Bankkunden per Brief und Anruf von Betrügern kontaktiert - Appinstallation

Aktuell werden Kunden mehrerer Banken per Brief und telefonisch von Betrügern kontaktiert. In beiden Fällen werden die Kunden aufgefordert, bei Besitz eines Android-Smartphones eine "mobileTAN Security App" für das mobileTAN-Verfahren zu installieren. Die App leitet eingehende SMS um, so dass die Betrüger TANs generieren und missbrauchen können. Der Kontakt erfolgt zielgerichtet und schriftlich wie mündlich in gutem Deutsch. Der Betrugsversuch ist daher vermutlich schwer zu erkennen.

Aktuell liegt uns noch kein Schreiben vor, in dem Kunden einer Volks- und Raiffeisenbank aufgefordert werden, die angebliche **"mobileTAN Security App"** zu installieren. Kunden anderer Banken wurden mit einem Schreiben kontaktiert, das folgenden Wortlaut hat:

"[...] mit dem vorliegenden Schreiben möchten wir sie darüber informieren, dass es zu unserem Bedauern aktuell immer mehr zu Unregelmäßigkeiten im Bereich des Online-Bankings kommt. Das Smartphone, welches viele Kunden mittlerweile immer häufiger auch für das mobileTAN-Verfahren nutzen, spielt hierbei zunehmend eine tragende Rolle. Der vielfältige und somit auch leichtfertige Einsatz des Smartphones durch den Benutzer kann unter Umständen ein Sicherheitsrisiko darstellen.
Um dem rechtzeitig entgegenzuwirken, erweitert die [Bank] nun das mehrstufige Sicherheitskonzept um einen weiteren Schritt. In Einzelfällen wird dazu die Mithilfe von unseren Kunden benötigt. In diesem Zusammenhang wird Sie in den nächsten Tagen einer unser Mitarbeiter telefonisch kontaktieren um Ihnen alles weitere in Bezug auf Ihre Sicherheit und den sicheren Umgang mit Smartphones im mobileTAN-Verfahren zu erläutern.
In Ihrem Fall zu dem von Ihnen hinterlegten Mobiltelefon mit der Rufnummer: [Rufnummer des Kunden]
Dieser Service ist für Sie als [Bank] Kunde selbstverständlich kostenfrei. Wir bedanken uns im Vorfeld für Ihr Verständnis und bitten Sie, die möglichen Umstände zu entschuldigen".

In einem uns bekannten Fall wurde ein Bankkunde kurze Zeit später telefonisch von einem Betrüger kontaktiert, der ihn in akzentfreiem Deutsch dazu aufforderte, eine App von einer bestimmten URL (uns leider unbekannt) zu installieren. Die App ist nach unserem Kenntnisstand derzeit nur für **Android Smartphones** verfügbar.

Es ist davon auszugehen, dass die Betrüger Informationen über Adresse, Rufnummer und Bank des Kunden im Vorfeld in Erfahrung gebracht haben, beispielsweise durch **Einsatz des ZeuS-Trojaners** oder eines anderen Schädlings auf dem PC des Bankkunden. Diese sind in der Lage, sämtliche Eingaben des Benutzers am PC mitzuschneiden, z. B. beim Ausfüllen eines Formulars. So können die Betrüger leicht an alle benötigten Daten kommen. Möglicherweise erfolgen die Angriffe nun im Rahmen einer "Welle", um vor öffentlichem Bekanntwerden der Betrugsmasche möglichst viel Gewinn zu erzielen. Hat der Bankkunde einen Trojaner auf seinem PC, durch den die Betrüger an die Zugangsdaten für das eBanking gekommen sind, und installiert zusätzlich die "mobileTAN Security App", so können die Betrüger beliebig Transaktionen auf dem Konto des Bankkunden ausführen. Wenn der Trojaner nicht durch einen Virenscanner entdeckt wird und sich nicht wie bisher durch eine seltsame Aufforderung dem Benutzer gegenüber zu "erkennen" gibt (Aufforderung zu einer Testüberweisung, Rücküberweisung o. ä.), ist es für den Bankkunden kaum noch feststellbar, dass ein Betrugsversuch vorliegt, da er bei entsprechend seriösem Schreiben und Anruf vermutlich davon ausgehen wird, tatsächlich von seiner Bank kontaktiert zu werden.

Bei der Analyse der "mobileTAN Security App" durch Sicherheitsexperten wurde festgestellt, dass die Betrüger durch das Senden von SMS von einer bestimmten Rufnummer aus ein- und ausschalten können, ob der Besitzer des Smartphones eine SMS erhält oder nicht. Die Betrüger setzen diese Funktion vermutlich gezielt ein, um nur die SMS abzufangen, mit denen sie eigene TANs für Überweisungen generieren. So schöpft der Kunde keinen Verdacht. Es ist ebenfalls davon auszugehen, dass ein vorhandener Trojaner den Kontostand des Kunden im eBanking wie bisher so verschleiert, dass die betrügerischen Transaktionen erst bei Erhalt des Kontoauszugs oder bei eBanking auf einem "sauberen" PC auffallen.

Quelle: intern