# 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 Angriffs

Bei diesem so genannten „Man-in-the-Middle"-Angriff sendet der Angreifer eine klassische Phishing-Mail, so wie sie z.B. unter www.a-i3.org dokumentiert sind, an das Opfer. Dieses wird mit einer falschen, aber plausiblen Begründung dazu gebracht, auf einen in der E-Mail enthaltenen Hyperlink zu klicken, und wird so mit der Webseite des Angreifers verbunden. Die aufgerufene Webseite sieht einer echten Webseite der Postbank zum Verwechseln ähnlich. Das Opfer könnte den Unterschied zwar durch Klicken auf das Schlosssymbol im unteren Rand des Browsers erkennen, dies unterblieb bei allen bisher bekannt gewordenen Phishing-Fällen in Deutschland aber aus Unwissenheit. Auf der gefälschten Webseite wird das Opfer zunächst aufgefordert, Kontonummer und PIN einzugeben. Sobald diese Daten beim Server des Angreifers eingetroffen sind, baut dieser eine Verbindung zum echten Postbankserver auf. Die bei einer Transaktion gestellte Frage nach der bestimmten iTAN wird dann automatisch an das Opfer weitergeleitet. So erhält der Angreifer genau die von der Postbank gewünschte iTAN und kann z.B. eine Überweisung tätigen.

## Einschätzung des Angriffs

Auf die Anfälligkeit des iTAN-Verfahrens gegen „Man-in-the-Middle"-Angriffe wurde nach Einführung dieses Verfahrens schon wiederholt hingewiesen (z.B. Pressemeldung von Redteam, RWTH Aachen). Bei der vorliegenden „Proof-of-Concept"-Implementierung kommt die Möglichkeit einer Aufwandsabschätzung hinzu. Diese lag für einen nicht-spezialisierten Programmierer bei etwa einem Personentag. Der Aufwand für die Anpassung eines solchen Angriffs auf weitere Banken wird als weitaus geringer eingeschätzt.

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 bzw. einfach nicht verstehen.

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

## Weitere Informationen

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