SECURITY SPECIAL

AUF DER SICHEREN SEITE

So schützen Sie sich vor Abzock-Apps, Viren und Diebstahl

Die Offenheit von Android und vor allem die App-Veröffentlichungspolitik im Android Market haben nicht nur Vorteile. Die Kehrseite dieser Medaille sind Anfälligkeit gegen Viren und eine hohe Anzahl von Malware- und Abzock-Apps im Market. Auf Smartphones und Tablets sind aber nicht nur private Daten zu holen, vielen Kriminellen geht es auch um nichts Geringeres als Ihr Geld. Grund genug also, um uns auf den folgenden Seiten dieser Problematik in einem ausführlichen Sicherheits-Spezial zu widmen.

Raphael Schön
Chefredakteur

Frag Raphael zum Artikel:
www.androidmag.de/heft/security

Mit Tipps von

Eddy Willems
Security Evangelist

Vielfältige Bedrohungen

Wenn unseriöse Apps Kontaktdaten oder SMS-Nachrichten ausspionieren und an dubiose Server im Internet weiterleiten, ist das natürlich unangenehm, in der Regel aber immerhin nicht mit Folgekosten verbunden. Meist werden diese Daten verkauft und machen sich dann in weiterer Folge als lästige Spam-Mails oder nicht weniger nervige Marketing-Telefonanrufe bemerkbar. Eine weitaus größere Bedrohung stellen hingegen Apps dar, die es direkt auf Ihr Geld abgesehen haben. Für Eddy Willems, Sicherheitsexperte der ersten Stunde und derzeit bei G Data tätig, liegt genau hier das größte Risiko für Android-Nutzer. „Die unbemerkte Kommunikation mit teuren Premium-Nummern und das Ausspionieren von Online Banking-Applikationen sind die beiden größten Sicherheitsrisiken", sagte Willems im Gespräch mit dem Android Magazin.

Während der Sicherheitsexperte positiv hervorhebt, dass bei Android sämtliche Applikationen in einer virtuellen Maschine laufen, sieht er in der Versions-Zersplitterung einen der größten Schwachpunkte des Betriebssystems. Im September 2011 verwendeten etwa noch immer über 50% der Nutzer die nicht mehr aktuelle Version 2.2 und sogar noch 13% die veraltete Version 2.1 des Betriebssystems. Ein Problem ist das vor allem deshalb, weil so gut wie alle Hersteller Android modifizieren und Updates erst verspätet oder gar nicht mehr ausliefern. Der Trojaner DroidDream nutzte etwa eine Sicherheitslücke aus, die erst mit Version 2.2.2 geschlossen wurde. Wer (gezwungenermaßen) eine alte Android-Version auf seinem Smartphone oder Tablet installiert hat, sollte daher unbedingt auf Anti Viren-Software zurückgreifen.

Vertrauen ist gut, Kontrolle ist besser

Nicht unproblematisch ist auch die Tatsache, dass neue Apps völlig ungeprüft im Android Market landen, und erst später (nach einigen User-Beschwerden), einer Prüfung unterzogen werden. So kommen ständig neue zwielichtige Apps hinzu, die erst dann gelöscht werden, wenn sie bereits Schaden angerichtet haben. Der Trojaner DroidDream hatte so etwa genug Zeit, um Informationen wie IMEI-Nummer des Smartphones, SMS-Nachrichten oder Telefonnummern auszulesen und an Server von Internetkriminellen weiterzuleiten. Wenn die befallene App dann von Google überprüft und aus dem Android Market entfernt wird, wird sie in der Regel auch per Fernlöschung von allen Geräten entfernt, auf denen sie installiert wurde. Die privaten Daten sind dann aber dennoch bereits erbeutet worden. Eddy Willems rät zu einer Kombination aus vorsichtiger Herangehensweise an neue, unbekannte Apps und der Verwendung einer vernünftigen Anti Viren-App.

Fragwürdige Berechtigungen und Market-Alternativen

Ein Sicherheitsrisiko, das sich ganz einfach durch ein wenig Vorsicht in den Griff bekommen lässt, ist das Thema Berechtigungen. Wenn Sie eine neue App installieren, werden Ihnen im Webbrowser oder direkt am Android-Gerät meist eine Reihe von Berechtigungen aufgelistet, die die App benötigt. Selbst Apps von bekannten Anbietern wollen häufig mehr Berechtigungen, als eigentlich nötig wäre. Sie sollten daher immer überprüfen, worauf welche App Zugriff einfordert und im Zweifelsfall von einer Installation der App absehen. „Häufig werden Berechtigungen erst im Zuge von Updates ausgeweitet. Hier kann man auch als vorsichtiger Benutzer schnell den Überblick verlieren", so Eddy Willems zur Update-Problematik. Wie bereits angesprochen, ist Google vor allem seit dem Auftauchen immer neuer Schad-Apps sehr darum bemüht, diese weitestgehend einzudämmen. Doch da ist noch ein weiterer Unsicherheitsfaktor, auf den Google selbst überhaupt keinen Einfluss hat, nämlich der Vielzahl an alternativen App-Märkten und den dort angebotenen Apps. Sollten Sie neue Apps also häufig von alternativen Android-Markets herunterladen, kann ein erhöhtes Maß an Vorsicht sicherlich nicht schaden.

Die größten Android-Sicherheitsrisiken

- Automatisiertes versenden von SMS an teuren Premium-Nummern
- Ausspionieren von Online Banking-Applikationen
- Kleinere Malware Apps, die verschiedene private Daten versenden
- Zersplitterung der Android-Versionen
- Fragwürdige App-Berechtigungen (und deren Ausweitung durch Updates)
- Inoffizielle Markets mit fragwürdigen Kontrollmechanismen

Vier Tipps für mehr Sicherheit

Mögliche Sicherheitsrisiken gibt es bei Android viele. Mit diesen vier grundlegenden Tipps sind Sie aber schon ganz gut gegen die meisten Bedrohungen gewappnet.

1 Smartphone abriegeln

Eine simple aber ebenso effektive Absicherung gegen Diebe und neugierige Zeitgenossen ist die Verwendung einer Display-Sperre. Die entsprechenden Einstellungsmöglichkeiten finden Sie, indem Sie die Menütaste drücken und dann „Einstellungen > Standort & Sicherheit > Display-Sperre einrichten" auswählen. Dort können Sie festlegen, ob für das Entsperren des Gerätes die Eingabe eines Musters, PINs oder Passworts nötig ist.

2 Vorsicht mit WLAN- und Bluetooth-Verbindungen

Wer sich häufig in offene WLAN-Netze einwählt, sollte sich bewusst sein, dass dadurch der Datenverkehr des eigenen Gerätes relativ leicht ausgelesen werden kann. Ebenso vorsichtig sollte man mit automatischen Bluetooth-Handshakes sein, da findige Hacker auch hier Methoden entwickelt haben, um die Kontrolle über das Smartphone zu erlangen. Am besten Sie aktivieren die WLAN- und Bluetooth-Verbindungen in den Einstellungen unter „Drahtlos & Netzwerke" nur dann, wenn Sie diese auch brauchen. Das spart nicht nur Akku, sondern erhöht auch die Sicherheit.

3 Apps vor der Installation immer überprüfen

Wie bereits erwähnt, sollten Sie immer ein wachsames Auge auf die benötigten Berechtigungen einer App werfen. Vor der Installation sollten Sie auch immer den App-Entwickler überprüfen, denn häufig werden im Market gefälschte und virenbefallene Versionen von besonders erfolgreichen Apps wie etwa Angry Birds angeboten. Übrigens: Studien zufolge schnüffeln etwa auf 60% der im Apple AppStore verfügbaren Apps in den privaten Daten der User. Der Vorteil bei Android ist, dass bei der Installation zumindest auf die benötigten Berechtigungen hingewiesen wird.

Häufig verschicken Apps wie diese unbemerkt Abo-Anmeldungen an chinesische Premium-Nummern und fangen dabei auch gleich die Anmeldebestätigung ab. Das böse Erwachen erfolgt dann erst beim Einsehen der Handy-Rechnung. Fatal: Hier hilft auch kein Virenscanner weiter, da den Berechtigungen bei der Installation zugestimmt wurde. Abhilfe schafft die App LBE Privacy Guard (siehe Seite 54).

4 Eine Anti-Viren App verwenden

Android hat mit ähnlichen Problemen zu kämpfen, wie – zumindest früher – auch Windows: (auf den meisten Geräten) seltene Updates, teils größere Sicherheitslücken und aufgrund seiner Offenheit bietet es viel Angriffsfläche. Der Unterschied besteht aber darin, dass schadhafte Apps eigentlich immer

Lesen Sie weiter auf Seite 50 der Ausgabe Nov/Dez 2011.
Das Heft finden Sie ab 6. Oktober überall im Zeitschriftenhandel!