Kein Opfer einer Mobilspionage werden

So schützt man sich vor der Mobilspionage

Die Mobilspionage ist ein immer öfter vorkommendes Geschehnis in der heutigen Zeit. Bei derselben bekommt ein Hacker, bzw. ein Mobilspion den Zugriff auf das Handy, kann die Handyortung anonym durchführen oder sich die Daten, die auf einem Handy gespeichert sind, wie beispielsweise Telefonnummern oder Bilder, herunterladen und für seine Zwecke verwenden. Die Mobilspionage wird deshalb immer populärer unter den Hackern, weil auf den Handys immer mehr private Daten gespeichert werden, wie beispielsweise PIN Nummern für Online Banking oder die Zugangsdaten für Paypal und andere Zahlungsservices, die mit Geld zu tun haben, und diese Daten für Hacker sehr interessant sind.

Wie die Mobilspione dabei vorgehen

Um Zugriff auf ein Handy zu bekommen und es kontrollieren zu können, muss eine Spionagesoftware in Form einer App auf das Handy übertragen werden. Dies geht entweder, indem sich das Opfer der Mobilspionage selbst eine infizierte App aus dem Internet herunterlädt oder aber eine App mit Sicherheitslücken (beispielsweise bei einer alten Version) infiziert wird. Die Hacker nutzen dabei die meist ständig aktive Internetleitung um den stetigen Zugriff zu bekommen. Das Opfer selbst merkt meist nicht, dass es spioniert wird und bis der Angriff auffliegt, ist es meist schon zu spät, weil die meisten Daten weg sind.

Weshalb Täter nur sehr selten überführt werden können

Im Normalfall stehen die Daten wie die IP Adresse des Servers über den die Hacker den Zugriff ermöglichen, in der App selbst drin. Zwar kann herausgefunden werden, wer der Täter war, doch wird dieses Unterfangen oft davon beeinträchtigt, dass die Täter Proxy Server genutzt haben, welche die wahre Identität des Täters verbergen. Oft gibt es auch private Server in Fernost, die keine privaten Daten rausrücken und in diesem Fall hat man Pech gehabt. Bestenfalls richtet man die erforderlichen Einstellungen ein, damit die Mobilspionage erst gar nicht ermöglicht wird.

Welche Sicherheitsvorkehrungen getroffen werden müssen

Um der Mobilspionage zu entgehen, kann man schon mit nur einigen Sicherheitsvorkehrungen viel erreichen. Dazu gehört beispielsweise das Deaktivieren der Internetleitung, wenn diese nicht genutzt wird. Dies raubt den Hackern die Substanz, weil keine Angriffe ohne beständige Internetleitung durchgeführt werden können. Auch Funktionen, die genutzt werden können, wie die Handyortung, sollten nur bei Bedarf eingeschaltet werden. Durch diese Störungen werden Hacker sehr schnell entmutigt. Neben dem Entziehen der Grundlage für die Mobilspionage sollte man aber auch darauf achten, dass man zwielichtige Apps nicht installiert und seine Installierten gut kontrolliert.

Apps als Sicherheitsfalle

Apps sollten nur aus offiziellen Bezugsquellen heruntergeladen werden, weil diese die Sicherheit der Nutzer gewährleisten können. Inoffzielle Apps oder Apps aus inoffiziellen Quellen enthalten oft schädliche Bestandteile, die zur Mobilspionage genutzt werden. Alle Apps, die man bereits auf dem Handy installiert hat, sollte man immer auf dem neusten Stand halten oder bei Nichtbenutzung deinstallieren. Auf diese Weise entledigt man sich aller Sicherheitslücken, die vorhanden sind und von Hackern benutzt werden könnten. Auch wenn man mit diesem Vorgehen relativ sicher sein kann, sollte man von Zeit zu Zeit prüfen, ob ausgeschaltete Apps in den Prozessen immer noch laufen. Falls ja, sollte man sie immer per Hand schließen, damit nichts passieren kann.

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.