

Link: <https://www.channelpartner.de/a/was-taugt-die-eingebaute-sicherheit,3042525>

Security-Features bei iOS und Android

Was taugt die eingebaute Sicherheit?

Datum: 06.06.2014

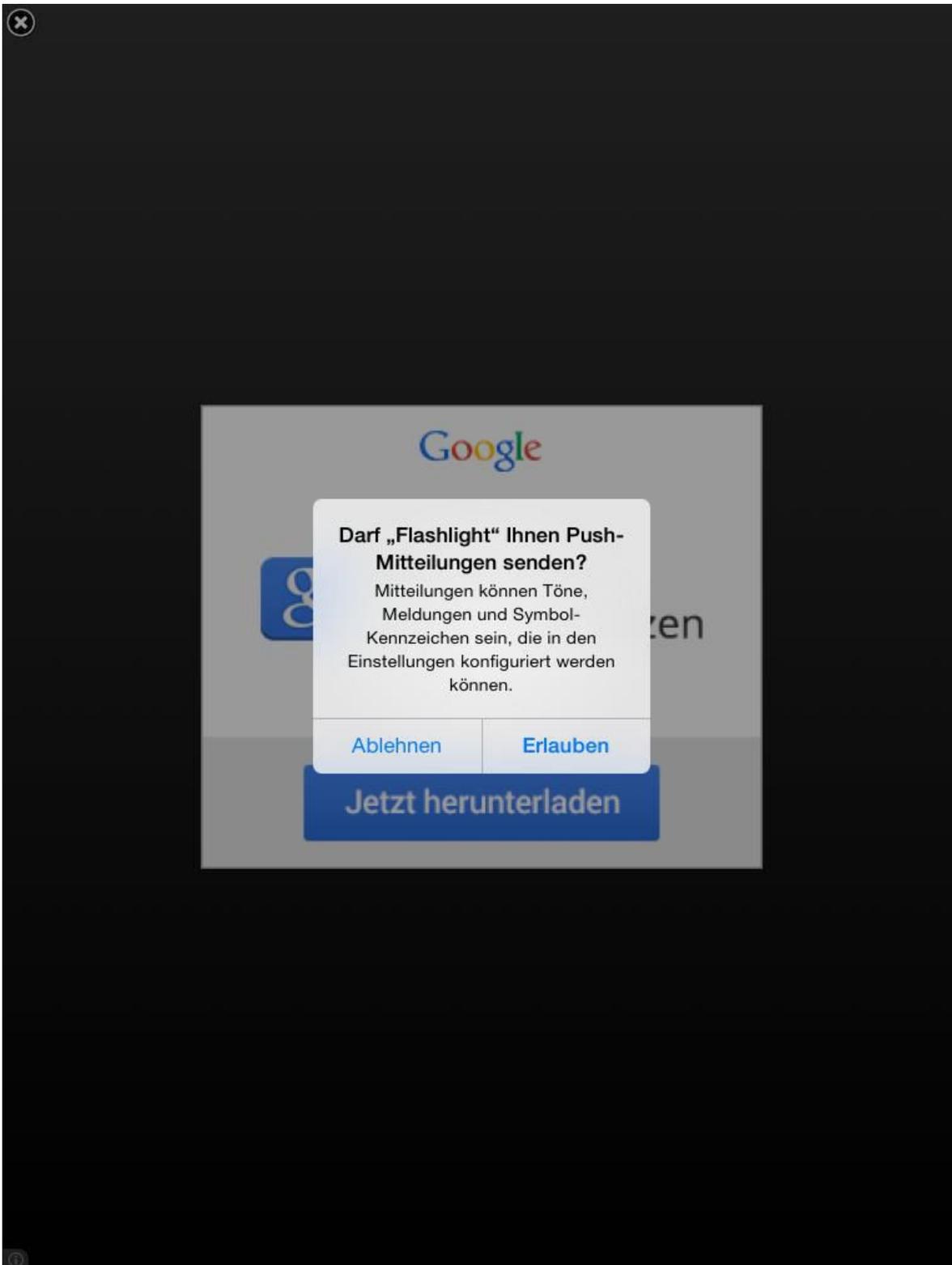
Autor(en): Frank-Michael Schlede, Thomas Bär

Bestimmte Apps können Daten von einem Smartphone oder Tablet auslesen und diese über das Internet versenden. Wie schützen die Hersteller vor diesem Risiko?

Smartphones sind kleine Computer und verbinden die Funktionen von Telefon, Media-Player, Handspielkonsole, Informationsdatenbank oder Navi in einem einzigen Gerät. Kein Wunder also, dass Smartphones allen soeben genannten Gerätetypen langsam aber sicher den Rang ablaufen. Aufgrund des umfassenden Angebots und des deutlich günstigeren Preises erfreuen sich Android-basierte Smartphones der höchsten Verbreitung, gefolgt vom Quasi-Erfinder des modernen Telefons, der Firma Apple. Windows-basierende Geräte sind zwar durchaus auf dem Vormarsch, spielen aber weiterhin **in Europa nur eine kleinere Nebenrolle**¹.

Allen Anbietern ist ein gemeinsames Konzept bei der Bereitstellung der Software für ihre Plattformen gemein. Es gibt je einen zentralen Anlaufpunkt, um die vom Benutzer ausgewählten Programme, die Apps (Abkürzung für Application - auf Deutsch Anwendung), auf das Mobilgerät verteilen. Dieser konzeptionelle Unterschied zu den Desktop-Betriebssystemen oder Frühformen der Mobile Devices auf **Palm**²- oder **Windows CE/Mobile-Basis**³ wirft eine entscheidende Frage auf: "Wie schützen uns die Anbieter vor schlecht programmierten Apps, die für mich ein Sicherheitsrisiko darstellen können?".

Gute Frage:
Wozu braucht
eine



Taschenlampen-App den Zugriff auf Push-Mitteilungen?

Grundsätzlich unterscheidet sich das Risiko zwar nicht vom herkömmlichen Desktop-Rechner, da dort Programme sogar aus beliebigen Quellen stammen können. Da aber Google, Apple und Microsoft über ihre Stores nun als alleiniger Händler für ihre Plattformen auftreten, erhöht sich automatisch der Anspruch an den Anbieter, da keine Alternative zur Verfügung steht: Der Hersteller produziert das Gerät, liefert die Infrastruktur und verkauft letztendlich als Zwischenhändler die gesamte Software - bei soviel gefühltem Monopol auf einem Haufen sollte das grundsätzliche Sicherheitskonzept stimmen.

Wirtschaftliche Schäden und Datenschutzrisiko

So praktisch die kleinen Miniprogramme auch sind, sie haben nicht nur Gutes. Insbesondere bei kostenlosen Apps muss sich der Anwender darüber im Klaren sein, dass das Programm oder die Dienstleistung zwar umsonst ist, der Benutzer zahlt aber dafür mit seinen Daten. Das gibt Dr. Julian Schütte von der **Fraunhofer-Einrichtung für Angewandte und Integrierte Sicherheit**⁴ AISEC in Garching bei München **zu bedenken**⁵.

Bei diesen Daten handelt es sich um den aktuellen Aufenthaltsort, E-Mail-Daten oder Adress-Informationen. Diese Daten münden in personen- oder ortsbezogener Werbung. Das sei ja gar nicht so schlimm, könne man meinen, wenn es sich nur um Privatinformationen geht. Übermitteln die Apps jedoch Informationen aus geschäftlichen E-Mails mit unternehmenskritischen Inhalten, Geopositionen von Mitarbeitern oder vertrauliche Kontaktdaten, so könnte ein wirtschaftlicher Schaden drohen, so Schütte weiter.

[Hinweis auf Bildergalerie: **Bildergalerie: Samsung Galaxy Tab 10.1**] gal1

Kostenlose Apps stellen bezüglich der Datensicherheit grundsätzlich ein Risiko dar, da die Verarbeitung von gefundenen Daten das eigentliche Geschäftsmodell des Anbieters darstellt. Auf welche Informationen eine App Zugriff haben möchte, gibt sie bei der Installation bekannt. Ohne Frage benötigt eine "Taschenlampen-App" wohl kaum den Zugriff auf das Adressbuch. Wem der Datenzugriff zu weit geht, der wählt eine andere App mit ähnlichem Leistungsumfang. Da es für jeden erdenklichen Einsatz mehrere Apps gibt, besteht stets die Hoffnung, auf eine solche Alternative zu stoßen.

Namhafte Anbieter reduzieren lieber den Leistungsumfang ihrer Lite-Editionen und hoffen so, den Interessenten zum Erwerb der kostenpflichtigen Vollversion zu erwärmen. Die Weiterverarbeitung von persönlichen Daten zu Werbezwecken gilt bereits schon als verpönt.

Apples Sicherheitskonzept beginnt mit dem Booten

Apple verfolgt einen eher "geschlossenen Ansatz" und versucht möglichst nichts und niemanden an die direkten Betriebssystemressourcen heranzulassen. Einen klassischen Explorer oder Finder, der sich für den Zugriff auf das Dateisystem eignet, wie bei Android, gibt es überhaupt nicht. Da Apps ausschließlich Ressourcen nutzen können, die das Betriebssystem bereitstellt, ist es von entscheidender Bedeutung, dass sich das OS stets in einem sicheren Status befindet.

Bereits beim Systemstart eines Apple-Geräts, der so genannten Initialisierungsphase der Hardware, wird das Einschleusen von Schadprogrammen durch das Zusammenspiel von Betriebssystem und Hardware verhindert. Durch kryptographisch signierte Komponenten, darunter der **Kernel**⁶ und der **Bootloader**⁷, verhindert Apple, dass das iOS heimlich modifiziert wird. Kommt es zu Abweichungen, unterbricht das Gerät den Startvorgang und verlangt nach einem Firmware-Upgrade, zumeist über die Apple-eigene Verwaltungssoftware iTunes.

Die so genannte "System Software Personalization" von Apple verhindert das Rücksetzen auf eine ältere, möglicherweise durch Sicherheitslücken anfällig gewordene iOS-Version. Bedingt durch die Tatsache, dass Apple jedem Gerät eine eindeutige Kennung mit auf dem Weg gibt, die **ECID**⁸, und stets eine Verknüpfung mit einem iTunes-Account verlangt wird, ist es für den Anbieter recht einfach, eine Historie von Betriebssystemversion und Nutzer vorzuhalten. Diese Maßnahmen, und andere, beispielsweise die permanent aktive Geräteverschlüsselung, die fehlende Möglichkeit, den Speicher durch externe Medien zu erweitern, sorgen letztendlich dafür, dass das Betriebssystem nur in einem gesicherten Status starten kann.



Empfehlenswerte Lektüre des BSI - das Überblickspapier Apple iOS.

Überblickspapier Apple iOS



Auch wenn es treue Apple-Kunden nicht so gern hören, so gab es auch bei iOS Schwachstellen, die zu verschiedenen Sicherheitsproblemen führten. Nicht nur einmal ließ sich der Passcode durch einen einfachen Trick umgehen. Allein zwischen den Version 5 und 6 von iOS musste Apple, laut Informationen eines **Überblickspapiers des BSI**⁹, 197 Sicherheitslücken schließen. Nur wenn das Betriebssystem sicher ist, können möglicherweise fragwürdige Apps diese Lücken nicht für ihre Zwecke missbrauchen. Apple erinnert den Benutzer bei jedem Blick auf die Systemeinstellungen daran, dass Updates eingeschpielt werden müssen.

Ebenfalls warnt das BSI bei Geräten mit dem iOS-Betriebssystem vor indirekter Ausspähung des Benutzers durch Dienste oder Apps. Ein Beispiel wären die so genannten Geolocation-Dienste, bei denen der Standort des Benutzers erfasst und mit einem Dienst verknüpft wird. Mit solchen Diensten lassen sich unter Umständen Zugangsbeschränkungen umgehen oder persönliche Informationen abgreifen. Oder der Beschleunigungssensor, dessen Daten missbraucht werden könnten, um Eingaben über den Touchscreen auszuspähen.

iOS ständig am Senden Richtung Apple

Wenig bekannt sein dürfte der permanente Datenabfluss eines iOS-Geräts in Richtung Apple. iPhones & Co. senden seit iOS-Version 6 im Hintergrund laufend Protokoll-Log-Dateien und Fehlerberichte an den Hersteller. Nur falls der Benutzer bei der Installation des Updates dieser Übermittlung nicht explizit widerspricht, handelt es sich um das Standardverhalten. Da diese Daten durchaus auch vertrauliche oder persönliche Informationen enthalten können, handelt es sich, mit Blick auf den Datenschutz, um eine äußerst fragwürdige Funktionalität. Zudem können legitim installierte Apps, so das BSI, diese Daten, auch ohne Wissen des Anwenders, an Dritte weitergeben.

Sicherheitsrelevante Software ist für iOS kaum verbreitet, da Apple durch das Design des Betriebssystems und der Technik des Sandboxing (keine Applikation darf auf die Daten und Ressourcen einer anderen App zugreifen) davon ausgeht, dass ein kritischer Sicherheitsstatus nicht erreicht werden kann. Regelmäßige Updates des Betriebssystems seien ausreichend. Sofern es also nicht das iOS selbst ist, das unerwünscht auf App-Daten zugreift, gibt es keine Notwendigkeit für Virenschutz & Co. Ganz anders sieht es aus, sofern der Benutzer das Gerät durch einen "Jailbreak" öffnet, um auf die Ressourcen selbst direkt zugreifen zu können. Diese Geräte sind eine Gefahr für den Benutzer und insbesondere für alle darauf gespeicherten Unternehmensdaten.

Android orientiert sich am klassischen PC

Viele der Sicherheitsfunktionen, die Apple dem iOS mit auf den Weg gegeben hat, sind auch in der traditionellen PC-Branche nicht unbekannt. Sie heißen nur anders und entgegen der Vermutung, dass es ein Vorteil wäre, dass alles aus einer einzigen Hand stammt, funktioniert es bei Linux oder Windows auch ohne monopolistische Anbieter. Android hat eine deutliche Anlehnung an Linux und ist - entsprechend dieser Konzeption - viel offener. Neben dem Linux-Grundgerüst nutzen Android-Apps Java und dessen virtuelle Maschinen für den Betrieb.

Wie iOS, so setzt auch Android auf eine starke Isolation von Apps und der Regelung, dass diese nur auf dedizierte Systemressourcen zugreifen können. Diese Isolierung schützt nicht nur die Apps untereinander, sondern auch das Betriebssystem vor ungewollten Änderungen. Sofern es eine App nicht gelingt, den so genannten "Administrator-Level-Mode" zu erreichen, was faktisch nur durch das bewusste "Rooten" passieren kann, können Apps das Android-OS nicht anpassen. Zwar dürfen Apps nicht auf den Speicherbereich anderer Apps zugreifen, sie können jedoch sehr wohl - über das Betriebssystem - herausfinden, welche anderen Apps in welcher Version auf dem Gerät installiert sind.

Zudem sind die meisten Apps unter Android in der Lage, alle unverschlüsselten Daten einer SD-Karte auszulesen, jedoch ohne Schreibzugriff. Sollten sich auf der SD-Karte jedoch persönliche Informationen befinden, beispielsweise Fotos oder Dokumente, so könnte eine App diese für eigene Zwecke nutzen und beispielsweise über das Internet verschicken. Trotz der Isolierung ist es unter Android für eine App durchaus möglich, andere Apps zu starten.

Letztendlich benötigt der Anwender, wie bei einem typischen PC, eine Sicherheitssoftware, die feststellt, dass die installierten Apps und aktiven Prozesse keine Gefahr für das System darstellen.

Dem Entwickler auf die Finger schauen

Im direkten Vergleich zu Android-Anbieter Google setzt Apple auf eine sehr restriktive Politik, was die Erweiterbarkeit hinsichtlich der Software und vor allem der Hardware angeht. Software-Entwickler, die ihre Apps über den App Store anbieten, müssen ihre Software zunächst durch Apple in Tests prüfen lassen, ehe sie im Store verfügbar sind. Dieses Konzept, auch wenn es denkbare Lücken gibt, führte bisher dazu, dass es, im Gegensatz zu Android, wenig Schadsoftware gibt und kaum erfolgreiche Attacken auf iOS-Geräte dokumentiert sind.

Während es für iOS über den Enterprise Store schon seit längerer Zeit eine recht ausgefeilte Lösung gibt, mit Hilfe einer Lösung für das Mobile Device Management (MDM) dafür zu sorgen, dass nur zulässige Apps auf iPad, iPhone & Co. gelangen, waren derlei Einschränkungsmöglichkeiten für Android-Systeme in dieser Form lange Zeit nicht umsetzbar. Ende 2013 veröffentlichten Wissenschaftler am AISEC einen App-Store-Filter für Android. Dieser filtert problematische Android-Apps automatisch aus und bietet den Mitarbeitern nur mobile Anwendungen an, die konform der unternehmenseigenen Vorgaben zur IT-Sicherheit sind.

Fazit: Keine hundertprozentige Sicherheit

Wie dieser kleine Ausflug in die Sicherheitskonzepte von iOS und Android zeigt, gibt es keine hundertprozentige Sicherheit. Handelt es sich bei dem Gerät um ein rein privates Device, so bleibt die klassische Sicherheitsempfehlung, nur so wenig Apps wie eben nötig auf dem Gerät zu installieren. Für Unternehmen ist - nicht nur aus diesem Grund - die Verwendung einer Mobile-Device-Management-Software angeraten. Entsprechende Lösungen sind in der Lage, Apps im Sinne einer Whitelist oder über einen eigenen Enterprise Store zur Verfügung zu stellen oder in extrasicheren Containern abzuschirmen. Natürlich sind auch geeignete Mitarbeiter, die sich mit den Plattformen explizit auskennen, notwendig. Am allerwichtigsten ist es jedoch, Mitarbeiter, Freunde oder Verwandte für das Thema Sicherheit zu sensibilisieren. (mb/cvi)

Links im Artikel:

- ¹ <http://www.techstage.de/news/Marktanteile-iOS-schrumpft-Windows-Phone-legt-zu-2098360.html>
- ² http://de.wikipedia.org/wiki/Palm_OS
- ³ http://de.wikipedia.org/wiki/Windows_CE
- ⁴ <http://www.aisec.fraunhofer.de/>
- ⁵ <http://www.fraunhofer.de/de/presse/presseinformationen/2013/November/sicherer-app-store-android.html>
- ⁶ http://de.wikipedia.org/wiki/Kernel_%28Betriebssystem%29
- ⁷ <http://de.wikipedia.org/wiki/Bootloader>
- ⁸ <http://theiphonewiki.com/wiki/ECID>
- ⁹ https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2013/Ueberblickspapier_Apple_iOS_30072013.html

Bildergalerien im Artikel:

gal¹ **Bildergalerie: Samsung Galaxy Tab 10.1**

Table 1

Resisting attack types

Resistance to:	Apple iOS	Google Android
Web-based attacks		
Malware attacks		
Social Engineering attacks		
Resource Abuse/Service attacks		
Data Loss (Malicious and Unintentional)		
Data Integrity attacks		

iOS und Android - Integrierte Sicherheitsfunktionen

Bereits vor drei Jahren sah Symantec eine deutliche Gefahr für Android-basierte Geräte gegenüber Datenverlust und Malware-Angriffen. Daran hat sich grundlegend nichts geändert.

Table 2

Security feature implementation

Security Pillar	Apple iOS	Google Android
Access Control		
Application Provenance		
Encryption		
Isolation		
Permission-based Access Control		

iOS und Android - Integrierte Sicherheitsfunktionen

Die Funktion der App-Isolation sieht Symantec bei Android besser als bei iOS.

Überblickspapier Apple iOS



10:26

EINSTELLUNGEN

Handyspeicher

Zeigen Sie die Speicherplatznutzung an.
Tippen Sie auf die Balken unten, um
weitere Informationen anzuzeigen.

Handy
6,07 GB genutzt 7,23 GB

SD-Karte
Nicht gefunden

Sie können den Speicherort für Musik,
Videos und Bilder ändern.

Neue Musik + Videos speichern auf

Handy

Neue Bilder speichern auf

iOS und Android - Integrierte Sicherheitsfunktionen

Trotz hoher Sicherheit erlaubt das Windows Phone von Microsoft die Verwendung von SD-Karten, kann sich am Markt jedoch immer noch nicht so recht behaupten.



Search

Kind



Alte Programme.doc

3/20/2014, 8:27 nachm. 24.00 KB



Test-Word.docx

3/24/2014, 9:18 nachm. 12.36 KB



Begrüßungsscan.jpg

12/8/2013, 4:52 nachm. 504.32 KB



ita_good_2.rtf

3/24/2014, 8:45 nachm. 36.64 KB

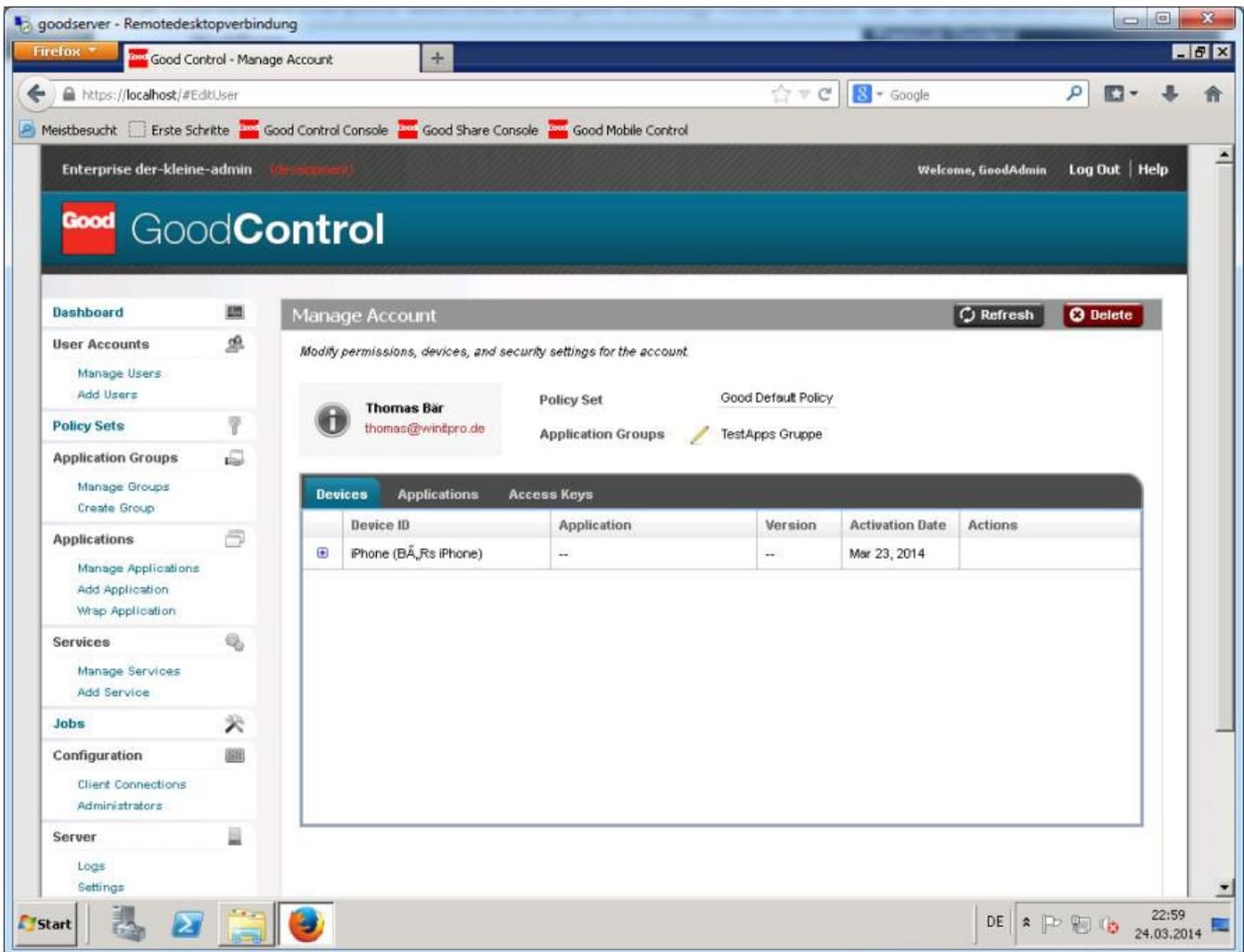


TEST-Excel.xlsx

3/24/2014, 9:17 nachm. 8.58 KB

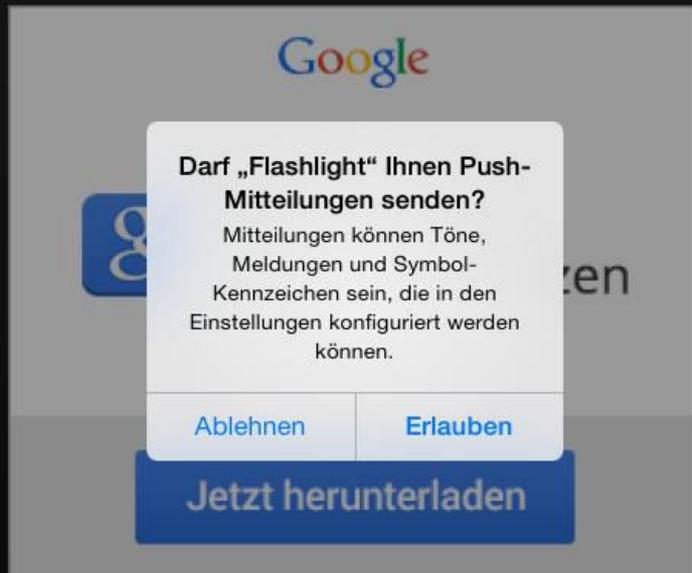


iOS und Android -
Integrierte
Sicherheitsfunktionen
Professionelle Enterprise-
Lösungen, hier von Good
Technology, sorgen dafür, dass
Unternehmensdaten in einem
strenger geschützten
Speicherbereich liegen.



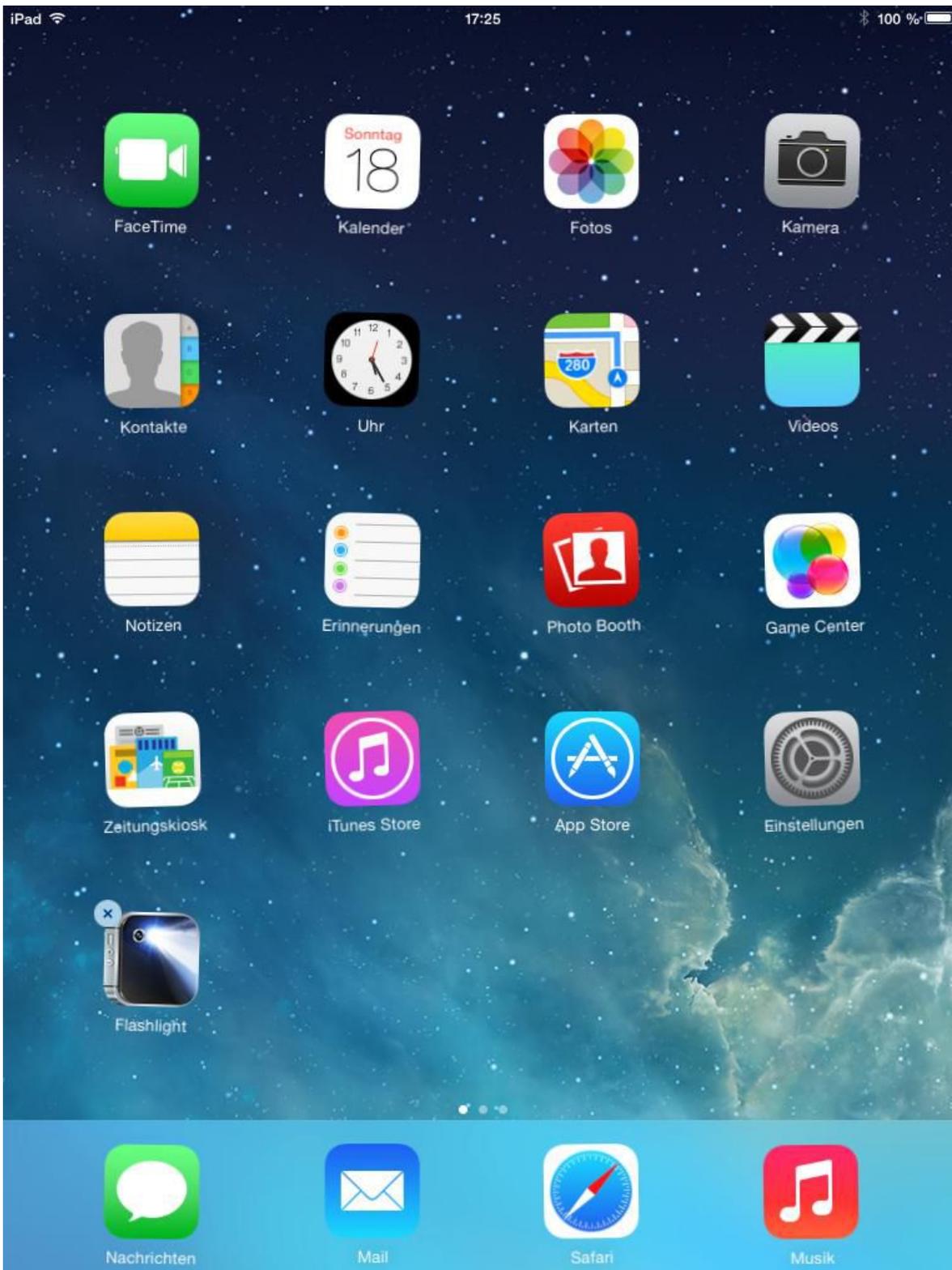
iOS und Android - Integrierte Sicherheitsfunktionen

Ohne professionelles Mobile Device Management, hier von GOOD Technology, ist ein sicherer Betrieb von mobilen Geräten im Unternehmen kaum möglich.



Sicherheitsfunktionen

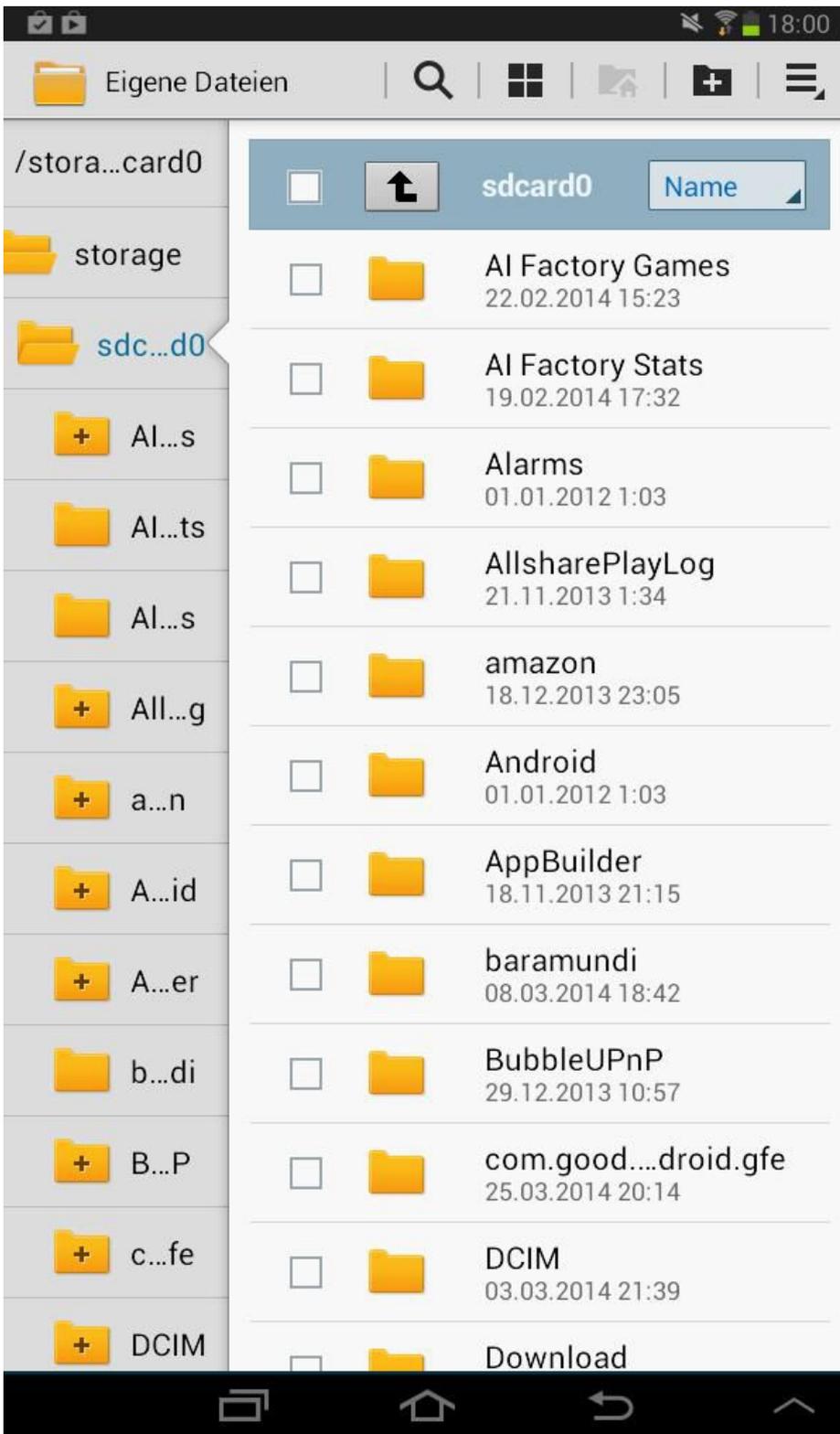
Wozu braucht eine Taschenlampen-App den Zugriff auf Push-Mitteilungen?



iOS und
Android -
Integrierte

Sicherheitsfunktionen

Im Zweifelsfall nicht mehr benötigte Apps einfach deinstallieren.



iOS und Android - Integrierte Sicherheitsfunktionen

Zugriff auf das Dateisystem gibt es nur bei Android.

IDG Tech Media GmbH

Alle Rechte vorbehalten. Jegliche Vervielfältigung oder Weiterverbreitung in jedem Medium in Teilen oder als Ganzes bedarf der schriftlichen Zustimmung der IDG Tech Media GmbH. dpa-Texte und Bilder sind urheberrechtlich geschützt und dürfen weder reproduziert noch wiederverwendet oder für gewerbliche Zwecke verwendet werden. Für den Fall, dass auf dieser Webseite unzutreffende Informationen veröffentlicht oder in Programmen oder Datenbanken Fehler enthalten sein sollten, kommt eine Haftung nur bei grober Fahrlässigkeit des Verlages oder seiner Mitarbeiter in Betracht. Die Redaktion übernimmt keine Haftung für unverlangt eingesandte Manuskripte, Fotos und Illustrationen. Für Inhalte externer Seiten, auf die von dieser Webseite aus gelinkt wird, übernimmt die IDG Tech Media GmbH keine Verantwortung.