Oliver M. Achten, Norbert Pohlmann

Sichere Apps

Vision oder Realität?

Mobile leistungsstarke Endgeräte sind immer und fast überall nutzbar, multifunktional und einfach zu bedienen. Mit „Location Based Services" kommen nützliche und innovative Dienste hinzu, welche die Vorteile von geobasierten Daten ausnutzen. Ein besonderes Herausstellungsmerkmal, aber auch gleichzeitig die Achillesverse der Smartphones, sind ihre Apps! Viele dieser Applikationen übermitteln vertrauliche Daten, eindeutige Gerätekennungen, Aufenthaltsort oder sogar ganze Adressbücher zum Teil ohne, dass es dem Anwender bewusst ist. Dieser Beitrag klärt über Risiken von Apps auf und gibt Handlungsempfehlungen, wie der richtige Umgang mit Apps in Unternehmen aussehen könnte.

1 Motivation

Die Nutzung mobiler Endgeräte erlaubt es Unternehmen, vorhandene Geschäftsprozesse zu optimieren, neue zu etablieren oder komplett neue zu realisieren. Dieser Mehrwert steht aber in direkter Konkurrenz zu den Gefahren, die eine Integration von Smartphones in ein Unternehmen mit sich bringt. IT-Verantwortliche müssen wissen, welche Bedrohungen von diesen innovativen Computern im Hosentaschenformat ausgehen und welche Strategie ergriffen werden müssen, um diese mobilen Geräte sicher zu nutzen und in die Unternehmensinfrastruktur einzubinden.

Apps, Kurzform von Applications, sind Anwendungen für Smartphone/Tablet-Betriebssysteme. Bei den meisten Apps wird der eigentliche Dienst auf einem Server des Anbieters im Internet durchgeführt. Die entsprechende App stellt eine optimierte Schnittstelle zwischen dem Benutzer und dem Smartphone/Tablet dar. Mit Hilfe des Multitouchscreen können mit wenigen Aktionen des Nutzers die Apps für spezielle Anwendungen sehr schnell und einfach ihre Dienste erbringen.

Was ist aber mit Daten auf dem Smartphone/Tablet, die ohne das Wissen der Betroffenen im Hintergrund gespeichert werden? Wo liegen die Probleme und Gefahren, wenn der Nutzer einer App gar nicht weiß, welche Daten von ihm im Hintergrund erhoben werden? Und was hat das alles mit Smartphones und ihren Apps zu tun? Dieser Artikel wird Antworten auf diese Fragen liefern und Handlungsempfehlungen zum richtigen Umgang mit Apps geben, um das IT-Sicherheits- und Datenschutzbewusstsein der Anwender weiter zu schärfen.

Oliver M. Achten

ist Informatikstudent im Bereich Echtzeitsysteme und Robotik an der FH Gelsenkirchen. Seit 2008 ist er Mitarbeiter des Institut für Internet-Sicherheit und Projektleiter der Forschungsbereiche Mobile Security und Cloud Computing. Des Weiteren ist er Mitglied des Forschungsteams Identity Management und vermittelt, als Hacker in Awareness Performances, welche Sicherheitsrisiken mit dem Internet und der digitalen Welt verbunden sind.
E-Mail: achten@internet-sicherheit.de

Prof. Dr. Norbert Pohlmann

ist seit 2003 Informatikprofessor für Verteilte Systeme und Informationssicherheit im Fachbereich Informatik und geschäftsführender Direktor des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen. Außerdem ist er Vorstandsvorsitzender des IT-Sicherheitsverbandes TeleTrusT.
E-Mail: norbert.pohlmann@internet-sicherheit.de

2 Gefahren und Risiken die von Apps ausgehen

Heutige Smartphones werden ab Werk mit einem rudimentären Betriebssystem ausgestattet. Die Funktionen sind auf die wesentlichen Dinge, wie Telefonie, SMS und wenige andere Anwendungen begrenzt. Weitere Funktionen oder Spezialisierungen müssen über Drittanbieter in Form von optionalen Anwendungen, Apps, bezogen werden. Allein Apples App Store bietet derzeit ca. 500.000 Apps an, welche im Monat millionenfach heruntergela-

den werden[1]. Weitere App-Markets sind Google Android Market, Amazons Appstore und Microsofts Windows Phone 7 Marketplace.

Aber egal wo und welche App heruntergeladen wird, Benutzer müssen immer entscheiden, ob sie der App den Zugriff auf weitere Daten, wie Kontakte, E-Mails, Fotos, Name, Adresse, (aktuellen) Aufenthalts- /Wohnort, Anmeldedaten (Benutzername/Passwort) und andere sensible Daten erlauben. Dies ist in zweierlei Hinsicht problematisch, denn erstens wissen die Benutzer nicht oder können nicht kontrollieren, was die Apps mit diesen Informationen genau machen. Zum Zweiten ist der Trend „Masse statt Klasse" in den verschiedenen Markets zu erkennen. Dadurch steigt die Wahrscheinlichkeit, dass fehlerhafte und, aus sicherheitstechnischer Sicht, bedenkliche Apps, auf dem Market angeboten werden. Diese Apps stellen ein erhöhtes Sicherheitsrisiko dar, wenn sie auf die Smartphones herunter geladen bzw. darauf installiert werden.

2.1 Datenabfluss

Das Wall Street Journal hat in einer groß angelegten Studie über 100 Apps für iPhone und Android auf Informationsweitergabe hin analysiert[2]. Einige Apps gaben Alter, Geschlecht und andere personenbezogene Informationen weiter. Mehr als die Hälfte aller analysierten Apps gaben, ohne die Einwilligen oder die in Kenntnissetzung des Benutzers, die IMEI des Telefons weiter. Die IMEI ist ein eindeutiger Identifier, den jedes Smartphone besitzt. Mit ihr ist nicht nur die Zuordnung des Highscores eines Spiels, sondern auch die Profilbildung über mehrere Apps hinweg möglich. Es können somit Informationen aus unterschiedlichen Apps gesammelt werden, die in ihrer Gesamtheit einen größeren Wert für den Betreiber bilden. Meist werden die gesammelten Informationen an sogenannte Werberinge übermittelt, denn der monetäre Mehrwert bei fast allen Apps, die persönlichen Informationen des Anwenders sammeln, ist der Grund, weshalb überhaupt sensible Informationen weiter gegeben werden.

Das Geschäftsmodell „Bezahlen mit persönlichen Informationen" gibt es aber nicht erst seit dem es Apps gibt. Internetseitenbetreiber versuchten schon immer, so viele persönliche Informationen wie möglich über ihre Besucher herauszufinden bzw. zu sammeln. Nur die Art und Weise hat sich geändert. War es früher noch möglich seine persönlichen Informationen durch die Angabe von falschen Inhalten oder Synonymen in Formularen zu verbergen bzw. zu schützen, so greifen die Apps diese persönlichen Informationen nun an Stellen ab, von denen sie sicher sein können, keine Fehlinformation zu bekommen. Die Quelle der Daten kann das komplette Telefonbuch des Smartphones sein, aber auch eine Datenbank mit Geokoordinaten, mit deren Hilfe ein Bewegungsprofil erstellt werden kann.

2.2 Kontrollmechanismen für Apps

Durch den großen Erfolg von Apples App Store und Googles Android Market ist die Entwicklung von Apps ein attraktiver und lukrativer Geschäftszweig geworden. Datenschützer treten zunehmend an die Anbieter von Apps heran, die zum Teil falsch mit diesen nicht freiwillig zugänglich gemachten *Informationen* umgehen oder diese gar missbrauchen. Persönliche Daten können auf verschiedene Weisen weiter gegeben werden. Bei einer aktiven Weitergabe ist der Benutzer bei einem Dienst angemeldet oder nutzt gerade aktiv diesen Dienst. Die Weitergabe wird also bewusst vom Benutzer eingeleitet, und es werden nur solche Informationen übermittelt, die vom Benutzer dazu ausgewählt wurden. Ein Beispiel wäre die Statusänderung seines Nutzerprofiles. Als eine passive Weitergabe würde die Übermittlung der Informationen an Dritte bezeichnen. Das findet statt, wenn der Besitzer des Dienstes die Profilinformationen an einen Werbering weiterleitet. Ein weiterer nicht zu unterschätzender Risikofaktor ist die im Hintergrund stattfindende Informationsweitergabe, wenn der Benutzer eine App gerade gar nicht aktiv verwendet oder eingeloggt ist. So könnte die App beispielsweise Passwörter bzw. Zugangsdaten in einem unsicheren Netz verschicken. Der Anwender, der weiß, dass in einem unsicheren Netzwerk keine sensiblen Daten unverschlüsselt verschickt werden sollen, will eventuell nur den Wetterbericht lesen. Im Hintergrund ruft eine App aber automatisch die neusten Informationen aus einem sozialen Netzwerk ab. Dabei überträgt die App die Anmeldedaten des Anwenders in einem potenziell unsicheren Netzwerk, ohne dass er diesen Vorgang gestartet oder bemerkt hat.

Kontraproduktiv sind in diesem Zusammenhang ebenso fehlerhafte oder kompromittierte Apps, die einen unbemerkten Abfluss, das Stehlen oder Zerstören von sensiblen Informationen ermöglichen. Jüngste Vorfälle mit kompromittierten Apps[3], die im Android Market gefunden wurden, zeigen, dass auch Smartphones genauso wie Computer zur Zielscheibe von Malware geworden sind.

Durch die Validierung bzw. vorherige Prüfung der einzelnen Apps, damit diese gar nicht erst in den Market aufgenommen werden, haben die Markets eine signifikante Sicherheitsfunktion, die das Sicherheitsniveau der mobilen Endgeräte maßgeblich beeinflussen könnte. Eine zu meisternde Herausforderung ist die Umsetzung dieser Sicherheitskontrollen. So gibt es begrenzte manuelle, automatisierte oder gar keine Vorkehrungen, die Integrität der zu verteilenden Apps sicher zu stellen. Bei der manuellen Prüfung analysieren Experten des jeweiligen Markets oder ausgelagerte Sicherheitsfirmen die Apps. Bei der automatisierten Prüfung durchläuft die App mehrere Kontrollinstanzen. Innerhalb dieser Instanzen wird beispielsweise der Programmcode auf bösartige Funktionen untersucht, aber auch die Reputation des Entwicklers und andere Faktoren spielen für die endgültige Freigabe der App eine wichtige Rolle.

Leider hat die Vergangenheit gezeigt, dass dieses Vorgehen auch nicht das Ideale ist und bösartige Apps ihren Weg in den Market gefunden haben[4][5]. Umso kritischer ist die Entwicklung zu betrachten, dass viele Nutzer ihre Verantwortung bezüglich ihrer Daten an den jeweiligen App-Marktet abgeben und sich darauf verlassen, dass die Kontrollmechanismen dieser Markets kompromittierte Apps bzw. den Missbrauch von Rechten erkennen.

Leider sind es aber gerade die Anwender, die als letzte Instanz entscheiden, ob eine App den Weg auf das Smartphone findet. Die Anzahl der Apps, die von einem Durchschnittsanwender installiert werden, ist rasant gestiegen. So werden beispielsweise im

1 http://www.apple.com/pr/library/2011/12/12Apples-Mac-App-Store-Downloads-Top-100-Million.html

2 S. Thrum and Y. Kane. Your Apps are Watching You. Wall Street Journal, http://online.wsj.com/

3 http://www.msnbc.msn.com/id/41867328/ns/#.TvyeoJhnS-g

4 http://www.reuters.com/assets/print?aid=USTRE6BR1Y820101228

5 http://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/

Schnitt ca. 60 Apps auf ein iPhone gespielt[6]. Alleine in der Woche nach Heiligabend wurden weltweit 1,2 Milliarden Apps aus Apples App Store und Googles Marketplace heruntergeladen. Davon ca. 40 Millionen in Deutschland[7].

Für die korrekte Funktionsweise all dieser Apps, müssen sie Zugriff auf sensible Daten haben. Dies können Daten sein, die das Smartphone direkt zur Verfügung stellen kann (Anmeldedaten, Passwörter, Kontakte, GPS, Kamera, Mikrophone und andere), aber auch Cloud-Dienste (Google, Facebook, Twitter, etc.). Bei Apple bekommt der Anwender überhaupt keine Informationen bezüglich der Daten auf die eine App zugreifen wird, bevor diese installiert wird. Google hingegen hat sich bei seinem Betriebssystem Android dafür entschieden, dem Anwender anzuzeigen, welche Zugriffsrechte die App nach der Installation auf das System haben wird. Diese Technik bietet aber auch keinen ausreichenden Schutz vor Missbrauch, denn es fehlen die Kontrollmechanismen um festzustellen, ob die App nur auf die Informationen zugreift, die sie vorgibt zu brauchen.

Als Beispiel wäre eine Diktiergerät-App durchaus in der Lage, mit ihrem berechtigten Zugriff auf das Mikrophon nicht nur das Diktat aufzuzeichnen, sondern auch das Firmenmeeting, einschließlich seines brisanten Inhalts. Dazu kommt noch, dass ein Anwender die Informationen, welche Rechte gefordert werden, einfach bestätigen kann, ohne diese überhaupt gelesen zu haben.

Als letzte Instanz, die für den Schutz der Daten des Anwenders zuständig ist, bleibt somit nur noch das Betriebssystem. Dies ist auch einer der Hauptunterschiede von PCs und Smartphone bzw. Programmen und Apps. Der Basisschutz, bestehend aus Antivirenschutz und Firewall, ist für ein sicheres Arbeiten mit dem PC unverzichtbar. Die Firewall warnt sofort bei ausgehenden Verbindungen eines Programmes. Diese Art des Schutzes ist noch nicht bis zu den Smartphones vorgedrungen. Eingehende und ausgehende Verbindungen werden komplett am Anwender vorbei aufgebaut, sodass eine Regulierung nicht möglich ist. Beispielsweise kann nicht überwacht werden, ob vielleicht eine Taschenlampen-App eine Verbindung zum Internet aufbaut, um Daten zu verschicken oder zu empfangen.

Dies gilt nicht nur für explizit aufgebaute bzw. fragwürdige Verbindungen. Bei bestehenden Verbindungen, ist es auch am PC fast nicht möglich, automatisiert den Informationsfluss zu überwachen. Spätesten wenn die Verbindung verschlüsselt ist, kann nicht analysiert werden, ob beispielsweise nur eine Nachricht verschickt wurde oder noch weiter Daten. Zurzeit existiert (noch) kein Betriebssystem, dass diese Arten der Informationsweitergabe erkennt bzw. ermittelt[8].

4 Der Richtige Umgang mit Apps im Unternehmen

Der stärkste Treiber für den Einsatz von Smartphones im Unternehmenseinsatz sind die Mitarbeiter der Firmen. Die Funktionsvielfallt und Arbeitserleichterungen, die im privaten Umfeld geschaffen wurden, wollen die Mitarbeiter auch für ihren Arbeitsalltag nutzten.

4.1 Device Management Konzept

Ein Unternehmen steht bei der Nutzung von privaten Smartphones vor dem Problem ein weiteres Gerät, und somit eine weitere potenzielle Schwachstelle, in die Unternehmensinfrastruktur zu integrieren. Entscheiden sich die IT-Verantwortlichen für ein einheitliches Gerätemodell, das ausgerollt werden soll, kann ein Mangel an Akzeptanz der Mitarbeiter dazu führen, dass das private Smartphone stärker genutzt wird. Die zurzeit oft diskutierte Methode „bring your own device" hat weniger ein Akzeptanzproblem, da der Mitarbeit das mobile Gerät seiner Wahl nutzen kann. Es besteht aber ein Managementproblem, da eine sehr heterogene Gerätelandschaft aufgebaut wird. Bei beiden Methoden ist ein ganzheitliches Device Management Konzept ein entscheidender Sicherheitsfaktor. Denn durch ganzheitliche und erfolgreich umgesetzte Sicherheitsrichtlinien ist es heute durchaus möglich, die mobilen Geräte sicher zu integrieren.

Für den erfolgreichen Firmenalltag ist es essenziell, private und geschäftliche Daten zu trennen. Dies kann per Software erfolgen, aber langfristig sollte hier auf eine starke Isolation und Separierung der unterschiedlichen Bereiche gesetzt werden, die dann schon auf Hardwareebene beginnt. Somit können Apps, die im Privatbereich des Smatphones arbeiten, nicht auf die sensiblen Daten aus dem Firmenbereich zugreifen.

4.2 Reputationssystem

Eine besondere Herausforderung stellen einzelnen Apps dar, die bewusst für den Firmenbereich installiert werden sollen bzw. müssen. Durch das rasant wachsende Angebot an Apps und die jeweilige Weiterentwicklung der einzelnen Apps, ist es fast unmöglich für ein einzelnes Unternehmen eine Liste mit analysierten, sicheren und vertrauenswürdigen Apps zu führen. Aber ein Kooperations-Netzwerk, das gemeinsam Information zur Verfügung stellt, wie eine App mit persönlichen Informationen umgeht bzw. ob die App sicher ist, könnte ein Lösungsansatz sein, eine höhere Vertrauenswürdigkeit zu erzielen. Diese Idee kann mit Hilfe eines Reputationssystems umgesetzt werden, das zum einen Informationen über bestimmte Apps bereit stellt und zum anderen Alternativen nennt, die andere Nutzer vorgeschlagen haben.

Die Anwender müssen in der Lage sein zu erkennen, was mit ihren Informationen eventuell passieren könnte, wenn sie eine bestimmte App nutzen. Dazu bedarf es Informationen oder Werkzeuge, die verantwortungsbewusste Anbieter oder organisierte Netzwerke zur Verfügung stellen. Eine Anwendung, die den Nutzer warnt, dass die von ihm gewählte App alle seine Kontakte an einen Spam-Versender schicken wird, ist hilfreicher als im Nachhinein aufzuzeigen, dass dies passiert ist. Dieser Ansatz ist nicht neu und wird bereits für Webseiten und auch für Apps genutzt bzw. angeboten. Web Of Trust (WOT)[9] und WhatApp[10] sind Beispiele für solche Reputationssysteme, in denen Experten und Anwender Seiten und Apps bewerten.

6 http://www.asymco.com/2011/01/16/more-than-60-apps-have-been-downloaded-for-every-ios-device-sold/ - 2011

7 http://blog.flurry.com/bid/79928/Holiday-2011-Breaking-the-One-Billion-App -Download-Barrier

8 Privacy Revelations for Web and Mobile Apps, D. Wetherall, D. Choffnes, 2011

9 Web of Trust. http://www.mywot.com/ , 2011.

10 WhatApp. http://whatapp.org/ , 2011.

4.3 Awareness

Ein weiterer wichtiger Sicherheitsaspekt für den richtigen und sicheren Umgang mit Apps bzw. Smartphones im persönlichen und beruflichen Umfeld, ist die Sensibilisierung und der Aufbau eines Sicherheitsbewusstseins der Anwender. Verschiedene Anwender haben unterschiedliche Ansichten hinsichtlich des Datenschutzes und der Datensicherheit. Einfach nur darauf hinzuweisen, dass Informationen weitergegeben bzw. abgegriffen werden können, ist aus Erfahrung weniger effektiv, als eine praktische Demonstration von solchem Fehlverhalten. Das Institut für Internet-Sicherheit zeigt beispielsweise im Rahmen von Live-Hackings-Shows den Zuschauern, wie einfach es sein kann, an sensible Information mit Hilfe manipulierter Apps zu kommen, wenn angefragte Zugriffsrechte einfach bestätigt werden. Die Erfahrung zeigt, dass ein Anwender sich vor der nächsten Installation einer App eher an diesen „Aha-Effekt" aus der Live-Demo erinnert, als an den dritten Spiegelstrich der 42 Folien einer Schulung. Der Nutzer, der das Smartphone bedient, muss ebenso *up to date* gehalten werden, was den Umgang mit aktueller Technik betrifft, wie die eingesetzte Software im Unternehmen. Nur so wird dem Nutzer das Risiko bewusst, und er kann entsprechend reagieren.

5 Die sichere App

Um eine sichere App zu entwickeln, muss das Thema Sicherheit in der kompletten Entwicklungsphase Beachtung finden. Es reicht nicht aus, im Nachhinein ein Rollenkonzept oder eine Verschlüsselung aufzusetzen, sondern es müssen bereits in der Designphase klare Sicherheitskonzepte beachtet werden.

Für die Entwickler von Apps stellen alle Betriebssystemherstellern sogenannte Development Guidelines zu Verfügung die Konventionen und Best Practice Beispiele für das jeweilige Betriebssysteme beschreiben. Für viele Entwicklungsprobleme gibt es bereits anerkannte Lösungen und der Entwickler ist nicht gezwungen „das Rad neu zu erfinden".

Das Institut für Internet-Sicherheit hat eine securityNews[11] App entwickelt, bei deren Entwicklungsphase diese Grundsätze beachtet und darüber hinaus auch auf Datensparsamkeit geachtet wurde. So werden aktuelle Sicherheitsinformationen bezüglich Software und Betriebssystemen ohne eine Art von Registrierung, abgesehen von der App Store Anmeldung, tagesaktuell angezeigt. Erst wenn der User individuelle Informationen will, muss er sich anmelden, sodass die zu sendenden Informationen auf seine Vorgaben angepasst werden können. Bei aller Vorsicht und Gewissenhaftigkeit bei der Entwicklung von Apps, darf nicht vergessen werden, dass Menschen beteiligt sind. Menschen machen Fehler und diese sogar statistisch erfassbar. So hat eine Studie ergeben[12], dass auf 100 Zeilen Code ein Fehler programmiert wird. Diese Fehler sind zum Teil auch potentielle Schwachstellen und können für einen Angriff genutzt werden.

Entwickler von Apps sollten zwei Punkte beachten: Sie müssen dem Anwender die Möglichkeit geben, Kontakt aufzunehmen, um auf gefundene Fehler von Anwendern aufmerksam machen zu können. Zudem muss ein Updatemechanismus eingerichtet werden, so dass behobene Fehler schnellst möglich korrigiert werden können. Hier liegen die Stärken von App-Markets, die ein Ausrollen der neuen Version der App stark vereinfacht haben und somit maßgeblich zur Aktualität der Software auf den Smartphones beitragen.

Der zweite Punkt ist die Vertrauenswürdigkeit. Aktuell hat ein Anwender keine Möglichkeiten zu prüfen, ob eine angebotene App, die in einem App-Market angeboten wird, auch wirklich von dem beschriebenen Entwickler kommt. Dem Anwender bleibt nur eine Recherche außerhalb des Market, denn auch die Bewertungen innerhalb des Marktes können gefälscht sein und trojanisierte App-Versionen unter dem fast gleichen Namen erfolgreicher Apps anbieten[13]. Die Hauptinformationsquelle sollte dabei die Entwicklerseite sein, deren Authentizität über ein Zertifikat bewiesen werden sollte. Wenn nun eine detaillierte Beschreibung der App auf der Herstellerseite zu finden ist und sogar noch ein Verweis zu der App im Market, dann kann der Anwender vor der Installation der App davon ausgehen, die richtige App des beschriebenen Entwicklers gewählt zu haben. Was diese App dann alles macht und ob sie vertrauenswürdig ist, bedarf einer weiteren Recherche oder der Nutzung eines Reputationssystems.

6 Fazit und Ausblick

Smartphones/Tablets mit Apps werden definitiv in den nächsten Jahren noch stärker genutzt werden. Der Spruch „there is an app for that" trifft momentan mehr denn je zu und wird uns auch in Zukunft verfolgen. Die Unternehmen stehen nun wieder vor denselben Problemen wie bei der Einführung des PCs und dem Internet, als Angestellte anfingen, selbstständig Software auf ihren Arbeitsrechnern zu installieren. Fremde Software, die nicht von der IT-Abteilung vorgesehen war, ist also kein unbekanntes Problem.

Entscheidend war und ist das Verhältnis zwischen Mensch und Technik. Bei den Anwendern und Entwicklern von Apps muss ein Sicherheitsbewusstsein aufgebaut werden, aber gleichzeitig muss die Technik vorhanden sein, das Erlernte auch umsetzen zu können.

Aus heutiger Sicht ist festzustellen, dass das Vorhandensein von Schwachstellen in Software kurzfristig nicht zu ändern ist, d.h. die Fehlerdichte von Software wird zwar kleiner, Fehlerfreiheit ist zurzeit aber für große Software nicht erreichbar. Dazu kommt bei den Apps noch, dass der notwenige App-Market nicht den Sicherheitsanforderungen entsprechen, die bei einer so zentralen Rolle, notwendig wären. Die Kontrollmechanismen befinden sich noch am Anfang ihrer Entwicklung und müssen weiter verbessert werden, so dass die zentralisierte Verteilung als Vorteil genutzt werden kann. Die Analyse des Informationsflusses, die eine App tätigen wird, muss ebenso verbessert werden, wie die Authentizitätsnachweise der Apps. Es müssen präventiv Informationen an den Anwender geben werden. Ein Anwender muss gewarnt werden, *bevor* er eine App installiert, die sein gesamtes Telefonbuch an Dritte verschickt.

Sichere Apps könnten Realität sein, wenn die IT-Sicherheit in diesem neuen Businessmodell eine besondere Rolle spielen würde. Die Sicherheitsmechanismen sind bekannt und könnten intelligent und sicher eingesetzt werden, um sichere Apps zu nutzen.

11 https://www.it-sicherheit.de/ratgeber/securitynews/iphoneapp/

12 Fehler in Software, Dr.-Ing. Matthias Werner, TU Chemnitz 2007

13 http://nakedsecurity.sophos.com/2011/12/12/malicious-cloned-games-attack-google-android-market/