



Schwerer Sicherheitsfehler in Apps

Falsche SSL-Implementierung ermöglicht Angriff auf mobile Geräte Nutzer sollten betroffene Apps aktualisieren

(Mynewsdesk) Darmstadt, den 9. Dezember ? Viele beliebte Apps der Android-Plattform haben einen schwerwiegenden Sicherheitsfehler, darunter auch Apps von Banken, Verlagen und anderen großen Organisationen. Das stellten Mitarbeiter des Testlabors am Fraunhofer-Institut für Sichere Informationstechnologie in Darmstadt fest. Angreifer können mithilfe der gefundenen SSL-Schwachstelle Zugangsdaten stehlen und damit zum Teil großen Schaden anrichten. Das Fraunhofer-Institut hat über 30 betroffene Unternehmen informiert, davon haben bislang 16 reagiert und die Sicherheitslücke geschlossen. Hierzu gehören unter anderem Apps von Amazon, Spiegel Online, Lidl oder der Volkswagen Bank. Eine Liste der Apps, für die Sicherheitsupdates zur Verfügung stehen, findet sich im Internet unter www.sit.fraunhofer.de/app-security-list.

Das entstandene Sicherheitsrisiko für die Nutzer ist abhängig vom jeweiligen Anwendungszweck: Bei mancher App droht lediglich die Manipulation der eigenen Foto-Bestände, im Falle einer Banking-App lassen sich hingegen die Zugangsdaten unter Umständen auch für unberechtigte Überweisungen oder andere Manipulationen des Bankkontos nutzen. Besonders gravierend kann das Risiko bei Apps sein, die Single-Sign-On z.B. zu den Google- oder Microsoft-Diensten nutzen, denn dort werden die Zugangsinformationen für eine Vielzahl von Diensten wie E-Mail, Cloud-Speicher oder Instant Messaging genutzt.

Bei der gefundenen Schwachstelle handelt es sich um eine fehlerhafte Verwendung des Secure Socket Layer-Protokolls (SSL). Das SSL-Protokoll dient zur Absicherung von Internet-Verbindungen, setzt aber die korrekte Prüfung der verwendeten Echtheitszertifikate der angesprochenen Server voraus. Diese Prüfung ist bei den betroffenen Apps jedoch falsch umgesetzt. ?Dies ist technisch gesehen ein kleiner Fehler, aber er hat große Auswirkungen für die Sicherheit?, sagt Dr. Jens Heider vom Fraunhofer SIT. Um an die Zugangsdaten zu gelangen, müssen Angreifer zum Beispiel nur die Kommunikation beim Surfen über WLAN manipulieren. Dies ist überall besonders leicht, wo die WLAN-Kommunikation unverschlüsselt ist, etwa an vielen öffentlichen Zugangspunkten wie in Flughäfen, Hotels und Restaurants. Gerade in diesen Situationen soll die SSL-Verschlüsselung die Kommunikation schützen.

?Die Lücke ist prinzipiell ganz einfach zu schließen?, sagt Heider. Er und sein Team haben die Hersteller bereits vor mehreren Wochen informiert und um die Beseitigung der Schwachstelle gebeten. Einige Unternehmen haben entsprechend reagiert, die Volkswagen Bank stellte sogar innerhalb eines Tages ein entsprechendes Sicherheitsupdate zur Verfügung. Jede neue Version prüfte das Testteam erneut. ?Dort, wo die gefundene Lücke beseitigt ist, sollten Nutzer die entsprechende App einfach aktualisieren?, sagt Heider. Insgesamt raten die Experten des Fraunhofer SIT zu einer vorsichtigen Nutzung von Apps in öffentlichen WLAN-Bereichen. Aufgefallen ist die Lücke während des Pilotbetriebs für das neue Testframework ?Appicaptor?, mit dem sich die Sicherheit von Apps automatisiert prüfen lässt. Die Fraunhofer-Experten testeten insgesamt 2000 Android-Apps.

Shortlink zu dieser Pressemitteilung:

<http://shortpr.com/tdlf8z>

Permanenterlink zu dieser Pressemitteilung:

<http://www.themenportal.de/it-hightech/schwerer-sicherheitsfehler-in-apps-39216>

=== Sicherheitsschwachstelle in Apps (Bild) ===

Vorsicht bei der App-Nutzung

Shortlink:

<http://shortpr.com/7ot0kf>

Permanenterlink:

<http://www.themenportal.de/bilder/sicherheitsschwachstelle-in-apps>

=== App-Security-List (Dokument) ===

Liste der Apps, in denen die Schwachstelle festgestellt und bereits behoben wurde.

Shortlink:

<http://shortpr.com/jyemdg>

Permanenterlink:

<http://www.themenportal.de/dokumente/app-security-list>

Pressekontakt

Fraunhofer-Institut für Sichere Informationstechnologie

Herr Oliver Küch
Rheinstraße 75
64295 Darmstadt

presse@sit.fraunhofer.de

Firmenkontakt

Fraunhofer-Institut für Sichere Informationstechnologie

Herr Oliver Küch

Rheinstraße 75
64295 Darmstadt

sit.fraunhofer.de
presse@sit.fraunhofer.de

Die Informationstechnologie hat bereits weite Teile unseres Alltags durchdrungen: Ob Auto, Telefon oder Heizung ohne IT-Einsatz sind die meisten Geräte und Anlagen heute nicht mehr denkbar. Insbesondere Unternehmen nutzen IT-Systeme zur effektiven Gestaltung ihrer Arbeitsprozesse. Das Fraunhofer-Institut für Sichere Informationstechnologie beschäftigt sich mit dem Schutz dieser Systeme vor Ausfällen, Angriffen und Manipulationen.

Das Institut ist für Unternehmen aller Branchen tätig. Viele erfolgreiche Projekte mit internationalen Partnern sind ein drucksvoller Beweis für eine vertrauensvolle und zuverlässige Zusammenarbeit. Zu unseren Kunden zählen unter anderem die Deutsche Bank, SAP, Deutsche Telekom und das Bundesamt für Sicherheit in der Informationstechnik.