E-Banking: Angreifer haben es auf Aktivierungsbriefe abgesehen

Ende 2016 hat MELANI in einem Newsletter darauf hingewiesen, dass Kriminelle vermehrt mobile Authentifizierungsmethoden beim E-Banking im Visier haben. Nun gehen die Angreifer einen Schritt weiter und versuchen Opfer dazu zu bringen, eine Kopie des von der Bank erhaltenen Briefes, welcher Aktivierungsdaten für die die Zwei-Faktor Authentifizierung (2FA) des E-Bankings enthält, an die Betrüger zu senden.

Seit 2016 versuchen Angreifer mit Hilfe von Schadsoftware («Malware») wie beispielsweise «Retefe» mobile Authentifizierungsmethoden auf dem Smartphone mittels Social Engineering zu umgehen. Betroffen von solchen Angriffen sind Benutzerinnen und Benutzer von PhotoTAN, CrontoSign und SecureSign. Dies ist unabhängig von dem verwendeten Smartphone-Betriebssystem (Android, iOS).

Seit rund zwei Wochen beobachtet die Melde- und Analysestelle Informationssicherung (MELANI) nun auch vermehrt Angriffe, bei welchen die Angreifer versuchen, an Briefe von Banken mit Aktivierungsdaten zu gelangen. Dieser Aktivierungsbrief enthält üblicherweise ein Mosaikbild, welches beim erstmaligen Login eines Gerätes ins E-Banking mit einer App wie PhotoTAN, CrontoSign oder SecureSign eingescannt bzw. abfotografiert werden muss. Anschliessend wird das entsprechende Gerät von der Bank für die mobile Authentifizierungsmethode zugelassen. Diese Briefe werden in der Regel von der Bank per Briefpost an die Kundinnen und Kunden versendet. Die Angreifer versuchen nun, mittels Social Engineering an die Aktivierungsdaten zu gelangen und fordern das Opfer dazu auf, diesen Brief einzuscannen oder zu fotografieren und an die Betrüger zu übermitteln.

Betrüger fordern das Opfer nach dem Login ins E-Banking auf, den Aktivierungsbrief einzuscannen und den Betrügern zu übermitteln.

Durch die Bekanntgabe der Information, welche im Aktivierungsbrief in Form eines Mosaikbildes hinterlegt sind, ist es den Betrügern unter Umständen möglich, sich in das E-Banking des Opfers einzuloggen, indem sie ein weiteres Smartphone für die Zwei-Faktor Authentifierzung (2FA) aktivieren. Ab diesem Zeitpunkt können sich die Angreifer jederzeit in das E-Banking Portal einloggen und ohne das Wissen des Opfers betrügerische Zahlungen von dessen Konto in Auftrag geben.

Im Umgang mit E-Banking empfiehlt MELANI:

- **Den Aktivierungsbrief, welchen Sie von der Bank erhalten haben, ist persönlich. Teilen Sie diesen mit niemanden, auch nicht mit der Bank, selbst wenn Sie dazu aufgefordert werden. Im Zweifelsfall kontaktieren Sie telefonisch Ihre Bank oder Ihren Kundenberater.**
- **Stellen Sie sicher, dass Sie beim Login-Vorgang ins E-Banking auf dem mobilen Gerät (beispielsweise Smartphone oder dediziertes PhotoTAN-Gerät) wirklich das Login bestätigen und dass es sich nicht bereits um die Visierung einer Zahlung handelt.**
- **Falls Sie eine Zahlung visieren, lesen Sie immer den ganzen Text auf dem mobilen Gerät und überprüfen Sie Betrag und Empfänger (Name, IBAN) der Zahlung, bevor Sie diese freigeben.**

- Installieren Sie Smartphone-Apps nur aus dem offiziellen App-Store (Google Play bzw. Apple App Store). Installieren Sie niemals Apps aus unbekannten Quellen, auch nicht wenn Sie dazu aufgefordert werden. Modifizieren Sie Ihr Gerät nicht so, dass wesentliche Sicherheitsmechanismen ausgehebelt werden (z.B. „rooten", „jailbreaken").
- Spielen Sie Sicherheitsupdates sowohl für den Computer wie auch für das Mobiltelefon ein, sobald eine solche Aktualisierung vorhanden ist.
- Sollten Sie beim Login in das E-Banking Unregelmässigkeiten feststellen, kontaktieren Sie unverzüglich Ihre Bank. Solche Unregelmässigkeiten sind beispielsweise:

  Sicherheitsmeldung **vor dem Login** ins E-Banking. Zum Beispiel „*In Zusammenhang mit der Modernisierung des Sicherheitssystems kann von Ihnen beim Einloggen ins Benutzerkonto eine zusätzliche Identifizierung angefordert werden. […]*"

  Fehlermeldung **nach dem Login** ins E-Banking. Zum Beispiel „*Fehler! Wegen eines technischen Problems sind wir unfähig, die Seite zu finden, nach der Sie suchen. Versuchen Sie bitte in 2 Minuten noch einmal.*

  Sicherheitsmeldung **nach dem Login** ins E-Banking (z.B. „*Sicherheitsmassnahme*"), bei welcher Sie dazu aufgefordert werden, Festnetz- oder Handy-Nummer einzugeben

  Aufforderung zur Installation einer Mobile-App **nach dem Login** ins E-Banking

  Nach dem Login ins E-Banking erfolgt eine Weiterleitung auf eine Website, die nicht in Zusammenhang mit der Bank steht (z.B. auf google.ch).

  Timer **nach dem Login** ins E-Banking. Zum Beispiel: „*Bitte warten… (Bitte warten Sie eine Minute, die Seite nicht neu laden)*"

Links:

E-Banking: Angreifer zielen auf mobile Authentifizierungsmethoden
(/melani/de/home/dokumentation/newsletter/mobileauthentifizierungsmethoden.html)

Schadsoftware: Vorsicht ist geboten - unabhängig vom Betriebssystem
(/melani/de/home/dokumentation/newsletter/malware---si-raccomanda-prudenza-indipendentemente-dal-sistema-o.html)

MELANI/GovCERT-Blog - The Retefe Saga
(https://www.govcert.admin.ch/blog/33/the-retefe-saga)

✉ Fachkontakt
(mailto:info@melani.admin.ch)

Letzte Änderung 17.08.2017

E-Banking: Angreifer zielen auf mobile Authentifizierungsmethoden
(/melani/de/home/dokumentation/newsletter/mobileauthentifizierungsmethoden.html)

https://www.melani.admin.ch/content/melani/de/home/dokumentation/newsletter/e-banking--angreifer-haben-es-auf-aktivierungsbriefe-abgesehen.html