wenn sich ein Angreifer die PIN für das Banking-Konto erschleicht, kann er keine Überweisungen tätigen, da ihm der zweite Faktor fehlt. Aktuelle TAN-Konzepte setzen auf ein zweites Gerät. Bei mTAN ist das etwa ein Handy, das die TAN per SMS empfängt.

Heutzutage bieten jedoch immer mehr Banken neben der Banking-App auch TAN-Apps für Smartphones und Tablets an. Dabei findet neben der Überweisung auch die Generierung der TAN auf ein und demselben Endgerät statt. Man kann die TAN sogar oft direkt in die Banking-App übertragen. Das ist praktisch und äußerst bequem, aber ein gefundenes Fressen für Hacker, weil die beiden Faktoren nicht aus unterschiedlichen Quellen stammen.

Angriff nicht trivial

Die Kommunikation zwischen den Apps findet verschlüsselt statt und ein auf einem Smartphone installierter Trojaner kommt nicht ohne Weiteres an die Daten ran. Das Konzept ist aber durchaus angreifbar, wie die Sicherheitsforscher Vincent Haupert und Tilo Müller schon 2015 am Beispiel der TAN-App der Sparkasse demonstrierten. Nun haben sie erneut die Unsicherheit des bequemen Online-Bankings aufgezeigt und eigenen Angaben zufolge 31 Banking-Apps erfolgreich attackiert – darunter etwa die Comdirect, Commerzbank und Fidor-Bank. Eine vollständige Liste wurde bislang nicht veröffentlicht. Bei diesen Apps realisiert die Firma Promon die Absicherung und Verschlüsselung.

Doch um etwa Überweisungen mit ihrem Angriff zu manipulieren, mussten sie einige Hürden überwinden. Als Erstes sind sie über eine bekannte, aber nicht näher beschriebene Sicherheitslücke in ein Smartphone eingestiegen. Ob es sich dabei um ein Android- oder iOS-Gerät handelt, ist derzeit nicht bekannt. Die Sicherheitsforscher wollen Einzelheiten erst auf dem 34C3 des Chaos Computer Clubs vorstellen. Nach ihrem erfolgreichen Angriff auf das Smartphone befanden sich die Forscher in einer Position, in der sie die Banking-Apps über Sicherheitslücken attackieren konnten. Dabei haben sie die von der Firma Promon implementierten Sicherheitsmechanismen komplett umgangen. Das sei aber sehr aufwendig gewesen, schildern die Sicherheitsforscher. Promon ist im App-TAN-Bereich ein großer Fisch und hat eigenen Angaben zufolge rund 100 Kunden mit insgesamt 100 Millionen Nutzern.

Am sichersten ist es, wenn man die TAN mit einem zweiten Gerät erzeugt.

Updates in Sicht, aber …

Promon versichert, dass es bisher keinem Hacker in freier Wildbahn gelungen ist, ihre Sicherheitsmechanismen auszuhebeln. Die Interessenvertretung der Kreditinstitute Deutsche Kreditwirtschaft (DK) unterstreicht diese Aussage und sie halten „die Sicherheit der von den Banken und Sparkassen angebotenen Banking-Apps weiterhin für gewährleistet“. Viele abgesicherte Apps sollten mit Erscheinen des Heftes bereits veröffentlicht sein. Zum Zeitpunkt dieser Meldung hieß es von der DK, dass eine Reihe von Banken „in den nächsten Tagen“ Updates bereitstellen will. Doch die Updates lösen nicht das Grundproblem: Finden das Banking und die TAN-Generierung auf ein und demselben Gerät statt, ist dies ein erfolgversprechenderes Angriffsziel, als wenn beide Vorgänge auf getrennter Hardware stattfinden. Wer die Sicherheit beim Online-Banking steigern will, sollte also auf Zwei-Faktor-Authentifizierung mit zwei Geräten setzen. Derartige Geräte haben im Grunde alle Banken im Programm. Zum Beispiel stellen die Commerzbank und einige Volksbanken den Kunden Lesegeräte für das photoTAN-Verfahren zur Verfügung. Damit scannt man einen farbigen Barcode von einem Bildschirm, um eine Transaktionsnummer zu generieren. Auch das chipTAN-Verfahren ist eine Alternative. Dabei generiert ein EC-Kartenleser die TAN. Am besten fragen Sie Ihre Bank, ob diese Extra-Hardware zur TAN-Generierung anbietet.

Weit verbreitet ist das mTAN-Verfahren. Doch auch dieses Verfahren bietet Angriffspotenzial. Gängig ist etwa, dass Betrüger bei der Bank versuchen, die hinterlegte Nummer zu ändern.

Ernstfall

Man braucht vor dem Hintergrund der Analyse zur Sicherheit der TAN-Verfahren aber nicht in Panik zu verfallen: Letztlich ist die Bank dafür verantwortlich, dass die eingesetzten Verfahren ausreichend sicher sind. Ist das nicht der Fall und kommt es zu erfolgreichen Angriffen, muss die Bank für den entstandenen Schaden aufkommen. Das ist diesen auch durchaus bewusst. Etwa die in diesem Fall betroffenen Banken Comdirect und Commerzbank versicherten gegenüber c’t, dass sie im Schadensfall Privatkunden die vollständige Summe erstatten. *(des@ct.de)* c't