



23. November 2009

# PRESSEMITTEILUNG

## **Online-Banking: Erfolgreicher Angriff gegen chipTAN comfort-Verfahren**

Beim chipTAN comfort-Verfahren gefährden neu aufgedeckte Angriffsmöglichkeiten die Sicherheit des Online-Banking. RedTeam Pentesting gelang es, Überweisungen trotz des Einsatzes von chipTAN comfort unbemerkt auf dritte Konten umzuleiten.

Aktuell wird das chipTAN comfort-Verfahren unter anderem von den Sparkassen als neues, sicheres Online-Banking-Verfahren eingeführt.

### **ChipTAN comfort**

ChipTAN comfort ist ein neues Verfahren, welches die Sicherheit im Online-Banking verbessern soll. Statt klassischer TAN- oder iTAN-Listen wird ein zusätzliches Gerät mit eigenem Bildschirm verwendet. Dieses zeigt dem Benutzer die Transaktion zur Bestätigung an. So soll verhindert werden, dass Daten unbemerkt manipuliert werden.

### **Man-in-the-Middle-Angriffe auf chipTAN comfort**

Die vorgestellten Angriffe auf chipTAN comfort sind sogenannte Man-in-the-Middle-Angriffe. Dabei kontrolliert ein Angreifer den Datenverkehr zwischen dem Bankkunden und der Online-Banking-Webseite. Insbesondere sind auch Manipulationen des Datenverkehrs möglich. Solche Angriffe, zum Beispiel mittels Phishing und Trojanern, sind heute bereits gängige Praxis. Die gegen chipTAN comfort entwickelten Angriffe lassen sich trotz des zusätzlichen, vertrauenswürdigen Geräts nicht sicher erkennen. Die Anzeige des Geräts bestätigt die Anzeige der Online-Banking-Webseite.

RedTeam Pentesting hat innerhalb weniger Tage ein Beispielprogramm entwickelt, welches einen der vorgestellten Angriffe automatisiert durchführt. Im Rahmen einer Demonstration wurde von diesem Programm eine Überweisung auf ein anderes Konto umgeleitet.

Die von RedTeam Pentesting aufgedeckten Angriffsmöglichkeiten ähneln den bekannten Angriffen auf das iTAN-Verfahren und erfordern einen vergleichbaren Aufwand. Die entsprechen-



den Angriffsmöglichkeiten gegen iTAN wurden von RedTeam Pentesting bereits 2005 vorgestellt. Seit 2008 werden solche Angriffe auch in der Praxis beobachtet (vergleiche BKA: Kernaussagen zur IuK-Kriminalität 2008).

<http://www.redteam-pentesting.de/advisories/rt-sa-2005-014>  
[http://www.bka.de/lageberichte/iuk/2008/kernaussagen\\_iuk\\_2008.pdf](http://www.bka.de/lageberichte/iuk/2008/kernaussagen_iuk_2008.pdf)

Es ist zu vermuten, dass bei einer entsprechenden Verbreitung des chipTAN comfort-Verfahrens auch dieses vermehrt angegriffen wird.

Genaue technische Details zu den Angriffen sind unter

<http://www.redteam-pentesting.de/publications/MitM-chipTAN-comfort>  
veröffentlicht.

## RedTeam Pentesting GmbH

RedTeam Pentesting bietet individuelle Penetrationstests, durchgeführt von einem Team spezialisierter IT-Sicherheitsexperten. Ein Penetrationstest bezeichnet die Sicherheitsüberprüfung eines IT-Systems durch einen kontrollierten Angriff.

RedTeam Pentesting hat bereits 2005 Schwachstellen im iTAN-Verfahren aufgedeckt. Diese erstmalige Veröffentlichung von Angriffsmöglichkeiten auf das gerade neu eingeführte Verfahren wurde in der Öffentlichkeit viel beachtet.

## Kontaktmöglichkeiten

RedTeam Pentesting GmbH  
Dennewartstr. 25-27  
52068 Aachen

Tel. : +49 241 963-1300  
Fax : +49 241 963-1304  
E-Mail: [kontakt@redteam-pentesting.de](mailto:kontakt@redteam-pentesting.de)

<http://www.redteam-pentesting.de/>