Presse berichtet über geknacktes mTAN-Verfahren

Diverse deutsche Medien berichten aktuell, dass das mTAN-Verfahren - in der Fiducia IT AG unter dem Namen mobileTAN umgesetzt - ausgehebelt werden kann. In einer Stellungnahme der Deutschen Kreditwirtschaft wird das Verfahren weiterhin als hinreichend sicher betrachtet. Das mobileTAN-Verfahren der Fiducia beinhaltet weitere Sicherheitsfeatures.

Aktuell berichten mehrere deutsche Medien, dass das mTAN-Verfahren erfolgreich missbraucht wurde, ohne dass der Bankkunde hierbei durch offensichtliches Fehlverhalten den Missbrauch ermöglicht hat. Die Betrüger nutzten statt dessen aus, dass mindestens ein Mobilfunkanbieter anscheinend ohne ausreichende Authentifizierung seiner Kunden Ersatz-SIM-Karten oder Multi-SIM-Karten herausgab. Zusammen mit den vorher über einen infizierten PC abgephishten Zugangsdaten konnten die Betrüger nun beliebig Überweisungen ausführen.

Den Medienberichten zufolge entstand trotz der bisher geringen Anzahl von bekannt gewordenen Missbrauchsfällen ein vergleichsweise hoher Schaden im sechsstelligen Bereich, da gezielt besonders hohe Beträge von den betroffenen Konten abgephisht wurden. Beiträge zu dem Thema finden Sie unter anderem hier:

- Spiegel Online
- NTV
- Zeit.de
- Stern.de

Die Deutsche Kreditwirtschaft (DK), welcher auch der Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V. angehört, hat mit einer Stellungnahme auf die Medienberichte reagiert. In der Stellungnahme wird das mTAN-Verfahren als weiterhin hinreichend sicher bewertet, wenn alle Beteiligten ihrer Sorgfaltspflicht nachkommen. Hierzu zählt die Absicherung des PCs und des Smartphones durch den Kunden gegen Schadcode ebenso wie das Verhalten der Telekommunikationsunternehmen.

Das in der Fiducia eingesetzte mobileTAN-Verfahren erschwert den beschriebenen Angriff insofern, als dass im Online Banking nicht die komplette Handynummer des Kunden angezeigt wird. Dies erschwert potentiellen Angreifern die Arbeit, da eine direkte Zuordnung von Konto und Handynummer des Benutzers nicht mehr ohne größeren Aufwand möglich ist. Wegen der inzwischen sehr ausgefeilten Funktionen von Trojanern wie ZeuS und SpyEye ist es dennoch möglich, dass Angreifer an die Handynummer des Benutzers gelangen, beispielsweise, wenn dieser die Nummer in einem Formular einer anderen Webseite eingibt.