Apps als Sicherheitsgefahr

Welche Gefahren Apps mit sich bringen

Handys waren früher zum Telefonieren und zum Schreiben von SMS geeignet und konnten darüber hinaus nicht wirklich viel. Geändert hat sich dies mit dem Erscheinen der Apps, die Apple als erstes Unternehmen für seine iPhones auf den Markt gebracht hat. Andere Hersteller haben dieses Konzept schnell übernommen und heutzutage hat jedes Smartphone, abgesehen vom Hersteller, die Möglichkeit Apps zu installieren, welche die Funktionsvielfalt eines Gerätes erweitern. Die Apps, so gut und vorteilhaft sie auch sind, können aber auch sehr unsicher sein und dafür sorgen, dass die Mobilspionage ausgeführt wird, was eine ernsthafte Bedrohung für die Privatsphäre und Sicherheit sein kann.

Was genau die Mobilspionage ist

Eine Mobilspionage ist der Fall, wenn ein Hacker es schafft mit Hilfe von einiger Methoden Zugriff auf ein Handy zu erlangen, sich die dort gespeicherten Daten herunterzuladen, das Handy zu bedienen oder aber auch die illegale Handyortung im Internet durchzuführen. Die Mobilspionage wird dabei in den meisten Fällen durch Apps ermöglicht, die sich bereits auf dem Handy befinden oder aber auf dem Handy installiert werden. Teilweise werden die Apps für Mobilspionage über das Internet "an den Mann gebracht" aber auch durch einen kurzzeitigen Besitzverlust eines Handys bekommen Mobilspione die Möglichkeit entsprechende Apps schnell zu installieren.

Sicherheitsgefahr unsichere Downloadseiten

Im Internet gibt es zahlreiche Downloadseiten auf denen man kostenlose Apps herunterladen kann. Diese Seiten sollte man aber meiden, weil sie keine hohe Qualität genießen, nicht regelmäßig kontrolliert werden und deshalb auch riskant sind, weil man sich unter Umständen Apps herunterladen könnte, mit denen eine Mobilspionage durchgeführt wird. Seine Apps sollte man aufgrund dessen jederzeit nur aus dem Store beziehen, die der Handyhersteller vorschlägt, weil nur dort alle Apps geprüft und zugelassen werden müssen. Standardmäßig verbietet eine Option im Handy auch die Installation von Apps aus unbekannten Quellen. Diese Option sollte man auf jeden Fall aktivieren, so dass nichts schief gehen kann.

Sicherheitsgefahr bei der Weitergabe des Handys

Eine andere Sicherheitsgefahr, mit der es zur Mobilspionage kommen könnte ist, dass jemand selbst Software für die Mobilspionage auf dem Handy installiert. Dies passiert, wenn man jemandem das Handy überlässt. Aus diesem Grund ist es äußerst wichtig immer darauf zu achten, was derjenige mit dem Handy macht. Wenn man oft unterwegs ist und Freunde ab und an mal das Handy in die Hände bekommen könnten, lohnt es sich eine Bildschirmsperre einzurichten, die ein Passwort abfragt um den Zugriff auf das Handy zuzulassen. Oft gibt es solche Bildschirmsperren kostenlos im App Store.

Sicherheitslücken im System sofort beseitigen

Auch ein enormes Sicherheitsrisiko stellen Sicherheitslücken dar, die auf dem Handy vorhanden sind. Dies betrifft manchmal das Betriebssystem selbst aber in den meisten Fällen die Apps, die manchmal nur selten geupdatet werden, weil sie so selten benutzt werden. Wer sein Handy sicher nutzen und der Mobilspionage vorbeugen möchte, sollte alle angebotenen Updates installieren, weil mit diesen Sicherheitslücken geschlossen werden und den Hackern das Handwerk gelegt wird. Wer wartet und sehr lange keine Updates durchführt, lädt Mobilspione praktisch ein Zugriff auf sein eigenes Handy zu bekommen und setzt somit auch seine Sicherheit aufs Spiel.

Pressekontakt

Boris Schneider

Herr Boris Schneider
Brunnenpfad 10
60489 Frankfurt am Main

mobilspionage.de/
boris@ultimode.com

Firmenkontakt

Boris Schneider

Herr Boris Schneider
Brunnenpfad 10
60489 Frankfurt am Main

mobilspionage.de/
boris@ultimode.com

Seit 2008 professioneller Schreiber und Redakteur. Tätig für viele bekannte und kleinere Unternehmen und Nachrichtenblätter. Meine Themengebiete sind vielfältig.