Viele Android-Apps sind anfällig für Datendiebstahl

Wissenschaftler der Universitäten Hannover und Marburg haben 13.500 kostenlose Android-Apps aus dem Play Store auf ihren Umgang mit dem SSL-Protokoll zur Verschlüsselung persönlicher Daten untersucht. Der Bericht soll zeigen, dass persönliche Daten bei vielen Android-Apps nicht ausreichend geschützt seien.

Laut dem Forschungsteam akzeptierten von den 13.500 untersuchten Apps 1.074 jegliche Art von Zertifikaten und Hostnames, was ein Auslesen der übermittelten Daten bei einer Attacke ermöglichen kann. Die Forscher konzentrierten sich auf die sogenannte Man-In-The-Middle-Attacke (MITMA). Hierbei liest ein Hacker sensible Daten aus, indem er die Kommunikation zwischen dem Endgerät und dem Router mitverfolgt oder sogar beeinflusst. Zur Analyse hat die Forschungsgruppe ein eigens entwickeltes Programm eingesetzt, welches mögliche Schwachstellen in der Verwendung des Protokolls ermitteln soll.

Basierend auf den Ergebnissen dieser ersten Analyse hat das wissenschaftliche Team 100 Programme aus den 13.500 Apps genauer untersucht. In 41 Fällen haben sie nach eigenem Bericht erfolgreich eine MITMA durchgeführt und sind an Kreditkartendaten, Bankdaten sowie weitere geheime Informationen gelangt. Dabei ist allerdings zu berücksichtigen, dass die betroffenen Apps bereits nach der Voranalyse als potentiell unsicher galten. Die untersuchten Apps haben laut der Forschergruppe eine Verbreitung von 39,5 bis 185 Millionen Nutzern.

Die Durchführung einer MITMA ist in einem ungeschützten öffentlichen Netzwerk einfacher als in einer geschützten Umgebung. Da sich Smartphone-Nutzer häufig in solchen ungesicherten Umgebungen aufhalten, sei eine MITMA eine durchaus denkbare Bedrohung, so die Wissenschaftler. Falls dann persönliche Daten nicht ausreichend oder gar nicht verschlüsselt seien, könnten sie leicht von Angreifern ausgelesen werden.

Google selbst betont in seinem Android Developers Blog die Wichtigkeit von sicheren Verbindungen in öffentlichen Netzwerken. Die Implementierung des SSL-Protokolls ist jedoch bisher den Entwicklern selbst überlassen. Das Forscherteam schlägt daher unter anderem vor, diese Entscheidungsmöglichkeit durch Google strenger zu reglementieren. Ein weiterer Lösungsvorschlag ist, den Nutzer über das Betriebssystem besser darüber zu informieren, ob er gerade eine sichere Verbindung benutzt oder nicht.