Dangerous Apps - Spione im Smartphone

Dangerous Apps - Spione im Smartphone

TÜViT und mediaTest digital präsentieren Sicherheitslösungen auf der CeBIT / Drei beliebte Apps mit gravierenden Sicherheitslücken
Mobile Apps sind ständige Begleiter für Nutzer von Smartphones und Tablets. Ihr Potenzial entfalten sie in der Regel erst mit den verwendeten Nutzerdaten. Sind diese nicht ausreichend geschützt, können sie von Hackern und Datensammlern abgefangen werden. Oft sind davon sogar die populärsten Apps in den Stores betroffen. Die Experten für Mobile Security und Anbieter von IT-Sicherheitsdienstleistungen von mediaTest digital und TÜViT (TÜV NORD GROUP) warnen insbesondere vor der unverschlüsselten Übertragung vertraulicher Informationen und Datenschutzverstößen.
Im Testlabor von mediaTest digital werden täglich Apps für alle gängigen Betriebssysteme auf Datensicherheit und die Einhaltung von Datenschutzrichtlinien des deutschen Bundesdatenschutzgesetzes geprüft. Anhand der drei beliebten Apps "DFB" (iOS), "wetter.de" (Android) und "Weight Watchers" (Android) stellen die Fachleute Anwendungen mit schwerwiegenden Sicherheits- und Datenschutzverstößen vor.
DFB (iOS), Version 2.4.3
Mit der offiziellen DFB-App erhalten Fußballinteressierte Informationen und Neuigkeiten zu deutschen Nationalmannschaften und Ligen. Um über die Profis und Turniere auf dem Laufenden zu bleiben, ist die iOS-App hilfreich, jedoch ist sie sicherheitstechnisch äußerst problematisch: Passwort, Benutzername, Vorname, Nachname, Adresse, Telefonnummer und E-Mail-Adresse werden unverschlüsselt an den App-Anbieter übertragen. Insbesondere die unverschlüsselte Übertragung des Passworts birgt Risiken, die weit über das einzelne Konto hinausgehen. Alle Konten, in denen das gleiche Passwort genutzt wird, sind damit bedroht.
Die Experten von mediaTest digital empfehlen Nutzern der DFB-App für iOS, ihren Account zu löschen und die App zu deinstallieren. Anschließend sollten unbedingt die Passwörter aller Dienste geändert werden, in denen dasselbe Passwort verwendet wird. Die Sicherheitslücke der DFB-App ist leider kein Einzelfall. Doch obwohl es für Verbraucher kaum ersichtlich ist, ob eine Anwendung Passwörter unverschlüsselt überträgt, können Nutzer mit einfachen Verhaltensregeln für mehr Sicherheit sorgen: Es sollte niemals dasselbe Passwort für mehrere Dienste verwendet werden. Zudem sollten Passwörter regelmäßig geändert werden. Das Bundesamt für Sicherheit in der Informationstechnik empfiehlt eine Länge von mindestens zwölf Zeichen und die Verwendung von Groß- und Kleinbuchstaben sowie Sonderzeichen.
wetter.de (Android), Version 2.0.2
Die Android-App "wetter.de" ist die mobile Version des Dienstes für Wetterberichte und -vorhersagen von RTL interactive. Während sich die iOS-App noch relativ "harmlos" verhält und lediglich den Standort unverschlüsselt überträgt, hat es die Android-App umso mehr in sich: Hier werden die eindeutige Gerätekennung IMEI (International Mobile Equipment) sowie exakte Standortdaten unverschlüsselt an ein Werbe- und Analytics-Netzwerk übertragen. Dass darüber hinaus Suchanfragen und die Android Werbe-ID ohne Verschlüsselung übermittelt werden, wirkt daneben fast trivial. Die IMEI fungiert als Fingerabdruck von mobilfunkfähigen Geräten. Sie spielt beispielsweise beim Sperren von gestohlenen oder verloren gegangenen Mobiltelefonen eine Rolle. Eine unverschlüsselte Übertragung der IMEI-Nummer an fremde Server - im Fall von wetter.de an ein Werbe- und Analytics-Netzwerk - ermöglicht die Erstellung von Nutzerprofilen durch unbefugte Dritte. mediaTest digital warnt davor, dass die IMEI bei fehlender Verschlüsselung für Hacker mit Leichtigkeit abzufangen sei. Auch die unverschlüsselte Übertragung von Standortdaten ist bedenklich. Von der Nutzung der "wetter.de"-App für Android wird in Anbetracht der Sicherheitsverstöße abgeraten. Insgesamt machen sich nur wenige App-Anbieter die Mühe, Lokalisierungsdaten zu verschlüsseln. Daher sollte nach Möglichkeit auf standortbasierte Informationsdienste verzichtet werden, so die Fachleute von mediaTest digital und TÜViT.
Weight Watchers (Android), Version 3.5.3.21
Der Vorsatz, mit Hilfe von Diäten und Fitnessprogrammen abzunehmen, ist weit verbreitet. Während sich Weight Watchers als Anbieter für Diätpläne großer Beliebtheit erfreut, ist die Android-App in Punkto Datenschutz und Sicherheit problematisch. Im Security-Test wurde die unverschlüsselte Übertragung der Android Geräte-ID an ein Werbe-Netzwerk festgestellt. Zudem übermittelt die App sowohl Standortdaten an den Anbieter als auch unverschlüsselte Suchanfragen an einen Kartendienst. Ebenfalls unverschlüsselt findet die Übermittlung von Suchanfragen und Lebensmitteleinträgen an ein Analytics-Netzwerk statt. Weight Watchers für Android ist eine von vielen Apps, die anstelle der von Google vorgeschriebenen Werbe-ID die Geräte-ID zu Werbezwecken verwendet.
Die Verwendung der Werbe-ID hat für Nutzer zwei entscheidende Vorteile: In den Geräteeinstellungen kann der Verwendung der Werbe-ID zu interessenbasierter Werbung widersprochen werden. Zudem kann die Werbe-ID jederzeit zurückgesetzt werden. Bei der Geräte-ID ist dies nur über Umwege möglich. Indem Weight Watchers die Geräte-ID an ein Werbenetzwerk überträgt, widersetzt sich die App den "Google Play-Programmrichtlinien für Entwickler" und missachtet das Recht der Nutzer auf angemessene Verwendung ihrer Daten.
TÜViT und mediaTest digital auf der CeBIT
Auf der diesjährigen CeBIT klären TÜViT und mediaTest digital darüber auf, wie Datenschutz und Sicherheit auf mobilen Endgeräten im Unternehmensumfeld gewährleistet werden kann. Dort spielt der Schutz von sensiblen Daten eine herausragende Rolle: "Mobile-Verantwortliche und CIOs müssen die gewohnte Absicherung der IT mit Firewall und Geräteverwaltung lückenlos auf den mobilen Bereich übertragen. Das hört sich trivial an, ist aber eine Herkulesaufgabe", sagt Sebastian Wolters, Geschäftsführer bei mediaTest digital. In Kooperation mit TÜViT betreibt das Hannoveraner Unternehmen das Application Security Center, eine Plattform für die Absicherung von mobilen IT-Infrastrukturen. "Die Einbindung von mobilen Geräten in die IT-Infrastrukturen unter Beibehaltung der Sicherheitsstandards der Unternehmen ist die große Herausforderung", ergänzt Antonius Sommer, Geschäftsführer TÜViT.
Auf der CeBIT in Hannover präsentieren die beiden Anbieter ihre Lösungen für sicheres Enterprise Mobility und Application Management an ihrem Gemeinschaftsstand L23 in Halle 6.
Über TÜViT
Die TÜV Informationstechnik GmbH - kurz TÜViT - mit Sitz in Essen hat sich auf die Prüfung und Zertifizierung von IT Sicherheit und IT Qualität spezialisiert. Als "Trust Provider" unterstützt TÜViT Unternehmen bei der Umsetzung und Einhaltung von speziellen Anforderungen, Gesetzen und Richtlinien (Compliance). Die Prüfung und Zertifizierung der Sicherheits- sowie Qualitätseigenschaften von IT-Produkten, IT-Systemen, IT-Services und IT-Infrastrukturen erfolgt anhand anerkannter Kriterien und Standards (z. B. Common Criteria oder ISO/IEC 27001). Das Portfolio an nationalen und internationalen Akkreditierungen der TÜViT ist auf dem deutschen Markt einzigartig. Mit den "TRUSTED MOBILE AUDITS" prüfen und evaluieren die Experten der TÜViT mobile Infrastrukturen von Unternehmen, Internetdienste von Service Providern und mobile Individuallösungen. Durch diese ganzheitliche Betrachtung können Schwachstellen nicht nur innerhalb der mobilen Kerndisziplinen (z. B. innerhalb des Mobile Device Managements), sondern auch in Bezug auf die Vernetzung des Systeme untereinander aufgedeckt werden.
 www.tuvit.de
Über mediaTest digital
mediaTest digital ist Europas Marktführer für Mobile Security Lösungen im Segment des Mobile Application und Enterprise Mobility Managements. 2012 gegründet, sichert das Unternehmen heute weltweit mehr als 600.000 betrieblich genutzte mobile Endgeräte für Großkunden wie Lufthansa oder Deutsche Bahn. Insgesamt 10 der größten 25 deutschen Unternehmen sowie zahlreiche mittelständische und kleine Unternehmen aus Wirtschaftszweigen wie Banken, Automotive, Energieversorgung oder Commerce zählen heute zu den Kunden von mediaTest digital. "APPVISORY" ermöglicht als erste integrierte "Software as a Service"-Lösung, App Risk Management flächendeckend im Unternehmen zu betreiben. Dank der standardisierten Integration in an alle gängigen Mobile Device Management Systeme wie AirWatch oder MobileIron lässt sich APPVISORY als einzige am Markt erhältliche Lösung nahtlos in jede mobile IT-Infrastruktur einbetten und bis auf Geräteebene durchsetzen.
In Kooperation mit TÜViT (TÜV NORD GROUP) betreibt mediaTest digital das Enterprise Mobility Management Portal "Application Security Center" www.appsecuritycenter.com .

TÜV NORD GROUP
Carolin Roterberg
Fon +49 (0) 40 8557-1987
E-Mail: presse@tuev-nord.de
 www.tuev-nord.de/presse
mediaTest digital
Felix Sievers
Telefon +49 (0) 511 35 39 94 22
E-Mail: baer@mediatest-digital.com
 www.mediatest-digital.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=590115" width="1" height="1">

Pressekontakt

TÜViT

45141 Essen

presse@tuev-nord.de

Firmenkontakt

TÜViT

45141 Essen

presse@tuev-nord.de

Als Vertrauensvermittler für IT-Sicherheit und IT-Qualität hat sich TÜViT auf die Bewertung, Prüfung und Zertifizierung von IT-Produkten, IT-Systemen und IT-Prozessen aller Art spezialisiert sowie auf die Überprüfung der Einhaltung von speziellen Anforderungen, Gesetzen und Richtlinien (eCompliance). Ihre fachliche Kompetenz weist TÜViT durch Akkreditierungen nach, die durch regelmäßige Audits bestätigt werden und somit die gleichbleibend hohe Qualität der Prüfdienstleistungen gewährleisten. Des Weiteren bietet TÜViT Schulungen für ausgewählte Sicherheits- und Qualitätsthemen an.www.tuevit.de