06.09.2011

Risiko Smartphone
Wie sicher ist das Bezahlen mit dem Handy?

Hendrik Loven, Annette Peter

Wir treffen Hacking-Experten in Europa. Sie werden uns gravierende Sicherheitslücken von Smartphones zeigen - bis hin zum Ausspähen von Konto- und Benutzerdaten

Technische Universität Darmstadt.

Prof. Sadeghi und sein Team zeigen uns, wie man Smartphones ausspionieren kann. Und zwar beim Online-Banking. Die Bedrohung ist real: In den USA wurden bereits Konten von Smartphone-Besitzern ausgespäht. Durch ein Spionage-Programm - genannt ZeusTrojaner. Eine große Sicherheitslücke: die bei den Benutzern so beliebten Apps. Sadeghi und sein Mitarbeiter simulieren extra für report MÜNCHEN den Angriff. Sie haben eine App für das Handy programmiert, wie sie derzeit tausendfach auf Smartphones geladen wird: vordergründig eine harmlose Einkaufs-Hilfe.

Sven Bugiel, TU Darmstadt: *"Was sie aber jetzt im Hintergrund gemacht hat, dass sie sich zu unserem Attack-Server verbunden hat und bei dieser Verbindung hat sie direkt mit übertragen z.B. die Telefonnr. dieses Gerätes, also der SIM-Karte, die Geräte-Identifizierer also die EMI-Nummer oder auch die Nummer der SIM-Karte."*

Das ist nicht alles: Der Trojaner wandert vom Smartphone auf den PC, wenn man es zum Akkuaufladen oder Synchronisieren von Terminen anschließt. Und wie auf dem Smartphone kopiert er auch hier alle Daten wie z.B. das Bankpasswort und sendet es unbemerkt an den Server des Hackers. Jetzt verschicken wir eine SMS wie von einer Bank, mit einer TAN-Nummer - so wie beim Online-Banking auch und die landet direkt beim Hacker

Sven Bugiel, TU Darmstadt: "*Ich sehe hier direkt im Text die TAN für die Einzelüberweisung vom 31. August über € 39,85 für das Konto so und so lautet: 79415."*

Mit TAN und Bankpasswort können die Hacker jetzt Überweisungen auf andere Konten leiten oder den Zugang ganz sperren.

Prof. Ahmad-Reza Sadeghi, TU Darmstadt: *"Das sind auch Kriminelle, die sich damit beschäftigen oder organisierte Experten, die gezielt eine bestimmte vielleicht Person angreifen wollen oder die Bank."*

report MÜNCHEN fragt beim Bankenverband *"Deutsche Kreditwirtschaft"* nach. Hier gibt man die Verantwortung an den Kunden weiter.

Antwort Bankenverband:
"Der Kunde sollte auf keinen Fall ein und dasselbe Smartphone für die Übermittlung der TAN

und das Online-Banking selbst nutzen. Hält der Kunde seine Sorgfaltspflicht ein, ist er auch im Schadensfall auf der sicheren Seite."

Verbraucherschützer halten diese Antwort für weltfremd

Sascha Straub, Verbraucherzentrale Bayern: *"Die Banken setzen hier voraus, dass man zwei Smartphones besitzt. Dass geht an der Lebenswirklichkeit des Durchschnittsverbrauchers aber vorbei."*

Google - führender Hersteller für Smartphone-Betriebssysteme wie Android, antwortet uns auf die Frage nach der Sicherheit:

"Unser Ziel ist es, für jedermann die sichere Nutzung von Android zu gewährleisten. Unter dieser Zielsetzung hat das Android-Team hart daran gearbeitet, die Sicherheitsrisiken von Android-Geräten zu minimieren."

Wir fragen auch bei Apple nach:
Existieren bereits Sicherheitsprogramme z.B. Anti-Trojaner-Programme, um das Ausspionieren oder anderen Missbrauch auf Apples iPhone auszuschließen?

Die Antwort:
"Dazu geben wir keinen Kommentar."

In der Nähe von Zürich sind wir bei einer Firma für Datensicherheit. Sie zeigen uns weitere Sicherheitslücken. Angriffe durch die beliebte SMS. Die Experten der Firma simulieren für report MÜNCHEN eine typische SMS-Attacke, so genanntes Phishing.

Marco di Filippo, Compass Security: *"Diesen Angriff, der wird sehr häufig genutzt um letztendlich an Bankdaten und Zugangsdaten von Online-Shops zu kommen und letztendlich da wiederum die kompletten Informationen und Inhalte auszulesen."*

Als Angreifer verschickt er eine SMS an das potentielle Opfer. Er tarnt sich als Firma.
Der Nutzer öffnet den Link in der SMS. Die falsche Seite des Angreifers sieht aus wie das Original - sie ist aber eine Kopie. Gibt das Opfer seine Daten ein, leitet er sie unbemerkt weiter an die Datenbank des Hackers. Hat der Angreifer Name und Passwort, kann er sich mit den geklauten Daten einloggen und dann völlig ungestört hinterlegte Daten wie die Kreditkartennummer stehlen.

Marco di Filippo, Compass Security: *"Ich könnte auch die Kreditkartendaten nehmen und damit auf anderen Shops einkaufen gehen."*

In Hannover treffen wir Wulf Bolte. Er ist Berater für Datensicherheit. Für report MÜNCHEN lässt er sein Handy ausspionieren: SMS, Telefonate, Adressbuch, und Passwörter. Sie spionieren mit einem Programm, dass man für rund 20 Euro im Internet kaufen kann. Funktioniert es so simpel?

Seine Daten kommen bei seinem Kollegen Dennis Weber an.

Dennis Weber, Praemandatum:
"Das war eine ankommende SMS und wir sehen auch von welcher Telefonnummer die SMS kam. Und kurz danach wurde auch schon geantwortet: Super, bis dann."

So eine Spionage-Software ist kinderleicht zu bedienen - wie uns diese Anleitung zeigt. Spionage-Apps für jedermann - mit denen man sogar illegal Bank-TANs ausspionieren könnte.

Wulf Bolte, Praemandatum:
"Ich halte es für grundsätzlich falsch diese alten etablierten Kommunikationskanäle für Authentifizierung von Bezahlverfahren zu nutzen. Eine SMS ist ein leicht abzuhörendes, leicht zu manipulierendes Objekt - da darf ich keine Transaktionen mit legitimieren. (…)"

Wir konfrontieren das Bundesinstitut für Sicherheit in der Informationstechnik vom Innenministerium in Bonn mit unseren Recherchen. Im BSI bestätigt man unsere Recherchen

Gerhard Schabhüser, Bundesinstitut für Sicherheit in der Informationstechnik: *"Das BSI ist der Überzeugung, dass künftig die Hersteller deutlich stärker IT-Sicherheit in ihre Produkte einführen müssen. Das ist besonders deshalb wichtig, weil wir erwarten, dass kommerzielle Anwendungen, mobile Banking, aber auch geschäftliche Prozesse auf den Smartphones abgewickelt werden, doch der Schaden heute durchaus nur bei den Nutzern liegt."*

Verbraucherzentralen warnen:

Sascha Straub, Verbraucherzentrale Bayern: *"Wir empfehlen daher, keine Smartphones für das Online-Banking einzusetzen!"*

Die Smartphone-Hacker bleiben übrigens meist unerkannt, können daher strafrechtlich auch kaum belangt werden.