idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Friedrich-Alexander-Universität Erlangen-Nürnberg
Dr. Susanne Langer

20.10.2016
http://idw-online.de/de/news661628

Forschungsergebnisse
Gesellschaft, Informationstechnik
überregional

PhotoTAN-Banking nicht sicher

Mobiles Banking mit dem Smartphone – an jedem Ort, zu jeder Zeit, mit nur einem Gerät. Immer mehr Menschen nutzen diese bequeme Art des Online-Bankings, und immer mehr Banken bieten diesen Service an. Das Problem: Transaktionen via Smartphone sind nicht sicher. Das haben Informatiker der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) mit einem erfolgreichen Angriff auf die photoTAN-Verfahren dreier Kreditinstitute bewiesen. Erst im vergangenen Jahr hatten die Wissenschaftler mit einer Manipulation der pushTAN-App der Sparkasse die konzeptionelle Schwäche des Ein-Geräte-Bankings aufgezeigt.

Die photoTAN-App ist eine beliebte Authentifizierungslösung für mobiles Banking, die gerade in Deutschland und in der Schweiz weite Verbreitung findet. Beim photoTAN-Verfahren muss der Nutzer einen Matrixcode vom PC, Notebook oder Tablet abscannen; die Smartphone-App generiert daraus eine TAN. „Das ist grundsätzlich ein sicheres Verfahren, weil daran zwei voneinander unabhängige Geräte beteiligt sind“, sagt Vincent Haupert vom Lehrstuhl für IT-Sicherheitsinfrastrukturen der FAU. „Um hier eine Manipulation vornehmen zu können, müsste der Angreifer beide Geräte kontrollieren.“ Genau dieses Sicherheitskonzept aber wird beim mobilen photoTAN-Banking ausgehebelt: Weil man den auf dem Smartphone bereitgestellten Matrixcode nicht mit demselben Gerät abscannen kann, greift die Banking-App direkt auf die TAN-App zu, um die Transaktion auslösen zu können.

PhotoTAN-Verfahren erfolgreich manipuliert
Dass die Zusammenführung der Zwei-Faktor-Authentifizierung auf einem Gerät zu Sicherheitslücken führt, haben Vincent Haupert und sein Kollege Dr. Tilo Müller jetzt erneut gezeigt: Die Informatiker haben die photo-TAN-Apps der Deutschen Bank, der Commerzbank und der Norisbank – exemplarisch für weitere Banken, die dieses System anbieten – auf einem Smartphone gehackt und sowohl den Empfänger als auch den Betrag einer Transaktion in Echtzeit manipuliert. „Während auf dem Display eine Überweisung von zehn Cent an das Finanzamt angezeigt wurde, haben wir in Wirklichkeit 13 Euro auf ein privates Konto überweisen“, sagt Haupert. „Die manipulierte Transaktion war für den Nutzer zu keiner Zeit sichtbar.“ Den Wissenschaftlern ist es sogar gelungen, die photoTAN-App auf das Gerät des Angreifers zu kopieren. Die replizierte Version der App generiert daraufhin die gleichen TANs wie die des Originals. Haupert: „Wenn es einem Angreifer gelingt, die Zugangsdaten der Banking-App zu erlangen, kann er letztlich beliebige Transaktionen zu Lasten des Opfers vornehmen.“

Alle App-basierten Verfahren des mobilen Bankings betroffen
Brisant sind die Ergebnisse der FAU-Informatiker auch vor dem Hintergrund der im Januar 2016 in Kraft getretenen Zweiten Zahlungsdiensterichtlinie (PSD II), die nach einer Übergangsphase von zwei Jahren für alle Zahlungsdienstleister verbindlich wird. Hierfür hat die Europäische Bankenaufsichtsbehörde EBA vor kurzem einen Entwurf zur konkreten Ausgestaltung der obligatorisch werdenden starken Kundenauthentifizierung vorgelegt. Danach müssen Onlinezahlungen mit zwei unabhängigen Authentifizierungselementen aus dem Bereich Wissen (Passwörter, Codes), Besitz (EC-Karte, TAN-Generator, Smartphone) und Inhärenz (biometrische Merkmale wie Fingerabdruck oder Iris) autorisiert werden. Darüber hinaus muss die Unabhängigkeit der verwendeten Elemente garantiert werden, so dass ein kompromittierter Faktor nicht auch das zweite Authentifizierungselement kompromittiert. „Unsere Untersuchung

stellt die Unabhängigkeit der Authentifizierungselemente infrage, wenn beide Faktoren – im konkreten Fall die Banking-App und die photoTAN-App – auf demselben Smartphone betrieben werden“, erklärt Vincent Haupert. „Diese Erkenntnis gilt nicht nur für die von uns analysierten pushTAN- und photoTAN-Verfahren, sondern lässt sich grundsätzlich auf alle App-basierten Authentifizierungsverfahren im Onlinebanking übertragen.“

TAN-Generator schafft Sicherheit
Auf den Komfort des mobilen Bankings müsse man dennoch nicht verzichten, sagen die FAU-Wissenschaftler, allerdings sollte man für seine Transaktionen einen dedizierten photoTAN-Generator nutzen, den die Bank zur Verfügung stellt. Ein solcher Generator übernimmt die Funktion der photoTAN-App des Smartphones, scannt den Matrix-Code der Banking-App und stellt eine TAN für die entsprechende Transaktion bereit – wie wir es vom bewährten chipTAN-Generator des Online-Bankings kennen. „Ein photoTAN-Generator ist klein und handlich und lässt sich leicht mitführen“, sagt Vincent Haupert. „Da er ausschließlich für die Generierung von TANs konstruiert ist und keine sonstigen Funktionen und Schnittstellen bietet, ist er auch nicht zu hacken oder mit Schadsoftware zu infizieren. Das macht mobiles Banking deutlich sicherer.“

Weitere Informationen:
Vincent Haupert
vincent.haupert@cs.fau.de