Geheime Datensammler auf dem Smartphone enttarnen

Mitteilung: Fraunhofer-Institut für Sichere Informationstechnologie SIT

Fraunhofer SIT entwickelt im Rahmen des Forums Privatheit neues Datenschutz-Tool für mobile Apps – MetaMiner enttarnt und blockiert Tracking-Dienste in Apps, die Verbraucher insgeheim ausspionieren.

Die Verfolgung von Benutzeraktivitäten im Netz, sogenanntes Tracking, ist seit Langem ein bekanntes Datenschutzproblem. Im Hintergrund werden Informationen darüber gesammelt, welche Seiten sich Benutzer im Internet anschauen und welche Interessen sie haben. Für Internetbrowser existieren bereits zahlreiche Lösungen, die dem Nutzer die Tracker sichtbar machen und ihn schützen. Dass dieses Problem allerdings auch bei der Nutzung von Apps auf dem Smartphone besteht, wissen bislang meist nur Experten. Für Endnutzer entwickelt das Fraunhofer-Institut für Sichere Informationstechnologie SIT im Rahmen des vom Bundesministerium für Bildung und Forschung finanzierten Forschungsverbunds Forum Privatheit das Tool MetaMiner. Mit MetaMiner können Nutzer das Tracking durch mobile Apps sichtbar machen und auch unterbinden. Öffentlich vorgestellt wurde das Tool erstmals auf dem Web Monday am 20. November in Darmstadt.

Für einen immer größer werdenden Teil der Internetaktivitäten nutzen Menschen Smartphones. Laut Eurostat surften 2016 bereits acht von zehn Nutzern mit ihrem Smartphone mittels Apps mobil im Internet. Für viele Funktionen von Apps werden Zusatzbibliotheken verwendet, die es ermöglichen, Details über die App-Nutzer zu erfassen. Im besten Fall sind dies Informationen, die die Anbieter zur Verbesserung ihrer Services verwenden. Werbetreibende verwenden die Informationen oft, um Nutzerprofile zu erstellen und so zum Beispiel maßgeschneiderte Werbung einzublenden. Die Zusatzbibliotheken sind jedoch häufig auch Einfallstore für Cyber-Angriffe, da sie oft Sicherheitslücken aufweisen. Welche Apps betroffen sind, konnten Nutzer bislang nicht erkennen. Bestehende Lösungen für PC und Laptop greifen bei mobilen Apps nur bedingt. Radikalere Lösungen auf Basis des sogenannten Rooten des Smartphones setzen die Gewährleistung der Geräte außer Kraft und verhindern gegebenenfalls danach die Beseitigung von Sicherheitslücken wegen eingeschränkter Patchfähigkeit der Firmware.

„Verstecktem Tracking in mobilen Apps wurde bisher nur wenig Beachtung geschenkt, so dass sich App-Nutzer oft nicht bewusst sind, zu welchen Werbenetzen bzw. bösartigen Internetbereichen das Smartphone im Verborgenen Onlineverbindungen aufbaut“, erläutert

Hervais Simo Fhom, Projektleiter am Fraunhofer SIT. „Anders als bestehende Tools ist MetaMiner nach den Prinzipien Privacy by Design und Privacy by Default entworfen: Daten werden unmittelbar auf dem Gerät des Endnutzers verarbeitet und interpretiert, ohne Sicherheitskompromisse am Gerät einzugehen. Das Tool ist leicht bedienbar und durch interaktive Visualisierung und klare Grafiken sehr übersichtlich." Dem Benutzer werden Diagramme und Grafiken angezeigt, auf denen er sehen kann, in welche Apps welche Zusatzbibliotheken für Tracking und Werbung eingebettet sind, wann und mit welchen Drittservern das Smartphone heimlich kommuniziert und wohin diese Daten fließen.

Bisher existiert ein Prototyp des Tools für Android. Die Forscher arbeiten jetzt an weiteren Funktionen, um das Tool in Zukunft Endverbrauchern als App zur Verfügung stellen zu können.

Mehr Informationen zu MetaMiner: www.sit.fraunhofer.de/metaminer

PM v. 21.11.2017
Oliver Küch
Presse- und Öffentlichkeitsarbeit
Fraunhofer-Institut für Sichere Informationstechnologie SIT
Quelle: idw-online.de