FAQ

Achim Barczok

Schnüffel-Apps

Antworten auf die häufigsten Fragen

Schnüffler identifizieren

Woran erkenne ich, ob eine App vertrauenswürdige Daten ungefragt weitergibt?

Apps in flagranti beim Schnüffeln zu erwischen ist aufwendig: Um wirklich sicherzugehen, muss man den Datenverkehr einer App protokollieren und auslesen, zum Beispiel am PC über die Netzwerk-Tools Wireshark oder Burp [1]. Nach unseren Erfahrungen können Sie aber davon ausgehen, dass die meisten kostenlosen und viele kostenpflichtige Apps zumindest Daten wie Identifikationsnummern oder Standortinformationen sammeln und auch an Werbepartner weitergeben – wenn sie darauf zugreifen dürfen.

Sie sollten deshalb in jedem Fall Vorkehrungen treffen, um Schnüffeln auf dem Smartphone zu vermeiden. Unter Android können Sie beispielsweise vor der Installation überprüfen, welche Rechte eine App anfordert; Sie sollten keine Apps installieren, die mehr Daten abrufen wollen, als sie für ihre Funktionen eigentlich brauchen.

Unter iOS können Sie den Zugriff auf Kontakte und Standort für jede einzelne App kontrollieren, bei Windows Phone immerhin die Ortsdaten für individuelle Apps deaktivieren. Unter Android können Sie solche Zugriffe nur mit der kostenpflichtigen Zusatz-App SRT Appguard einschränken, was allerdings das nachträgliche Manipulieren der Installationspakete erfordert und manche App zum Absturz bringt [2].

Kostenpflichtige Apps

Sind kostenpflichtige Apps unkritisch?

Nein. Wir haben auch kostenpflichtige Apps beim Schnüffeln ertappt. Aber die meisten Schnüffler-Apps sammeln für Werbepartner; deshalb findet man bei werbefinanzierten Apps tendenziell häufiger Schnüffler.

Android, iOS, Windows Phone

Ist das Problem unter Android schlimmer als unter iOS und Windows Phone?

Ja. Zum einen können Android-Apps Zugriff auf viel mehr Smartphone-Daten wie gespeicherte Dateien oder installierte Apps anfordern, zum anderen kann man unter Android den individuellen Zugriff besonders schlecht regulieren. Trotzdem sollten Sie auch unter iOS und Windows Phone darauf achten, welche Apps Sie installieren und worauf diese zugreifen.

App auf unterschiedlichen Systemen

Muss ich davon ausgehen, dass sich die von c't in [3] auf Android enttarnten Schnüffel-Apps unter iOS und Windows Phone gleich verhalten?

Nein. Das ist schon allein deshalb nicht wahrscheinlich, weil der Zugriff auf vertrauliche Daten unterschiedlich geregelt ist.

Virenscanner

In der c't wurden mobile Virenscanner unter anderem deshalb kritisiert, weil einige selbst Daten sammeln. Gibt es denn überhaupt empfehlenswerte Virenscanner für Smartphones?

Das Problem von mobilen Virenscannern ist, dass sie in der Regel gleichzeitig eine Schutzfunktion gegen Diebstahl bieten und dafür vertrauliche Daten wie Ortsinformationen nach Hause schicken – selbst wenn man diese Funktion gar nicht nutzt.

Unserer Erfahrung nach benötigt man auf Smartphones sowieso keinen Virenscanner, solange man darauf achtet, nur Apps aus den offiziellen Stores zu laden und ein Auge auf Bewertungen und Zugriffsberechtigungen hat.

Besondere Vorsicht ist bei Android-Apps geboten, die nicht aus den offiziellen App-Stores stammen. Diese sollten Sie vor Installation auf Schnüffel- und Schad-Software überprüfen, zum Beispiel auf der Webseite apkscan.nviso.be oder virustotal.com.

Datenverkehr trotz Flugmodus

Ich habe erstaunt beim Network-Monitoring über Wireshark festgestellt, dass mein Smartphone auch dann per WLAN aktiv ist, wenn ich das Gerät im Flugmodus betreibe. Gibt es Schnüffel-Apps, die den Flugmodus umgehen können?

Theoretisch ist das denkbar, wenn ein Angreifer physischen Zugriff auf Ihr Smartphone hatte und heimlich Spionage-Software installiert hat. Viel wahrscheinlicher ist aber, dass Sie auf ein Feature von Android 4.3 und höher gestoßen sind: Seit 4.3 bleibt nämlich die optionale Standorterkennung über WLAN auch dann aktiv, wenn man das WLAN-Modul (vermeintlich) deaktiviert hat. Überprüfen können Sie das unter „Einstellungen – WLAN – Erweitert"; ist dort das Häkchen bei „Erkennungsfunktion immer verwenden" gesetzt, so sucht das Smartphone die Umgebung nach WLAN-Hotspots ab. In älteren Android-Versionen können Apps das WLAN außerdem nachträglich aktivieren – dann ist aber auch wieder das WLAN-Icon in der Status-Anzeige von Android sichtbar.

Versteckte Schnüffler

Wie finde ich heraus, ob auf meinem Android-Smartphone versteckte Schnüffel-Apps installiert sind?

Überprüfen Sie zuerst unter „Einstellungen – Apps – Heruntergeladen" und unter „Einstellungen – Sicherheit – Geräteadministratoren", ob in den beiden Listen Apps auftauchen, die Ihnen unbekannt sind. Falls Letzteres auf Ihrem Smartphone nicht geht, können Sie dafür auch die App „Hidden Device Admin Detector" (siehe c't-Link) verwenden. Sonst bleibt nur, bei konkretem Verdacht das Gerät zurückzusetzen.

(acb@ct.de)

c't Schnüffel-Apps identifizieren: ct.de/yxgg

Literatur

[1] Achim Barczok, Ronald Eikenberg, David Wischnjak, Durchleuchtet, Schnüffel-Apps durch Analyse und Monitoring aufdecken, c't 9/15, S. 130

[2] Stefan Porteck, Verrammelt, Android-Apps mit Tricks und Tools unter Kontrolle bringen, c't 9/15, S. 126

[3] Achim Barczok, Appgehört, Smartphone-Schnüfflern auf der Spur, c't 9/15, S. 122