Wie sich Sicherheitslücken auf mobile Banksysteme auswirken - Ein Kommentar von Michael Flossman, Security Research Services Lead EMEA bei Lookout

Immer mehr Geldhäuser sehen sich gezwungen, in ihre Systeme für den Geldtransfer zusätzliche Sicherheitskontrollen einzubauen. Denn die Kosten, die sie ihren Bankkunden aufgrund von gefälschten und illegalen Transaktionen erstatten müssen, sind immens.

Beispiele für solche Vorfälle liefern die Desktop-Malware-Familien SpyEye und Zeus, die sensible Informationen, darunter auch Bankdaten, von den infizierten PCs abgreifen. Diese Desktop-basierten Bedrohungen sind zumindest mitverantwortlich dafür, dass einige Banken mittlerweile den Einsatz so genannter mTANs (mobile transaction authentication numbers) implementiert haben. Damit erfordert jede Online-Transaktion einen speziellen Token, der an das mobile Endgerät des Users geschickt wird. Die beiden genannten Malware-Familien haben sich bereits entsprechend angepasst: Sie ergänzen ihr traditionell Desktop-basiertes Malware-Arsenal um mobile Komponenten - in diesem Fall Spitmo und Zitmo – um weiter profitabel zu bleiben.

Immer mehr Banken in Westeuropa verabschieden sich daher von mobilen TANs und verwenden stattdessen physische, nicht mit dem Internet verbundene Tokens, die eine Zwei-Faktor-Authentisierung bieten. Ein Beispiel hierfür ist der Smart Card Reader PINsentry von Barclays: Nachdem der User seine Bankkarte damit eingelesen und die PIN eingegeben hat, erhält er einen kurzzeitig gültigen Code für die gewünschte Transaktion. Dieser Ansatz macht es Angreifern wesentlich schwerer und schließt Attacken via Fernzugriff, bei denen betrügerische Transaktionen auf dem betroffenen Smartphone erfolgen, so gut wie aus.

Es gibt allerdings nach wie vor eine Reihe von aktiven Bank-Trojanern, die Kunden von Finanzdienstleistern im Visier haben, bei denen es derartige Schutzmechanismen nicht gibt. Meist handelt es sich dabei um Malware aus Regionen, in denen das Sicherheitsniveau der Banken relativ gering ist. Vermutlich sind diese Trojaner deshalb auch in Osteuropa besonders stark verbreitet. SpyEye und Zeus waren die Antwort auf die vermehrte Nutzung von mTANs. Jetzt bin ich gespannt, auf welche Taktiken sich diese Malware-Familien in Märkten verlegen, in denen die Banken strenge Sicherheitskontrollen im Transaktionsbereich – zum Beispiel PINSentry – implementiert haben.

In den letzten Jahren ist eine Vielzahl von Anwendungen auf den Markt gekommen, mit denen Kunden untereinander schnell Geld transferieren können - darunter Pingit, Swish Payments, Apple Pay, Google Wallet und sogar der Facebook Messenger. Gleichzeitig verschärfen viele Banken ihre Sicherheitsmaßnahmen. Die entscheidende Frage ist jetzt, wie die betrügerischen Akteure darauf reagieren – zum Beispiel, ob sie sich künftig nur noch auf mobile Bezahlanwendungen konzentrieren, für die kein physischer Token erforderlich ist.

Pressekontakt:

Gabi Ölschläger
Telefon: 07071 / 93872 - 217
E-Mail: g.oelschlaeger@storymaker.de

Unternehmen

Storymaker Agentur für Public Relations GmbH
Derendinger Straße 50
72072 Tübingen

Internet: www.storymaker.de