News-Meldung vom 23.11.2009 11:06

chipTAN-Verfahren der Sparkassen ausgetrickst

Der Sicherheitsdienstleister RedTeam Pentesting hat Wege **aufgezeigt[1]**, wie sich das derzeit von den Sparkassen eingesetzte "chipTAN comfort"-Verfahren angreifen lässt, sodass Betrüger eigene Überweisungen durchführen könnten.

Bei chipTAN comfort erzeugt ein spezielles Gerät die TAN für eine Transaktion. Nach Eingabe seines Auftrags hält der Kunde seinen optischen TAN-Generator mit eingebauten Fototransistoren vor den Bildschirm, auf dem die Bank einen Schwarz-Weiß-Blinkcode (Flickercode) sendet. Der Code enthält die Überweisungsdaten sowie weitere zur Berechnung der TAN benötigten Daten. Das Gerät zeigt nach dem Einlesen des Codes den Überweisungbetrag und das Konto an – eine Manipulation der Transaktion durch einen Betrüger oder Trojaner sollte normalerweise sofort auffallen. Nach dem Drücken der Bestätigungstaste erhält man die TAN. Soweit so gut.

Zumindest bei der Sparkasse lässt sich das Verfahren in Zusammenhang mit Sammelüberweisungen per Man-in-the-Middle-Attacke aushebeln. In einer Sammelüberweisung kann der Kunde einzelne Überweisungen zusammenfassen und mit einer einzigen TAN legitimieren. Der Haken an der Sache: Anders als bei Einzelüberweisungen erscheinen im "chipTAN comfort"-Gerät bei einer Sammelüberweisung nur die Gesamtsumme und die Anzahl der Überweisungen. Einzelne Zielkonten zeigt das Gerät nicht an. Somit hat der Kunde keine Möglichkeit eine Manipulation der Transaktionsdaten festzustellen. Ein Trojaner könnte beispielsweise die vom Kunden abgeschickten Daten im Browser abfangen und durch eigene Austauschen, sodass zwar die Summe und die Zahl der Überweisungen gleich, die Zielkonten aber andere sind.

Aber auch Einzelüberweisungen ließen sich auf diesem Wege manipulieren, wenn der Kunde nicht aufpasst. Dazu fängt ein Trojaner die Einzelüberweisung einfach ab und wandelt sie in eine Sammelüberweisung mit nur einer Überweisung um und schickt sie an die Bank. Den dann von der Bank übertragenen sogenannten Flickercode leitet der Trojaner an das Opfer weiter. Auf dessen Gerät erscheint nun die Summe, als Anzahl der Überweisung eine 1 und die TAN. Fällt dem Opfer nicht auf, dass das Gerät die Kontonummer des Empfänger nicht anzeigt und gibt es anschließend die TAN ein, so hat der Angreifer sein Ziel erreicht.

Aber auch die seit rund zwei Jahren mögliche **SEPA-Überweisung[2]** in Staaten der EU, Norwegen, Island, Liechtenstein und der Schweiz bietet Angriffsmöglichkeiten. Bei solchen Überweisungen zeigt der TAN-Generator den Betrag sowie das dritte und vierte sowie die letzten vier Zeichen der **IBAN[3]**, also einer internationalen Kontonummer an. Laut RedTeam Pentesting könnte ein Trojaner die IBAN austauschen und anschließend die auf der Webseite angezeigten Anleitung zur Prüfung der einzelnen Zeichen der IBAN manipulieren. Der Kunden würde beispielsweise als Hinweis sehen, dass er das siebte und achte Zeichen der Original-IBAN mit der Anzeige im Gerät vergleichen sollte.

RedTeam Pentesting hat nach eigenen Angaben innerhalb weniger Tage ein Beispielprogramm entwickelt, welches einen der vorgestellten Angriffe automatisiert durchführt. Dabei wurde eine Überweisung auf ein anderes Konto umgeleitet. Während die Angriffe auf Einzelüberweisungen und SEPA-Überweisungen von aufmerksamen Kunden bemerkt werden können, ist dies bei Sammelüberweisungen nicht möglich. Abhilfe brächte nur, alle Zielkonten ebenfalls im Gerät anzuzeigen und vom Kunden abnicken zu lassen.

Ob das von den Volks- und Raiffeisenbanken verwendete "Sm@rtTAN optic"-Verfahren ebenfalls angreifbar ist, schreibt Redteam in seinem Bericht nicht. Auf Nachfrage wollte sich Jens Liebchen, Geschäftsführer von Redteam Pentesting nicht festlegen. Man habe dort noch keine Tests durchgeführt, allerdings seien die Verfahren sehr ähnlich, sodass es sich vermutlich auf den gleichen Wegen aushebeln ließe.

Mit der Einführung der chipTAN-Verfahren hatten die Banken auf die immer erfolgreichereren Angriffe auf das iTAN-Verfahren reagiert, bei dem der Kunden gar keine Kontrollmöglichkeit hat, welche Transaktionen er legitimiert. Trojaner können so unbemerkt die Transaktionsdaten austauschen. Bei den neueren Verfahren sind die Auftragseinreichung und die TAN-Übermittlung zwei voneinander getrennte Prozesse. Auch bei mTAN respektive SMS-TAN sind die Prozesse getrennt. Hier wird aber die TAN auf einem vom PC unabhängigen zweiten Kanal per Handy zum Kunden übertragen. Leider bieten sich auch dort Angriffsmöglichkeiten, wenn der Kunde die mitgeschickten Kontrolldaten nicht sorgfältig prüft.

Siehe dazu auch:

- **BKA: iTAN-Verfahren keine Hürde mehr für Kriminelle[4]**
- **Zahl oder Karte, Sicherer Zugriff aufs Online-Konto[5]**

(**dab[6]**/c't)

URL dieses Artikels:
http://www.heise.de/security/meldung/chipTAN-Verfahren-der-Sparkassen-ausgetrickst-866115.html

Links in diesem Artikel:
[1] http://www.redteam-pentesting.de/en/publications/MitM-chipTAN-comfort/-man-in-the-middle-attacks-against-the-chiptan-comfort-online-banking-system
[2] http://de.wikipedia.org/wiki/%C3%9Cberweisung_%28Zahlungsverkehr%29#SEPA-.C3.9Cberweisung
[3] http://de.wikipedia.org/wiki/International_Bank_Account_Number
[4] http://www.heise.de/meldung/BKA-iTAN-Verfahren-keine-Huerde-mehr-fuer-Kriminelle-219497.html
[5] http://www.heise.de/ct/artikel/Zahl-oder-Karte-291676.html
[6] mailto:dab@heise.de