erschienen in der FIfF-Kommunikation,
herausgegeben von FIfF e.V. - ISSN 0938-3476
www.fiff.de

Carsten Seeger

Android? Aber sicher!?

Die Pleiten-, Pech- und Pannenserien unserer mobilen Welt

Unser Handy ist mittlerweile ein Standard-Accessoire, so wie Schlüssel und Portemonnaie. Es ist nutzbringend, einfach zu bedienen, und man ist immer erreichbar. Früher im Wesentlichen zum Telefonieren und SMS-Schreiben gebraucht, ist es heute ein multimediales Erfolgskonzept. Facebook, Twitter, YouTube, und das alles auch noch drahtlos mit Breitband-Internet. Doch welchen Preis zahlen Nutzerinnen und Nutzer für diesen Komfort?

Google gilt als einer der Monopolisten der modernen Internetgesellschaft, unter anderem durch sein mobiles Betriebssystem Android. Mit durchschnittlich mehr als 70 % aller verwendeten mobilen Systeme ist es das weitverbreitetste Betriebssystem für Handys und Tablets.[1]

Wie sicher ist aber unser geliebtes Android-Handy wirklich? Google hat sich ja schließlich schon einige Pleiten geleistet. Während anfangs lediglich einzelne Sicherheitslücken zu verkraften waren[2], wird es heute selbst für geübte Benutzer immer schwieriger zu überprüfen, ob ihre Apps auch wirklich das tun, was sie sollen.

Überprüfen der Berechtigungen von Apps

Was eine App darf und was nicht, wird über deren Berechtigungen abgebildet. Dass man vor der Installation schauen sollte, welche Berechtigungen verwendet werden, ist keine Neuheit und wurde schon öfter diskutiert[3]. Denn es kommt häufiger vor, als man denkt, dass Apps gerne von Datenkraken verwendet werden.

Mit Einführung der neuen Berechtigungsgruppen im letzten Jahr wurde der Aufschrei wieder einmal größer und das zu Recht[4]. Denn Googles neues Gruppenkonzept ist zwar einfacher geworden, dafür aber auch unübersichtlicher. Es wurden 13 neue Gruppen eingeführt[5]. Die zunächst wichtigste Änderung beschreibt Google aber wie folgt: „*These days, apps typically access the Internet, so network communication permissions including the full Internet access permission have been moved out of the primary permissions screen.*“ Internet-Zugriff wird also künftig jeder App gewährt, denn es ist ja jetzt Standard und der Benutzer muss sich nicht darum kümmern.

Was heißt das nun für uns Android-User? Jede App, egal ob nun Taschenlampe oder Facebook, erhält Zugang zum Internet und das, ohne dass es bei der Installation einen Hinweis dafür gibt. Für Social-Media-Apps wie Facebook, Twitter etc. oder Chat-Apps wie das weitverbreitete WhatsApp kommt der Nutzer ja durchaus noch selbst dahinter, dass Internet-Zugang ein notwendiges Übel ist. Was ist aber mit unserer Taschenlampen-, Batterie- oder Wecker-App? Dem Nutzer wird die Information für diese Apps nur noch über Umwege angezeigt: Dies geht nur noch über die Berechtigungsansicht der App unter den Einstellungen des Systems.

Die nächste Pleite des neuen Konzeptes folgt auf dem Fuße, denn bereits installierte Apps bekommen über die automatische Updatefunktion auch neue Berechtigungen ohne die Erlaubnis des Nutzers. Sofern also die automatische Updatefunktion aktiviert ist, darf jede App, die bereits auf dem System läuft, mit dem Update ihre Berechtigungen innerhalb der vorhandenen Berechtigungsgruppen beliebig erweitern. Das erschwert dem Benutzer ein feingranulares Steuern der Berechtigungen. Besser

ist es da, die Updates manuell durchzuführen, denn dann wird für jede App explizit gefragt, wenn neue Berechtigungen benötigt werden[6].

Hier hat man zwar dem Nutzer keine Informationen vorenthalten, aber zu Gunsten der Einfachheit einige durchaus sicherheitsrelevante Informationen an den wichtigen Stellen weggelassen. Zwar lassen sich Apps im Nachhinein auf ihre einzelnen Berechtigungen prüfen, aber dafür muss diese eben auch erst einmal installiert werden. Ein durchaus fragwürdiges Konzept.

Unterlaufen des Berechtigungskonzeptes

Berechtigungen zu *überprüfen* heißt außerdem noch nicht, dass eine App nicht auch andere Wege findet, um Dinge zu tun, die sie eigentlich nicht dürfte. Ein chinesisches Forscherteam hat uns dazu einen Einblick gewährt. In dessen Android App *VoicEmployer* wird die Sprachsteuerung benutzt, um diverse Befehle auf dem Handy auszuführen.

Diese App kann z. B. gefälschte SMS oder E-Mail schreiben, Daten auslesen und übertragen, die GPS-Position ermitteln oder teure Premium-Rufnummern anwählen[7]. Dabei werden einfach mittels vorkonfigurierter Sprachdateien Sprachbefehle auf dem geräte-eigenen Lautsprecher ausgegeben, auf die das Handy mit der Sprachsteuerung Google Voice Search (GVS) reagiert und die Befehle ausführt. Und das alles auch noch ohne eine einzige Berechtigung, denn der Lautsprecher wird einer App standardmäßig zur Verfügung gestellt.

Schließlich demonstriert uns Tod Beardsley noch einige Lücken im Android Browser[8], über die es möglich ist, Befehle auf dem Handy auszuführen oder Apps ohne Erlaubnis des Benutzers zu installieren[9], vom Session Hijacking mittels der zahlreichen gespeicherten Cookies ganz zu schweigen. Dabei surft der Nutzer doch nur auf seinen Lieblingsseiten im Netz …

„Vertrau mir", sagte Google, „bei mir sind deine Daten sicher"[10]

Dass Google selbst kein unbescholtener Mitspieler ist und unverhohlen als Datenkrake agiert, ist sogar in den unternehmenseigenen AGB nachzulesen. Das Stichwort hier ist unsere geliebte Cloud. Mittlerweile lässt sich alles mit der Cloud verknüpfen, Kontaktadressen, Email-Adressen, Backups und natürlich auch alle Apps, die man so installiert hat. Zitat aus den Google-Nutzungsbedingungen: „*Wenn Sie Inhalte in unsere Dienste hochladen oder auf andere Art und Weise in diese einstellen, räumen Sie Google (und denen, mit denen wir zusammenarbeiten) das Recht ein, diese Inhalte weltweit zu verwenden, zu hosten, zu speichern, zu vervielfältigen, zu verändern, […] zu kommunizieren, zu veröffentlichen, öffentlich aufzuführen, öffentlich anzuzeigen und zu verteilen.*"[11] Oder kurz gesagt, was einmal in der Cloud ist, mit dem dürfen Google (und Sie wissen schon wer) alles anstellen, was ihnen in den Sinn kommt. Aber unsere Daten sind ja dort angeblich sicher eingelagert, mit direkten Sicherheitskopien in den diversen Nachrichtendiensteinrichtungen gleich nebenan.

Sicher ist hier wohl nur, dass nichts sicher ist!

Anmerkungen

1 International Data Corporation (IDC): Smartphone OS Market Share, Q4 2014, https://www.idc.com/prodserv/smartphone-os-market-share.jsp

2 Denise Bergert: Schwere Sicherheitslücke betrifft 99 % aller Android-Geräte, 18.5.2011, http://www.pcwelt.de/news/Sicherheit-Schwere-Sicherheitsluecke-betrifft-99-aller-Android-Geraete-1911546.html

3 Florian Schmidt: Aufgedeckt: AGB von App-Anbietern durchleuchtet, 17.6.2011, http://www.computerbild.de/artikel/cb-News-Sicherheit-Allgemeine-Geschaeftsbedingungen-AGB-App-Abzocke-Sicherheit-Datenschutz-6271809.html

4 Reddit: What latest changes to Play Store app means for privacy, 8.6.2014, https://www.reddit.com/r/Android/comments/27n7yr/what_latest_changes_to_play_store_app_means_for/

5 Google: Vereinfachte Berechtigungen bei Google Play, 2014, https://support.google.com/googleplay/answer/6014972?p=app_permissions&rd=1

6 XDA Developers: Play Store Permissions Change Opens Door to Rogue Apps, 10.6.2014, http://www.xda-developers.com/play-store-permissions-change-opens-door-to-rogue-apps/

7 Wenrui Diao, Xiangyu Liu, Zhe Zhou, Kehuan Zhang: Your Voice Assistant is Mine: How to Abuse Speakers to Steal Information and Control Your Phone. In Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices (SPSM '14), Scottsdale, AZ, 3.-7.11.2014, S. 63-74. Vorabversion http://arxiv.org/pdf/1407.4923v1.pdf

8 Tod Beardsley: R7-2015-02: Google Play Store X-Frame-Options (XFO) Gaps Enable Android RCE, 10.2.2015, https://community.rapid7.com/community/metasploit/blog/2015/02/10/r7-2015-02-google-play-store-x-frame-options-xfo-gaps-enable-android-remote-code-execution-rce#comments

9 Heise: Android-Exploit schleust beliebige Apps ein, 15.2.2015, http://www.heise.de/security/meldung/Android-Exploit-schleust-beliebige-Apps-ein-2549172.html

10 Frei nach: Google: Häufig gestellte Fragen. Abgerufen am 2.5.2015, https://www.google.com/intl/de_de/policies/faq/

11 Google: Nutzungsbedingungen, Stand 11. November 2013, https://www.google.com/intl/de/policies/terms/

Carsten Seeger

Carsten Seeger erwarb an der Friedrich-Schiller-Universität Jena einen B.Sc. in Information and Management Science und einen M.Sc. in Informatik. Beide Abschlussarbeiten schrieb er im Bereich IT-Sicherheit. Beruflich ist er mit Datenbanken, Software-Entwicklung und -Test, Web-Design sowie Server-Administration befasst.