Professional Series

Das inoffizielle Android-Handbuch

von
Andreas Itzchak Rehberg

2., überarbeitete Aufl.

Franzis-Verlag 2012

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 645 60163 4

Andreas Itzchak Rehberg

Know-how ist blau.

AndroidPIT
Fill up your mobile

2. aktualisierte und erweiterte Auflage

Das inoffizielle Android-Handbuch

> Entscheidendes Androiden-Know-how für alle Fälle

> Die wichtigsten Tipps für die besten Android-Apps

> Android-Tuning: So holen Sie das Beste aus Ihrem Smartphone heraus

In Zusammenarbeit mit AndroidPIT, dem größten deutschsprachigen Android-Forum!

FRANZIS

Andreas Itzchak Rehberg

Das inoffizielle Android-Handbuch

2. aktualisierte und erweiterte Auflage

Andreas Itzchak Rehberg

2. aktualisierte und
erweiterte Auflage

Das inoffizielle Android-Handbuch

Mit 155 Abbildungen

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte Daten sind im Internet über http://dnb.ddb.de abrufbar.

Lektorat: Anton Schmid
Satz: DTP-Satz A. Kugge, München
art & design: www.ideehoch2.de
Druck: Bercker, 47623 Kevelaer
Printed in Germany

ISBN 978-3-645-60163-4

Vorwort

Bei diesem Buch handelt es sich um eine Übersicht, die den Einstieg beim Umgang mit einem Android-Gerät erleichtern soll. Im hinteren Teil sind aber auch viele Inhalte für Fortgeschrittene enthalten ...

Entstanden ist das Ganze aus meiner Tätigkeit als AndroidPITide. Was soll das sein? Ein AndroidPITide ist ein Mitglied der Community bei *AndroidPIT (www.androidpit.de)*. Jeder ist natürlich jederzeit willkommen, auch einer zu werden (so er es nicht bereits ist).

www.androidpit.de

Als Grundlage für die Inhalte dienen meine App-Reviews nach Einsatzzweck bei AndroidPIT, die ich hier sinnvoll zusammenzufassen versucht habe. Viele der Links in diesem Buch, die über QR-Codes eingebunden sind (siehe nächste Seite), führen daher auch dorthin – zur Vertiefung eines Themas etwa, oder für weitere Details. Und nicht zuletzt für aktualisierte Informationen: Es kommen ja ständig neue Apps dazu, und natürlich ebenso wertvolle Benutzer-Erfahrungen. Darüber hinaus lassen sich im Forum auch *Fragen zum Buch stellen* (und Antworten erwarten), ebenso wie zu hier nicht behandelten Themen.

http://www.androidpit.de/de/android/forum/thread/409715/

Gedacht ist das Ganze so, dass dieses Buch einen Überblick verschafft. Für die tiefer schürfenden Dinge kann man auf das Forum zurückgreifen. Dort ist man nicht nur in Bezug auf Android-Fragen in guten Händen!

Und noch eins muss ich loswerden: Viele der hier kurz vorgestellten (oder auch nur genannten) Apps habe ich nicht selbst getestet – etwa, weil ich nicht die Voraussetzungen dazu habe (ich nutze kein Facebook, und meinen Androiden auch nicht zum Spielen, um nur zwei Dinge zu nennen). Trotzdem habe ich sie – der Vollständigkeit halber – beschrieben und greife dabei auch auf Erfahrungen der Nutzer in der Community zurück, die diese Apps benutzen.

Hinweise zur Benutzung des Buches

Am Seitenrand finden sich hin und wieder so seltsame Quadrate mit eckigen Mustern drin: die schon erwähnten QR-Codes. Sie sollen helfen, den Anschluss ins Internet zu finden: Sind sie schwarz, führen sie zu weiteren Informationen. In Grau führen sie direkt zur besprochenen App.

Um die QR-Codes nutzen zu können, brauchen Sie zwei Zutaten: Ein Android-Gerät mit integrierter Kamera und eine App, die sich auf QR-Codes versteht. Für Letztere gibt es weiter hinten im Buch einige Hinweise (im Kapitel 4.9 *Büro, Office und Verwaltung*). Ersteres hat der Leser dieses Buches in der Regel bereits (falls nicht, stehen die zugehörigen Adressen zusätzlich unter den Codes, damit Sie auch mit anderen Geräten an die Infos rankommen).

Wie werden diese Codes also nun genutzt? Ganz einfach: Androiden zücken, den QR-Code-Reader starten und die Kamera auf den QR-Code richten. Um alles weitere kümmert sich die entsprechende App dann selbständig: Sie öffnet in der Regel den Web-Browser und ruft die durch den Code festgelegte Webseite auf. Ganz bequem also.

Dass sich mit diesen Codes noch weiteres anstellen ließe, und was alles – diese Informationen befinden sich in Kapitel 4.9.1 *Barcodes*.

Danksagung

Ja, hört der denn mit der Vorrede gar nicht mehr auf? Gleich, gleich. Aber dieser Abschnitt muss noch sein:

Denn bedanken muss ich mich auf jeden Fall. Nicht nur, weil sich das halt so gehört – sondern weil ich dazu viele gute Gründe habe. Ohne den Rückhalt der Community bei AndroidPIT wäre es nie zu diesem Buch gekommen! Und so bedanke ich mich besonders herzlich bei Evelyn für ihre tatkräftige Unterstützung und Hilfe (was hätte ich nur ohne dich gemacht?) und Sabine für ihr fleißiges Gegenlesen und Aufspüren von »Leichen« (leider verschwand doch so die eine oder andere App wieder aus dem Market, bevor ich das Buch fertig hatte. Zum Glück ist so etwas nicht die Regel!). Auch Alexander möchte ich für seine zahlreichen Hinweise danken. Und all den anderen, die ich hier jetzt nicht alle namentlich aufführen kann: Leute, ihr seid Klasse!

Und von der Community gesprochen: Auch die M&Ms waren mehr als nur hilfreich. M&Ms? Nun ja, die Moderatoren und die »Macher«. Mein besonderer Dank geht hier an Mario, Michael, Fabien und Philipp.

Und ein ganz besonderer Dank geht an meine Frau, die schon glaubt, ich wäre mit dem Computer zusammengewachsen. Zum Glück brachte sie statt einer Säge oder eines Tranchiermessers Nervennahrung an meinen Schreibtisch. Danke für Deine Geduld mit mir!

Abschließend noch meinen Dank an die Leser dieses Buches, die es bis hierhin durchgehalten haben. Und die hoffentlich auch noch ein wenig weiter lesen: Viel Spaß bei der Lektüre!

Inhaltsverzeichnis

3 Sicherheit

3.1 Was brauche ich wirklich?

http://www.androidpit.de/de/android/forum/thread/425367/

[Übersicht: Verhüterlis, Anti-Malware, Virus-Wechisses]

Anti-Virus, Anti-Malware, Diebstahlschutz ... Was braucht es eigentlich wirklich auf dem Androiden? Klar gibt es auch hier wieder für alles eine App – und natürlich auch eine passende Übersicht im AndroidPIT-Forum. Das Wichtigste sollte man jedoch (hoffentlich) nicht allzu lange suchen müssen:

3.2 GMV

GMV

GMV sollte bereits im biologischen Speicher vorinstalliert sein. Leider wird es oft mit Worten wie »No risk, no fun!« deaktiviert – was dann meist unschöne Folgen hat. In der Regel taucht der/die Betroffene kurz darauf im Forum auf und öffnet einen Thread mit dem aussagekräftigen Titel »HILFEEEE!« (aha, GMV noch immer deaktiviert).

GMV? Was ist das denn nun wieder? Oh-oh ... Das sollte eigentlich jeder haben, zumindest ein wenig davon: **G**esunder **M**enschenverstand. Hilft enorm. Auch gegen »Viren« und »Malware«.

Seien wir doch mal ehrlich: Wie viele Viren gibt es wirklich für Android? Und wie kommen die aufs Gerät? Wie kommt Malware aufs Gerät? Indem man ohne nachzudenken auf alles klickt, was sich bewegt? Indem man eine »böse App« installiert? Die wichtigsten Regeln beachtend, kann so etwas eigentlich kaum passieren. Vor der Installation einer App sollte man sich z. B. folgende Fragen stellen:

- Ist die Quelle vertrauenswürdig?

  Positiv-Beispiele: AndroidPIT-Market, AppCenter, Android Market, Website des bekannten (!) Entwicklers

  Negativ-Beispiele: Bei Rapidshare »gefunden«, in einer Tauschbörse aufgetrieben, per eDonkey aus unbekannter Quelle gezogen ...

- Sehen die Permissions vernünftig aus?

Positiv-Beispiele: Ein Webbrowser muss ins Web, eine SMS-App kann natürlich SMS lesen/schreiben/schicken und braucht ggf. auch (lesend) Zugriff aufs Adressbuch

Negativ-Beispiele: Eine Wallpaper-App braucht in der Regel keine Telefonnummern, ein Ballerspiel muss keine SMS senden.

Besondere Vorsicht: Apps, die auf persönliche Daten (Kontakte, Kalender, Nachrichten) zugreifen und gleichzeitig ins Internet wollen. Leider lässt sich bei Letzterem (Internet) die Frage der Notwendigkeit nicht so einfach beantworten – es könnte auch einfach nur für Werbung-Laden gebraucht werden ...

- Was sagen andere Nutzer zur App/zum Entwickler (Bewertungen, Forum)?

  Auch hier wieder GMV aktivieren. Kommentare wie »Geil!«, »Super«, etc. sagen nicht wirklich etwas aus (da hat eher jemand bei deaktiviertem GMV einen Kommentar hinterlassen).

  Gleiches gilt für manchen negativen Kommentar: Nicht gerade selten passiert es, dass jemand einfach zu blöd war. Oder die Anforderungen der App gar nicht verstanden hat.

  Nicht alle Bewertungen beziehen sich wirklich auf die App. Die kann schließlich nix dafür, wenn der Market mal wieder klemmt, und daher der Download nicht funktioniert. Oder die HD-Video-App, die mindestens WVGA benötigt, mit dem Motorola Flipout (mini-Display) im Market nicht gefunden wird ...

  Ganz neue App? Noch keine Bewertungen? Im Zweifelsfall im Forum nachfragen, ob schon jemand die App kennt und etwas dazu sagen kann.

Natürlich können andere Apps aus der »Sicherheits-Abteilung« eine gute Ergänzung zu GMV sein. Insbesondere bei *Verlust des Gerätes* – denn dagegen macht auch GMV nicht immun ...

3.3 Rundum-Sorglos-Pakete

Bild 3.1: *NetQin Antivirus* bietet Schutz gegen Viren, Malware und Diebstahl.

NetQin Antivirus

Das sind die Apps, die gleich alle Bereiche abdecken. Also *Anti-Virus*, *Anti-Malware* und »*Diebstahlschutz*« in einem. Ein Beispiel dafür ist **NetQin Antivirus** (in verschiedenen Varianten, u. a. für verschiedene Android-Versionen bzw. mit unterschiedlichem Funktionsumfang und »Pricing«, verfügbar; siehe Screenshot). Der Name lässt bereits auf die Haupttätigkeit schließen: Das Vorgehen gegen Viren und Malware. Und zwar sowohl in »Echtzeit« (App läuft im Hintergrund), als auch »On Demand« (»auf Verlangen«: Sie lässt sich also bei Bedarf veranlassen, das gesamte Gerät zu prüfen).

Geht das Gerät einmal verloren (d. h. es wurde entweder verlegt, oder ein Langfinger hat es »abgegriffen«), kann man z. B. einen lauten Alarm auslösen. Oder aber in wilder Panik gleich alle Daten löschen und das Gerät sperren lassen. Sowas geht einfach per SMS mit dem entsprechenden »Codewort«. Natürlich kann man auch erstmal seinen GMV aktivieren und sich auf der Karte (Google Maps) zeigen lassen, wo sich der Androide gerade herumtreibt. Ob dafür allerdings ein Account benötigt wird, und wie das genau funktioniert, fand ich leider nirgendwo beschrieben ...

Hinzu kommen noch Tools zum Sichern persönlicher Daten, Memory-Booster, Task-Killer, Traffic-Monitor, File-Manager ... (was soll das Ding eigentlich nicht machen?!?). Bei so vielen Features ist auch die Anzahl der geforderten Permissions entsprechend umfangreich.

3.4 Anti-Virus und Anti-Malware

Bild 3.2: *Dr. Web Anti-virus Light* ist kostenlos verfügbar.

Viren und Malware (nein, hier sind jetzt keine Apps zum Malen gemeint – sondern bösartige, hinterhältige Apps wie Trojaner) lassen sich schwer trennen. Und da es von Ersteren für Android nicht viele gibt, kümmert sich auch eine »reine Antivirus-App« wie selbstverständlich gleich mit um Letztere.

Dr. Web

Als reine Anti-Virus-App wäre hier sicher **Dr. Web Anti-virus Light** (siehe Screenshot) eine gute Empfehlung: Sparsam in Sachen Permissions, gratis im Markt verfügbar, beste Bewertungen.

Die Gratisversion scannt einfach auf »böse Dateien« und sperrt diese in die »Quarantäne«. Hierbei scheint sowohl ein Echtzeit-Scan zu erfolgen als auch die Möglichkeit zu einem »On-Demand-Scan« zu bestehen. Außerdem lässt sich noch einstellen, dass auch die SD-Karte bei jedem Einbinden geprüft werden soll. Die Vollversion bietet dazu auch eine Filterung eingehender Anrufe und SMS, inklusive Blacklist (z. B. für nervige Werbe-Anrufer und Spam-SMS).

Bild 3.3: Benachrichtigungen von *Antivirus-Free*.

Antivirus-Free

Auch **Antivirus-Free** ist durchaus eine gute Alternative: Fast genau so gut bewertet, und absolut sauber, was die Permissions angeht, klinkt sich diese App offensichtlich in den System-Event für »App installiert« ein – und prüft sodann die neu installierte App auf »Schädlingsbefall«. Eine entsprechende Notiz findet sich dann in der »Notification Area« (siehe Screenshot): »Application install detected: package com.entwickler.appname is xxx«. Wobei »xxx« dann entweder »clean« (sauber) oder »malicious« (schädlich) heißt.

3.5 Bei Diebstahl und Verlust

Bild 3.4: *WatchDroid Pro* als Diebstahlschutz.

Eine App, die wirklich gegen Diebstahl und Verlust schützt, muss sicher erst noch erfunden werden. Apps in dieser Kategorie werden also i. d. R. erst dann aktiv, wenn das Kind bereits in den Brunnen gefallen ist. Nur ist es dann natürlich für eine Installation meist zu spät – darum sollte man sich also bereits im Vorfeld kümmern!

Zu empfehlen wäre hier u. a. **WatchDroid Pro** (siehe Screenshot), sofern eine »Stand-Alone-Lösung« gewünscht ist.

WatchDroid Pro

Krach schlagen und SMS mit GPS-Daten verschicken geht sogar schon mit der Gratisversion, sodass man erst einmal in Ruhe testen kann. Auch diese begibt sich bereits in eine Art »Stealth Modus«, sodass sie für einen »unberechtigten Abgreifer« (sprich: Dieb) nicht sofort offensichtlich erkennbar (und damit Ziel einer Löschung) ist. So richtig interessant wird es aber erst mit der Pro-Version: Lock und Wipe stehen dann mit auf der Feature-Liste, und die App erkennt auch einen eventuellen SIM-Karten-Wechsel – und verschickt in einem solchen Fall automatisch eine SMS an den hinterlegten Empfänger. Jaja, der Trend geht zum Zweit-Handy ...

3.6 Worauf Apps Zugriff haben

Bild 3.5: *RL Permissions* informiert darüber, welche Permissions an welche Apps vergeben wurden.

Wer hat sich nicht schon mal gefragt, was eigentlich bei der Installation einer neuen App aus dem Market der seltsame Hinweis sagen möchte: »Diese App darf auf folgendes zugreifen:« – gefolgt von einer teilweise recht langen Liste komischer Dinge? Nun: Der so Fragende ist hier genau richtig. Zu viele Benutzer ignorieren das nämlich einfach, ohne darüber nachzudenken. Und am Monatsende ist die Überraschung dann gelungen, wenn beim Blick auf die Mobilfunkrechnung die Frage aufkommt: »Moment – ist das jetzt der Betrag oder die Kontonummer für die Überweisung? Wer hat denn da so viele Premium-SMS ... und all die Anrufe bei 0900-*???«


RL Permissions

Was also darf eine App? Oder, anders herum gefragt: Welche App darf denn ...? Auf beide Fragen gibt z. B. **RL Permissions** (siehe Screenshot) gute und aussagekräftige Antworten. Eine Ampel zeigt nämlich jeweils an, wie schwerwiegend der *potenzielle* Schaden ist, der mit der jeweiligen Berechtigung angerichtet werden *könnte*. Was natürlich nicht heißt, dass die jeweilige App das auch tut – denn natürlich muss eine SMS-App SMS verschicken können, sonst macht sie ja nun wirklich wenig Sinn. Eine Wallpaper-App hingegen muss das nicht unbedingt.

Außerdem erklärt die App auch immer gleich, wofür die entsprechende Permission eigentlich gedacht ist. So hat man diese Information gleich im passenden Kontext. Eine kurze Übersicht mit ausgewählten Permissions sowie einer kurzen Beschreibung derselbigen findet sich übrigens auch im Anhang A.3. Und eine Liste alternativer Apps zum Thema, wie gewohnt, bei AndroidPIT.

5 Tiefergehendes für Fortgeschrittene

Nachdem sich die ersten Kapitel dieses Buches hauptsächlich an Einsteiger gerichtet haben, sollen auch die Fortgeschrittenen unter den Lesern nicht zu kurz kommen. Die hier behandelten Themen sind mit Sicherheit nichts für Neueinsteiger: Bevor ihr euch an die Umsetzung der »schweren Kost« macht, solltet ihr mit eurem Android-Gerät schon recht gut vertraut sein.

Dennoch heißt das nicht, dass Einsteiger jetzt das Buch aus der Hand legen müssen. Ich werde versuchen, möglichst allgemeinverständlich zu schreiben (auch auf die Gefahr hin, dass sich der eine oder andere mitlesende Profi ein wenig langweilen könnte). Dies verschafft zumindest einen Überblick über sich bietende Möglichkeiten. Und als Nebeneffekt findet sich (insbesondere im Tuning-Bereich) sicher auch der eine oder andere hilfreiche Tipp für Neulinge.

Aber genug der Vorrede – kommen wir zum Thema. Oder besser zu den Themen:

5.1 Der Super-User »root«

Kauft man einen Windows-PC, gibt es auf diesem einen Account für den Benutzer »Administrator« – dem man bei der Ersteinrichtung ein Passwort verpasst. Installiert man Linux, heißt das Pendant »root«. Android basiert auf Linux – aber trotzdem gönnen uns die Hersteller den root-Zugang in der Regel nicht, sondern drohen: »Wer sich root-Zugang zu seinem Gerät verschafft, verwirkt damit den Garantieanspruch.«

So, damit ist nun klar, um was es bei dem Wort »root« geht: Um den administrativen Zugang zum System, mit dem man alles (kaputt) machen kann. Naja, fast alles – die Hardware wohl eher nicht. Weshalb die Warnung mit der Garantie wohl letztendlich vor Gericht kaum haltbar sein dürfte, wenn man z. B. das Display wechseln lassen muss oder der interne Speicher den Geist aufgibt (anders sieht es aus, wenn die CPU verglüht, weil man sie hoffnungslos übertaktet hat).

Also was nun: Braucht man den root-Zugang wirklich? Ja und nein. Wer mit seinem Gerät, dessen Funktionen sowie der verwendeten Software bereits rundum zufrieden ist, bei wem alles so läuft wie gewünscht und wer »eigentlich« nichts vermisst – der braucht auch keinen root-Zugang. Er hat ja bereits alles, was er braucht. Hat man hingegen ein Problem, das sich ohne den root-Zugang nicht lösen lässt, sieht das schon anders aus: Je

nachdem, wie schwer es einen trifft, neigt sich das Zünglein an der Waage immer mehr der Anzeige zu, die mit »mach mich root!« beschriftet ist.

Welche Vorteile sind es denn nun, die man mit einem root-Zugang erlangt – und welche Risiken sind damit verbunden?

5.1.1 Vorteile des root-Zugangs

Verschiedenste Einstellungen und Änderungen lassen sich ohne root-Zugang gar nicht vornehmen:

- Anpassen der CPU-Taktfrequenz (siehe auch *Akkuleistung*)
- Entfernen/Deaktivieren vorinstallierter Apps (Deaktivieren geht ab Android 4.0 auch ohne root)
- Bearbeiten der Start-Events (siehe *Apps am automatischen Starten hindern*)
- Optimierung der Speicherverwaltung (siehe *Tuning*)
- Swap-Datei anlegen
- Automatische Datenbereinigung (Reste deinstallierter Apps; siehe *Unnütze Apps raus!*)
- App2SD bei Android < 2.2 (siehe *Tuning*)
- Aufspielen alternativer Firmware (»Custom ROM«)
- Ändern der Systemschriftart(en)
- Erstellen eines wirklich vollständigen Backups des Android-Systems
- Einrichten einer Firewall (*DroidWall*)


DroidWall

Diese Liste ist keinesfalls vollständig (natürlich auch nicht nach Relevanz sortiert – die wäre ohnehin wieder sehr subjektiv). Mit root hat man quasi überall Zugang – keine Ecke des Android-Systems bleibt verschlossen. Genau da liegt auch das Risiko – aber da liegt es auch beim root-Zugang auf dem Linux-PC, oder dem Administrator-Zugang beim Windows-PC.

5.1.2 Risiken des root-Zugangs

Die Risiken sind schnell mit einem Satz beschrieben: Setzt man seinen root-Zugang falsch ein, kann man damit das System unbrauchbar machen. Im schlimmsten Fall

verwandelt man gar seinen Androiden in einen Ziegelstein – wenn man z. B. ohne Sinn und Verstand die CPU hoffnungslos übertaktet und diese schließlich den Hitzetod stirbt. Mit Wissen und Verstand genutzt, ist der root-Zugang ein mächtiges und nützliches Werkzeug. Quasi wie ein Autoschlüssel: Setzt sich der 8-jährige Steppke damit hinters Steuer ... Womit wieder bewiesen ist, dass man uns für absolut unmündig hält ...

Noch ein Wort zu vermeintlichen Risiken: »Wenn ich mein Phone gerootet habe, können dann alle Apps mit Super-User-Rechten jeden Mist machen?« Im Prinzip ja, aber ... Da gibt es eine App, die nennt sich **SuperUser**. Die kommt mit jedem root-Zugang mit. Und an der müssen die Apps vorbei, die System-Rechte haben wollen. Die App lässt sie aber nicht so einfach durch: Es erscheint ein Pop-Up, welches man bestätigen muss: Darf/darf nicht, nur diesmal/immer. Also z. B. »Darf« »nur diesmal«, »Darf nicht« »immer«. Oder umgekehrt. Fazit: Im Prinzip kann jetzt jede App Mist bauen – aber nur, wenn der Anwender es ihr explizit erlaubt.

5.1.3 Wie bekomme ich root-Zugang?

Das jetzt so zu erklären, dass es für jeden gilt, führt ein wenig zu weit. Für diese Übersicht kurz zusammengefasst, gibt es da mehrere Möglichkeiten – und je nachdem, um welches Gerät es geht, greift davon eine, keine oder mehrere.

Da ist zum einen »Software-root«: Man lädt sich die passende App auf den Androiden, startet sie und bestätigt: »Ja, ich will root!«. Fertig. Toll: Mit so einem Gerät fühle ich mich absolut sicher. Wer sagt mir, dass eine andere App das nicht im Hintergrund tut, ohne mich zu fragen?

OK, auch die zweite Variante ist im Prinzip eine Art »Software-root« (schließlich geht es ja um Software-seitigen Zugang). Nur geht es hier nicht um eine »einfache App«, sondern es ist schwieriger: Zunächst muss das USB-Debugging im Gerät aktiviert werden (explizierter Schritt, schwer von einer App auszuführen). Dann ist der Androide per USB-Kabel mit dem PC zu verbinden (unmöglich, dass das eine App im Hintergrund macht). Und schließlich muss man auf dem PC die »root-Software« starten, die über das Kabel auf das Android-Gerät zugreift. Die Schritte sind noch immer einfach und nachvollziehbar – aber hier habe ich keine Bedenken, dass das ohne mein Zutun passieren könnte.

Welche Variante jetzt für ein bestimmtes Gerät verfügbar ist und welche Software dafür benötigt wird, recherchiert man am besten im Forum. Bei AndroidPIT gibt es gerätespezifische Foren (z. B. eines für das *Wildfire*, eines für das *Desire*, für das *Motorola Milestone*, und so weiter). Jedes dieser Foren hat ein Unter-Forum für root-Fragen – dort finden sich die Informationen, die für das jeweilige Gerät zutreffend sind. Auch ein Blick in den root-Artikel des AndroidPIT-Wikis kann sich für weitere Informationen als nützlich erweisen.

5.1.4 Laufen dann alle Apps mit root-Rechten?

Eine oft aufkommende Befürchtung – zum Glück unbegründet. Also die kurze Antwort: Nein, nicht ohne ausdrücklichen Wunsch des Anwenders.

Für eine detaillierte Antwort muss ich etwas tiefer greifen. Und wir müssen uns in Erinnerung rufen: Ein Android-System läuft ja mit Linux, also gelten hier auch entsprechende Richtlinien. Und jede App läuft darüber hinaus unter einem eigenen Benutzer. Auch *root* ist ein Benutzer, wenn auch ein ganz spezieller. Und wenn eine »normale App« etwas mit root-Rechten ausführen möchte, muss sie »root« dazu auffordern. Der Befehl dazu heißt *sudo*, was wir in unserem speziellen Kontext mit »Super-User, do ...« wiedergeben können.

Wenn eine App selbst unter »root« läuft, braucht sie auch kein »sudo«. Das betrifft aber unter Android nur System-Apps, auf die der Anwender in der Regel keinen (direkten) Zugriff hat.

Läuft sie jedoch nicht unter »root« (und das ist bei Android die Regel: Jede App läuft, wie bereits gesagt, unter einem eigenen User), dann muss sie für Aktionen, die root-Rechte benötigen, root halt höflich bitten – und das tut sie, indem sie dem auszuführenden Befehl ein »sudo« voranstellt. Also »sudo <Befehl>«. Derart geweckt, schaut der *SuperUser* in seiner »Datenbank« nach, ob die App denn sowas darf. Beim ersten Aufruf steht sie da noch nicht drin: Die Folge ist ein Popup der *SuperUser*-App »App xyz möchte etwas mit Super-User-Rechten machen. Darf sie das?«. Dazu zwei Buttons für »Ja« und »Nein«, sowie eine »Checkbox«, ob sich *SuperUser* diese Entscheidung für die Zukunft merken soll.

Bild 5.1: Eine Meldung, die anzeigt, dass einer App Super-User-Rechte eingeräumt wurden.

Bei jedem weiteren Aufruf findet der *SuperUser* die App in seiner Datenbank mit dem Vermerk »die darf das immer«, und führt den Befehl direkt aus. Zur Sicherheit wird dieser Fakt jetzt nochmals als Hinweis eingeblendet (siehe Screenshot). Die App wird dabei nicht gebremst, es ist auch keine Interaktion nötig. Daher sollte das in diesem Falle

dann sogar vom Lockscreen aus funktionieren. Etwas störend ist das natürlich im Falle einer Screenshot-App, wie das Bild zeigt – da dieser Hinweis dann auf jedem Bild verewigt ist. Deshalb lässt er sich auch in den Einstellungen der *SuperUser*-App abschalten.

5.2 Apps am automatischen Starten hindern

Wer kennt das nicht: Man schaltet sein Handy ein, es fährt hoch, und ist eine gefühlte Ewigkeit später auch »betriebsbereit«. Besonders üppig mit RAM ausgestattet sind unsere Androiden ja eher selten – und trotzdem tummeln sich schon zu diesem Zeitpunkt sackweise Apps in selbigem, die ich selten oder gar nie benötige: Flickr, FM-Radio, Google Maps, Peep ... Wozu? Und wie kann ich das verhindern?

Hier soll es nun nicht um »aggressive Task-Killer« gehen, die (ausgenommen vielleicht einer Exclude-List) wild alles abschießen, was »peep« sagt (und nein, auch das Für und Wider derselben steht hier nicht zur Debatte). Stattdessen möchte ich Möglichkeiten nennen, gezielt die nicht (ständig) benötigten Apps an einem automatischen Start zu hindern (manchmal auch nachträglich, ooops).

Für Details gleich an dieser Stelle der Verweis zum zugehörigen Foren-Thread.

http://www.androidpit.de/de/android/forum/thread/408715/

[Apps am automatischen Starten hindern]

Startup Auditor

Bild 5.2: *Startup Auditor*

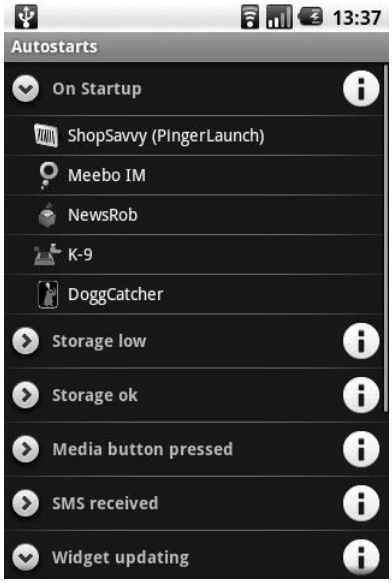

Bild 5.3: *AutoStarts* legt fest, welche App bei einem bestimmten Ereignis automatisch gestartet werden soll.

AutoStarts

Ja, es gibt sie: Apps wie **Startup Auditor** und **AutoStarts** (siehe Screenshots). Sie brauchen in der Regel Root-Rechte, um ihre Tätigkeiten auszuführen. Und sie unterscheiden sich zum Teil stark – sowohl in ihrer Bedienbarkeit, Übersichtlichkeit, Wirksamkeit, als auch in der Art ihrer Vorgehensweise.

Dazu ein wenig Hintergrund-Information: Es ist nicht so, dass es da einen »Startup-Folder« gäbe. Vielmehr können sich Apps für »Events« registrieren, bei denen sie gern gestartet werden möchten. Der gewöhnlichste, der jedem sofort einfällt, nennt sich »boot completed« – unmittelbar, nachdem das System komplett hochgefahren ist. Aber das ist bei weitem nicht alles! Wer einmal mit o. g. *AutoStarts* sein System durchforstet, bekommt beim ersten Mal sicher Kulleraugen, wie viele solcher »Start-Rampen« es gibt. »USB-Kabel angesteckt« fällt einem vielleicht noch ein. Aber wer denkt sogleich an Dinge wie »eingehende SMS«, »abgehender Anruf«, »Speicher knapp«? Klar, jetzt fällt einem sicher auch »battery low« ein ...

Je nachdem, welche dieser »Start-Rampen« unsere App nun also kennt, findet sie mehr oder weniger Kandidaten, die vom automatischen Starten abgehalten werden sollen. AutoStarts findet zum Beispiel sehr viele – Startup Auditor etwas weniger.

Und wie werden die Apps am Starten gehindert? Die meisten unserer »Verhinderer« warten einfach auf deren Auto-Start und schießen die App dann über den Haufen. Anders *AutoStarts*: Hier wird die App quasi gleich von der Rampe genommen – und *AutoStarts* merkt sich App und zugehörige Rampe, um die Aktion ggf. später wieder rückgängig machen zu können. Das ist natürlich weit effektiver (und auch Ressourcen-schonender), birgt aber eine Gefahr: Sollte man *AutoStarts* einmal deinstallieren, ohne

zuvor die Änderungen rückgängig gemacht zu haben – dann kann man sie gar nicht mehr rückgängig machen (es sei denn, man hat ein gutes Backup der App-Daten von *AutoStarts* – oder installiert die betroffene App einfach neu). Hat also alles seine Vor- und Nachteile.

Bild 5.4: *Autorun Manager* wird verwendet, um das Autostart-Verhalten von Apps zu erkennen und ggf. zu verändern.

Autorun Manager

Achtung: Wer die Apps nicht direkt »von der Rampe nimmt«, sondern jeweils »nach dem Start abschießen lässt« (im Falle von Unsicherheit gilt Letzteres), sollte anschließend prüfen, was dabei passiert. Bei einigen Apps (z. B. *Peep* oder *Aktien*) passiert es gern, dass sie nach dem »Abschuss« einfach wieder starten. Das artet dann in einen Kreislauf aus, der alles andere als Ressourcen-schonend ist! Es gibt allerdings eine App, die so etwas selbst erkennt: **Autorun Manager** (siehe Screenshot) markiert eine sich so verhaltene App als »Selbst-Restarter«, sobald dieser Fall aufgetreten ist. Damit ist dann klar, dass sich diese nicht auf diese Weise am Starten hindern lässt ...

Autorun Manager unterstützt übrigens beide Modi: Im »einfachen Modus« (kein root erforderlich) verhält sie sich wie *Startup Auditor*, und schießt die Apps nach dem Auto-Start einfach über den Haufen. Hier werden auch nur wenige Events berücksichtigt – also wahrscheinlich nicht alle Elemente erwischt. Im »Erweiterten Modus« (erfordert root) hingegen verhält sie sich wie *AutoStarts*, und »deregistriert« die jeweilige App vom jeweiligen Event. Hier muss man dann vor einer eventuellen Deinstallation daran

denken, *vorher* die ursprünglichen »Defaults« wieder herzustellen (geht allerdings einfach: »Rescue-Mode«, und fertig).

5.3 Vorinstallierte Apps entfernen

Das kann echt nervig sein: Was hat mein Provider (bzw. der Telefon-Hersteller) da alles an Apps vorinstalliert, die »kein Mensch« braucht? Und wie werde ich »den Schrott« los? Jetzt kommt das böse Wort: »Ohne *root*? Gar nicht.« Da wären wir also wieder ...

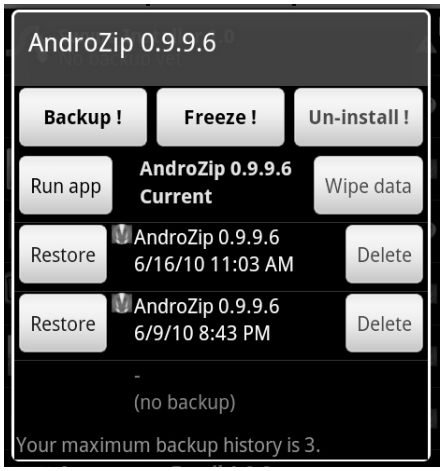

Bild 5.5: *Titanium Backup* kann Apps nicht nur entfernen, sondern auch »einfrieren«.

Titanium Backup

Und mit root? Ja, da gibt es Möglichkeiten. Die bekannteste dürfte wohl **Titanium Backup** sein: Mit dieser App lässt sich jede ungewünschte App komplett vom System entfernen, wenn es denn sein soll. Wem das zu heikel ist, der hat auch eine Alternative: Einfrieren (was Android ab Version 4.0 auch von Haus aus ermöglicht). Damit taucht die App in keiner Liste (außer bei *Titanium Backup*) mehr auf, wird nicht mehr (automatisch) gestartet – und kann dennoch jederzeit wieder »aufgetaut« werden.

Nebeneffekt der App – der Name lässt es erahnen: Man kann damit vollständige Backups machen. Von einzelnen Apps. Von deren Daten. Vom ganzen System. Und natürlich bei Bedarf Daten, Apps und System aus einem Backup zurückholen. Klasse Sache bei einem Geräte- oder ROM-Wechsel (aufpassen: Unterschiedliche Geräte/ROMs = unterschiedliche Systemdateien; hier nur die Apps und ggf. deren Daten wiederherstellen, die System-Dinge nicht anfassen).

Stichwortverzeichnis

Andreas Itzchak Rehberg

2. aktualisierte und erweiterte Auflage

Das inoffizielle Android-Handbuch

Flexibel, offen und Apps ohne Ende: Android-Smartphones stehen dem iPhone in nichts nach, und das Systemtuning ist auch noch legal! Dieses Buch macht Ihr Android-Gerät sicherer, schneller und hilft bei der Jagd nach den besten Apps. Denn hier finden Sie das geballte Android-Know-how von AndroidPIT, dem größten deutschen Android-Forum. Schließlich kennt niemand bessere App-Empfehlungen, Tuning- und Sicherheitstipps als die Android-Community selbst! Dieses Buch ist die beste App für Ihr Android-Smartphone!

Android-Apps: Unendliche Weiten?

Täglich erscheinen jede Menge neue Apps im Android Market von Google und auf anderen Websites. Aber welche Apps sind die besten und was bringen sie? Wie installiere und verwalte ich meine Apps und wie werde ich sie später wieder los, damit sie nicht unnötig Speicherplatz und Rechenpower verbrauchen? Hier finden Sie die entscheidenden Antworten.

Mit Android auf Reisen

Von der Routenplanung bis zum Reisetagebuch – und sogar für die Versendung der ganz persönlichen Urlaubspost gibt es Android-Apps. Lesen Sie hier die besten Empfehlungen für Sprachführer, Übersetzer, Wörterbücher, Navigations-Apps, Staumelder, Pannenhilfen, Reiseführer, Virtual Sightseeing und vieles mehr. Und installieren Sie die gewünschten Apps schnell und einfach mit Hilfe der abgedruckten QR-Codes.

Tuning: Mehr Power fürs Smartphone!

Passen Sie Ihr Smartphone Ihren Bedürfnissen an und machen Sie es schneller. Schaffen Sie mehr Platz im internen Speicher und verlängern Sie die Laufzeit Ihres Akkus durch konsequentes Umsetzen der Tipps und Empfehlungen, die Sie hier finden.

Aus dem Inhalt:

Über den Autor

Andreas Itzchak Rehberg ist Informatiker und freiberuflicher Oracle-Datenbank-Administrator. Als begeisterter Android-User ist er seit 2010 Mitglied bei AndroidPIT, der größten Android-Community in Deutschland, und zählt dort zu den Top Ten der Aktiven.

9 783645 601634

25,– EUR [D]
ISBN 978-3-645-60163-4