A-I3 Pressemeldung:
iTAN nur in Verbindung mit SSL sicher

Bochum, den 11.11. 2005

Zusammenfassung
Mitgliedern der *Arbeitsgruppe Identitätsschutz im Internet e.V.* ist es gelungen, einen funktionsfähigen Angriff auf das iTAN-Verfahren, das in letzter Zeit von vielen Banken als Schutz vor Phishing eingeführt wurde, zu implementieren. Es ist so gelungen, über eine gefälschte Webseite einen symbolischen Betrag von € 1 auf ein beliebiges anderes Konto zu transferieren.

Beschreibung des „Proof-of-Concept"-Angriffs
Durch einen „Man-in-the-Middle"-Angriff ist es einem Phisher möglich, durch Abfrage von Kontonummer/PIN und einer iTAN eine Überweisung durchzuführen und Geld vom Konto eines Opfers auf ein beliebiges Konto zu transferieren. Die Kommunikation zwischen dem Angreifer und dem Opfer wird automatisch von einem Skript auf dem Server des Angreifers durchgeführt. Das Skript leitet dabei die eingegeben Daten an den Bankserver weiter und reagiert auch auf die Rückfragen der Bank.

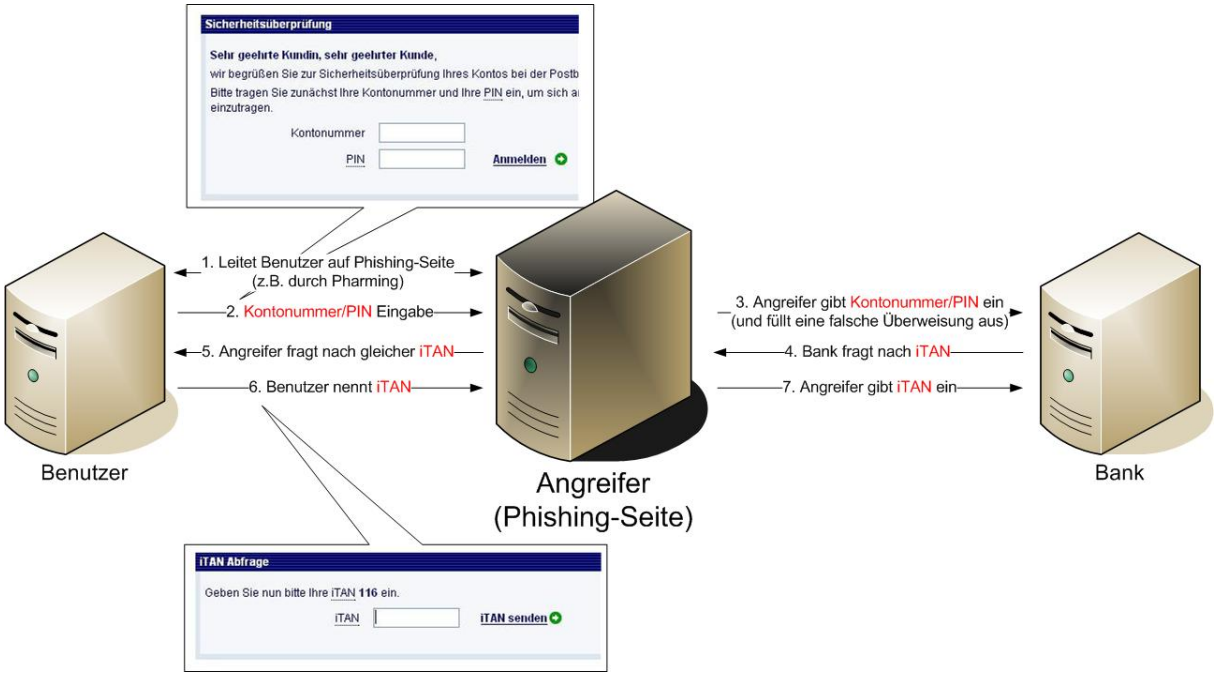

Abbildung 1: Funktionsweise des Man-in-the-Middle-Angriffs für iTAN-Verfahren. Der Angreifer sitzt hier in der Mitte zwischen dem Benutzer und der Bank.

Der Angreifer schickt seinem Opfer eine Phishing-Mail, so wie sie u. a. unter http://www.a-i3.org dokumentiert sind. Das Opfer wird unter einem konstruierten Vorwand (z. B. einer fingierten Sicherheitsüberprüfung des Kontos) durch einen Link in der E-Mail auf eine gefälschte Webseite des Angreifers geleitet, die der Bankenseite ähnelt (vgl. Schritt 1 in der obigen Abbildung). Auf dieser Webseite soll das Opfer zunächst die Kontonummer und die PIN angeben (Schritt 2). Mit diesen Kontodaten meldet sich dann das Skript, welches auf dem Server des Angreifers läuft, bei der richtigen Bank an: Das Skript „klickt" sich durch die einzelnen Webseiten der Bank, gibt die abgefragten Kontonummer und PIN ein, öffnet ein Überwei-

sungsformular und füllt dieses aus, sodass Geld vom Konto des Opfers auf ein Konto des Angreifers überwiesen wird (Schritt 3). Zum Absenden des Überweisungsformulars fragt der Bankserver nach einer iTAN (Schritt 4). Das Skript gibt diese Anfrage an das Opfer weiter, indem es z. B. vorgibt, dass zum Abschluss der Sicherheitsüberprüfung nach Eingabe von Kontonummer und PIN nun eine iTAN benötigt wird (Schritt 5). Nach der Eingabe dieser iTAN durch das Opfer (Schritt 6) gibt das Skript die iTAN an den Server der Bank weiter, um die Überweisung abzuschließen (Schritt 7).

Einschätzung des Angriffs

Auf die Anfälligkeit des iTAN-Verfahrens gegen „Man-in-the-Middle"-Angriffe wurde nach Einführung dieses Verfahrens schon wiederholt hingewiesen [1, 2].

Bei der vorliegenden „Proof-of-Concept"-Implementierung kommt die Möglichkeit einer Aufwandsabschätzung hinzu. Diese lag für einen nicht-spezialisierten Programmierer bei etwa einem Personentag. Somit kann nachgewiesen werden, dass iTAN marginal sicherer als das konventionelle TAN-Verfahren ist. Aufgrund des geringen Aufwandes ist daher damit zu rechnen, dass die Angriffe kurz- bis mittelfristig in der Praxis zum Einsatz kommen werden.

Die Arbeitsgruppe Identitätsschutz im Internet e.V. möchte betonen, dass sowohl TAN als auch iTAN-Verfahren bei korrekter Überprüfung der SSL-Verbindung sicher sind. Allerdings haben bisherige Phishing-Angriffe gezeigt, dass die Betroffenen den Schutzmechanismus SSL schlichtweg ignorieren. Hinweise zur korrekten Überprüfung von SSL-Zertifikaten sind z. B. unter [3] zu finden.

Das iTAN-Verfahren kann also kein Ersatz für SSL sein, sondern das Verfahren nur ergänzen. Hier ist bei den Kunden weitere Aufklärungsarbeit zu leisten.

Referenzen

[1] Arbeitsgruppe Identitätsschutz im Internet (A-I3)
https://www.a-i3.org

[2] Redteam: *Forschungsgruppe "RedTeam" der RWTH Aachen warnt vor trügerischer Sicherheit des neuen iTAN Verfahren.*
http://www.redteam-pentesting.de/press/iTAN.txt

[3] A-I3: *SSL als Schutz gegen Phishing und Pharming*. (08.11. 2005);
https://www.a-i3.org/content/view/407/28/

Weitere Informationen

Prof. Dr. Georg Borges
Juristische Fakultät der RUB
Tel. 0234/32-26775
E-Mail: georg.borges@rub.de