Security Alert: Aktiv ausgenutzte Sicherheitslücke in iOS - Expertenkommentar von Tim Berghoff

Gleich zwei kritische Sicherheitslücken in iOS-Geräten bedrohen Nutzer - Apple warnt sogar selbst vor Angriffen. Tim Berghoff von G DATA ordnet den Vorfall ein.

Eine ernste Warnung

Apple warnt derzeit vor einer aktiv ausgenutzten Sicherheitslücke in seinem Betriebssystem iOS - das bedeutet, dass bereits Angriffe gegen Nutzer stattfinden. Die Sicherheitslücken finden sich im Kernel und in Apples eigener "Webkit"-Technologie, die für die Darstellung von Internetseiten verwendet wird. Die Webkit-Lücke kann zudem aus der Ferne ausgenutzt werden. Betroffen sind alle iPhone-Geräte ab der Version 6.

"Dass Apple selbst vor aktiv ausgenutzten Sicherheitsproblemen warnt, hat absoluten Seltenheitswert", sagt Tim Berghoff, G DATA Security Evagenlist. "Mit dem Kernel und Webkit sind darüber hinaus zwei hochkritische Komponenten des Betriebssystems betroffen. Nutzer sollten also nicht auf die automatischen Updates warten, sondern umgehend selbst aktiv werden."

Das von Apple beschriebene Problem im iOS-Kernel ermöglicht einer App, die eigenen Berechtigungen zu erweitern. Somit können Angreifer Zugriff auf Daten nehmen, die der App eigentlich nicht zugänglich wären und umgehen damit die Schutzmechanismen des Betriebssystems.

Erweiterte Berechtigungen und Remote-Codeausführung

Das von Apple beschriebene Problem im iOS-Kernel ermöglicht einer App, die eigenen Berechtigungen zu erweitern. Somit können Angreifer auf Daten zugreifen, die der App eigentlich nicht zugänglich wären und umgehen damit die Schutzmechanismen des Betriebssystems.

"Die Webkit-Lücke ermöglicht sogar die Ausführung von Code aus der Ferne - viel problematischer kann eine Sicherheitslücke eigentlich nicht sein", sagt Berghoff. "Für entsprechende Exploits werden auf dem grauen Markt für Sicherheitslücken zum Teil Millionenbeträge gezahlt."

Aufgrund der vielen gespeicherten persönlichen Daten sind Smartphones ein sehr beliebtes Angriffsziel für Cyberkriminelle. Apple versorgt seine Geräte sehr lange mit Sicherheitsupdates, sodass Nutzer sich an dieser Stelle wenig Sorgen machen müssen. Gerade günstige Android-Geräte werden im Vergleich dazu oft nur für kurze Zeit mit Patches versorgt - Nutzer stehen dann ohne Schutz gegen aktuelle Gefahren da.