# Your Smartphone is Watching You: Gefährliche Sicherheitslücken in Tracker-Apps

*Mitteilung: Fraunhofer-Institut für Sichere Informationstechnologie SIT*

***Fraunhofer-Forscher finden Schwachstellen in Apps: Komplette Überwachung von Smartphones möglich. Millionen Installationen betroffen.***

Viele Tracker-Apps, mit denen beispielsweise Eltern ihre Kinder orten können, haben gravierende Sicherheitslücken. Forscher des Fraunhofer-Instituts für Sichere Informationstechnologie haben beliebte Tracker-Apps aus dem Google Play Store untersucht – das Ergebnis: Keine einzige davon war sicher programmiert, alle hatten teils gravierende Schwachstellen. Angreifer können diese ausnutzen, um Bewegungsprofile zu erstellen, Chats und SMS-Nachrichten zu lesen und Bilder anzusehen. Besonders brisant: Angreifer müssen nicht jedes Smartphone einzeln überwachen, sondern können zeitgleich Millionen von Nutzern angreifen, die diese Apps auf ihrem Smartphone installiert haben. Zum ersten Mal vorgestellt haben die Wissenschaftler ihre Ergebnisse am 11. August auf der DEF CON Hacking Conference in Las Vegas.

Mit sogenannten Monitoring- oder Tracker-Apps können Smartphone-Nutzer überwacht werden. Beispielsweise nutzen Eltern eine solche App, um jederzeit zu wissen, wo sich ihre Kinder befinden oder welche Nachrichten und Bilder sie verschicken. Die Nutzung dieser Apps ist legal, sofern der oder die Ausspionierte damit einverstanden ist. Wissenschaftler des Fraunhofer SIT haben 19 legale Apps, die im Google Play Store angeboten werden, untersucht. Die Apps wurden laut Google mehrere Millionen Mal installiert. Die Wissenschaftler haben geprüft, wie die hochsensiblen Nutzerdaten, die diese Apps erheben, geschützt sind. Das Ergebnis: Alle Apps haben gravierende Schwachstellen, keine einzige Anwendung war sicher programmiert. Insgesamt haben die Forscher 37 Sicherheitslücken gefunden.

Die hochsensiblen Daten werden meist im Klartext auf einem Server abgespeichert, ohne durch korrekte Verschlüsselung abgesichert zu sein. „Wir mussten lediglich eine bestimmte Webseite aufrufen und einen Nutzernamen in die URL eingeben oder raten, um das Bewegungsprofil einer Person aufzurufen“, erklärt Fraunhofer-Projektleiter Siegfried Rasthofer, der gemeinsam mit der Fraunhofer Hacking-Gruppe TeamSIK die Apps untersucht hat. Die Forscher fanden auf den Servern nicht nur Daten einzelner Personen, sondern konnten von allen Nutzern dieser Apps komplette Bewegungsprofile auslesen, die ungesichert auf einem Server gespeichert waren. „Damit ist eine Echtzeitverfolgung von Tausenden Menschen

möglich“, sagt Rasthofer. Über die unsicher programmierten Apps können Angreifer nicht nur Metadaten wie Aufenthaltsorte abrufen, sondern auch Inhalte wie SMS-Nachrichten und Bilder der überwachten App-Nutzer lesen und ansehen. „Damit ist eine komplette Überwachung möglich“, erklärt Stephan Huber, Mitglied von TeamSIK und Forscher am Fraunhofer SIT.

Darüber hinaus ist es den Wissenschaftlern gelungen, die Anmeldeinformationen der App-Nutzer auszulesen. Auch diese waren bei den meisten Apps unverschlüsselt gespeichert oder nur mit völlig ungenügender Verschlüsselung gesichert – das Team um Siegfried Rasthofer und Stephan Huber hatte beispielhaft bei einer App 1.700.000 Login-Daten gefunden. Die Fraunhofer-Wissenschaftler haben die App-Anbieter sowie den Google Play Store über ihre Entdeckungen informiert. 12 der 19 untersuchten Apps sind inzwischen aus dem Play Store entfernt worden. Andere Anbieter hingegen haben gar nicht reagiert.

*PM v. 13.8.2018*
*Oliver Küch*
*Presse- und Öffentlichkeitsarbeit*
*Fraunhofer-Institut für Sichere Informationstechnologie SIT*
*Quelle:*
*www.sit.fraunhofer.de*
*www.idw-online.de*