Das AndroidPITiden-Buch

Kleiner Androiden-Führer
für
Einsteiger und Fortgeschrittene
von
Andreas Itzchak Rehberg

Version 42

Die jeweils aktuellste Version dieses eBooks findet sich hier.

Cover-Design: AndroidPIT

Unter dem Namen **Das inoffizielle Android-Handbuch** (ISBN: 978-3-645-60163-4) gibt es eine Print-Ausgabe dieses Buches vom Franzis-Verlag.

ANDREAS ITZCHAK REHBERG

Das AndroidPITiden-Buch

AndroidPIT
Fill up your mobile

creative commons

Inhalt

Vorwort

AndroidPITiden? Was ist das denn? Wer hinter diesem Begriff die Community bei AndroidPIT vermutet, liegt goldrichtig. Meine App Reviews nach Einsatzzweck im dortigen Forum bildeten nämlich die Grundlage für die ersten Ausgaben dieses Buches – bei denen es sich, mehr oder weniger, noch um reine App-Übersichten handelte. Mit der Zeit hat sich dieser Charakter ein wenig gewandelt, und es ist ein ausgewachsenes Android-Handbuch daraus geworden.

Ein AndroidPITide ist also ein Mitglied der Community bei AndroidPIT. Jeder ist herzlich willkommen, ein solcher zu werden (so er/sie dies nicht bereits ist). Alles klar?

Es handelt sich bei diesem eBook auch um eine Übersicht, die den Einstieg erleichtern soll – weit mehr Details finden sich unter den angegebenen Forums-Links. Dort sind die Informationen naturgemäß i. d. R. auch aktueller, vor allem was die Apps betrifft. Es kommen ja ständig neue hinzu. Und außerdem kann ich nicht alle Benutzer-Erfahrungen hier aufnehmen. Außerdem kann man im Forum auch seine Fragen stellen (und auf Antworten hoffen) – was mit einem eBook allein etwas schwierig sein dürfte.

Gedacht ist das Ganze also so, dass man sich mit diesem eBook einen Überblick verschafft – und für die tiefer schürfenden Dinge auf das Forum zurück greift. Die meisten Links hier führen ohnehin zu AndroidPIT – wo man in guten Händen ist!

Noch eins muss ich loswerden: Viele der hier kurz vorgestellten (oder auch nur genannten) Apps habe ich selbst nie getestet – etwa, weil ich nicht die Voraussetzungen dazu habe (ich nutze kein Facebook, und mein Smartphone auch nicht zum Spielen, um nur zwei Dinge zu nennen). Ein Grund mehr, auf die Erfahrungen der Community zurückzugreifen: Bei AndroidPIT ist man jederzeit herzlich willkommen! Auch für Feedback sowie Fragen zu diesem eBook findet sich dort ein Plätzchen.

Zu guter Letzt noch ein kleiner technischer Hinweis: Sofern der verwendete eBook-Reader die StyleSheets korrekt unterstützt, lassen sich verschiedene Arten von Links an ihrer Textfarbe: Rote gehen "nach draußen" (öffnen also wahrscheinlich einen Web-Browser), während grüne auf Begriffserklärungen im Anhang verweisen, und auch blaue "drinnen bleiben" (also Querverweise innerhalb dieses eBooks sind). Des Weiteren sind Ausführungen, die root voraussetzen, entsprechend farblich hinterlegt.

Doch nun: Viel Spaß bei der Lektüre!

GRUNDLAGEN FÜR DEN EINSTEIGER

Im ersten Teil dieses kleinen Handbuches geht es um die Grundlagen. Fortgeschrittenere Anwender können diesen also getrost überspringen – und gleich zum zweiten oder gar dritten Teil schreiten...

Die erste Inbetriebnahme und Grund-Einrichtung des Androiden erlaube ich mir an dieser Stelle zu überspringen: Zum Einen unterscheiden sie sich je nach Hersteller ein wenig, zum Anderen liegt dem Gerät zumindest dafür in der Regel eine Kurzanleitung bei. Wer dennoch Starthilfe benötigt, findet sie z. B. in einem Workshop bei Chip.DE.

Wie soll Steve Jobs am Ende seiner Vorstellung des ersten iPhone gesagt haben: "Ach ja, telefonieren kann man damit auch." Natürlich sind wir mit Android im "ganz anderen Lager" (laut Stevie in der Schmuddel-Ecke – aber wir wissen es natürlich besser). Dennoch gehe ich hier ähnlich vor, und klammere das Telefonieren zunächst aus. Stattdessen steige ich mit den Anwendungen ganz allgemein ein: Wie bekomme ich die auf meinen Androiden – und ggf. auch wieder runter? Wie organisiere ich sie, sodass ich mich auch nach der 50sten installierten App noch darin zurechtfinde? Und wie erstelle ich Sicherungen meiner Daten, falls es denn doch einmal "knallt"?

Grundlegendes zur Bedienung des Androiden

Zuallererst jedoch einige grundlegende Bedien-Hinweise.

Knöpfe

Auch wenn ein Androide überwiegend über den TouchScreen bedient wird, gibt es da doch noch ein paar Knöpfe, die sich drücken lassen. Was so ein richtiger Power-Riegel ist, der verfügt auch über einen gleichnamigen Knopf. Kein Gerät kommt ohne diesen. Und was lässt sich damit nun so besonderes Anstellen, dass er an dieser Stelle extra erwähnt werden muss?

Zunächst das triviale: Das Gerät lässt sich damit anschalten. War es zuvor komplett ausgeschaltet, muss der Power-Knopf dafür ein wenig länger gedrückt werden. Anders sieht es aus, wenn nur das Display ausgegangen ist (das tut es, um Strom zu sparen) – dann genügt ein kurzes Antippen. Das Gleiche noch einmal, und der Bildschirm geht wieder aus. Noch immer trivial. Allerdings wird der Bildschirm dabei auch gleich gesperrt – sodass man ihn bei erneutem Anschalten zunächst auch wieder entsperren muss. Das verhindert zum einen unbeabsichtige Bedienung in der Hosentasche – kann aber, sofern die Sperre mit einem PIN, Muster oder Kennwort-Schutz versehen wurde, auch vor unbefugtem Zugriff schützen.

Interessanter wird es, drückt man diesen Knopf bei aktivem Display ein wenig länger – denn dann kommt plötzlich ein Menü zum Vorschein. Je nach Android-Version lassen sich hier verschiedene Dinge auswählen: Gerät Herunterfahren / Neustarten sind fast generell dabei. Spannende Dinge gibt es jedoch gelegentlich auch: Spätestens ab Android 4.0 lässt sich bei den meisten Geräten über dieses Menü auch ein Bildschirm-Foto auslösen. Und manche Geräte bieten an dieser Stelle auch einen schnellen „Profil-Wechsel" an – etwa eben einmal auf lautlos stellen, oder in den Flugzeug-Modus wechseln...

Doch auch weitere „Knöpfe" bietet das Android-Gerät. Die zur Lautstärke-Regelung seien nur kurz erwähnt, und auch zum Auslösen der eingebauten Kamera ist gelegentlich ein Knopf reserviert. Und dann sind da noch drei bis vier weitere, die meist nicht ganz so offensichtlich sind: Auf neueren Androiden handelt es sich hier nämlich nicht um „Hardware-Knöpfe", sondern um so genannte „Soft Keys", die meist bei eingeschaltetem Display auch beleuchtet (und bei ausgeschaltetem Display ohne Funktion) sind.

Symbole sollen diese Knöpfe intuitiv bedienbar machen. In den meisten Fällen ganz rechts außen findet sich eine Lupe – zwar ohne Hut, aber der Detektiv steht anbei: Hiermit steht vielerorts eine Suchfunktion zur Verfügung. Dann ist da ein Haus: Dies ist der so genannte „Home-Key", der von überall sofort auf den „Home-Screen" führt. Die gerade genutzte Anwendung wird dabei nicht beendet,

sondern wartet im Hintergrund. Und damit muss auch die zweite Belegung dieser Taste sofort erwähnt werden: Ein langes Drücken öffnet eine Liste der zuletzt gestarteten Apps, sodass man auch wieder zur wartenden App zurückgelangen kann.

Weiterhin wäre da noch der „gebogene Pfeil", der fast schon „Bitte wenden!" zu rufen scheint. In Menüstrukturen hat er die Funktion „Zurück", was auch bei vielen Apps gilt: So letztere nicht explizit einen Knopf zum Beenden bieten, soll diese Taste das erledigen. Gelegentlich hilft ein langer Druck hier, eine App auch wirklich zu beenden – doch in der Regel ist so etwas speziellen Custom-ROMs vorbehalten.

Einen haben wir noch – einen Knopf, meine ich. Mal eine Liste, mal mit vier Quadraten, von denen eines ausgemalt ist. Nein, das ist nicht der Knopf, um schnell Yatzee (oder ein anderes Würfel-Spiel) zu starten – sondern der Menü-Knopf (so vorhanden – denn ab Android 4.0, und mit Einführung des Holo-Designs, verliert er langsam seine Bedeutung). Bei vielen Apps (und auch auf dem HomeScreen) lassen sich damit Zusatz-Funktionen aufrufen.

Ab Android 4.0 haben sich die Softkeys ein wenig verändert. In aktuellen Geräten sind sie nun nicht mehr fest integriert, sondern werden dynamisch vom System behandelt: Steht beispielsweise keine Menü-Funktion zur Verfügung, wird die "Menü-Taste" auch gar nicht angezeigt. Auch die Funktionalität hat sich im Vergleich zu früheren Versionen leicht geändert:

- Die "Zurück-Taste" ist geblieben, und funktioniert wie gehabt.
- Auch die Taste mit dem Haus führt nach wie vor zum Homescreen. Bei langem Drücken öffnet sich jedoch nicht mehr die Liste zuletzt geöffneter Apps – stattdessen poppt ein "Google" Kreis auf, über den man zu "Google Now" gelangt.
- Neu ist die Taste mit den zwei Rechtecken, die man "Multi-Tasking-Taste" benennen könnte: Hierüber öffnet man nun die Liste der zuletzt genutzten Apps. Unerwünschte Kandidaten lassen sich mit einer Wisch-Bewegung aus selbiger entfernen.
- Die "Menü-Taste" ist nun ein "senkrechter Strich", und (wie beschrieben) nur sichtbar, wenn auch Menü-Funktionen zur Verfügung stehen.

Der TouchScreen

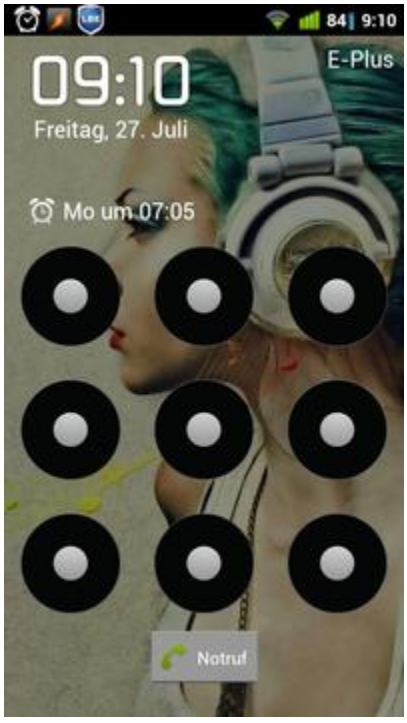
Android-Geräte werden i. d. R. Über einen Touchscreen bedient – nur wenige bieten zusätzlich eine Tastatur. Während es noch offensichtlich ist, dass sich eine App durch einfaches Antippen des zugehörigen Icons starten lässt, sind viele Interaktionen für den Anfänger ein wenig „versteckt". Da wären zum einen die Menüs, die sich – sofern vorhanden – über die Menütaste aktivieren lassen. Und oftmals fördert ein „langes Drücken" ein Kontext-Menü zutage.

In vielen Apps finden zusätzlich Wischgesten Verwendung: So gelangt man etwa durch waagerechtes Wischen zu weiteren Bildschirmen (bei einer eBook-Lese-App etwa zur vorigen bzw. nächsten Seite), oder kann durch senkrechtes Wischen entlang der linken Bildschirmkante die Helligkeit des Displays regeln. Beliebt sind auch Zwei-Finger-Gesten, wie etwa das sogenannte „Pinch-to-Zoom":

Hierbei berührt man das Display mit zwei Fingern, und zieht diese auseinander – um etwa in ein Bild hinein zu zoomen. Umgekehrt verkleinert man das ganze wieder, indem man die Finger aufeinander zu bewegt. Das klappt nicht nur beim Betrachten von Bildern in der Galerie, sondern beispielsweise auch in den meisten Webbrowsern.

Der Sperrbildschirm

Wie bereits erwähnt, schaltet man mit dem Power-Knopf den Bildschirm an. Um ein versehentliches Bedienen in der Hosentasche zu vermeiden, wird an dieser Stelle ein Sperrbildschirm (auch als „Lock-Screen" bezeichnet) aktiv. Je nach Android-Version sieht dieser unterschiedlich aus; gemein ist jedoch allen Versionen, dass er sich mit einer Wisch-Bewegung entriegeln lässt. Oftmals verbergen sich hier auch Zusatzfunktionen – so lassen sich gleichzeitig mit dem Entriegeln etwa auch noch Aktionen ausführen. Die rechte Abbildung zeigt einen Lock-Screen unter Android 2.3 (Gingerbread): Mit dem Schloss als Ausgangspunkt (den man nach rechts zieht) wird das Gerät entsperrt; zieht man hingegen das Lautsprecher-Symbol nach links, wird das Gerät lediglich stumm geschaltet. Der Dritte Kreis (in der Mitte) ist hier mit einer Zusatz-Funktion hinterlegt: Mit ihm lässt sich gleich eine konfigurierbare Anwendung starten bzw. in den Vordergrund holen – etwa die Telefon-App, damit man sofort schnell einen Anruf tätigen kann.



Sicherheit gegen unbefugte Bedienung bietet das jedoch noch nicht: Lässt man das Gerät etwa auf dem Kneipentisch liegen, während man auf die Toilette geht, haben die Freunde (oder auch andere Kneipen-Besucher) mit dieser Art von Sperrbildschirm leichtes Spiel – und könnten nicht nur problemlos auf die Inhalte zugreifen, sondern auch teure Anrufe tätigen oder gar Schadsoftware installieren. Doch auch dagegen lässt sich etwas unternehmen, indem man einen Sperr-Code einrichtet. Dies erledigt man in den System-Einstellungen unter „Standort & Sicherheit" im Menüpunkt „Displaysperre ändern". Standardmäßig ist keine Passcode-geschützte Sperre aktiviert – das wäre ja auch fatal, denn woher sollte der neue Anwender den Sperr-Code kennen?

Seit der ersten Android-Version mit dabei, freut sich das so genannte „Sperr-Muster" (auch als „Pattern-Lock" bekannt) großer Beliebtheit. Es ist auch wesentlich sicherer als der altbekannte PIN-

Code (bei dem viele Anwender entweder nur „1234“ oder das Geburtsdatum verwendeten – was sich mit ein wenig „Social Engineering“ schnell erraten lässt). Hier muss ein Muster gezeichnet werden, welches mindestens vier Punkte verbindet (siehe linke Abbildung). Da hilft das beste Social-Engineering nicht weiter, da ein Bezug zur Person höchst unwahrscheinlich ist.

Eine andere (und noch sicherere) Möglichkeit ist die Vergabe eines Passwortes – sofern hier nicht wieder obiges „1234“ verwendet wird. Ein sicheres Passwort besteht aus einer Kombination von Buchstaben und Ziffern (sowie ggf. Sonderzeichen), die sich nicht in einem Wörterbuch finden lässt. Wie man sich so etwas merken soll? Ganz einfach, beispielsweise mit einem Merksatz. Nehmen wir als Beispiel den Satz „Ich habe ein sicheres Passwort“. Und nun von jedem Wort den ersten Buchstaben: „IhesP“ - schaut doch schon recht kryptisch aus! Noch eine Ziffer eingebaut: „ein = 1“ ergibt sodann: „Ih1sP“. Steht in keinem Wörterbuch – und lässt sich (Dank des Satzes) dennoch einfach merken. Das rechte Bild zeigt, wie das dann aussehen könnte.

Eine kleine Unbequemlichkeit ergibt sich damit natürlich: Es dauert ein paar Sekunden mehr, bis man die nunmehr zwei Sperrbildschirme überwunden hat, und wieder mit dem Gerät arbeiten kann...

Schaltzentrale: Home-Screen, Widgets & "Home Replacements"

Wenn es bei Android so etwas wie eine "Schaltzentrale" gibt, ist dies sicher am ehesten der **Homescreen**: Hier starten alle Aktivitäten. Das ist es, was der Anwender nach dem Start seines Androiden zu sehen bekommt – von hier startet er seine Apps – hier platziert er (so er dies tut) seine Übersichten wie aktuelle Kalender-Ereignisse, News-Feeds, und so weiter. Daher macht es durchaus Sinn, dass sich das erste Kapitel dieses Abschnittes zunächst diesem widmet.

Eigentlich sollte ich besser sagen: "diese**n**". Klar gibt es einen "Standard-Launcher" bzw. "Stock-Launcher" ("Launcher" ist ein anderes Wort für den Homescreen, welches obigen Sachverhalt betont: Dass man von hier alle Aktivitäten "launcht", also startet). Auf fast allen Geräten ist jedoch bereits eine Alternative installiert: Da wäre HTC mit ihrem *Sense* Launcher, Motorola mit der *MotoBlur* Oberfläche, etc. pp.. Und zahlreiche Alternativen sind im Play Store verfügbar – wie etwa der Holo Launcher (linkes Bild), oder Apex Launcher (rechtes Bild). Jeder hat so seine Besonderheiten und Vorteile gegenüber den anderen. Da wären auf's Ressourcen-Schonen getrimmte Launcher, minimalistische Launcher (sowie deren Gegenstücke) – und, und, und. Ein genauerer Überblick findet sich natürlich wieder im passenden Forums-Thread.

Docking Bar

Das ist i. d. R. der Bereich "unten", in dem besonders häufig genutzte Funktionen verankert sind (auf obigen Screenshots auch gut zu erkennen). Bei einigen *Launchern* sind diese Aktionen "fest verdrahtet", und lassen sich nicht ändern/anpassen. Die Auswahl der Aktionen ist dabei für die Masse durchaus

tauglich: Telefon ist immer dabei (das Gerät heißt ja auch "Smart*Phone*", und nicht "MiniComputer" – auch wenn die Grenzen da schwer zu definieren sind), dazu kommen meist Anrufliste und Kurznachrichten, sowie der *App-Drawer*.

Die meisten (mir bekannten) *Launcher* erlauben es jedoch zumindest, die Aktionen selbst auszuwählen. So lassen sich entsprechende "Icons" z. B. bei o. g. *Apex Launcher* per Drag-and-Drop platzieren (und entfernen), auch die Reihenfolge lässt sich nachträglich ändern. Einige gehen sogar noch weiter, und lassen den Benutzer an die grafische Ausgestaltung direkt heran. Wer also alles individuell gestalten möchte, kann dies durchaus tun!

App-Icons

Diese lassen sich in der Regel auf dem Launcher (s. o.), und generell auf den HomeScreens platzieren. Letzteres gilt auch für die *Shortcuts* und *Widgets* (siehe unten). Für alle drei ist das Standard-Vorgehen zur Platzierung, eine freie Stelle auf dem "Desktop" "lange zu drücken". Daraufhin öffnet sich ein Kontext-Menü und fragt nach, was es denn sein darf – wobei unsere drei Kandidaten, und ggf. (je nach Launcher) auch noch weitere Dinge zur Auswahl stehen können. Spätestens ab Ice Cream Sandwich gibt es auch die Möglichkeit, App-Icons und Widgets direkt aus dem App-Drawer heraus auf den gewünschten Homescreen zu ziehen. Wieder entfernen lassen sie sich ebenfalls durch "langes Drücken" (diesmal auf das Icon selbst) und anschließendes "ziehen" auf die sich öffnende (meist rote) Mülltonne.

Unsere *App-Icons* haben nun keine weitere Funktion, als die zugehörige App zu öffnen. Nicht viel, aber mehr braucht es ja oft auch nicht: Von zentraler Stelle die wichtigsten Dinge schnell starten, ohne sich erst durch den "Drawer" (die komplette Applikationsliste) wühlen zu müssen. Benötigt man doch einmal etwas spezielleres, kommen unsere anderen beiden Kandidaten zum Einsatz:

Shortcuts

Nomen est Omen, wie der Latiner sagt: Hier geht es um "Abkürzungen", die einige Apps anbieten. Was auf dem HomeScreen wie ein gewöhnliches (gerade eben beschriebenen) *App-Icon* aussieht, ist es auch – nur mit ein wenig Zusatz-Funktionalität. Es springt bei der zugehörigen App gleich zu einem bestimmten Bildschirm, oder löst eine bestimmte Aktion aus. Ein "klassisches Beispiel" wäre bei Note Everything zu finden: Die Startseite (mit den Übersichten) überspringen, und direkt eine neue Notiz öffnen. Oder bei den weiter unten unter Apps Organisieren genannten "Organizern" das Öffnen eines bestimmten Ordners (was die beiden o. g. Launcher auch selbst anbieten). Bei diesen Dingen handelt es sich um *Shortcuts*.

Dazu muss gesagt werden, dass diese Shortcuts von den Apps selbst bereitgestellt werden müssen: Was die App nicht anbietet, steht da auch nicht zur Verfügung.

Widgets

Gleiches gilt auch für die Widgets: Grafische Elemente, die erweiterte Informationen zur Verfügung stellen – und optional auch noch als Shortcuts dienen können. Einige Beispiele dafür finden sich in den beiden obigen Screenshots:

Widgets von DroidStats, die Informationen zu aktuellen Statistiken (hier: Telefonminuten und SMS) geben – und bei "Antippen" die App gleich auf der zugehörigen Detail-Seite öffnen (links).

Widgets von Mini-Info, die über diverse System-Informationen auf dem Laufenden halten (rechts). Tippt man sie an, wird die App (ganz normal) gestartet.

Ein TaskManager-Widget, welches über freien Speicher sowie die Anzahl gerade laufender Prozesse informiert. Die bei Antippen ausgeführte Aktion ist konfigurierbar – etwa das Starten der App, oder Killen aller "black-listed" Apps. Übrigens: Auch die Uhr im Screenshot am Anfang dieses Kapitels ist ein Widget...

App-Drawer

Auch zu diesem zu guter Letzt noch ein paar Worte. Ich habe ihn ja bereits zuvor als die "unübersichtliche Lagerhalle von Icons installierter Apps" erwähnt (naja, nicht mit diesen Worten – aber so kommt es vielen und oft vor). Dem Hören-Sagen nach muss das nicht generell so sein. Es soll Launcher geben, die hier alternativen Implementierungen folgen, und Dinge wie "Reiter", "Unter-Ordner", "Kategorien", und ähnliches anbieten. Wer hier also gern ein wenig aufräumen würde, und einem "alternativen Launcher" nicht abgeneigt ist, sollte bei der Auswahl auch darauf achten. Womit er sich ggf. auch den unter Apps Organisieren genannten separaten "Organizer" erspart.

Wo wir gerade vom App-Drawer sprechen: Ab Android 4.0 („Ice Cream Sandwich") findet sich in diesem ein zusätzlicher Reiter, der verfügbare Widgets auflistet. Somit hat man endlich eine Übersicht darüber, welche Widgets verfügbar sind. Auf den Home-Screen kann man selbige dann befördern, indem man sie ganz dolle drückt: Der App-Drawer blendet sich dann aus, und man lässt das Widget schließlich an der gewünschten Stelle einfach "fallen".

MIT ANDROID ARBEITEN

Steuerzentrale: Einstellungen und "Switches"

Haben wir den *Home-Screen* als "Schaltzentrale" bezeichnet – so ist der Ort, an dem die ganzen Systemeinstellungen getätigt werden, ja wohl die "Steuerzentrale". Und es gibt so einiges einzustellen bei Android, die Liste ist also nicht unbedingt kurz. Hinzu kommt, dass vieles "historisch gewachsen" ist – und somit manche Dinge an den verschiedensten Orten zu suchen sind, obwohl sie aus subjektiver Sicht eigentlich zusammen gehören...

Klar, es handelt sich bei aktuellen Android-Versionen schon um recht komplexe Systeme, wo man an vielen Schräubchen drehen können muss. Doch insbesondere für Neueinsteiger sind das meist zu viele (wobei genau die, die man gerne hätte, natürlich fehlen). Doch auch hier gibt es einige Apps, die für Erleichterung sorgen: Entweder, weil sie die Auswahl auf wesentliche (häufig benutzte) Punkte zusammenstauchen – oder, weil sie in spezifischen Bereichen zusätzliche Einstellungsmöglichkeiten schaffen. Zu beiden Themen lässt sich meine Übersicht zu Einstellungen im Forum etwas ausführlicher aus.

Konfiguration

Bei Android lässt sich so einiges konfigurieren. Und mit jeder neuen Version kommen neue Dinge hinzu. Ich möchte jetzt nicht auf alles eingehen – doch einige zentrale Einstellungen finden sich hier erläutert.

Die folgenden Dinge sind alle in den "Einstellungen" von Android untergebracht. Wie man dorthin gelangt? Vom "Home-Screen" ausgegangen, geht es zunächst über die "Menü"-Taste ins Menü, und von dort in den Punkt "Einstellungen". Dann geht es entsprechend weiter, wie in den folgenden Abschnitten beschrieben...

WLAN

Klar, mit so einem Smartphone möchte man gern ins Netz. Und wenn man noch keinen vernünftigen Daten-Tarif gebucht hat: Was liegt da näher, als das heimische WLAN zu nutzen? Oder das bei Freunden und Verwandten? Zumal es in der Regel ja auch schneller ist als die mobile Datenverbindung. Was also ist zu tun?

In den Einstellungen wählen wir den Punkt "Drahtlos & Netzwerke". Hier lässt sich WLAN schon erst einmal generell aktivieren (indem man das passende Häkchen setzt). Sodann tauchen wir in den Punkt "WLAN-Einstellungen" ab – und gelangen zu einem Bildschirm, der dem rechts dargestellten ähnelt.

Der erste Punkt entspricht dem generellen Aktivieren der WLAN-Funktionalität (wie auf der vorigen Seite). Ist WLAN aktiv, und mit einem Netzwerk verbunden, wird das an dieser Stelle auch angezeigt. Mit dem zweiten Punkt kann man sich "unterwegs" über verfügbare offene WLAN-Netzwerke informieren lassen. Wer jedoch vertrauliche Daten auf seinem Androiden hat, sollte mit solchen Netzen vorsichtig sein: Man weiß ja nie...

Darunter nun werden alle aktuell verfügbaren WLAN-Netze aufgelistet. Auch wird dargestellt ob (und wenn ja wie) diese verschlüsselt sind. Hier sollte also auch das "eigene" WLAN (bzw. das, in welches sich eingebucht werden soll) nun stehen. Einfach antippen, ggf. den Schlüssel (das "Verbindungs-Passwort") eingeben, und auf "Verbinden" tippen – und wenige Sekunden später sollte die Verbindung stehen. Bei Bedarf lässt sich ab Android 4.0 nach Aktivieren der Checkbox *Erweiterte Optionen einblenden* auch ein für das jeweilige Netzwerk zuständiger Proxy-Server angeben.

Einmal eingegeben, merkt sich übrigens Android die Verbindungsdaten: Kommt man das nächste Mal bei aktiviertem WLAN in die Nähe dieses Netzes, erfolgt die Verbindung automatisch.

Mobiles Datennetz

Der "moderne Mensch" ist ja heutzutage permanent online. Unser WLAN können wir aber nicht überall hin mitnehmen. Was tun?

Die Antwort heißt: Einen passenden Daten-Tarif (Volumentarif oder Flatrate) buchen, und das "mobile Datennetz" konfigurieren! Ersteres gibt es beim Provider – und letzteres findet sich wieder unter "Drahtlos & Netzwerke". Bezeichnenderweise unter dem Punkt "Mobilfunknetze". Der führt dann zu einem Bildschirm, der dem links dargestellten stark ähneln dürfte.

Ein kurzer Blick auf das Bild dürfte auch bereits helfen, eine der größten Sorgen auszuräumen: Was ist mit meinen Daten-Kosten, wenn ich im Ausland bin? Ja was? Das hängt ganz davon ab, was auf dieser Seite konfiguriert wurde. Standardmäßig sind die Häkchen bei "Roaming" *nicht* gesetzt (also wie auf dem Bild zu sehen). Im Ausland bzw. generell im Netz eines "Fremdanbieters" wird daher die Datenverbindung gar nicht erst aufgebaut. Daher sollten hier auch keine diesbezüglichen Kosten entstehen.

Ganz unten ist bei mir noch ein Häkchen gesetzt, welches die Datenverbindung auf "2G" beschränkt. Das ist zwar nicht so schnell wie 3G oder gar 4G – spart aber u. U. einiges an Energie (siehe 2G versus 3G: Spart 2G wirklich so viel Akku?), sodass ich mit einer Akku-Ladung länger auskomme. Für ein wenig E-Mail und Web ist das auch völlig ausreichend. Sollte ich tatsächlich einmal mehr Durchsatz benötigen, kann ich das jederzeit umschalten.

Woher weiß Android denn nun, wie es ins Internet kommt? Diese Einstellungen verbergen sich hinter den "Zugangspunkten". So manch Custom-ROM (wie z. B. CyanogenMod) ermittelt diese Konfiguration automatisch: Anhand der SIM-Karte erkennt es den Anbieter, und ordnet die entsprechenden Zugangsdaten aus seiner Datenbank zu. Wer dieses Glück nicht auf seiner Seite hat, findet die passenden Zugangsdaten jedoch hoffentlich im Anhang – andernfalls lassen sie sich beim Provider erfragen.

Tethering

An dieser Stelle folgt oft die Frage: "Ich habe da noch ein Tablet/Notebook/... Kann ich jetzt irgendwie die mobile Datenverbindung mit nutzen?" Vor Android 2.2 (aka "Froyo" oder "Frozen Yoghurt") hieß die Antwort eindeutig: Jein. Mit root und einer App wie Wireless Tether ließ sich dies erreichen. Ansonsten galt der übliche Spruch: "Ohne root sich nix tut".

Zum Glück hat sich das eindeutig geändert: Seit Froyo gehört Tethering zur "Standard-Ausrüstung", und ist natürlich auch noch bei den aktuellen Versionen mit an Bord (Screenshot rechts). Wer sicher gehen möchte, dass kein Dritter "mitsurft", kann das Netzwerk über USB weiterreichen. Einfacher geht es jedoch, wandelt man seinen Androiden in einen "mobilen Hotspot" um. Hierzu wird der zweite Punkt aktiviert, und die Details werden unter "WLAN-Hotspot-Einstellungen" eingetragen: Eine SSID (Name für den Zugangspunkt) kann nach Gusto vergeben, eine Verschlüsselung gewählt, und natürlich auch der zugehörige Schlüssel/Passwort hinterlegt werden. Und schon steht dem Surf-Vergnügen nichts mehr im Wege...

Wer immer noch ein wenig unsicher ist, hat vielleicht bemerkt: Da gibt es noch einen Punkt namens "Hilfe". Stimmt. Und da wird das Ganze auch nochmal erklärt – falls dieses Buch gerade mal nicht zur Hand ist...

Internet-Telefonie

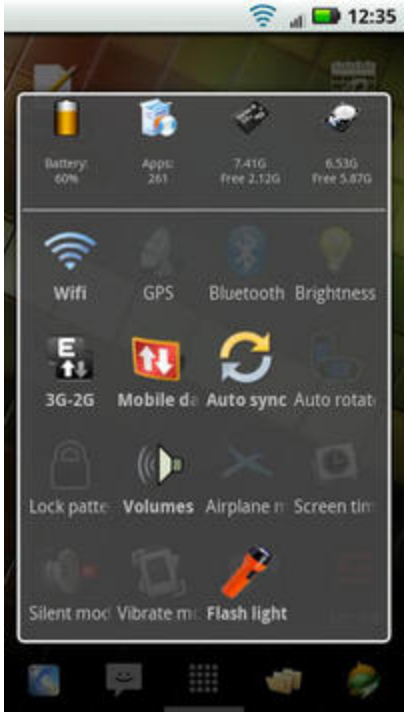
Oh nein, den Netzanbietern hat das sicher nicht sonderlich gefallen. Aber dennoch: Seit Gingerbread gehören die SIP-Einstellungen zu den Bordmitteln. Wer noch kein Gingerbread (oder eine aktuellere Version) auf seinem Androiden hat, muss dafür zu Drittanbieter-Software wie SIPGate greifen, kommt aber auch zum Ziel.

Versteckt sind diese Konfigurationsdaten unter den "Anrufeinstellungen" (also *nicht* unter "Drahtlos & Netzwerke"), und zwar ganz am Ende des Bildschirms (siehe Screenshot links). Von hier aus geht es über "Konten" in die Übersicht eingerichteter SIP-Konten – beim ersten Aufruf dürfte diese leer sein. Ein Button, beschriftet mit "Konto hinzufügen", wartet jedoch schon auf Betätigung. Die passenden Zugangsdaten gibt es beim VoIP-Anbieter. Essentiell sind Nutzername, Passwort und Server – etliche optionale weitere Einstellungen wie Proxy u. a. stehen ebenfalls zur Verfügung.

Mittels einer Checkbox lässt sich ein SIP-Konto als "primär" festlegen – was aber nur bei mehreren Konten interessant ist. Über dieses Konto werden dann ausgehende Anrufe geführt.

Mehr Übersicht, bitte!

Wer sich lieber auf Wesentliches beschränken möchte, greift am besten zu Apps wie Quick Settings (rechtes Bild):

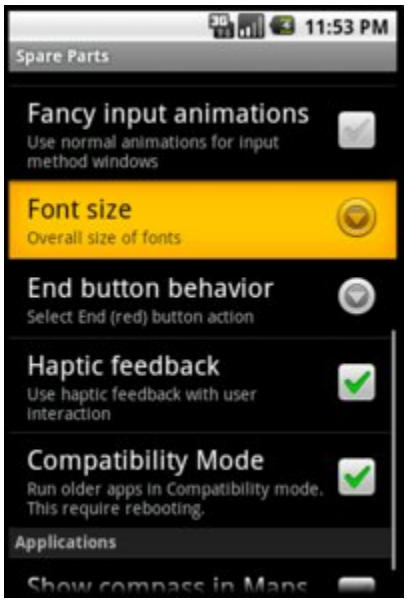


Die App bietet die Möglichkeit, sowohl die Auswahl als auch die Reihenfolge der angezeigten Einstellungs-Punkte zu konfigurieren. Auf diese Weise lässt sich eine sehr personalisierte Konfigurations-Seite erstellen. Sehr spezielle Punkte (die in der Regel selten benötigt werden) stehen aber oft nicht zur Auswahl.

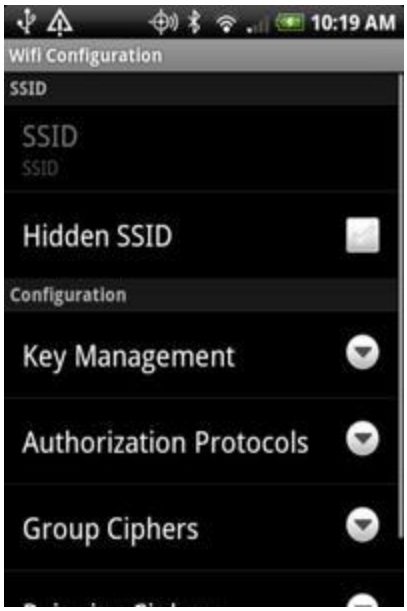
Zugriff auf häufig benötigte Einstellungen bietet ebenfalls die gleichnamige App eines anderen Entwicklers: Mit diesem Quick Settings (linkes Bild) lässt sich schnell einmal das WLAN deaktivieren, in die Netzwerk-Einstellungen schauen, die Lautstärke anpassen, und mehr. Die Reihenfolge der Icons lässt sich auch hier vom Anwender festlegen, ein eigenes Icon auf dem Homescreen ist überflüssig: Die App öffnet sich wahlweise durch langes Drücken der Such-Taste, der Kamera-Taste, oder aus der Notificatiion Area heraus.

Zusätzliche Einstellungen

Während die einen es lieber kompakter hätten, gibt es da auch noch die Gruppe derer, denen die vorhandenen Konfigurationsmöglichkeiten nicht ausreichen. Auch dieser kann (in einem gewissen Rahmen) geholfen werden:



So schaltet etwa die App Spare Parts (links) eine ganze Reihe zusätzlicher Schalterchen frei. Sie ist die umfangreichste App in diesem Bereich, und auch die, die bereits am längsten im Play Store verfügbar ist. Leider wurde sie aber auch schon ein Weilchen nicht mehr aktualisiert – Nutzer aktuellerer Android-Versionen (Ice Cream Sandwich und neuer) müssen also zunächst einmal prüfen, ob noch alles Bestehende passt – und können kaum darauf hoffen, dass neue Features bereits unterstützt werden.



Einige wenige zusätzliche Einstellungen bietet auch Extra Phone Settings (Bild oben rechts). Mit ihrer Hilfe lässt sich der Androide u. a. bei einem ausgehenden Anruf kurz zum Vibrieren bringen, sobald die Gegenseite "abgenommen" hat – eine Funktionalität, die bei einigen Geräten bereits von Haus aus dabei ist.

Zu guter Letzt sei noch eine besondere Spezialität kurz erwähnt: Der Wifi Config Editor (rechtes Bild) ermöglicht es, die Wifi-Einstellungen noch detaillierter vorzunehmen. Weit mehr Einstellungen, als der Standard-Dialog normalerweise anzeigt. Otto-Normal-Benutzer braucht das sicher kaum einmal – doch für manchen "Spezialisten" ist es sicher ein wertvolles Werkzeug.

Anwendungen verwalten

Um folgende Themen geht es in diesem Kapitel:

- Installieren von Apps
- Aktualisieren (neudeutsch: "Updaten") von Apps
- Apps Bereinigen (Cache löschen etc.)
- De-Installieren (Löschen) von Apps

Also im Prinzip der ganz normale "Lebens-Zyklus" einer App auf dem Androiden: Erst wird sie installiert (und benutzt), hin und wieder gibt es neuere Versionen, und schließlich – ist man ihrer überdrüssig geworden, oder hat etwas besseres gefunden – soll sie wieder vom Gerät verschwinden. Zwischendurch gilt es u. U. den Cache zu bereinigen: Entweder, um Platz freizuschaufeln, oder um diverse kleine Probleme zu lösen. Für all diese Aufgaben gibt es verschiedene Ansätze.

Apps? APK-Datei?

Zu allererst gilt es noch ein paar Begriffe zu klären...

App nennt man die Anwendungen unter Android (und übrigens auch bei Apples iOS). Dieses Kürzel leitet sich nicht etwa von *Apple* ab, wie einige meinen, sondern vom Wort *Application* – jaja, der "Aküfi" (Abkürzungs-Fimmel) ist nicht ausschließlich © Germany.

Eine APK-Datei enthält in der Regel eine solche App, und ist so etwas wie ein "Installations-Archiv". Erhältlich im Play Store, und oftmals auch auf den Webseiten der jeweiligen Entwickler – diese beiden Quellen können als relativ sicher gelten (sowohl was "Systemsicherheit" als auch was "Legalität" anbetrifft). Sie sind auch in der "freien Wildbahn" anzutreffen (etwa als Suchergebnis einer Google-Suche nach "`<AppName>.apk`"). Im letzteren Falle ist allerdings Vorsicht geboten: Zum einen sind derartige Angebote nicht selten illegal, zum anderen die hier auffindbaren APK-Dateien oftmals auch manipuliert (Stichwort: DroidDream).

Ergo: Das Futter für den Androiden sollte besser ausschließlich aus verlässlichen Quellen besorgt werden. Und die schauen wir uns jetzt an.

Bordmittel

Natürlich bringt Android passende Hausmittel für die genannten Aufgaben mit – irgendwie müssen ja die ersten "Früchtchen" in den Korb gelangen können. Zu diesem Zweck ist auf den meisten Androiden (einige Hersteller kochen hier wieder ihr eigenes Süppchen, so dass dies nicht pauschal für alle Android-Geräte gilt) eine App namens *Play Store* (ehemals *Google Market*) vorinstalliert. Dieser möchte ich zunächst ein wenig Grundwissen vorausschicken, bevor ich auf die App selbst eingehe:

Zunächst einmal ist der Playstore die wohl umfangreichste (und darüber hinaus auch die „offizielle“) Quelle für Android-Apps. Daher sind Entwickler natürlich bestrebt, ihre Produkte auf jeden Fall an dieser Stelle unterzubringen. Von wenigen Ausnahmen einmal abgesehen, kann man daher fast sagen: Eine App, die es hier nicht gibt, gibt es einfach nicht. Darüber hinaus ist der überwiegende Teil der Apps gratis verfügbar – was allerdings häufig mit Werbe-Einblendungen

in den jeweiligen Apps verbunden ist, denn irgendwie möchte der Entwickler ja auch für seine Mühe entlohnt werden. Eine Tatsache, die übrigens auch für andere App-Märkte gilt.

Die Nutzung des Google Playstore setzt einen gültigen Google-Account voraus. Diesen kann man sich direkt auf der Webseite gratis anlegen. Bei der Ersteinrichtung eines mit der genannten App ausgestatteten Androiden wird dieser auch abgefragt und kann, sollte man noch nicht über einen Account verfügen, direkt vom Einrichtungs-Assistenten aus erstellt werden (wer dies zunächst übersprungen hat, findet den entsprechenden Punkt in den "Einstellungen" unter "Konten & Synchronisation"). Will man auch kostenpflichtige Apps nutzen, muss zudem eine Kreditkarte mit dem Google-Account verknüpft werden – andere Bezahlmöglichkeiten sind leider, trotz zahlreicher Nutzerproteste, bislang nicht verfügbar. Aber hier tut sich etwas: Mobilfunk-Anbieter können auch die Bezahlung über die Telefonrechnung ermöglichen. Gebrauch machen davon in Deutschland Vodafon und T-Mobile bei von ihnen selbst verkauften (also entsprechend „gebrandeten", siehe Branding) Geräten, auch O2 hat mittlerweile nachgezogen.

Ist nun also eine Kreditkarte mit dem Google-Account verknüpft, lassen sich kostenpflichtige Apps über die Playstore-App ohne weitere Passwort-Abfrage (das Passwort ist ja bereits in den Geräte-Einstellungen hinterlegt) erwerben. Also darauf aufpassen, dass der Sprößling nicht auf Einkaufstour geht – oder Unbefugte am Gerät spielen und Schabernack treiben! Außerdem ist die Rückgabefrist bei Fehlkäufen mit derzeit 15 Minuten arg zu kurz geraten – hier gilt es also gegebenenfalls, schnell zu handeln, und den Fehlkauf sogleich wieder zu deinstallieren.

Übrigens: Da jede im Playstore erworbene App mit dem zugehörigen Google-Account verknüpft ist, lassen sich einmal gekaufte Apps auf allen mit diesem Account versehenen Androiden nutzen. Also keine Sorge, dass man bei Gerätewechsel alles neu erwerben muss!

Play Store

Über den *Play Store* (ehemals *Google Market*, siehe Screenshot rechts) soll der Android-Jünger sich seine Apps besorgen. Die Fülle an Apps kann hier grob nach Rubriken durchblättert oder, so der Name der gesuchten App bekannt ist, auch gezielt durchsucht werden. Letzteres ist natürlich auch nach Stichworten möglich, die in Namen oder der Beschreibung der Apps vorkommen. Aufgrund der großen Anzahl an im Play Store verfügbaren Apps ist das Ergebnis aber nicht unbedingt immer befriedigend. Filtermöglichkeiten (etwa das Ausblenden unerwünschter Entwickler oder das Ausschließen bestimmter Begriffe) gibt es in der App leider nicht.

Etwas komfortabler wird das Ganze, wenn man die Website des Play Store mit dem Browser am PC benutzt: Hier lassen sich viele der aus der "erweiterten Google-Suche" bekannten Tricks verwenden – etwa um mit dem Begriff vorangestellten "-" Zeichen Begriffe auszuschließen (sogar einige erweiterte Attribute des "großen Bruders", wie etwa "intitle:Begriff" wenn der App-Name "Begriff" enthalten soll, sind möglich). So findet man Apps z. B. zum Thema Scuba-Diving (Sporttauchen) durch eine Suche nach "+scuba -log" (oder "+dive -log" – jeweils ohne die Anführungszeichen) Apps zum Thema Scuba-Diving, schließt jedoch Logbücher aus. Die Informationen lassen sich am größeren Bildschirm auch weit bequemer sichten. Ist die gesuchte App gefunden, kann sie überdies, sofern man mit seinem Google-Account angemeldet ist, mit einem einfachen Klick auf den Button "Installieren" auf den Androiden befördert werden: Schon wenige Sekunden später sieht man dort in der Regel den Download und schließlich auch den Installationsprozess starten. Sind mehrere Geräte mit dem selben Google-Account verknüpft, lässt sich das gewünschte Zielgerät natürlich auswählen. Auch filtert der Play Store automatisch die Apps aus, die mit dem Zielgerät nicht kompatibel sind (siehe Anhang: "Warum finde ich die App im Play Store nicht?").

Um sich eine Übersicht über bereits installierte Apps zu verschaffen, scrollt man auf der Play Store Website einfach an das Ende der Seite. Ganz unten findet sich nämlich ein mit "Meine Bestellungen & Einstellungen" beschrifteter Link, der zu einer passenden Übersicht führt. Zunächst werden alle getätigten "Bestellungen" – also heruntergeladene Apps, Bücher etc, ob gratis oder gekauft – im Reiter "Bestellungen" aufgelistet. Das Anklicken eines Eintrags führt dabei zur Produktseite desselbigen.

Der zweite, mit "Einstellungen" beschriftete Tab erlaubt eine gewisse Konfiguration des Play Store. So kann man seinen Geräten Namen geben und festlegen, ob sie in den Menüs auf App-Seiten als Installationsziel auftauchen sollen (Altgeräte entfernen kann man leider nicht). Auch Wünsche zu Email-Benachrichtigungen (Angebote vom Play Store u. a. m.) lassen sich hier festlegen.

Wer genau hinschaut, hat oben rechts auf der Seite noch vier weitere Buttons entdeckt: "Meine Musik", "Meine Bücher", "Meine Filme", und "Meine Android Apps". Hinter letzgenanntem Button wird es besonders interessant: Nach Geräten gruppiert, werden die jeweils installierten Apps alphabetisch auf bis zu jeweils 20 Seiten mit jeweils 9 Einträgen aufgelistet (die Begrenzung könnte für einige ein Problem sein, da nach 9*20=180 Apps Schluss ist: Was weiter hinten im Alphabet steht, ist hier nicht mehr zu sehen). Über ein Mülltonnen-Icon lassen sich Apps deinstallieren. Sind Updates vorhanden, ermöglicht ein mit "Bestätigen" beschrifteter Button die direkte Installation auf diesem Gerät. Unterhalb der installierten Apps werden als "Andere Apps in meiner Bibliothek" all die Apps angezeigt, die man irgendwann einmal installiert hatte (siehe auch Wie kann ich de-installierte Apps aus der Übersicht *Andere Apps in meiner Bibliothek* entfernen?).

Um nun aber die Nutzung des *Play Store* auf dem Androiden zu verbessern bieten sich, abgesehen von "alternativen Market-Apps", auch diverse "Market-Ergänzer" an.

Anwendungen verwalten

Der Punkt "*Anwendungen verwalten*" (Screenshot links) findet sich unter *Einstellungen→Anwendungen* im Android-Menü, und ist in Tabs eingeteilt: Heruntergeladene (also selbst installierte; dieser Tab wird bei Aufruf von "Anwendungen verwalten" geladen), Alle, Auf SD-Karte, Ausgeführte. Die ersten drei Tabs sind ruck-zuck geladen, der vierte braucht ein paar Sekunden und ist ein vollwertiger Task-Manager...

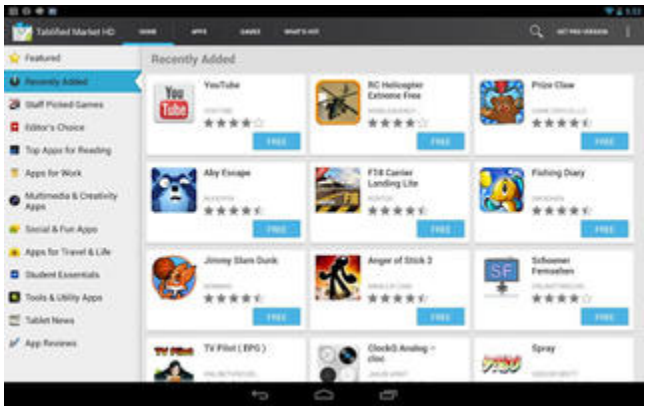
Ist die Liste aufgebaut, lassen sich Details zu den Anwendungen einsehen. Dies geschieht, indem die gewünschte App in der Liste kurz angetippt wird. Sodann offenbart sich: Wieviel Platz belegt die App selbst, wie viel ihre Daten. Wie viel Cache benutzt sie. Und so weiter. Von hier aus lassen sich dann z. B. auch der **Cache leeren**, die **Daten löschen** – oder die Anwendung deinstallieren (löschen).

Alternativen zur Cache-Bereinigung finden sich im Kapitel Tuning.

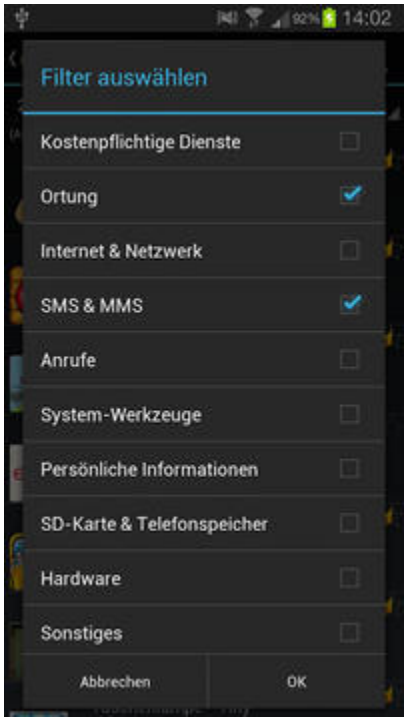
Playstore-Ergänzungen

Im Google Playstore findet sich eigentlich alles – die Frage ist nur, wie lange man für die Suche benötigt. Besonders Besitzer eines Tablets ärgern sich oft darüber, dass die Apps das größere Display nicht vernünftig ausnutzen. Oder dass es so schwierig ist, Apps zu finden, die dies tun. Zum Glück gibt es da Abhilfe:

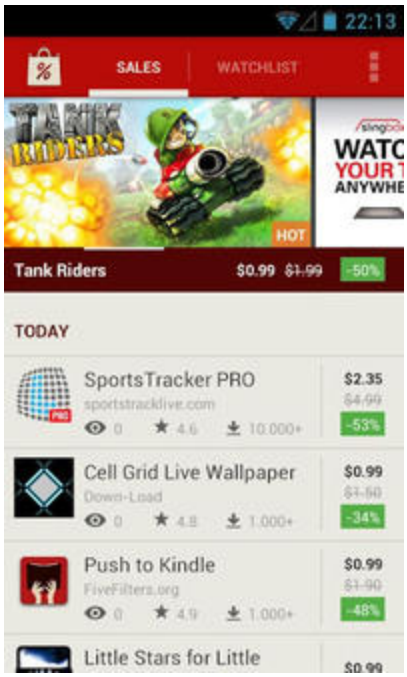
Die App Tablified Market HD hat sich nämlich darauf spezialisiert, nur Tablet-geeignete Apps aufzuspüren.



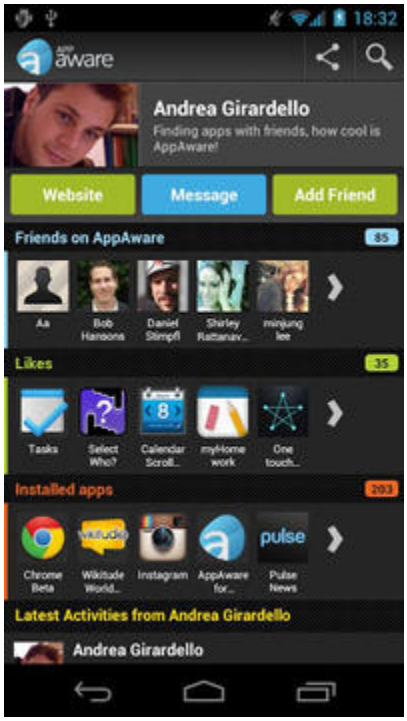
Wie vom Playstore gewohnt, wird man auch in dieser App von einer Liste mit empfohlenen Apps begrüßt, und eine Suchfunktion findet sich ebenfalls. Zusätzlich kann man gezielt einzelne Rubriken durchstöbern. Alle Apps, die sich hier finden, sind für die Benutzung auf Android-Tablets optimiert. Es handelt sich bei *Tablified Market HD* allerdings nicht um eine eigene Plattform: Quelle der Apps ist der Playstore, auf den man auch zur Installation von Apps weitergeleitet wird.



Ist jemand – nicht zu Unrecht – besonders besorgt bezüglich der Berechtigungen, die einige Apps verlangen, greift er für die App-Suche im Playstore am Besten auf APEFS (rechtes Bild) zurück. Diese App stellt ein alternatives Front-End für den *Google Playstore* dar – welches wesentlich aufgeräumter wirkt: Man wird nicht gleich auf der Startseite mit allerlei Empfehlungen bombardiert, sondern von einem Menü begrüßt, aus dem sich die gewünschte Aktion auswählen lässt. Neben den „Charts" (also den derzeitigen „Highlights" im Playstore) und der „Erweiterten Suche" hat man hier auch Zugriff auf bereits auf dem Gerät installierte Apps – womit sich diese auch nachträglich auf unerwünschte Berechtigungen untersuchen lassen.

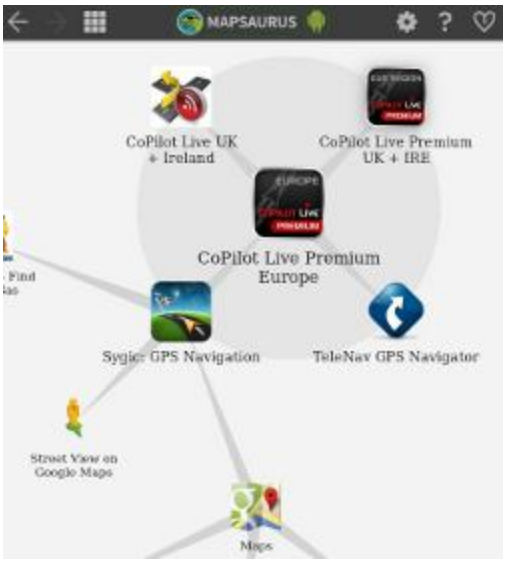


Für Schnäppchen-Jäger besonders interessant sein dürfte AppSales (linkes Bild): Nicht nur zeigt diese App aktuelle Rabatt-Aktionen auf. Sie erlaubt auch, eigene Filter zu setzen – um so die Inhalte auf die eigenen Interessen einzugrenzen. Und ist die Traum-App gerade zu teuer, setzt man sie auf eine "Watch-List" (Beobachtungs-Liste), um bei etwaigen Rabatt-Aktionen benachrichtigt zu werden.



Freunde sozialer Netzwerke werden AppAware zu schätzen wissen. Hier bekommt man u. a. die Apps seiner Freunde angezeigt (so diese mitmachen), in der eigenen Umgebung besonders intensiv genutzte Apps, und mehr. Erfahrungen lassen sich mit der Community teilen und diskutieren, es gibt aus der Community berechnete App-Listen, und auch Bookmarks sind möglich. All dies soll bei der Suche der optimalen Apps für den eigenen Bedarf helfen.

Für die Suche nach alternativen Apps sei schließlich noch Mapsaurus empfohlen. Diese App hat sich auf die Suche nach „ähnlichen Anwendungen" spezialisiert. Ist man etwa mit einer App nicht so wirklich zufrieden, hilft vielleicht ein Blick auf Alternativen mit Mapsaurus: Die bekannte App aufgesucht, führen vier „Fäden" zu Apps, die dieser ähneln. Wie ein Spinnennetz erweitert sich diese Ansicht, sobald man auf eine dieser Alternativen tippt – der Screenshot veranschaulicht dies recht gut.



Interessant dürfte für den Einen oder Anderen auch der Market Comments Reader sein. Er zeigt die "versteckten" Kommentare an (Schon mal gewundert, wie eine App x★ bei >0 Kommentaren kriegen kann, obwohl da kein Kommentar steht?).

Genervt von der aktuellen PlayStore-App? Verärgert, dass die Liste aller jemals gekauften (und u. U. nicht mehr installierten) Apps verschwunden ist? Ist das Android-Gerät gerootet (siehe Super-User "root"), kann Paul O'Brians Legacy Play Store Abhilfe schaffen. Paul hat eine ältere Version (als der Play Store noch Market hieß) gepatcht, sodass sie sich parallel zur ständig zwangsweise aktualisierten PlayStore-App installieren lässt (natürlich greift sie dabei auf die gleiche Quelle zu, wie auch Googles eigene Playstore-App). In diesem Fall lassen auch sich mit MarketEnabler die regionalen Beschränkungen aushebeln: Diese App gaukelt dem *Play Store* vor, man wäre mit einem ganz anderen Provider in einem ganz anderen Land unterwegs. Und mit AT&T in den Staaten dürfen "US only" Apps natürlich installiert werden 😂

Playstore-Alternativen

Derer gibt es viele: AndroitPIT, AppBrain, PDassi... Da fällt es schon bald schwer, über alle auf dem Laufenden zu bleiben, denn es kommen ja auch ständig neue hinzu. Daher kann diese Übersicht keinesfalls vollständig sein – vielmehr beschränke ich mich auf ein paar Beispiele, die mir besonders sinnvoll erscheinen.

Eines ganz zu Anfang: Auch wenn es durchaus Sinn machen kann, mit mehreren/verschiedenen dieser Alternativen parallel zu arbeiten empfiehlt es sich, Einkäufe immer an der gleichen Stelle zu machen. Sonst verliert man recht leicht den Überblick – und weiß etwa nach einer Neuinstallation oder dem Wechsel auf ein neues Gerät nicht mehr, aus welchem Market man nun die gekaufte App wieder bekommt, ohne sie nochmals bezahlen zu müssen.

AndroidPIT AppCenter

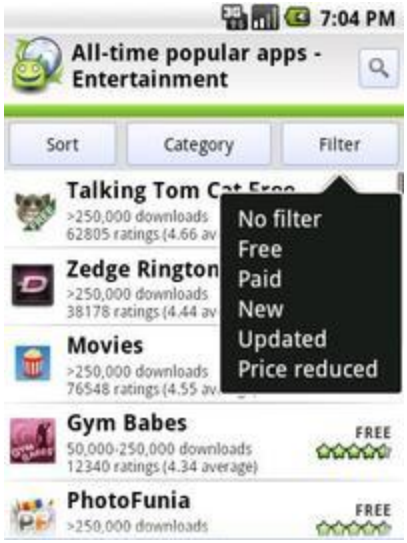
Wer auf der AndroidPIT-Website auf Apps klickt, findet zu vielen Apps nicht nur Bewertungen aus dem Play Store und von den AndroidPITiden – sondern oftmals auch Testberichte, die die ganze App durchleuchten, und so schon vor der Installation einen genaueren Einblick erlauben. Nicht selten sind es sogar mehrere Testberichte pro App, die sich dann auf unterschiedliche Versionsstände beziehen – so bekommt man auch gleich noch ein Gefühl dafür, wie sich die App entwickelt hat. Das findet man wirklich nicht überall! Wie auch die Möglichkeit, sich die Bewertungen und Kommentare aller Sprachen zusammen anzeigen zu lassen. Gerade bei wenig bewerteten Apps muss man so nicht lange nach diesen suchen. Nicht zu vergessen die themenbezogenen Übersichten im Forum (App Reviews nach Einsatzzweck), auf die in diesem Buch häufig Bezug genommen wird.

Wer das direkt auf seinem Androiden tun möchte, der greift zum AppCenter (siehe linkes Bild). Auch hier besteht die Möglichkeit, nach Kategorien zu browsen, Filter einzusetzen, und mehr.

Und ein weiteres Plus bietet AndroidPIT in dieser Hinsicht: Mehr Flexibilität, wenn es ums Bezahlen geht – denn neben der Kreditkarte wird auch Paypal unterstützt. Und weitere Zahlungsmöglichkeiten sind geplant. Einziger Haken: Nicht jede Kauf-App lässt sich hier erwerben (dazu müssen die Entwickler sich mit AndroidPIT entsprechend einigen). Aber auch das werden täglich mehr.

Ach ja: So manche App, die man evtl. mit einem "zu kleinen" Gerät im "offiziellen Market" (aka *Play Store*) gar nicht zu sehen bekäme, lässt sich hier mit Leichtigkeit finden und installieren. Und auch die Vorschläge von alternativen Apps sind nirgends so treffsicher wie hier – weil handverlesen und kontrolliert. Ganz zu schweigen von den Testberichten, die auch in der App einsehbar sind, und dem Zugang zum Forum...

AppBrain



Auch bei AppBrain kann sich die Kombination aus Website und App durchaus sehen lassen.

Es gibt einen rudimentären Filter (leider nur mit den dort sichtbaren festen Kriterien, siehe rechtes Bild), man kann Apps nach Kategorien durchstöbern, und die Ergebnisliste sortieren. Ergänzt wird dies von einer Liste mit Empfehlungen, die anhand der bereits installierten Apps ermittelt werden. Hier kann man "ungewünschte Artikel" auch entfernen, und bekommt dann wieder neue Vorschläge.

Gut gelöst ist auch das Update: Egal, aus welcher Quelle eine App installiert wurde – sofern sie im *Play Store* enhalten ist, wird sie auch von *AppBrain* gefunden. Nach der Synchronisation der Liste von auf dem Androiden installierten Apps mit der im eigenen AppBrain-Konto (der Login dort erfolgt mit dem eigenen Google-Konto) einmal auf den Button "Perform Installs" gedrückt, und ab die Luzie! wird alles in einem Rutsch gemacht. Naja, fast – eine kleine Mogelpackung ist es naturgemäß, schließlich muss der Telefon-Besitzer ja noch die "Permissions" abnicken. Und das erfolgt dann lustigerweise wieder in der originalen Play Store-App...

Ein weiteres Plus dieser App: Einzelne Apps lassen sich vom Update ausschließen. Bei diesen erfolgt dann auch keine Benachrichtigung über verfügbare Updates mehr, ebenso werden sie beim gerade beschriebenen Sammel-Update nicht mehr angefasst. Auch können einzelne Updates einer App übersprungen werden – dann erfolgt eine neue Benachrichtigung für diese erst wieder beim nächsten Update. Beides Dinge, die man in Googles *Play Store* vergeblich sucht.

Und auch mit dieser App bekommt man die gewünschten Dinge auf den Androiden, die man mit der Play Store-App vielleicht nicht findet. Was natürlich nicht heißt, dass diese Apps dann auch funktionieren – denn eigentlich gibt es für das "nicht Finden" ja einen guten Grund, zumindest in der Theorie: Der Entwickler hat Kriterien (z. B. eine mindest-Bildschirm-Auflösung) angegeben, die das Gerät nicht erfüllt. Oder vergessen, eine Einschränkung aufzuheben...

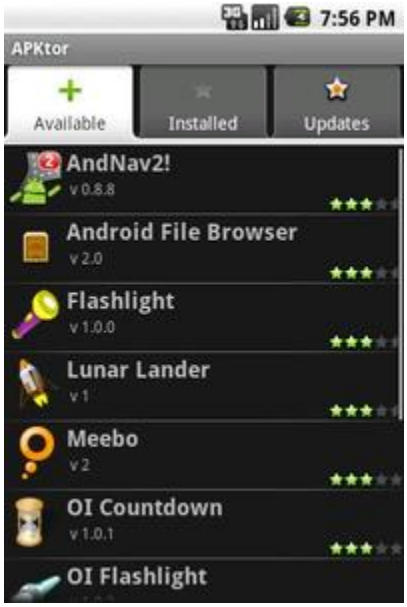
PDassi

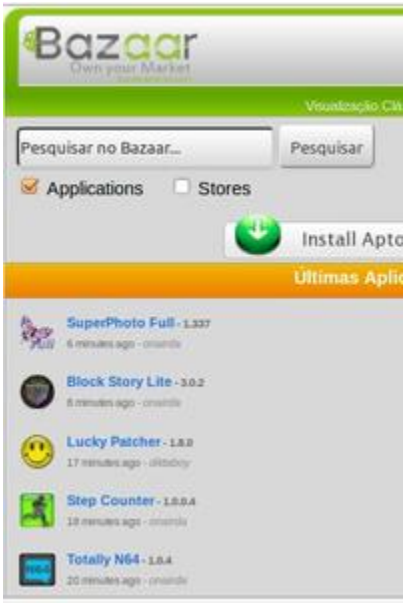
Der Vollständigkeit halber sei auch die App von PDassi an dieser Stelle kurz erwähnt. Diese bietet u. a. zusätzliche Bezahlmethoden wie z. B. Paypal, Bankeinzug oder Überweisung – für all jene, die entweder keine Kreditkarte haben oder diese nicht mit ihrem Google-Account verknüpfen möchten.

Öffentliche Märkte

Linux-Anwender kennen "Software Repositories": Diese halten Software-Pakete bereit (und pflegen Updates für selbige), welche die Entwickler selbst einstellen. Je nach Betreiber des jeweiligen Repositories sind Restriktionen für das Einstellen hier wenig bis gar nicht vorhanden. Der lesende Zugriff seitens der Anwender (für die Suche nach Software und deren Installation auf dem eigenen Rechner) ist entweder allen möglich ("public" bzw. "öffentliches" Repository), oder nur einem ausgewählten Personenkreis (z. B. firmenintern, oder für Produkt-bezogene Entwicklung).

Einer der bekanntesten Repository-Typen ist APT, das **A**dvanced **P**ackaging **T**ool – hauptsächlich bei Debian und dessen Derivaten im Einsatz. Gibt es aber auch für Androiden-Soft:





Mit Tools wie dem APKtor (linkes Bild) oder Bazaar News und Aptoide Install (rechtes Bild – der Name *Aptoide* ist ganz offensichtlich eine Kreuzung aus "APT" und "Androide") lässt sich auf derartige Repositories zugreifen. Da Tools zur Pflege solcher Repositories ebenfalls existieren (und zwar als OpenSource Anwendungen), steht auch dem eigenen Repository (etwa für Entwickler, oder auch Firmen) nichts im Wege.

Weitere

Ständig tauchen weitere Alternativen auf, die mehr oder weniger kurzlebig sind. Ein sicher langlebigerer Marktplatz dürfte der Amazon Appstore sein, in dem es auch ständig Sonderangebote gibt. Benötigt man einmal eine ältere Version einer App, hilft ein Blick in den Android Drawer: Hier finden sich `.apk` Dateien freier Apps sowohl in der aktuellen, als auch in historischen Versionen. Auch SlideMe ist kein Unbekannter in diesem Bereich.

Eine Übersicht alternativer Marktplätze findet sich bei AppDated.

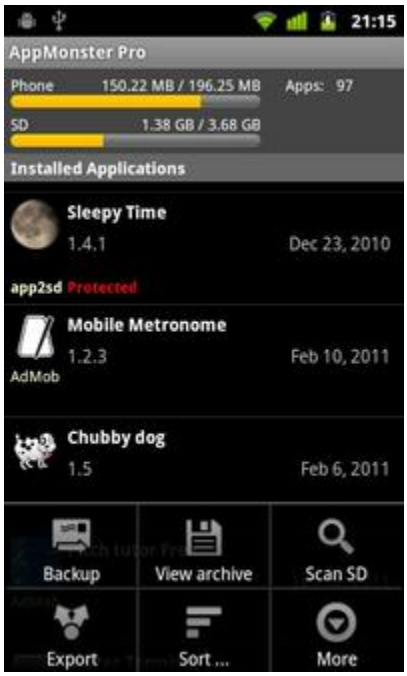
Alternative Verwaltung

So – jetzt haben wir alles mögliche installiert und in Gang gebracht. An dieser Stelle fragte schon Goethes Zauberlehrling:

Ach, da kommt der Meister!
Herr, die Not ist groß!
Die ich rief, die Geister,
Werd ich nun nicht los.

Wie bzw. wo also nun de-installieren? Die "Hausadresse" findet sich, wie bereits unter "Bordmittel" festgestellt, unter *Einstellungen → Anwendungen → Anwendungen verwalten* – ist aber keinesfalls die einzige Möglichkeit. So gut sie auch mittlerweile gelöst ist: Da gibt es einiges, was fehlt, oder sich besser machen ließe.

Höchste Zeit also für die Ghost Busters, Krümel- oder besser: AppMonster:



Wie am linken Screenshots unschwer zu erkennen, handelt es sich hier um einen vollwertigen Software-Manager. Für ca. drei Euro gibt es die Vollversion – nachdem man zunächst natürlich die gratis-Version ausgiebig testen kann. Einmal installiert, läuft die MonsterApp im Hintergrund (äh, nicht wirklich – genau genommen wird sie bei Bedarf vom Event-Manager aufgerufen; nämlich immer dann, wenn etwas neues installiert wurde). Wurde etwas neues installiert, schlägt das Monster zu – und macht sogleich ein Backup auf die SD-Karte. Kommt ein Update – schwupps, das gleiche. Wie, die neue Version tut nicht? AppMonster, hol mal die vorige raus! Kein Thema.

Whipe, Flash, neues ROM – na und? AppMonster installiert, "Batch Install" des aktuellen Backups – und schon sind alle Apps wieder da. Nagut, für die Daten braucht's dann schon ein richtiges Backup-Programm...

Was wollten wir eigentlich? Achso, loswerden wollten wir eine App – wie zu erwarten, findet sich dieser Punkt im jeweiligen Kontext-Menü (also lange auf den entsprechenden Eintrag "drücken"). Dazu muss die App natürlich erstmal aufgerufen werden – das dauert aber selbst unter Android 2.1 nicht einmal halb so lange wie beim "Bordmittel" (ab 2.2 ist die Ladezeit vergleichbar), da sich AppMonster ausschließlich für die vom Benutzer installierten Apps interessiert – und die anderen brav in Ruhe sanften lässt (oder so).

Fazit: AppMonster ist eine App, die auf keinem Androiden fehlen sollte. Eigentlich sollten die "Distributoren" diese App bereits vorinstalliert mit ihren Geräten ausliefern!

Alternative UnInstaller

Neben den "vollwertigen Software-Verwaltern" gibt es dann auch noch die für das schnelle "Iiiih – weg damit!" bei denjenigen, die täglich mehrere Apps "durchspielen". Als Beispiele seien da Fast Uninstaller und Shake - Uninstall genannt:

Beim *Fast Uninstaller* geht es um die schnelle De-Installation: Antippen – und weg ist die App. Klingt mir für meine Begriffe ein wenig riskant (hab es selbst nicht ausprobiert), tippt man mit seinen "Wurst-Fingern" doch schnell mal daneben. Sympatischer klingt mir da schon *Shake - Uninstall*: Das ist doch mal ein interessantes Konzept: Man aktiviert diesen Service – und dann schaut man sich all die Apps an, wo's einen ohnehin schüttelt. Fazit: Das Gerät ist anschließend gut aufgeräumt Interessant wird es nur, wenn man seinen Homescreen verbockt hat – was wohl passiert, wenn es einen da schüttelt?

Apps aus "alternativen Quellen"

Die Voreinstellung eines Android-Smartphones besagt: "Du sollst keine anderen Quellen haben neben mir". Und "mir" meint natürlich den *Play Store*. Dahinter steht der Sicherheits-Gedanke: Apps sollten nur aus vertrauenswürdigen Quellen installiert werden. Und die einzige derartige, die Google kennt, ist nun einmal Google.

Hin und wieder will/muss man aber mal eine App aus "alternativen Quellen" installieren: Sei es, dass einem der Entwickler was zum "testen" zugeschickt hat ("Schau mal, ob das Dein Problem löst!"), oder eine App mit dem Browser heruntergeladen wurde, da das Android-Gerät es im *Play Store* nicht findet – oder, oder, oder... OK, die `*.apk`-Datei haben wir nun – aber wie die App installieren?

Klar kann man das `*.apk` einfach in den passenden Ordner von *AppMonster* (siehe oben unter "Alternative Verwaltung") packen, und es dann damit installieren. Einfacher machen es zahlreiche Datei-Manager, die dann beim Antippen einer solchen Datei den Installer aufrufen. Zu den beliebtesten Kandidaten hier zählen Astro Dateimanager und ES Dateimanager – beide gut erweiterbar, und z. B. auch für den Zugriff auf lokale Netzwerke via FTP oder Windows-Freigaben (AKA "SMB") geeignet.

Welche dieser Möglichkeiten man aber auch verwenden will: Immer kommt der Hinweis "Du darfst hier nicht rein!" – denn zuerst muss die Installation aus "Fremdquellen" generell einmal erlaubt werden. Mit einem kleinen Häkchen an der richtigen Stelle. Dieses findet sich unter *Einstellungen* → *Anwendungen*, und ist dort mit "Unbekannte Quellen" beschriftet.

Apps organisieren

Jetzt sind jede Menge Apps installiert und die Frage drängt sich auf: Wie soll man da den Durchblick behalten? Öffnet man den "Drawer" (also die Liste der auf dem Gerät verfügbaren Apps), ist die Liste recht lang. Und nicht unbedingt übersichtlich. Alle 87 Apps (oder wieviel auch immer) teilweise ohne jede erkennbare Ordnung (oder im besten Falle alphabetisch sortiert) in einem Ordner.

Zwanzig mal hin-und-her scrollen auf der Suche nach der zu startenden App ist nicht jedermanns Sache. Wie leicht passiert es, dass man ein wenig "zu kräftig schubbst" – und schon scrollt die Liste in einem Wahnsinns-Speed vorbei. Oder man schubbst "zu langsam" – und das dumme Teil meint, die gerade unter dem Daumen befindliche App starten zu müssen... Und das "vollklatschen" aller Desktops mit Icons für jedes App ist auch nicht unbedingt die wahre Lösung. Was also tun?

Bordmittel

Bei aktuellen Android-Versionen (spätestens ab Version 4.0 aka Ice Cream Sandwich) bietet bereits der Standard-Launcher die Möglichkeit, auf dem Homescreen Ordner anzulegen – und auf diese Weise häufig genutzte Apps für den schnellen Zugriff zu gruppieren. Wem dies nicht genügt, der greift zu einem alternativen Launcher: Einige dieser Kandidaten verfügen über erweiterte Möglichkeiten, und lassen etwa Ordner auf der Schnellstart-Leiste ablegen, oder erlauben sie auch im App-Drawer.

Apps Organizer und *Folder Organizer*

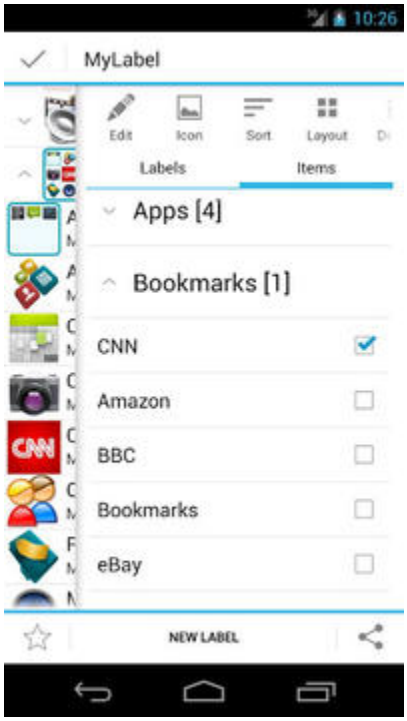
Zwei hilfreiche Kandidaten sind Apps Organizer und Folder Organizer.

Beim Start von *Apps Organizer* scannt dieser zunächst alle installierten Apps, was ein paar Sekunden dauert. Anschließend kann man jeder App ein oder mehrere Label zuweisen. Nun ist es möglich, die Apps nach diesen Labels zu

browsen (linkes Bild). Schon Mal ein Fortschritt – die zu durchsuchende Liste wird kürzer.

Aber das ist natürlich noch nicht alles – denn die App bietet auch passende Widgets (den Umgang mit diesen zeige ich noch ausführlich im Abschnitt Home-Screen & Widgets). Für jedes der erstellten Labels sowie für "Favoriten" (Apps können hier als solche definiert werden) lässt sich auf diese Art ein Icon auf den Home-Screens platzieren. Tippt man dieses an, öffnet sich ein Fenster, welches die zugehörigen Apps auflistet (siehe rechtes Bild). Je nach Bildschirmgröße (und -auflösung) sowie Anzahl der Apps mit dem zugehörigen Label ist nun oftmals gar kein Scrollen mehr nötig: Der Start einer App klappt jetzt also mit nur zwei Tapps! Na, das ist doch was!

Ganz ähnlich sieht es übrigens bei *Folder Organizer* aus (diese beiden Apps sind sich halt sehr ähnlich), der zusätzlich auch noch Transparenz und einiges anderes unterstützt:



Folder Organizer bezeichnet sich selbst als "the evolution of Apps Organizer". Es kann alles das, was Apps Organizer auch kann – und mehr: Nicht nur Apps können hier mit Labeln versehen werden, sondern auch Lesezeichen, Kontakte und "Shortcuts" (z. B. zu Systemeinstellungen). Wie bei *Apps Organizer* werden ebenso Iconsets unterstützt, um die Folder mit den passenden Bildchen zu versehen.

Diese zusätzlichen Funktionen wollen dann aber auch entsprechende "Permissions" bekommen: So fordert die App u. a. Kontaktdaten lesen, Kontaktdaten schreiben, und Telefonnummern direkt anrufen.

Weitere Kandidaten

Natürlich gibt es noch eine ganze Reihe weiterer Kandidaten – die sich jedoch im Groben und Ganzen letztendlich weitgehend mit einer der beiden gerade vorgestellten Apps vergleichen lassen. In meinem zugehörigen Thread bei AndroidPIT (Apps Organisieren) stelle ich diese näher vor. Außerdem bieten einige „alternative Launcher" (siehe Home Replacements) von Haus aus die Möglichkeit, Ordner direkt im „App-Drawer" oder auf dem Homescreen anzulegen, wie bereits erwähnt.

Bekannte Probleme

Einige der genannten Apps zeigen vielleicht das Problem, dass hin und wieder Icons vom Home-Screen verschwinden – oder unbrauchbar werden. In der Regel hat der Anwender dann ein HTC-Gerät, und verwendet die "Sense" Oberfläche – die sich leider nicht so ganz an die Android-Standards bei Widgets hält. Ob sich das umgehen lässt, bereits Lösungen existieren, oder HTC eventuell nachgebessert hat, weiß ich nicht zu sagen; hier hilft nur, im Forum zu fragen bzw. bei den Entwicklern und/oder HTC nachzuhaken.

Eine weitere mögliche Fehlerursache wäre, dass der Anwender die zum Widget gehörige App auf der (externen) SD-Karte installiert hat. Das sollte das System eigentlich unterbinden – doch schlau, wie der Anwender ist, hat er ja vielleicht einen Weg gefunden, das System auszutricksen. Auf der SD-Karte installierte Apps werden jedoch nicht informiert, wenn der Boot-Vorgang abgeschlossen ist (da die SD-Karte erst danach ins System eingebunden wird); somit können sie auch die von den Widgets benötigten Dienste nicht rechtzeitig bereitstellen. In diesem Fall hilft es, die betroffene App einfach wieder zurück in den internen Speicher zu verschieben (siehe Apps auslagern).

Datensicherung

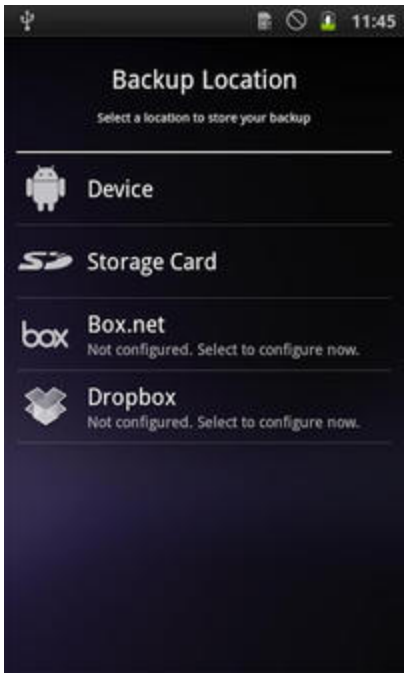
Jetzt ist klar, wie die Apps auf den Androiden (und auch wieder von selbigem herunter) kommen, wie man sie verwaltet und organisiert. Natürlich würde es völlig den Rahmen sprengen, die Funktionsweise aller möglichen Apps hier zu erklären – aber einen wichtigen Punkt gibt es noch: Backups. Vielleicht muss das Android-Gerät ja irgendwann auf Werkseinstellungen zurückgesetzt werden, ein neues Android-Gerät kommt ins Haus, oder ein Update "zerschießt" etwas! Die Apps lassen sich zur Not von Hand wieder zusammensuchen. Aber warum umständlich, wenn es auch einfacher geht? Darüber hinaus ist es gut zu wissen, dass die Daten dann wieder zur Hand sind – denn die lassen sich nicht so leicht wieder "irgendwo auftreiben".

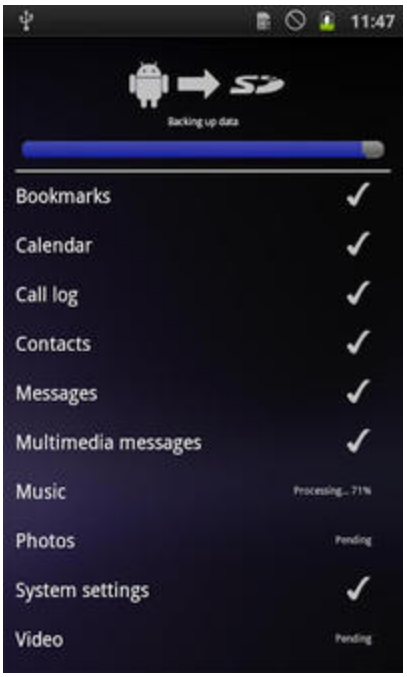
AppMonster habe ich ja bereits unter Anwendungen verwalten kurz vorgestellt: Es sichert bei jeder Installation (und jedem Update) die jeweilige App. So lässt sich nicht nur zu einer beliebigen, bereits zuvor einmal installierten, Version einer App zurückkehren – sondern auch auf einen Rutsch die jeweils aktuelle Version jeder zuvor installierten App aufspielen. Dies macht zum Beispiel bei einem Gerätewechsel, aber ebenso nach einem Werksreset viel Sinn – vor allem, wenn nicht alle Apps direkt über den *Google Play Store* installiert wurden. In diesem Falle ginge das nämlich auch über die Play Store-App – allerdings nur, solange die App auch noch im Play Store verfügbar ist.

Was aber ist mit Anwendungs-Daten? Was ist mit den Kurznachrichten, Telefonbüchern, und so weiter? Die Kontakte lassen sich noch aus der gleichnamigen App (*Menü→Importieren/Exportieren*) sichern bzw. wieder herstellen. Oder sie werden mit dem Google-Konto synchronisiert, was auch mit den Kalender-Einträgen geht. Was aber nicht unbedingt jeder will. Für alles andere steht gar kein Bordmittel bereit (warum eigentlich nicht?). Aber auch hier gibt es Abhilfe:

Allgemeine Backups

Wirklich *alles* vollständig sichern – das klappt mal wieder nur mit "root". Die Killer-App hierfür heißt Titanium Backup, und ich werde im Abschnitt Fortgeschrittenes (Kapitel Vorinstallierte Apps entfernen) näher auf sie eingehen – denn diese App setzt "root" voraus. Doch auch für nicht gerootete Androiden gibt es durchaus brauchbare Lösungen.





Wie zum Beispiel Sprite Backup (beide Bilder, Kosten: Knapp 4 Euro). Die App verspricht eine vollständige Sicherung – und interessanterweise ist hier nirgendwo etwas von root zu lesen; um App-Daten wird sich offensichtlich aber auch nicht gekümmert. Sicherungen können wahlweise auf der SD-Karte – oder aber auf externen Rechnern (z. B. via FTP) abgelegt werden. Auch Dropbox-Accounts lassen sich nutzen.

Diese beiden (und einige weitere) Apps sind somit grundlegende Lösungen, die die meisten Sachen abdecken sollten. Etwas derartiges gehört eigentlich auf jedes Android-Gerät – erstaunlich, dass es dort nicht bereits vorinstalliert ist.

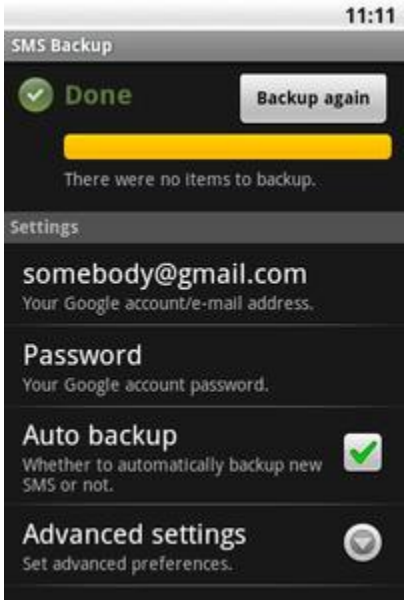
Daten-Backups auf die SD-Karte

Wer dedizierte Lösungen für spezielle Daten sucht, und letztere nicht irgendwo im Netz ablegen möchte, findet hier zahlreiche Lösungen. So lassen sich etwa Kurznachrichten (SMS) mit SMS Backup & Restore, TxtArchive SMS Backup, sowie TxtractLite MMS & SMS Backup (letztere unterstützt auch MMS) auf die SD-Karte sichern. Für Anruflisten tun dies z. B. Call Logs Backup & Restore und Backup Call History.

Um die Kontakte kümmert sich zum einen die Kontakte-App selbst (über *Menü→Importieren/Exportieren*), und zum anderen z. B. UiA – Backup Contacts, Lesezeichen können mit Bookmark Sort & Backup & Co. gesichert werden. Und dann gibt es noch diverse Kombi-Lösungen, die sich wie z. B. Mobile Backup II um Kalender, Kontakte, SMS, und Anruflisten kümmern.

Ausführlichere Infos dazu finden sich in diesem Forums-Beitrag.

Online-Backups



"Das Wetter. Heute ist es bewölkt." So in etwa begrüßte mich mein Androiden-Wecker (Alarm Droid) heute morgen. Und ja: Jetzt geht es um "Backups in die Cloud". Das heißt zum Einen: Die Daten sind fast immer von überall erreichbar. Zum Anderen heißt es aber auch: Sie landen auf fremden Servern. Abwägen muss das jeder für sich selbst.

Da wäre zunächst SMS Backup (Bild links) zu nennen, das Kurznachrichten in IMAP-Ordnern bei Google Mail ablegt – was für viele die "Vertrauensfrage" sicher bereits beantwortet. Voraussetzung dafür ist natürlich, dass IMAP dort aktiviert ist – was man vom PC aus erledigen kann. Sodann sind ebenso automatische Backups möglich. Auch SMS Backup + tut dies – nutzt aber zusätzlich den Google Kalender als Datenablage, und kümmert sich außerdem gleich mit um MMS und Anruf-Listen. Doch während sich derart gesicherte SMS auch wieder auf dem Androiden herstellen lassen, wird dies für MMS und Anruflisten (derzeit noch) nicht unterstützt.

Backups für spezielle Apps

Jaaa – und dann wären da noch die besonderen Spezialitäten. Böse, böse. Böse Vögel zum Beispiel: Hier lassen sich mit AngryBirds Backup die Daten sichern und wieder herstellen – und zwar sowohl für Angry Birds Original, Seasons, Rio, Space als auch Star Wars. Leider hat diese App (wie auch die Alternativen) derzeit Probleme mit der aktuellen Android-Version Jelly Bean.

Für Freunde des sozialen Netzwerkelns gibt es u. a. Photos Backup from Facebook (auch als gratis Trial oder, für ein paar Taler mehr, als ausgewachsene "Pro" Version). Damit läuft das Backup jedoch anders herum: Facebook-Bilder werden auf die SD-Karte geladen.

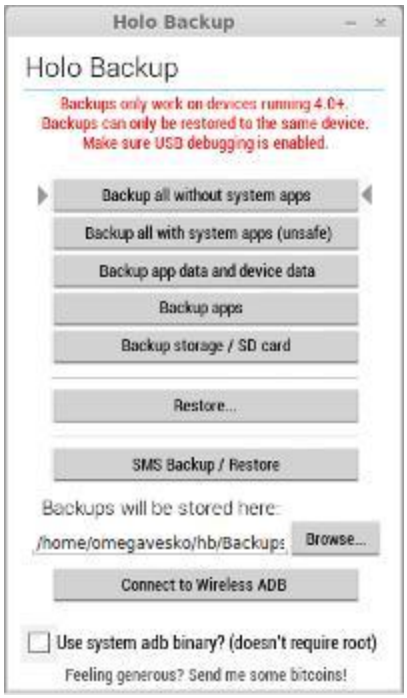
Als ganz nützlich bei einem anstehenden Wipe kann sich APN Backup & Restore erweisen. Diese App kümmert sich um die mobilen Internet- und MMS Zugänge. Also vor dem Wipe sichern, danach wieder herstellen. Statt alles wieder von Hand einzutippen.

Vollständiges Backup ohne root

Ein vollständiges Backup ohne root-Rechte ist erst ab Android 4.0 möglich – wo es still und heimlich über ADB-Daemon aktiviert wurde, ohne dass man groß darüber sprach: Aktiviert man in den Entwickler-Einstellungen das USB-Debugging, wird auf dem Android-Gerät der ADB Daemon gestartet, sodass er u. a. auch von einem auf dem PC installierten ADB Client angesprochen werden kann. Das war schon in früheren Android-Versionen der Fall – ab Android 4.0 jedoch erhielt der Daemon erweiterte Rechte. So lässt sich nun über den Befehl `adb backup` die Erstellung eines Backups anfordern, und zwar sowohl für einzelne Apps einschließlich ihrer Daten, oder auch für das gesamte System. Das Backup-Archiv wird dann an den Client übergeben, und kann so auf dem PC gespeichert werden.

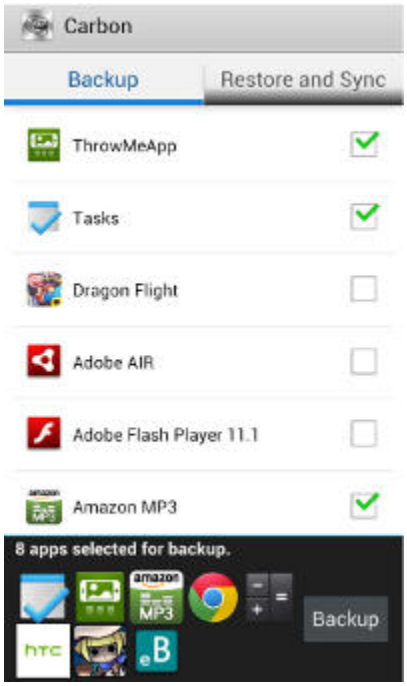
Details dazu finden sich etwa in einem Artikel bei StackExchange. Da der dort beschriebene Weg für Einsteiger etwas umständlich sein dürfte (es muss das Android-SDK installiert sein, und es wird die Bedienung der Kommandozeile vorausgesetzt), haben sich glücklicherweise ein paar Entwickler gefunden, und für einfachere Möglichkeiten gesorgt. Um auf diese Funktionalitäten ohne viel Umstand zugreifen zu können, stellen sie grafische FrontEnds bereit – die teilweise auch im genannten Artikel erwähnt werden. Eine davon möchte ich an dieser Stelle herausgreifen:

XDA-Developer omegavesko hat ein einfaches Programm erstellt, das den Backup-Vorgang (und natürlich auch die Wiederherstellung) gerade für Unerfahrene ermöglichen sollte. Holo Backup gibt es für Linux und Windows gratis im Forum der XDA-Developer zum Download.



Die Bedienung sollte eigentlich selbsterklärend sein – es ist ja alles beschriftet. Was beim Backup allerdings zu beachten ist: Man kann sich aus dem erstellten Backup nicht einzelne Dinge zur Wiederherstellung heraussuchen, es ist immer ein Alles-oder-Nichts. Also ggf. besser zusätzlich zum "vollständigen Backup" auch noch das eine oder andere kleinere Päckchen schnüren, etwa die wichtigsten Apps inklusive ihrer Daten jeweils separat.

Nachdem man in *Holo Backup* (oder auch von der Kommandozeile) ein Backup oder eine Wiederherstellung angestoßen hat, muss man diesen Vorgang noch auf dem Gerät selbst bestätigen. Dies dient als Sicherheits-Maßnahme, damit nicht etwa ein Unbefugter eben schnell ein Kabel anschließt, um sich die Daten herunter zu laden. Vor dem Bestätigen des Vorgangs lässt sich auch ein Passwort für die Verschlüsselung festlegen. Dieses Passwort sollte man sich gut merken: Ein verschlüsseltes Backup lässt sich nur mit dem vergebenen Passwort wiederherstellen.



Obwohl die Möglichkeit zur vollständigen Sicherung über ADB bereits ein großer Fortschritt gegenüber, ähm, gar keinem Backup ist, hat sie immer noch einen Haken: Sie benötigt einen PC. Unterwegs im Urlaub, oder auf einer Geschäftsreise, könnte sich das schwierig gestalten. Da dürfte es einige Herzen höher schlagen lassen zu lesen, dass Koushik Dutta aka Koush aka Mr. ClockworkMod wieder zuschlägt. Er arbeitet nämlich an einer App, die ein vollständiges Backup ohne root ermöglichen soll (siehe Bild)!

Vergleichbar mit dem beliebten *Titanium Backup* (welches root voraussetzt), sichert seine Helium Backup genannte App sowohl Apps als auch deren Daten – unabhängig von einem etwa angeschlossenen PC. Die Backups können auf der SD-Karte abgelegt, oder aber auch auf einen Server hochgeladen werden. Unterstützt werden dafür u. a. Cloud-Services wie GoogleDrive oder Dropbox.

Erwirbt man für knapp vier Euro die Lizenz zur Pro-Version, erhält man noch einige Extras: Keine Werbung mehr in der App, sowie eine Synchronisation von Apps zwischen mehreren Geräten sind damit jetzt bereits möglich. Ein Scheduler für zeitgesteuerte Backups soll in Kürze folgen.

Wer zum Start gern eine Kurzanleitung hätte, findet diese übrigens in einem Blog-Beitrag bei AndroidPIT.

Zurücksetzen

Zurück auf LOS! Was ist los? Wo ist LOS? Und was, bitte, wohin zurücksetzen?

Den "älteren Semestern" unter uns ist sicher die "Reset"-Taste am PC noch ein Begriff. So als Reißleine, Notbremse, letzte Ausflucht, wenn nichts mehr geht. Auch das ist eine Form von "Zurücksetzen". Unter Android gibt es da mehrere Rücksetz-Möglichkeiten, mit zum Teil recht unterschiedlichen Auswirkungen. Und daher auch recht unterschiedlichen Verwendungszwecken...

Softreset

Dieses "weiche zurücksetzen" lässt sich am ehesten mit dem "Affengriff" unter Windows (Strg-Alt-Delete) vergleichen. Nur dass die Tastenkombination, je nach Gerät, noch wesentlich abenteuerlicher ist. Bei HTC-Geräten z. B. üblicherweise das gleichzeitige Drücken der *Leiser*-Taste, der *Action*-Taste (Trackball), und des Einschaltknopfes. Möglichst ohne das Gerät dabei fallenzulassen...

Bewirken soll das Ganze dann ein "sanftes" Herunterfahren des Systems – üblicherweise wenn gar nichts anderes mehr funktioniert (sonst könnte man ja auch normal über das Menü abschalten).

Hardreset

In seltenen Fällen kann es vorkommen, dass das Android-Gerät komplett einfriert, und sich überhaupt nicht mehr bedienen lässt: Nichts reagiert mehr. Auch zu einem Softreset lässt es sich nicht mehr bewegen. Da hilft dann nur noch die harte Methode: Akku entfernen, bzw. bei Geräten mit fest verbautem Akku mit einem spitzen Gegenstand das Reset-Löchlein anpieksen...

Factory-Reset

Hierbei handelt es sich um das "Zurücksetzen auf Werkseinstellungen", was sich zum Beispiel über den genau so benannten Punkt unter *Einstellungen→Datenschutzeinstellungen* erreichen lässt. Dabei werden alle vom Anwender installierten Apps sowie sämtliche Einstellungen gelöscht – das Gerät ist somit wieder in einem "jungfräulichen" Zustand (abgesehen von der internen/ externen SD-Karte, die hier i. d. R. nicht angefasst wird).

Wird es anschließend wieder angeschaltet, muss mit der Einrichtung ganz am Anfang begonnen werden – genau so, als hätte man das Gerät gerade zum ersten Mal aus der Originalverpackung geholt. Das ist auch einer der Gründe, für den diese Funktionalität benötigt wird: Wenn das Gerät verkauft/verschenkt/ weitergegeben werden soll. Natürlich möglichst ohne private Datenspuren darauf zu hinterlassen.

A propos Datenspuren: Die verbleiben oftmals trotz eines "Factory-Reset". Zumindest etwas versiertere Anwender könnten gelöschte Daten wieder herstellen. Wer also ganz auf "Nummer Sicher" gehen möchte, nutzt eine App, die gründlich putzt. Die passenden Kandidaten finden sich natürlich wieder einmal in einer Übersicht bei AndroidPIT – ein sicherer Kandidat wäre jedoch Nuke My

Phone, welches zwar knapp einen Euro kostet, aber absolut Spitze bewertet ist. Wie das Ganze funktioniert? Statt die Daten einfach nur zu löschen, wird alles mit Zufalls-Daten überschrieben. Ein etwaiger Schnüffler findet dann nur noch Kauderwelsch...

Außerdem ist der "Factory-Reset" auch noch ein "Last Resort", wenn der Androide komplett verrückt spielt. Der Hersteller verlangt dies meist, um Probleme mit der Hardware ausschließen zu können: Löst ein *Werksreset* das Problem, ist die Hardware nämlich ganz offensichtlich unschuldig – es hat sich nur die Konfiguration verdreht.

Bevor man zu diesem Schritt greift, kann man noch folgendes versuchen:

Wipe des Dalvik-Cache

Dieser erzwingt die Neu-Übersetzung des Programmcodes aller installierten Apps (siehe Dalvik bei den Begriffs-Erklärungen). Das wäre ein Schritt, den man bei nicht behebbarem "ungewöhnlichen Verhalten" des Systems noch durchführen kann, ohne das ganze Gerät komplett auf Werkseinstellungen zurückzusetzen. Voraussetzung dafür ist allerdings, dass das Gerät gerootet ist – die Hersteller haben diese Möglichkeit von Haus aus leider nicht vorgesehen.

Android-Apps sind in Java geschrieben, und Java ist bekanntlich Plattform-unabhängig. Vereinfacht ausgedrückt, ist das ein Zwischending zwischen einem Skript wie einer Batch-Datei oder einem PHP-Skript, und einem kompilierten Programm. Vor der eigentlichen Ausführung muss da also noch eine Übersetzung in Maschinensprache stattfinden, die möglichst nah am verwendeten System ist. Bei Java nennt man dies "Byte-Code". Um die schmalen Ressourcen von mobilen Android-Geräten noch schonender zu nutzen, geht man bei Dalvik-VMs (so nennt sich die spezielle "Java-Variante" unter Android) noch einen Schritt weiter, und nutzt zusätzliche Optimierungs-Möglichkeiten.

Damit dies nun nicht bei jedem Aufruf einer App geschehen muss (das wäre unerträglich langsam), macht Android das unmittelbar nach der Installation einer App – und legt den optimierten "Byte-Code" im sogenannten Dalvik-Cache ab. Wird dieser gelöscht, erzwingt dies lediglich eine Neu-Übersetzung (sagte ich ja schon) – die Anwendungsdaten und Einstellungen bleiben jedoch vollständig erhalten.

Dieser Schritt ist definitiv zu empfehlen, wenn ein (neues/anderes) Custom-ROM eingespielt werden soll. Bei "offiziellen Updates" sollte sich der Hersteller darum kümmern, sofern dies nötig ist.

Von Taskkillern und anderen bösen Buben

Oh ja, ich höre schon die Schreie: "Taskkiller gehören verboten! Android kann das selbst!". Und gleich aus der Gegenrichtung: "Taskkiller muss man haben, mein System läuft jetzt viel flüssiger!".

Wer hat nun Recht? Beide. Keiner. Denn hier gibt es kein einfaches Schwarz und Weiß. Sicher ist jedoch: Wer nicht weiß, wie man eine Spritze setzt, sollte sich

nicht als Arzt ausgeben – das kann sonst gehörig in die Hose gehen. Ein guter Arzt weiß jedoch die genannte Spritze so einzusetzen, dass sie dem Patienten hilft.

Man sollte also schon genau wissen, was man tut – und Taskkiller, Autostart-Helfer, & Co. können sehr nützlich sein. Wer dies nicht weiß, lässt besser die Finger weg!

Kurz zusammengefasst (ausführliche Erläuterungen finden sich, wie gewohnt, in einem Forums-Thread): Hier handelt es sich um ein sehr kontrovers diskutiertes Thema. Worin mir allerdings (fast) jeder zustimmen dürfte: Eingriffe ins System setzen eine gute Kenntnis desselben voraus.

Es ist korrekt, dass Android sich um die Speicherverwaltung selber kümmert. Dennoch haben Task-Manager / Task-Killer durchaus ihre Berechtigung – solange man weiß, was man da tut:

- Falsch: "ich will den Speicher freiräumen". Dafür ist der "OOM Killer" (direkt im Android-System integriert, näheres dazu im Tuning-Kapitel) zuständig.
- Richtig: "eine App hat sich aufgehängt, und blockiert [irgendwas]". Hier ist der Task-Killer angesagt – weil bis der "OOM-Killer" hier zuschlagen würde... Und ein Reboot ist nicht gerade die wünschenswerte Alternative.
- Richtig: "eine App läuft Amok" (Panik-Mode: Man erwischt gerade eine App dabei, wie sie alle persönlichen Daten inkl. Nackt-Fotos auf eine berüchtigte Website hochlädt...). Ohja: Abschießen! Oder gleich abschalten. Weil: Bis der OOM-Killer... genau, da ist es dann eh zu spät...

Datenaustausch mit dem PC

Alles klar: USB-Kabel anschließen, und die Karte wird am PC freigegeben. Weiß doch jeder. – Ja, schon. Aber zum einen ist das umständlich, zum zweiten ist laut Murphy genau dann kein Kabel zur Hand, wenn man es bräuchte, und zum dritten ist das ja sowas von uncool und unzeitgemäß... Kurzum: Es gibt weit bequemeres, ohne Kabel. Wobei man dem Kabel natürlich zugute halten muss: Sichere Übertragung, und braucht keine Zusatz-Software...

Warum nicht auf dem Androiden Freigaben erstellen, und diese via WLAN nutzen? Sowas geht doch sogar unter Windows! Und was ist mit Android? Ja, auch bei Android. Auch da geht das. Einfach und ressourcenschonend als FTP-Server z. B. mit FTP Server (Bild links): Das Installationspaket unter Android bringt keine 80kB auf die Waage, und der Zugriff funktioniert unter Windows, MacOS und Linux gleichermaßen einfach: Browser öffnen, und die auf dem Android-Screen angezeigte URL eintippen. Schon lässt sich durch das Dateisystem navigieren. Tipp: Unter Windows in die Maske bei *Start→Ausführen*, bzw. unter Linux bei "Alt-F2" eingeben, das öffnet den Service dann im Explorer bzw. in Konqueror (KDE3) oder Dolphin (KDE4). Und wem das alles nicht zusagt, der greift auf dem PC halt zu Drittanbieter-Anwendungen wie z. B. Filezilla. Sofern es der Provider unterstützt, lässt sich mit *FTP Server* sogar über das mobile Datennetz der Dienst bereitstellen.

Zu spartanisch? Wer es lieber grafisch mag, und auch Fotos und Videos, sowie die Musiksammlung anhand von Covern verwalten möchte, der kann auch zu WebSharing greifen. Bezahlt wird dieser zusätzliche Komfort nicht zuletzt in Kilo- oder besser Megabyte, und derer gleich zwei – so groß ist nämlich diese App. Da liegen Welten dazwischen.

Auch "echte" Windows-Freigaben sind, z. B. mit Samba Filesharing oder Samba Server möglich. Nicht zu vergessen WebDAV mittels DavDrive vom Macher des im nächsten Kapitel beschriebenen *PAW Server*. Einzelheiten dazu können dem zugehörigen Forums-Thread entnommen werden.

Weitere Möglichkeiten zum Datenaustausch finden sich jedoch auch gleich im folgenden Kapitel, und ebenfalls bei den Datei-Managern.

Das Android-Gerät vom PC aus verwalten

Auch die zierlichsten Frauenhände stoßen auf dem Androiden schnell an ihre Grenzen – und so richtig Spaß macht das auf den kleinen Bildschirmen dann nicht wirklich. Abgesehen davon, dass man immer erst suchen muss: Wo war diese Option doch jetzt gleich noch? Und oftmals schmerzlich eine "richtige Tastatur" vermisst. War da noch was? Genau, Inhalte sollen ja ebenfalls noch von A nach B und umgekehrt, also zwischen PC und "dem Kleinen" ausgetauscht werden...

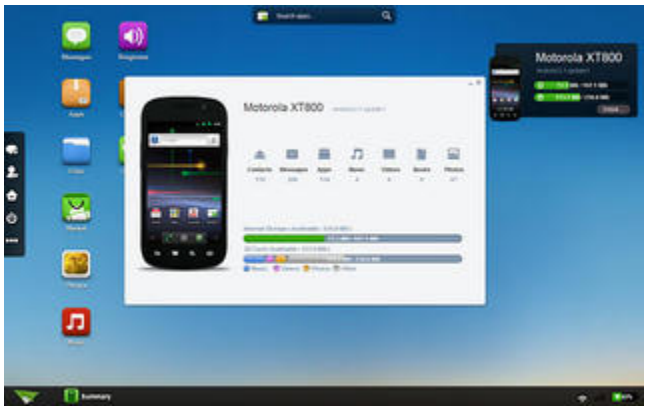
Die beliebteste Lösung für dieses Problem heißt MyPhoneExplorer – benötigt aber auf PC-Seite ein Windows-Programm, und ist somit nur für Windows verfügbar. Hier Vorgestelltes sollte aber möglichst für alle Anwender eine Option sein. Also greife ich nicht zum Nächstbesten, sondern zum Nächsten und Besten:

PAW Server ist unabhängig von jedweder Plattform, was den PC betrifft. Auf selbigem wird nur ein Web-Browser benötigt – alles andere erledigt die App unter Android, wobei der Androide über WLAN bereitgestellt wird. *PAW* lässt sich dabei sehr sicher konfigurieren: Nicht nur, dass sich ein gutes Passwort wählen lässt – auch das sicherere HTTPS-Protokoll steht hier zur Verfügung. So kann man durchaus erwägen, im Bedarfsfall eine Portfreigabe am Internet-Router zu erstellen, um sich z. B. von einem Fachmann helfen zu lassen. Auf der anderen Seite ist es auch kein Problem, bei Freunden/ Verwandten auf diese Weise auf seinen Liebling zuzugreifen: Es wird ja keine Zusatz-Software benötigt.

Wie auch beim eingangs genannten MyPhoneExplorer, lassen sich mit *PAW Server* Anruflisten, SMS, Kontakte etc. einsehen, Anrufe initialisieren, SMS schreiben... Und wenn der Hund sich "den Knochen" geschnappt und verschleppt hat, selbigen per Knopfdruck zum Klingeln bringen (den "Knochen", nicht den Hund!) um festzustellen, wo beide denn nun abgeblieben sind. Vorausgesetzt natürlich, die beiden haben beim Spielen nicht das WLAN-Signal verloren...

Natürlich ist auch ein Dateimanager enthalten. Fotos lassen sich ebenfalls durchstöbern (auf Wunsch sogar eines davon als neues Hintergrundbild festlegen), der Androide als Diktier- oder Vorlesegerät, Musik-Player oder auch WebCam nutzen, und vieles mehr.

Programmierern stehen darüber hinaus auch zahlreiche Schnittstellen zur Verfügung, mit denen sich die Funktionalität erweitern lässt – und umgekehrt können sie auch ihre Apps um Funktionalitäten des *PAW Server*s anreichern.



Der *PAW Server* ist also eine gute Wahl. Die beliebteste App zur Fernverwaltung des Androiden dürfte derzeit jedoch AirDroid sein. Der Funktionsumfang kann sich absolut sehen lassen: Man erhält volles Desktop-Feeling im Browser. Einschließlich der Möglichkeit, seine Kontakte zu verwalten, Nachrichten zu verschicken, Fotos und Videos zu betrachten, Klingeltöne zu konfigurieren, und mehr. Ein Dateibrowser ist auch hier mit dabei, die auf dem Androiden installierten Apps lassen sich ebenfalls verwalten. Sogar die Zwischenablage kann man mit dem PC teilen.

Natürlich ist die Verbindung bei *AirDroid* mit einem Passwort geschützt. Will man dieses nicht manuell abtippen, kann wahlweise auch der generierte QR-Code eingescannt werden. Auf Wunsch lässt sich auch die Verbindung selbst mit https verschlüsseln.

Wer sich vor einer Entscheidung noch mögliche Alternativen anschauen möchte, findet dazu – wie immer – auch einen passenden Thread im Forum.

Datenaustausch zwischen Android-Geräten

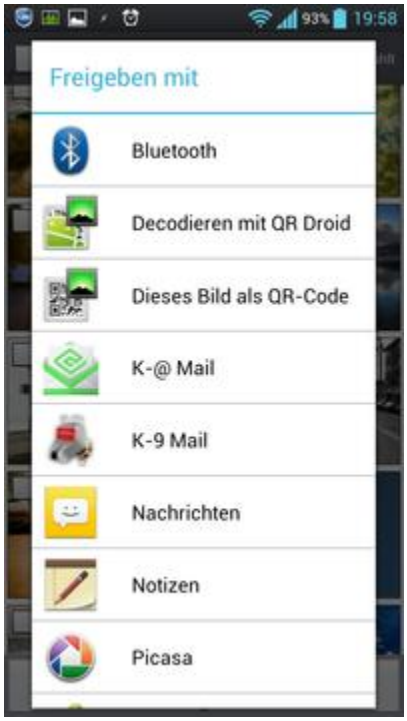
Sicher greifen hier einige der bereits vorgestellten Möglichkeiten. Und natürlich kann man Daten auch per Anhang an Mails/MMS oder über entsprechende Speicherplätze in der Cloud (wie z. B. Dropbox) austauschen. Aber das kann ja wohl nicht alles sein! Irgendwie muss sich doch auch ein direkter Datenaustausch zwischen zwei Android-Geräten erreichen lassen?

Aber sicher doch. Und einige der dafür vorhandenen Varianten wollen wir im Folgenden betrachten:

Bluetooth

Den Bluetooth-Standard gibt es bereits seit den 1990er Jahren. Verwendet wird er u. a. für schnurlose Tastaturen, Kopfhörer, Headsets, GPS-Mäuse, und mehr – aber auch zur Übertragung von Daten über kurze Instanzen. Und so konnten schon recht früh Visitenkarten und Dateien von einem Gerät zu einem anderen gesendet werden. Besonders schnell geht das Ganze nicht vonstatten: Anfangs waren es rund 100 "theoretische" Kilobit (also in der Praxis etwa 10 Kilobyte pro Sekunde), mit Bluetooth 2.0 ging es dann bereits mit 2.1 Megabit (also rund 250 Kilobyte pro Sekunde) vonstatten. Für eine 100 Megabyte Video-Datei darf man damit noch immer eine Übertragungsdauer von ca. 400 Sekunden (also knapp 7 Minuten), für ein 5 Megabyte großes Foto noch 20 Sekunden veranschlagen. Alles andere also als ein Full-Speed-Highway. Dennoch für kleinere Datenmengen (Visitenkarten, URLs) völlig ausreichend – und für ein "Schnell Mal eben" durchaus in Kauf zu nehmen.

Und wie geht das "Schnell Mal eben"? Über das so genannte „Share-Menü". Das findet sich an verschiedensten Stellen, und ist meist über ein Icon zu erreichen, das wie ein durch Verbinden dreier Punkte entstandenes, auf der Seite liegendes V aussieht. Tippt man dieses an, gelangt man zu einem Bildschirm, wie er rechts dargestellt ist (eventuell, nachdem man zuvor noch die zu Verteilenden Objekte ausgewählt hat). Schwer zu übersehen, gleich an aller oberster Position: Bluetooth.



Das muss nun natürlich auch auf beiden beteiligten Geräten aktiviert sein, sonst kann kein Kontakt zustande kommen. Per Default „versteckt" sich ein Gerät mit aktiviertem Bluetooth dennoch, um sich gegen Angreifer zu schützen. Also gilt es zumindest für den Empfänger, sein Gerät sichtbar zu machen, und ihm einen Namen zu geben. Dies geschieht unter *Einstellungen* → *Bluetooth*, wie im linken Bild ersichtlich. In den meisten Fällen bleibt das Gerät so für eine begrenzte Zeit "sichtbar", um anschließend automatisch zu verschwinden – nur von der Anzeige anderer Geräte, versteht sich, nicht vom Tisch.

Das muss aber auch einfacher gehen, dachte man sich bei Google. Und spendierte Android 4.0 ein neues Feature. Selbiges hört auf den Namen:

Android Beam

"Beam me up, Scotty!" ist sicher das Erste, was Startrek-Fans dabei in den Sinn kommt. Allerdings werden bei *Android Beam* nicht etwa materielle Dinge, sondern nur Inhalte transportiert. Falsch eingestellt ist der "Transporter" dabei sicherheitshalber ebenfalls, damit das Original erhalten bleibt. So lassen sich Kontakte, Websites, Apps, Maps, Routenplanungen und Youtube-Videos auf ganz einfache Weise von einem Smartphone zum anderen schicken. Dazu holt man sich den zu verschickenden Inhalt auf den Bildschirm, und hält Sender- und Empfängergerät mit dem Rücken aneinander. Ein Signalton sowie kurzes Vibrieren kündigen sodann von der Bereitschaft: "Ready to beam up!" Kurzes Antippen des nun verkleinert dargestellten Inhalts auf dem Sender-Gerät vollzieht schließlich den Transfer.

Welche Magie steckt dahinter? Auch wenn ich diesen Text an einem 1. April schreibe, handelt es sich definitiv nicht um einen Scherz. Trotzdem dürften sich Einige beim Lesen dieser Zeilen zu früh gefreut haben. Denn *Android Beam* setzt auf die so genannte Near Field Communication (NFC) auf, die leider nicht von jedem Gerät unterstützt wird. Vorausgesetzt wird nämlich ein kleines Stück Hardware, der NFC-Chip. Dieser ist zumeist im Akku bzw. der Gehäuse-Rückwand des Android-Gerätes verbaut – was auch erklärt, warum die Geräte mit dem Rücken aneinander gehalten werden müssen: Die Reichweite dieser Chips beträgt gerade einmal 4 Zentimeter.

Ein großes Rätsel dürfte hingegen bleiben, warum Google für die Datenübertragung dabei ausschließlich auf NFC setzt – ist doch damit die Übertragungsrate auf 424 Kilobit beschränkt (und somit langsamer als selbst die erste Bluetooth-Implementierung, siehe voriges Kapitel). So werden "größere Inhalte" wie Youtube-Videos oder vollständige Webseiten dann auch nicht direkt übertragen, sondern lediglich deren Link (wer sich für weitere Details interessiert, kann einen Blick auf einen passenden Artikel bei Golem werfen). Samsung hat hier einen Schritt weiter gedacht: Bei deren "S-Beam" erfolgt der Verbindungsaufbau

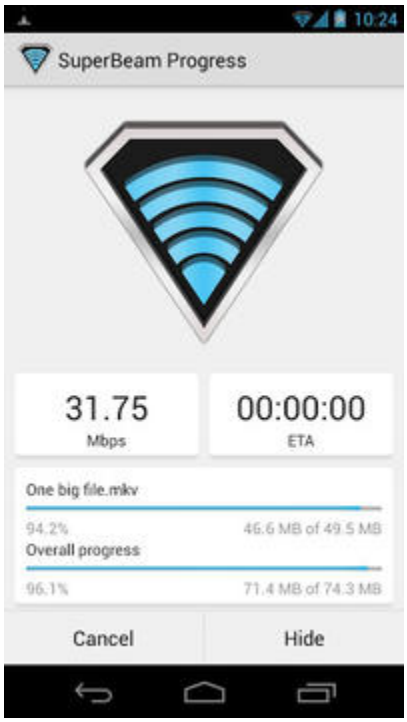
zwar ebenfalls über NFC. Für die eigentliche Daten-Übertragung verwendet man jedoch...

Wi-Fi Direct

Hierbei handelt es sich um einen WLAN-Standard, der ganz ohne Router auskommt. Da Wi-Fi Direct fähige Geräte von der Wi-Fi Alliance zertifiziert werden, sollte man eigentlich davon ausgehen, dass das Ganze herstellerübergreifend funktioniert. Leider ist das in der Praxis nicht immer so, wie auch ein Artikel bei Go2Android bescheinigt. Neben einem Sich-nicht-Finden oder Daten nicht übertragen können (was zwar ärgerlich, aber immer noch recht harmlos ist), weiß man dort von folgendem zu berichten:

> *Doch den Vogel schießt wohl der Test zwischen dem LG Optimus G und meinem Galaxy Note ab. Auch hier ein erfolgreiches finden und verbinden, doch sobald wir ein Bild an das Samsung Gerät schicken wollten, machte das Galaxy Note einen reproduzierbaren Softreset. Welchen rein koreanischen Disput man hier auf Softwareebene aus trägt, bleibt wohl ein gut gehütetes Geheimnis der Asiaten.*

Der gleiche Artikel weist aber auch auf mögliche Abhilfe hin: Wenn die Hardware etwas unterstützt, und die Hersteller lediglich bei der Implementierung ihrer Software aneinander vorbei gearbeitet haben, sollte eine passende App das Problem doch umgehen können?



Eine solche App wird auch gleich benannt: SuperBeam. Der Name lässt richtig vermuten, dass damit *Android Beam* imitiert wird: Zur Initiierung der Übertragung wird auch hier auf den NFC-Chip gesetzt. Doch auch, wer keinen solchen in seinem Gerät hat, muss auf diese App nicht verzichten. Alternativ erzeugt die App auf dem Sender-Gerät einen Barcode, der von der gleichen App auf dem Empfänger-Gerät einfach abgescannt wird. Eine Ausweich-Möglichkeit wäre etwa die App WiFiShare, die sich, wie bereits bei Bluetooth gezeigt, in das so genannte „Share Menü" einklinkt.

SICHERHEIT

Was brauche ich wirklich?

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 Forum. Das Wichtigste sollte man jedoch (hoffentlich) nicht all zu lange suchen müssen:

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).

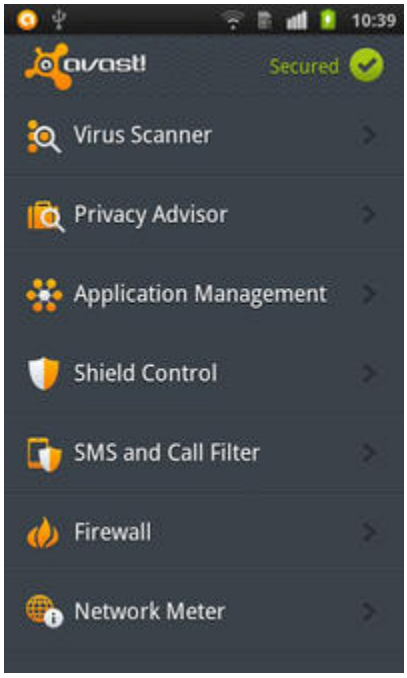
GMV? Was ist das denn nun wieder? Oh-oh... Das sollte eigentlich jeder haben, zumindest ein wenig davon: **G**esunder **M**enschen**v**erstand. Hilft enorm. Auch gegen "Viren" und "Malware".

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 beachtet, 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: Play Store, AndroidPIT-Market (AppCenter), 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 anrufen, 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 Play Store 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 Play Store 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...

Rundum-Sorglos-Pakete



Das sind die Apps, die gleich alle Bereiche abdecken. Also Anti-Virus, Anti-Malware, und "Diebstahlschutz" in einem. Ein Beispiel dafür ist avast! Mobile Security (Bild rechts). Die App will vor Viren und Malware schützen (On-Demand sowie Echtzeit-Scans), bietet einen "Privacy Advisor" zum Aufspüren von Apps mit verdächtigen Berechtigungen, einen Filter gegen unerwünschte Anrufe und SMS, eine Firewall, und mehr. Sogar ein Datenmonitor und eine App-Verwaltung sind mit an Bord.

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 ("DIEBE! ICH BIN EIN GEKLAUTES HANDY!" – äh, ich weiß nicht, wie es mit der Auswahl des Sounds aussieht...). 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. Damit das alles in vollem Umfang funktioniert (insbesondere der Diebstahlschutz), bedarf es allerdings eines Accounts beim Anbieter.

Bei so vielen Features ist jedoch auch die Anzahl der geforderten Permissions entsprechend umfangreich...

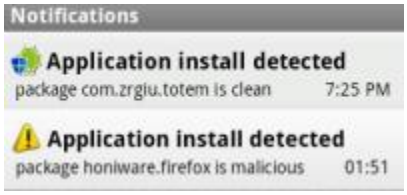
Anti-Virus und Anti-Malware

Viren und Malware (nein, hier sind jetzt keine Apps zum Malen gemeint – sondern bösartige, hinterhältige Apps wie Spartaner, äh, 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...

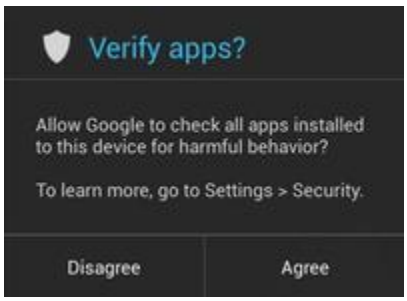
Zunächst sollte man sich an dieser Stelle vor Augen führen, dass ein Scan nach diesen bösartigen Komponenten anders als am PC i. d. R. nicht etwa direkt auf dem Gerät mittels Signaturen und Heuristiken erfolgt: Für viele Geräte wären dafür die benötigten Datenbanken ein wenig groß. Auch bringt so manches kleinere (Einsteiger-) Gerät nicht die dafür benötigte Leistung mit. Vielmehr wird häufig lediglich der Paketname der Apps mit einer Datenbank bekannter schädlicher Apps verglichen.

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

Die gratis-Version 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).



Auch Antivirus-Free ist durchaus eine gute Alternative: Fast genau so gut bewertet, 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 sodann in der "Notification Area" (Bild-Montage rechts): "Application install detected: package com.entwickler.appname is xxx". Wobei "xxx" dann entweder "clean" (sauber) oder "malicious" (schädlich) heißt.



Ab Android 4.2 aka Jelly Bean ist übrigens ein Malware-Scanner bereits im System integriert: Installiert man erstmals eine App aus „fremder Quelle" wird man gefragt, ob man dieses Feature aktivieren möchte. Auch bereits installierte Apps lassen sich damit überprüfen. Dabei wird anhand der App-Signaturen (jede APK-Datei ist mit einer solchen Signatur versehen) mit einer Liste auf den Google-Servern abgeglichen, ob die betroffene App potentiell gefährlich ist. Stellt Googles Cloud-Virenscanner dabei fest, dass es sich bei der zu installierenden App um Malware handelt, wird die Installation

abgebrochen. Erscheint die App lediglich verdächtig, erfolgt ein Warn-Hinweis – und der Anwender kann selbst entscheiden, ob mit der Installation fortgefahren werden soll.

Bei Diebstahl und Verlust

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 (Bild links) für nur anderthalb Euronen, sofern eine "Stand-Alone Lösung" gewünscht ist.

Krach schlagen und SMS mit GPS-Daten verschicken geht auch bereits mit der gratis-Version, 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...

Wer hierfür keine Apps von Drittanbietern einsetzen möchte, kann oftmals auch auf Services des jeweiligen Geräteherstellers zurückgreifen. Nach einer Registrierung auf der entsprechenden Webseite, soll sich auch hier das Gerät bei Verlust wieder aufspüren lassen: Bei aktuellen HTC-Geräten etwa über HTC Sense, bei Motorola via MotoBlur, und auch Samsung bietet entsprechendes an.

Welche Variante auch genutzt wird: Man sollte im Vorfeld prüfen, wie sie funktioniert (und ob sie dies überhaupt tut), damit man im Ernstfall gewappnet ist.

Was aber, wenn das Kind bereits in den Brunnen gefallen, und das Gerät verschwunden ist? In diesem Fall helfen Apps wie Android Lost – vorausgesetzt, der Akku ist noch ausreichend gefüllt, und das Gerät mit dem dem Daten-Netz des Anbieters verbunden. Dank Remote-Installations-Feature lässt sich die App dann nämlich auch noch aus der Ferne installieren, indem man die App-Seite im Playstore besucht, und dort den „Install" Button drückt. Das löst einen so genannten „Push Install" aus – der Playstore „schiebt" die App auf das Gerät.

Nach erfolgreicher Installation sollte sich der Androide nun per SMS steuern lassen, wofür eine ganze Reihe von Befehlen verfügbar sind. Darunter befinden sich solche, die still und unbemerkt im Hintergrund ablaufen (z. B. einen Status-Bericht anfordern, GPS anschalten und die aktuelle Position mitteilen, eine Tonaufnahme der Umgebung starten – oder die SD-Karte löschen bzw. gleich einen Wipe durchführen) – aber auch andere, die gar nicht unbemerkt bleiben sollen (Alarmsound abspielen, das Gerät einen Text sprechen ("Komm nach

Hause, Kleiner!") oder auf dem Display anzeigen lassen. Über die Website kann man ebenfalls auf die Inhalte seines Gerätes zugreifen, und so noch wichtige Daten in Sicherheit bringen bzw. löschen. Das Gerät lässt sich von hier aus sogar steuern – was besonders für Tablets ohne SMS-Funktionalität interessant sein dürfte.

Das alles setzt natürlich voraus, dass der Langfinger den auf dem Gerät eingerichteten Google-Account dort noch nicht gelöscht hat.

Worauf Apps Zugriff haben

Wer hat sich nicht schon einmal gefragt, was eigentlich bei der Installation einer neuen App aus dem *Play Store* 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-*???"

Was also darf eine App? Oder, anders herum gefragt: Welche App darf denn ...? Auf beide Fragen gibt z. B. RL Permissions (Bild rechts) gute und aussagekräftige Antworten. Eine Ampel zeigt nämlich jeweils an, wie schwerwiegend der *potentielle* 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. Und eine Liste alternativer Apps zum Thema, wie gewohnt, im Forum.

Wer sich bereits vor der Installation absichern möchte, keine Apps mit unerwünschten Berechtigungen auf sein System zu lassen, wirft am Besten einen Blick auf die unter Playstore Ergänzungen bereits beschriebene App *APEFS*, mit der sich schon im Playstore das Suchergebnis entsprechend filtern lässt.

Apps vor unbefugtem Zugriff schützen

Der Mensch ist von Natur aus neugierig. Was per se nicht schlecht ist – denn dieser Neugier haben wir so manche Entdeckung zu verdanken. Unschön wird es erst, wenn dabei die Privatsphäre verletzt wird. Wie kann man sich also vor "Schnüfflern" schützen?

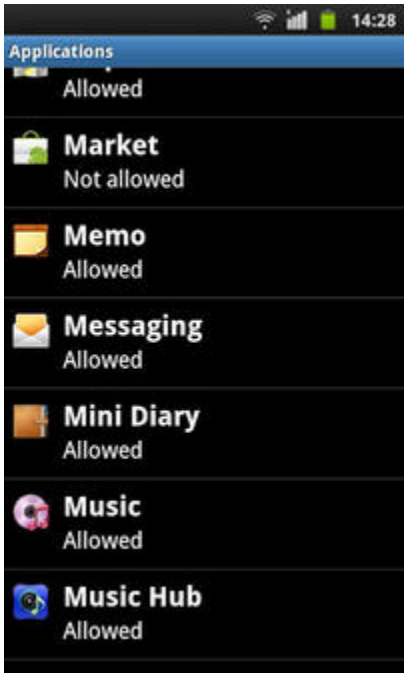
Zunächst einmal bringt Android von Haus aus entsprechende Schutzmechanismen mit. So lässt sich konfigurieren, dass bei jedem Einschalten des Displays zunächst ein Pin-Code bzw. Passwort eingegeben, oder ein Entsperrmuster gezeichnet werden muss. Ab Android 4.0 ist auch eine Gesichtserkennung zur Entsperrung möglich. Die entsprechenden Einstellungen finden sich im Menü *Standort & Sicherheit → Display-Sperre einrichten.*

Nicht immer möchte man jedoch das komplette Gerät sperren. Gibt man das Gerät zeitweilig aus der Hand, sollen bestimmte Apps aber unangetastet bleiben: Der Gast soll beispielsweise keine neuen Apps aus dem Playstore installieren, und auch die Finger von der einen oder anderen App lassen. Während sich ab Android 4.2 für solche Fälle ein Gast-Zugang einrichten lässt, können auch in früheren Versionen App-Locker gute Dienste leisten.

So kann beispielsweise Smart App Protector jede App mit einem "Zugangscode" versehen – ohne den sich selbige nicht mehr starten lässt. Das kann ein Pin-Code, ein Muster, ein Passwort, oder auch eine "Geste" (einfache Fingerzeichnung auf dem Display) sein – ohne den sich selbige nicht mehr starten lässt. Geht der Bildschirm aus, während eine entsperrte App geöffnet ist, muss der Zugangscode erneut eingegeben werden. Natürlich startet sich diese App automatisch nach dem Booten, damit der Schutz auch nicht einfach umgangen werden kann.

Mit 4,6 Sternen bei über 70.000 (Gratis-Version) bzw. fast 3.000 Bewertungen (Kaufversion) ist *Smart App Protector* überdurchschnittlich gut bewertet. Bedenklich stimmen lediglich die verlangten Berechtigungen zum Tätigen von Anrufen, Abfangen ausgehender Anrufe sowie dem Empfangen von SMS, die der Entwickler leider nicht erklärt. Wem dies Bauchschmerzen bereitet, der findet in der oben verlinkten Übersicht eine ganze Reihe von Alternativen, die ähnliches leisten.

Kinderschutz



Kinderschutz ist ein ganz eigenes Thema, das ich mit diesem Kapitel allenfalls anreißen kann. Den "politischen Teil" (ab wann sollte ein Kind überhaupt ein Smartphone bekommen, etc.) möchte ich dabei bewusst außen vor lassen – diese Entscheidung lässt sich weder pauschal, noch gar "von oben herab" treffen, sondern ist eine „private Angelegenheit" zwischen den jeweiligen Eltern und Kindern. Je früher man den Nachwuchs an diese Technik heranführen möchte, desto größer sind jedoch auch die Ansprüche an das Thema Sicherheit.

Zum Glück lassen uns die Entwickler mit diesem Thema nicht im Dunkeln sitzen – und die zugehörige Übersicht bei AndroidPIT gibt uns eine ganze Reihe Apps an die Hand. Herausgreifen möchte ich hier Vodafone Child Protect. Diese App erlaubt neben dem Sperren von Apps auch das Einschränken der Nutzungsdauer nicht gesperrter Apps (um beispielsweise nächtliches Spielen unter der Bettdecke zu unterbinden). Auch lässt sich festlegen, zu welchen Zeiten telefoniert/gesimst werden darf, und welche Kontakte überhaupt dafür in Frage kommen. Ein solides Grundpaket also, welches zudem noch gratis zur Verfügung steht.

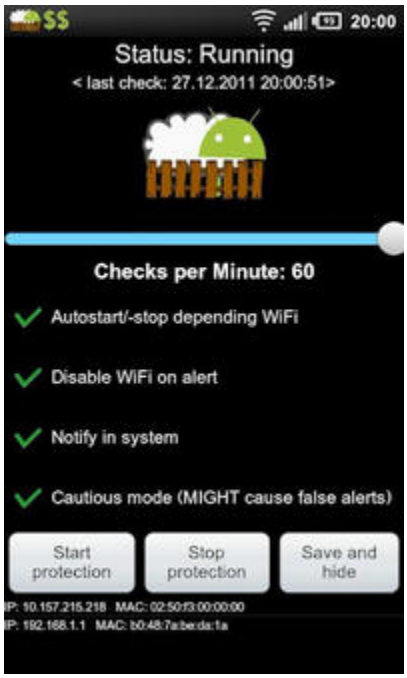
Damit hier nicht jemand den Schutzmechanismus außer Kraft setzt, gibt es gleich eine Zusatz-App obendrein: Sobald eine der beiden Apps deaktiviert/ deinstalliert wird, schickt die andere eine Alarm-SMS an das elterliche Telefon. Sofern der Nachwuchs nicht zuvor in den Flugzeugmodus gewechselt ist...

In fremden Netzen

Neben den Apps gibt es auch andere Dinge, die sich von Außen ihren Weg auf unsere Androiden bahnen wollen. Um beispielsweise Daten auszuschnüffeln, oder andere böse Dinge anzustellen. Die Rede ist von "Angriffen aus dem Netz". Während man im "mobilen Datennetz", dem heimischen WLAN, oder dem WLAN der Firma noch relativ sicher vor selbigen ist, lässt sich das für sogenannte "offene WLANs", wie sie häufig in Hotspots anzutreffen sind, nicht unbedingt behaupten: Hier kann sich schließlich jeder anmelden, eine Prüfung findet kaum statt.

Sind zwei Geräte im gleichen Netz (hier: WLAN) unterwegs, können mit passender Software alle Pakete des einen Gerätes mit dem anderen inspiziert werden. Im Klartext übertragene Daten (etwa bei Benutzung des unverschlüsselten HTTP-Protokolls) lassen sich, im Gegensatz zu verschlüsselt übertragenen (etwa HTTPS) auch im Klartext auslesen. Das können lapidare Dinge wie besuchte URLs sein – aber auch auf Webseiten eingegebene Passwörter, und andere Dinge. Auf diese Weise kann sich der Schnüffler also Zugang zu fremden Benutzerkonten verschaffen! Und da so mancher aus Bequemlichkeit die gleiche Benutzername/Passwort Kombination für verschiedene Konten nutzt, kann das recht böse enden...

Worauf sollte man also besonders achten, und wie kann man sich schützen?



- Insbesondere in offenen WLANs die Übermittlung vertraulicher Daten möglichst vermeiden
- Darauf achten, dass Daten (besonders Passwörter) verschlüsselt übertragen werden. Beim Browsen im Web beispielsweise weist ein "https://" (anstelle eines einfachen "http://") am Anfang einer URL auf eine verschlüsselte Verbindung hin (das "s" steht für "secured", also "abgesichert")
- Hintergrunddaten besser abschalten – besonders diejenigen, bei denen vertrauliche/private Daten übermittelt werden, und bei denen man nicht sicher ist, ob die Übertragung verschlüsselt geschieht. Im Zweifelsfall einfach die Hintergrunddaten komplett deaktivieren, während man sich in fremden Netzen herumtreibt. Zu finden ist das passende Schalterchen unter *Einstellungen → Konten & Synchronisierung,* und ist treffenderweise meist auch mit "Hintergrunddaten" beschriftet.
- Wer desöfteren auf die Nutzung fremder Netze angewiesen ist, sollte über die Einrichtung eines VPN nachdenken. Android unterstützt das von Haus aus.

Eine weitere Schutzmöglichkeit bietet z. B. die App DroidSheep Guard (Abbildung rechts). Diese überwacht die eigene Netzwerk-Schnittstelle auf Angriffsmuster bekannter Übeltäter wie DroidSheep, FaceNiff und Co. Wird ein solcher entdeckt, erfolgt sofort eine Benachrichtigung, und der Vorgang wird

protokolliert. Wer auf "Nummer Sicher" gehen will, kann in einem derartigen Fall auch gleich die Verbindung kappen lassen, und so dem Angreifer den Spaß verderben.

Einige der weiter oben genannten „Rundum-sorglos-Pakete“ versprechen auch, generell beim Surfen zusätzliche Sicherheit zu bieten – indem sie etwa vor potentiell gefährlichen Seiten (die in einer Datenbank gespeichert sind) warnen.

PRIVATSPHÄRE

Da sitzt man nach einem arbeitsreichen Tag beim Abendbrot (oder, als Schichtler, nach arbeitsreicher Nacht beim Frühstück), im Hintergrund läuft die Lieblingsmusik. Man beginnt, sich langsam zu entspannen. Und plötzlich klingelt das Telefon. Wer mag das sein? Sicher Sascha (oder Mascha), ein angenehmer Plausch war ohnehin längst fällig. Also freudig zum Hörer gegriffen, und... Nix Sascha, nix Mascha. Am anderen Ende meldet sich eine Firma, von der man zuvor nie gehört hat, und möchte einem etwas verkaufen. Woher haben die schon wieder meine Nummer? Oder auch die Absender all der an mich persönlich adressierten Werbepost, mit deren Absendern ich zuvor auch nie das "Vergnügen" hatte...

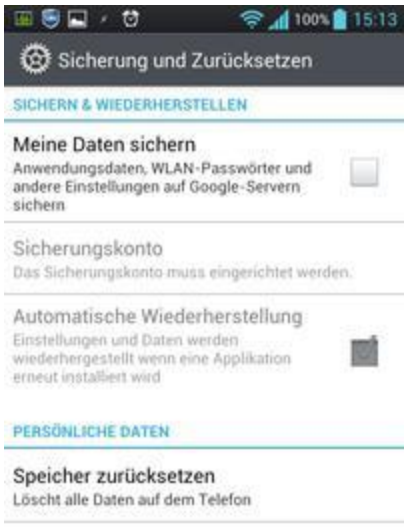
Auch in den "News" hört und liest man immer wieder von Skandalen mit Adresshandel. Oder von Hackern, die wieder einmal die Datenbank eines größeren Unternehmens kopiert haben, und somit nun in Besitz sämtlicher Kundenstammdaten sind. Wofür sie die erbeuteten Daten nun verwenden werden, darüber wollen wir besser nicht nachdenken: Verkaufen? In unserem Namen auf "große Einkaufstour" gehen? Mit den gestohlenen Identitäten gar Straftaten begehen?

Sollten die Firmen unsere ihnen anvertrauten Daten nicht besser schützen? Diese und ähnliche Fragen werden immer dann laut, wenn ein solcher Skandal an die Öffentlichkeit gelangt. Doch spätestens, wenn es zu Smartphones (und Tablets) kommt, sei eine weitere Frage erlaubt: Was tun wir eigentlich selbst für den Schutz unserer Privatsphäre? Wie viele Daten geben wir freiwillig (und oftmals ohne nachzudenken) Preis?

Privacy First?

Schon bei der Ersteinrichtung eines Google-Accounts auf einem Android-Gerät wird uns eine passende Frage serviert: "Möchten Sie Ihre Daten auf Google Servern sichern?" Ja, welche Daten sind das denn? Sehr viel wird dazu nicht mitgeteilt. Die Rede ist hier vom "Google Cloud Backup" – und gesichert werden neben den Anwendungs-Daten von Apps (die dies explizit unterstützen müssen, was bei Weitem nicht alle tun) und der Liste installierter Apps auch diverse System-Einstellungen, Anruflisten, Browser-History, WLAN-Passworte, und einiges mehr. Es sind also durchaus einige Daten darunter, die als "sensibel" betrachtet werden können. Und mit Fug und Recht darf man davon ausgehen, dass Google uns diese gratis Dienstleistung nicht aus rein altruistischen Gründen zur Verfügung stellt:

> *"Wenn man ein Produkt gratis bekommt, ist man nicht der Kunde. Man ist das Produkt. Der Bauer betreibt seine Farm nicht für das Vieh." (Eric Ries)*



Natürlich lassen sich diese Daten für gezielte Werbung verwenden: Welche Web-Seiten hat man besucht? Mit wem steht man in Kontakt? Auch die bevorzugten Einstellungen des Systems verraten einiges über unsere Vorlieben. Das alles ist mit unserem Google-Account verknüpft – über den übrigens auch unser E-Mail Verkehr läuft, sofern dafür GMail zum Einsatz kommt.

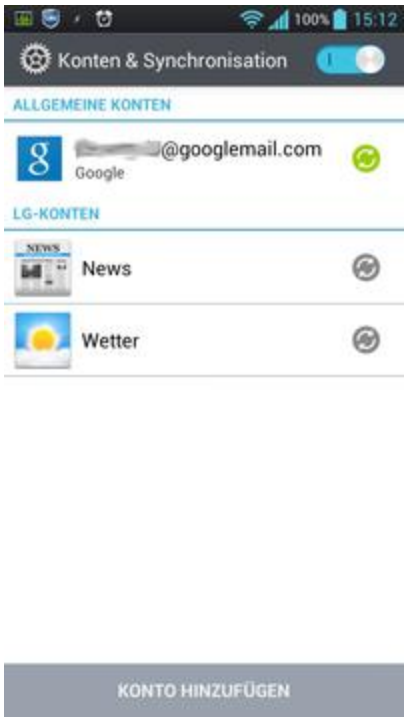
Damit stehen wir zwischen zwei Fronten. Die Einen sagen: "Meine privaten Daten gehen niemanden etwas an! Ich möchte davon nichts in der Cloud sehen!" Während den Anderen das völlig egal ist: "Ich habe schließlich nichts zu verbergen." Wie pflegt mein Vater immer zu sagen: "Ein weites Feld, Luise." Und so ist es auch: Es gilt immer abzuwägen, wie viel Privatsphäre wir für mehr Bequemlichkeit zu opfern bereit sind.

Zum Glück werden wir ja explizit gefragt: "Möchten Sie Ihre Daten auf Google Servern sichern?" Da respektiert also offensichtlich jemand unsere Privatsphäre. Wir können also hier einfach "Nein" sagen, und kümmern uns um unsere Datensicherung selbst (siehe Datensicherung; wer diese Einstellungen im Nachhinein anpassen möchte, findet sie unter *Einstellungen → Sicherung & Zurücksetzen*).

Denken wir zumindest...

Kontakte und Kalender

Und so erfassen wir freudig unsere Kontakte und Termine mit dem neuen Android-Gerät. Macht sich richtig gut, so haben wir überall Zugriff darauf – schließlich ist das Smartphone ja immer dabei. Und das Tablet zumindest einfacher mitgenommen als der heimische Computer oder Laptop. Doch spätestens, wenn ein zweites Android-Gerät mit dem gleichen Google-Account eingerichtet (oder die Web-Variante von GMail besucht) wird, staunt man nicht schlecht: Hoppla – wie kommen denn die ganzen Daten hierher? Adressen und Termine erscheinen wie von Geisterhand auf dem neuen Gerät – obwohl man doch die Frage "Möchten Sie Ihre Daten auf Google Servern sichern?" mit einem definitiven "Nein!" beantwortet hat?



Das sind also entweder keine "Daten" – oder die "Synchronisation" von Kalendern und Adressbüchern ist etwas grundlegend anderes als "sichern". Denn hier wird man nicht ausdrücklich um Genehmigung gebeten. Der "Wunsch" wird einfach vorausgesetzt. Natürlich nur zu unserem Besten, damit uns die Daten nicht verloren gehen. Doch nicht nur Paranoiker wissen, dass sich Kontakte und Kalenderdaten natürlich u. a. vorzüglich zur Personifizierung von Werbung eignen können. Wenn etwa jemand zwei Mal wöchentlich einen Termin im Sportverein hat, interessiert er sich für Sport – oder benötigt Sportkleidung, Fitness-Artikel, u. s. w..

Die zugehörige Einstellung findet sich auf dem Android-Gerät unter *Einstellungen → Konten & Synchronisation*. Und zwar für jeden eingerichteten Account separat. Ein grünes Symbol (das verdächtig an Recycling erinnert – uns also die Wiederverwendbarkeit unserer Daten vor Augen halten sollte) zeigt an, dass zumindest Teile dieses Kontos synchronisiert werden. Tippt man den Eintrag (nicht das Symbol) an, offenbaren sich die synchronisierten Details: Kalender, Kontakte, GMail, und mehr. Jeder Eintrag wieder mit dem bereits erwähnten „grünen Punkt" oder, wie im rechten Screenshot, einem einfachen Häkchen. Wer also seine Termine oder Kontaktdaten nicht auf fremden Servern sehen möchte, muss das hier explizit deaktivieren. Also nichts mit "Privacy First".

Damit kein falscher Eindruck entsteht: Natürlich hat es seine Vorteile, wenn die betroffenen Daten zum Einen gesichert, und zum Anderen von verschiedenen Geräten aus gleichermaßen zur Verfügung stehen. Die Entscheidung, ob man dies möchte (und wenn, ob dies über den Google-Service, oder aber über Lösungen von Drittanbietern umgesetzt wird), sollte jedoch dem Anwender überlassen werden. Und zwar nicht über ein "Opt-Out", sondern per "Opt-In": Wer es gern hätte, aktiviert es. Wie im vorigen Kapitel: "Möchten Sie, dass Ihre Kontakte, Termine, … über Google-Server synchronisiert werden?"

Ortsdaten

Google weiß immer, wo wir sind. Oder wo wir wann waren. Denn diese Daten werden über die so genannten "Location Services" (zu Deutsch: Ortsdienste oder Standortdienste) von uns bereitgestellt. Unter *Einstellungen → Standortdienste* kann man konfigurieren, was genutzt werden soll. Klar, GPS kommt ganz ohne die Google Cloud aus, wenn es separat genutzt wird. Doch bereits bei AGPS (Assisted GPS) kommen externe Datenbanken ins Spiel: Anhand der IDs gerade genutzter Mobilfunkzellen wird dabei der ungefähre aktuelle Standort ermittelt, um so den Aufbau der Verbindung zum Satellitennetzwerk zu beschleunigen.

Ähnlich sieht es beim "Google Standort Dienst" aus. Hinter diesem steht eine Google-Datenbank, in der die Positionen von Mobilfunk-Masten und WLAN Access Points gespeichert sind. Auf selbige muss das Gerät also zugreifen – wobei durchaus die Geräte-ID oder das verwendete Google-Konto preisgegeben werden können. Und schließlich fragt man sich sicher nicht zu Unrecht, was es wohl mit den "anderen Services" auf sich haben mag, für welche der Standort Verwendung finden soll.

Interessant ist in diesem Zusammenhang auch der Ortsdaten-Cache, der zur Beschleunigung der Standort-Ermittlung Verwendung findet (siehe auch Ortsdaten-Cache einsehen). Wer gerade noch an der Weltzeit-Uhr auf dem Berliner Alexanderplatz stand, kann sich schließlich fünf Minuten später kaum bereits am Londoner Trafalger Square befinden. Bis zur genauen Ortsbestimmung darf also getrost zunächst davon ausgegangen werden, dass der Anwender "in der Nähe" des Alex ist. Doch Dank dieses Caches kann sich ebenso jemand, der unbefugt Zugriff auf das Gerät "erhalten" hat, ein gutes Bild von unserem Tagesablauf machen. Mit Bordmitteln scheint es jedenfalls nach wie vor unmöglich, diesen Cache bei Bedarf manuell zu leeren. Zumindest nicht auf eine Art, die für den normalen Anwender ersichtlich wäre.

Welche Daten sammelt Google eigentlich?

Dieser Frage geht auch ein Artikel bei StackExchange nach. Eine umfassende Antwort sollte sich in Google´s Datenschutzerklärung finden.

Was Google sammelt

Da sind natürlich die Angaben, die ein Nutzer von sich aus und bewusst macht. Etwa bei der Erstellung eines Google-Accounts. Welche Angaben das umfasst, steht natürlich jedem selbst anheim (ebenso, ob diese den Tatsachen entsprechen – denn dies wird zumindest derzeit nicht geprüft).

Weitere Daten werden bei der Nutzung von Google Diensten erfasst. Welche dies sind, ist nicht unbedingt jedem sofort klar – schließlich findet diese Erfassung im Hintergrund statt. In diese Kategorie fallen u. a.:

- **Gerätebezogene Informationen:** Modell, Betriebsystem, eindeutige Gerätekennungen (z. B. IMEI/IMSI), Telefonnummern. Einige dieser Informationen werden u. U. auch automatisch mit dem verwendeten Google-Account verknüpft.
- **Protokolldaten:** Suchanfragen, IP-Adresse, Cookies, Geräte-Ereignisse (Abstürze, Hardware-Einstellungen, Browsertyp).
  Was vielen nicht bewusst ist: Aus dem Anruf-Protokoll des Android-Gerätes wird auch gespeichert, wen man wann, wie oft, etc. kontaktiert hat! Details dazu finden sich im Dashboard (s. u.).
- **Standort-Informationen:** Sensor-Daten, WLAN-Netzwerke, Sendemasten

Dies ist nur ein kurzer Auszug aus o. g. Datenschutzerklärung. Hinzu kommen noch weitere, dort nicht explizit genannte Dinge, die so manchem selbstverständlich erscheinen mögen. Bereits genannt wurden Kontakte und Kalender. Darüber hinaus nutzen viele jedoch weitere Dienste von Google, wie etwa Google Drive mit seinem "Online Office". Natürlich landen auch hier alle Daten auf Google´s Servern.

Was Google mit den gesammelten Daten macht

Auch davon spricht die Datenschutzerklärung. Die Einleitung des entsprechenden Abschnittes möchte ich an dieser Stelle einfach einmal zitieren:

> *Wir nutzen die im Rahmen unserer Dienste erhobenen Informationen zur Bereitstellung, zur Instandhaltung, zum Schutz sowie zur Verbesserung dieser Dienste, zur Entwicklung neuer Dienste und zum Schutz von Google und unseren Nutzern. Wir nutzen diese Informationen außerdem, um Ihnen maßgeschneiderte Inhalte anzubieten – beispielsweise um Ihnen relevantere Suchergebnisse und Werbung zur Verfügung zu stellen.*

Ferner ist die Rede davon, dass die gesammelten Informationen allen Google-Diensten zur Verfügung stehen. Datenschützer nennen so etwas ein "Super-Profil" (bei Spiegel gibt es dazu eine ganze Artikel-Serie, die beispielsweise in einer Box links auf dieser Webseite zusammengefasst ist): Die angebotenen Dienste sind derart umfangreich, dass sich mit ihrer Hilfe ein eben so umfangreiches Profil des Nutzers erstellen lässt.

Wo man die erfassten Daten kontrollieren kann

Einen vollständigen Einblick in alle gesammelten Daten bekommt der Anwender nicht (was sicher dem Schutz seiner Gesundheit dient, da dies die Gefahr eines Herzinfarktes drastisch erhöhen könnte). Doch zumindest grob thematisch lässt sich schauen, was denn da so gesammelt wurde. Dafür bietet Google das mit dem Account verknüpfte Dashboard. In diesem findet man:

- alle mit dem Account verknüpften Android-Geräte (die dazu gespeicherten Informationen lassen sich einsehen: IMEI, letzte Aktivität, wann registriert)
- Daten zu diversen Diensten, wie etwa Chrome Lesezeichen, GMail, Google Docs, Kalender. Informationen lassen sich hier teilweise verwalten, in wenigen Fällen (Chrome Lesezeichen) sogar löschen. Einige der Verwaltungs-Links führten leider ins Leere, im wahrsten Sinne des Wortes: Angezeigt wurde nämlich lediglich eine leere Seite, etwa beim Aufruf von "Mobilfunkgeräte verwalten" im Bereich Kalender.
- Webprotokoll: Immer, wenn man mit seinem Google-Account angemeldet eine Websuche durchführt, wird dies protokolliert. Wer das nicht wünscht, meldet sich am besten immer explizit ab, wenn dies möglich ist (und man nicht beispielsweise gerade auf seine Google-Mails zugreifen muss). Das Protokoll lässt sich hier allerdings auch löschen.
  Einen tieferen Einblick in das Webprotokoll erhält, wer auf einer Suchergebnis-Seite rechts oben auf das Zahnrad-Symbol klickt, und dort "Webprotokoll" auswählt: Hier sieht man nämlich alle erfassten Suchen. Jetzt noch einmal auf das Zahnrad-Symbol, und "Einstellungen" auswählen. So, hier lässt sich das Sammeln abschalten. Vorher gleich noch den Link zum Löschen aller Google-Suchaktivitäten betätigt, damit auch ältere Einträge verschwinden. Oder zumindest uns nicht mehr angezeigt werden: *Sicher ist [nur], dass nichts sicher ist. Und selbst das ist nicht sicher.* (Joachim Ringelnatz)

Welche Daten wohin weitergegeben werden

Auch dazu äußert sich die Datenschutzerklärung. Es würden keine Daten weitergegeben, außer...

- mit expliziter Einwilligung des Nutzers
- "Domain-Admistratoren" haben Zugriff auf die Daten. Dies betrifft u. a. Anwender von Google Apps.
- für Verarbeitung durch andere Stellen. Das sind "vertrauenswürdige Unternehmen", die im Auftrag von Google arbeiten, und an Google´s Datenschutzerklärung gebunden sind.
- aus rechtlichen Gründen (z. B. auf behördliche Anordnung hin)

Darüber hinaus werden möglicherweise "zusammengefasste, nicht-personenbezogene Daten" an Partner wie etwa Verlage, Werbeunternehmen, etc. weitergegeben.

Die Cloud

Noch eine? Im Prinzip ging es doch bereits in den vorigen Kapiteln um die "Google Cloud"! Das ist prinzipiell richtig – nur betraf es dort die bereits vorinstallierten und teilweise automatisch aktivierten Dinge. Aber es gibt noch weit mehr. Apps und Dienste, die wir oft ohne großes Nachdenken nutzen. So landen weitere Daten auf fremden Servern, und vervollständigen etwa über uns angelegte persönliche Profile. Ja, schimpft mich einen Paranoiker! Spätestens im nächsten Kapitel jedoch werde ich zeigen, dass solche "Profile" wirklich existieren.

Streut man seine Daten über möglichst viele verschiedene Dienste (natürlich von möglichst verschiedenen Anbietern), erschwert dies selbstverständlich die Bildung eines "Komplett-Profils". Nutzt man dazu noch unterschiedliche "Identitäten", hilft dies weiterhin der Verschleierung. Dummerweise widerspricht das jedoch der Bequemlichkeit: Wie fein ist doch ein "Single Sign-In". Man muss sich nur ein einziges Passwort merken, und kommt an alles heran. Das Google-Passwort wird bereits an so vielen Stellen akzeptiert, das es fast danach schreit: "Melden Sie sich mit Ihrem Google-Konto an!"

Neben den zahlreichen Google-Diensten (oh, Google Drive als bequeme Daten- und Dokumentablage habe ich noch gar nicht erwähnt? Oder Google's Picasa für die Bilder, die natürlich mit GeoTags versehen hochgeladen werden? Oder Google+ für den „sozialen Austausch"? Den Google Reader, der allerdings zum Leidwesen Vieler im Juli 2013 seine Pforten schließt?) gibt es ja durchaus noch weitere. Wer mich kennt, wartet sicher schon darauf, dass ich die Gruppe benenne: Ja, ich bezeichne sie als "asoziale Netzwerke", und habe dafür schon so manche Kopfnuss bekommen. So etwas ist halt Geschmackssache.

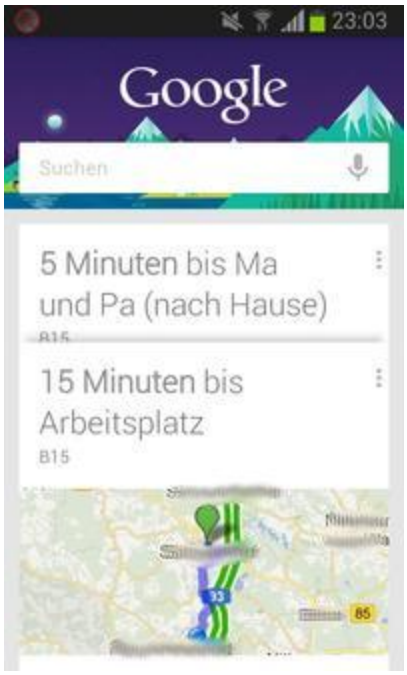
Da wären also noch Facebook und Twitter als namhafteste Vertreter, von denen ersteres desöfteren für Schlagzeilen aufgrund seiner sich ständig wandelnden "Datenschutz-Bestimmungen" sorgt (und man sich so manches mal fragt, vor wem die Daten da eigentlich geschützt werden sollen). Natürlich steht es jedem selbst zu, wie viel er wo von sich Preis gibt. Und zugegeben: Sogar ich habe ein Profil bei Xing, bin also auch ein wenig "asozial"...

Nicht zu vergessen auch Dinge wie Evernote, die beliebte Notiz-App, die längst ebenso auf Desktop-Systemen Einzug gehalten hat. Und so erfolgreich ist, dass Google mit seinem Keep die ganze Sache nachmacht. Was war da noch gleich... Oh, Dropbox & Co. als Datenspeicher. Oder aber, Last but not Least:

Google Now

Der neue Super-Service aus dem Hause Google, der mit Jelly Bean (Android 4.1) auf Android-Geräten Einzug gehalten hat, und Apple's Siri alt aussehen lässt wie eine Bahnsteigansage. Oder besser wie einen Info-Stand im Kaufhaus. Denn Google Now beantwortet unsere Fragen bereits, bevor wir sie stellen. Was meine Korrektur-Leserin Sabine mit Erschrecken erkannte:

> *Dass meine Standorte "überwacht" werden, war mir ja in der Theorie bekannt. Das in der Praxis ums Ohr geschlagen zu bekommen, war doch noch unheimlich. Sagt mir doch morgens Google, dass ich 15 Minuten zur **Arbeit** brauche (und kein besonderer Verkehr wäre)! Google hat quasi registriert, dass ich mich Tags zuvor mehrere Stunden an ein und der selben Stelle aufgehalten habe – und hat daraus geschlossen, dass ich dort arbeite.*
>
> *Zudem hat er gleich meine Kontakte im Hinterkopf und mir heute gesagt, dass ich fünf Minuten zu meinen Eltern brauche, nachdem ich Tags zuvor ein paar Minuten dort war. So deutlich ist es einfach gruselig.*
>
> ***Gewusst** hab ich's ja. Aber es so zu spüren ist doch nochmal eine andre Nummer!*



Wie bereits zuvor erwähnt, hat Sabine ja Google alle dafür notwendigen Daten bereitgestellt: Kontakte und Termine wurden mit Google synchronisiert, die Ortsdaten abgefragt, und so weiter. Wer bisher davon ausging, dass dies alles separate Dienste seien, ist damit nicht mehr auf dem aktuellen Stand: Im März 2012 hat Google seine Privacy Policy entsprechend angepasst – und versteht sich nunmehr als "ein großer Dienst mit mehreren Abteilungen", die sich den gemeinsamen Datenbestand teilen. Wogegen Europas Datenschützer aktuell wieder vorgehen, wie in einem Spiegel-Artikel vom 3.04.2013 zu lesen ist.

Die Nutzung dieses Dienstes erfordert jedoch (neben einer Android-Version von 4.1 oder höher) auch die aktive Einwilligung des Anwenders. Für den Zugriff auf die Daten, die er ohnehin schon hochgeladen hat? Der bereits zitierte Artikel von SeekingAlpha beschreibt es etwa folgendermaßen:

> *Wenn jemand sich aktiv für den Dienst anmeldet, wird er Google beim Versuch, den Dienst an seine Bedürfnisse anzupassen, unweigerlich mehr Daten bereitstellen, als er ursprünglich beabsicht hat.*

Ein Artikel bei ReadWrite beschreibt das Funktionieren von Google Now folgendermaßen:

> *Google Now aggregiert die Informationen, die Google ohnehin bereits auf täglicher Basis über den Benutzer sammelt: Zugriffe auf Mails, Kalender, Kontakte, Textnachrichten, den aktuellen Standort, Einkaufs-Gewohnheiten, Zahlungs-Gewohnheiten, ebenso wie die Vorlieben bei Musik, Filmen und Büchern. Es kann sogar die Fotos des Anwenders scannen und anhand ihres Themas (nicht nur des Dateinamens) identifizieren. Der einzige Aspekt unseres Online-Lebens, der hier noch nicht erfasst ist, sind auf Google+ zum Ausdruck gebrachte Meinungen. Aber das wird zweifellos noch folgen.*

Das klingt erschreckend – kann aber auch so erschreckend bequem sein, wie ein Artikel bei WebProNews feststellt:

> *Es teilt uns das Wetter mit, bevor wir in den Tag starten. Sagt uns, mit welchem Verkehr wir auf dem Weg zur Arbeit rechnen müssen. Steht man auf dem Bahnsteig, tut es kund, wann der nächste Zug kommt. Oder es verkündet den aktuellen Spielstand des gerade laufenden Fussballspiels. Das Beste daran: Das alles geschieht automatisch. Die Karten tauchen den ganzen Tag über immer genau dann auf, wenn man sie braucht.*

Nicht nur Privatpersonen sehen den Dienst allerdings kritisch. Besonders Sicherheits-Abteilungen in Firmen haben starke Bedenken, wie u. a. CSOOnline berichtet:

> *Während Vertreter der Konsumenten sich über die Privatsphäre sorgen, denken Firmen über die Implikationen nach, Google Now auf dem gleichen Gerät installiert zu wissen, mit dem der Angestellte auch auf das firmeneigene Intranet oder den Mailserver zugreift. Zumindest sind Firmen daran interessiert, hier die Kontrolle zu bekommen, das Feature zu deaktivieren.*

Fragt sich da jemand, ob das noch steigerungsfähig ist? Ohja, aber sicher doch. Nach *Google Now* folgt *Google Glass*. Und dann wird auch noch aufgezeichnet, was man sieht. Wie lange man worauf schaut. Spätestens dann wird es wichtig, in den richtigen Augenblicken auch einmal abzuschalten...

Wer sich für weitere kritische Lektüre zu *Google Now* interessiert, kann sich u. a. an folgende (größtenteils bereits zitierte) Artikel halten:

- Google Now: Trading Your Privacy For The Future (SeekingAlpha)
- "Google Now" Knows What You're Doing, Right Now (PMG.Co)
- "Google Now" Knows More About You Than Your Family Does - Are You OK With That? (ReadWrite.Com)
- 'Google Now's' Terrifying, Spine-Tingling, Bone-Chilling Insights Into Its Users (Forbes)
- Google Now: Do You Want Google Using Your Information In This Way? (WebProNews)
- Google Now draws caution among security experts (CSOOnline.Com)

Zwischenbilanz

Wer bis hier hin mitgelesen hat, hält mich nun mit Sicherheit für einen Paranoiker, der alles schwarz malt. Und hinter jedem Baum einen Spion sieht. Ich will das gar nicht von vornherein bestreiten – aber ein wenig korrigieren: Ich sehe, dass hinter jedem Baum ein Spion stehen *könnte.*

Keinesfalls möchte ich hier die Nutzung "der Cloud" im Allgemeinen, oder gewisser "sozialer Netze" im Speziellen verteufeln oder "madig machen". Das Eine oder Andere nutze ich ja zugegebenermaßen selbst. Aber mit einem kritischen Blick die Dinge hinterfragen, das sollte man auf jeden Fall. Sich die Hintergründe bewusst machen. Wissen, wie es läuft – und was dahinter steht. Und dann wissend entscheiden, welche Dienste man nutzen möchte – oder, anders ausgedrückt: Wie viel Privatsphäre man bereit ist, für wie viel Bequemlichkeit aufzugeben.

Weitere Aspekte

Soziale Netzwerke sind nicht die einzigen, denen wir unsere Daten überlassen. So manche App sammelt im Hintergrund ebenfalls fleißig – ohne dass wir genau wissen was, wann, und wozu. Und niemand kann sagen, er hätte ihnen das nicht erlaubt: Wir haben ja, von den vorinstallierten Apps einmal abgesehen, schließlich unsere Zustimmung gegeben, als wir bei ihrer Installation die Berechtigungen abgenickt haben – da dürfen wir uns jetzt nicht beschweren, dass sie unsere Kontakte und Kalenderdaten lesen, auf den Telefon- (IMEI/IMSI, Netzanbieter) und Netzwerkstatus (WLAN-Netze in der Nähe? Wo ist das Gerät eingebucht?), die Liste konfigurierter Konten, die Log-Dateien, Kurznachrichten, Besitzer-Informationen, und anderes zugreifen, und jederzeit mit den gesammelten Daten "ins Internet" verschwinden können. Und wir nicht einmal wissen, auf welchen Servern wir die Daten letztendlich wiederfinden...

Auf das Thema „Zugriffsrechte" wurde ja bereits im Kapitel Worauf Apps Zugriff haben besprochen. Eine Übersicht über die gebräuchlichsten "Permissions" und

ihre Bedeutung findet sich überdies in Anhang Google Permissions und was sie bedeuten. Daher möchte ich an dieser Stelle auch nicht weiter in die Tiefe gehen. Nur erwähnt werden sollte es, denn auch das betrifft die Privatsphäre.

Ob und warum wir auf unsere Privatsphäre achten sollten, damit befasst sich übrigens auch ein lesenswerter Artikel bei Lifehacker (leider auf Englisch) – und geht dabei auf interessante Hintergründe und Zusammenhänge ein.

Werbefinanzierte Apps

"No money, no honey", heißt es für den Entwickler. Auch er muss von etwas leben – und nicht jeder Entwickler betrachtet die Erstellung von Apps als reines Hobby. Manch einer möchte daher seine erbrachte Leistung gern honoriert sehen. Da leider nicht jeder Anwender bereit ist, für selbige ein paar Cent zu investieren (oder dies nicht tun kann, da die Voraussetzung einer mit dem Google-Konto verknüpften Kreditkarte eine Hürde darstellt), muss eine Alternative her.

"Jeder Depp hat 'ne App" – das ist auch den Betreibern von Werbe-Netzwerken kein Geheimnis mehr. Und so kommen die Beiden zusammen: Werbenetzwerke stellen fertige "Werbe-Module" bereit, die von Entwicklern lediglich in ihre Apps eingebunden werden müssen. Auf den ersten Blick eine typische Win-Win-Situation, wären da nicht gewisse Nebeneffekte...

Schauen wir uns beispielsweise einmal an, welche Voraussetzungen derartige Werbe-Module verlangen. Für MobFox und AdMob, zwei der größten Kandidaten, beschreibt dies ein Artikel bei TechRepublik. Diese beiden Werbe-Module fordern folgende Berechtigungen:

- `INTERNET` (uneingeschränkter Internetzugriff):
  - Guter Cop: Zum Laden des Anzeigen-Materials.
  - Böser Cop: Anzeigen sind Nebensache. Hier sollen fleißig Daten gesammelt, und auf die Server der Werbeindustrie zur Profil-Erstellung hochgeladen werden! Was für Daten das sein können, sehen wir ja gleich.
- `ACCESS_NETWORK_STATE` (Netzwerkstatus anzeigen):
  - Guter Cop: Nur zur Ermittlung, ob auch eine Netzverbindung möglich ist.
  - Böser Cop: Auslesen, mit welchem Netz der User verbunden ist. IP-Adressen und WLAN-Namen abgreifen!
- `ACCESS_COARSE_LOCATION` (ungefährer Standort):
  - Guter Cop: Für Standort-basierte Werbung. Was interessieren schließlich einen Anwender in Deutschland Sonderangebote von Walmart in den USA?
  - Böser Cop: Wissen, wo sich der Anwender wann und wie oft aufhält. So etwas ist für ein gutes Nutzerprofil unheimlich sinnvoll!
- `READ_PHONE_STATE` (Telefonstatus lesen und identifizieren):
  - Guter Cop: Damit dem Anwender die Werbung nicht bei Telefonaten in die Quere kommt.
  - Böser Cop: Netzwerk-Anbieter ermitteln. Eindeutige Identifikation des Anwenders anhand von IMEI und IMSI. Rufnummer des

Anwenders feststellen. Herausfinden, mit wem er so alles telefoniert.

Die geforderten Zugriffs-Berechtigungen lassen sich vom "guten Cop" durchaus alle positiv erklären. Sollte er also Recht haben, wäre dagegen gar nichts einzuwenden. Wie der "böse Cop" allerdings aufzeigt, ist das Missbrauchs-Potential nicht gerade gering: Mit den so verfügbaren Daten lässt sich ein umfangreiches Anwender-Profil erstellen (und sicher auch gut verkaufen). Da mag der Entwickler der App noch so vertrauenswürdig sein: Er hat kaum Einfluss darauf, was die Werbemodule treiben. Oftmals ist ihm diese Problematik nicht einmal bewusst. Und nicht nur diese Problematik, denn es kommt noch schlimmer:

Da App und Werbe-Modul aus Android-Sicht eine Einheit bilden, erhält das Werbemodul auch alle Berechtigungen, die der Entwickler für die App vorgesehen hat. Darf die App also z. B. auf Kalender und Adressbuch zugreifen, stehen Termine und Kontakte auch dem Werbemodul offen.

Ist das nun lediglich ein theoretisches Risiko – oder müssen wir uns wirklich Sorgen machen? Wo solches Potential lauert, bleibt es sicher nicht lange ungenutzt. Und so schreibt FirstPost von einer Studie: 100.000 Apps wurden hinsichtlich der von ihnen verwendeten Werbemodule untersucht. 48% sammelten die Standort-Informationen, 18,5% die IMEI, 4% sogar die Telefonnummern. Einzelne Werbemodule wurden dabei ertappt, Anruf-Protokolle auszulesen, auf Kalender und Kamera zuzugreifen, oder dynamisch weiteren Programm-Code nachzuladen. Die Schlussfolgerung ist daher naheliegend:

> *The new findings point to a flaw in the business model behind apps, Jiang says. Developers rely on revenue from ad libraries to support free apps, but they have no control over what those libraries do. "The current model of embedding ad libraries in mobile apps for monetization purposes poses security and privacy risks. These ad libraries will essentially have the same set of permissions granted to the apps that enclose them. And certain ad libraries may abuse them for other unwanted purposes."*

Zu gut Deutsch:

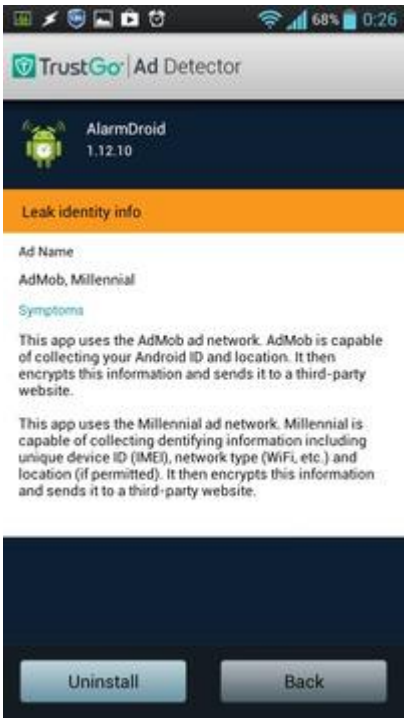
> *Diese neuen Ergebnisse zeigen eine Schwachstelle im Geschäftsmodell hinter Apps auf, so Jiang (Xuxian Jiang leitete die Untersuchung, Anm. d. Ü.). Entwickler sind auf die Einnahmen über die Werbemodule angewiesen, um ihre Apps gratis zur Verfügung stellen zu können – aber sie haben keinerlei Kontrolle darüber, was diese Module tun. "Das aktuelle Modell des Einbettens von Werbemodulen in mobilen Apps zu deren Finanzierung stellt eine Gefahr der Sicherheit und der Privatsphäre dar. Diese Werbemodule können prinzipiell auf dieselben Berechtigungen zugreifen wie die App, in der sie eingebettet sind. Und gewisse Werbemodule könnten sie zu unerwünschten Zwecken missbrauchen."*

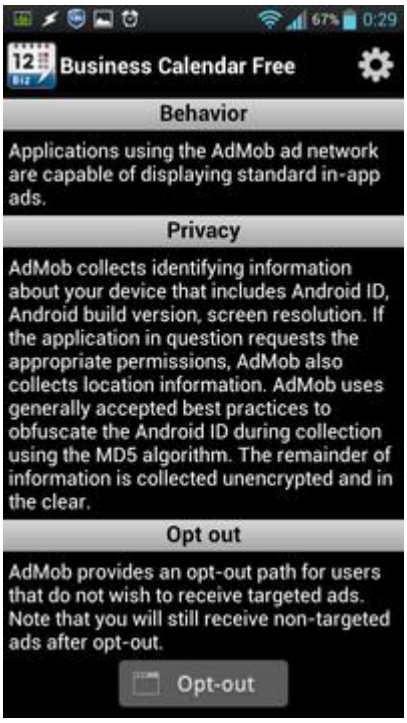
Für den eingangs genannten Artikel bei TechRepublik wurde übrigens auch eine Befragung durchgeführt. Den Teilnehmern wurden einige Beispiele eingeblendeter Werbung gezeigt. Anschließend wurde ihnen erklärt, wie man die von einer App geforderten Berechtigungen liest. Zuletzt kam die Frage: Kann das Werbemodul (wörtlich: die Werber, also die Firmen dahinter) auf sämtliche Informationen zugreifen, die der App selbst zur Verfügung stehen? 16% der Befragten antworteten mit "Nein", 42% wussten keine Antwort. Nur 42% der Teilnehmer sagten "Ja". Wie wir gesehen haben, lag die letzte Gruppe – leider – richtig.

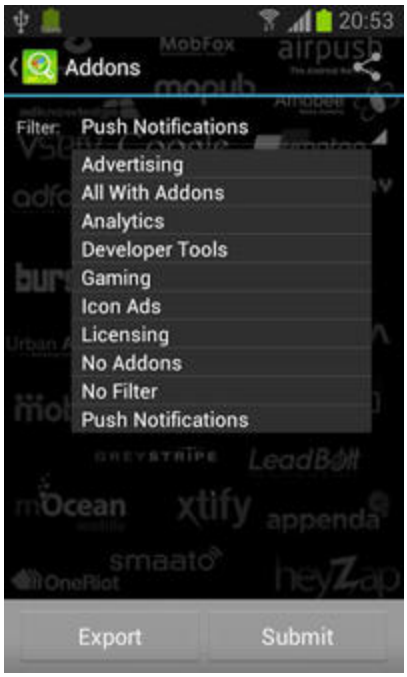
Wer an weiteren Details und Quellen zu diesem Thema interessiert ist: In einem Artikel bei StackExchange habe ich einiges zusammengetragen.

Wie kann man sich schützen?

Zuerst einmal gilt es, mögliche Kandidaten aufzuspüren – wofür sich mehrere Helferlein gern zur Verfügung stellen. In Sachen Werbemodule dürfte TrustGo Ad Detector besonders interessant sein: Wie der Name es richtig vermuten lässt, hat sich diese App auf das Aufspüren von Werbemodulen spezialisiert. Dabei wird auch aufgezeigt, was diese im Einzelnen tun. Lookout Ad Network Detector informiert zusätzlich über das Verhalten der jeweiligen Netzwerke. Die "Treffermenge" war in meinem Kurzvergleich identisch. Während *TrustGo* die schönere Oberfläche bietet, finden sich bei *Lookout* jedoch die detaillierteren Informationen – einschließlich der Möglichkeit eines "Opt-Out", so denn das betroffene Werbenetzwerk diese bietet. Nicht ganz nebensächlich in diesem Zusammenhang: Die App von Lookout verlangt keinerlei Permissions, während *TrustGo* selbst `READ_PHONE_STATE` verlangt (allerdings ohne Netzwerk-Zugriff).







Wer sich nicht allein auf Werbe-Module konzentrieren will, greift vielleicht eher zu Addons Detector – welcher sich auch mit Lizenz-Modulen, Analytics, und weiteren auskennt.

Hat man "furchterregende Übeltäter" entdeckt, stellt sich die Frage, wie man mit ihnen umgeht. Natürlich kann man die betroffenen Apps einfach deinstallieren – das wäre zwar die einfachste, aber nicht unbedingt die wünschenswerteste Lösung. Ein vernünftiger erster Schritt, so man die App weiter nutzen möchte, ist ein Blick in den Google Playstore: Gibt es evtl. eine Kaufversion, die ohne das gefährliche Addon auskommt? Die paar Cent tun niemandem weh. Bei fehlender Kreditkarte hilft oft eine Anfrage beim Entwickler, der eventuell auch eine alternative Bezahlmöglichkeit sieht. Bei der Gelegenheit sollte man ihn auch gleich auf den Grund aufmerksam machen – er könnte durchaus zu jenen 58% gehören, denen dieser Umstand noch gar nicht bewusst ist. In diesem Fall schaut er sich ggf. nach einem weniger gefährlichen Werbemodul um.

Greift all dies nicht: Auch andere Mütter haben schöne Töchter. Im Playstore finden sich mit Sicherheit weitere Alternativen. Und auch wenn diese etwas kosten: Ein paar Cent sollte einem die Privatsphäre schon Wert sein. Findet sich auch dort nichts, gibt es noch die alternativen Märkte...

APPS MACHEN DAS PHONE SMART

Wie viele gibt es da gerade? Ich schreibe hier besser gar keine Zahl – die würde ohnehin bereits nicht mehr stimmen, kaum dass ich auf "Speichern" drücke. Einigen wir uns auf "echt viele". So viele, dass man den Durchblick schnell verliert.

Wer nun meint, ich würde jetzt hier jede Menge Apps vorstellen: Weit gefehlt. Dann müsste ich wahrscheinlich im Wochen- oder doch zumindest Monatsrhythmus eine neue Version dieses eBooks veröffentlichen. Und das ist mir zu umständlich. Dem Leser wahrscheinlich auch, weil der dann immer schauen müsste, ob er auch die aktuellste Version hat – und wenn nicht, an welcher Stelle sich denn nun was geändert hat. Daher habe ich eine bessere Lösung:

Ja, genau – es ist wieder einmal AndroidPIT. Und ja, wieder das Forum. Denn hier pflege ich u. a. eine besondere Liste: App-Reviews nach Einsatzzweck. Eine reine Link-Liste – wobei die Links wiederum auf Forums-Threads verweisen, in denen ich verschiedene Apps kurz vorstelle. Diese widmen sich immer jeweils einem bestimmten Thema, sodass sich mögliche Alternativen bereits im Vorfeld halbwegs vergleichen lassen. Und das sogar ohne sie vorher im *Play Store* selber suchen zu müssen.

Hinzu kommen Kommentare und Ergänzungen anderer Benutzer, Rückfragen und Antworten, sowie zusätzliche Links und Informationen. Und auch für den Fall, dass jemandem ein Themenbereich fehlt, ist gesorgt: In diesem Thread können neue Themen vorschlagen werden. Sobald ich dann wieder Zeit (und Lust) finde, kümmere ich mich dann darum...

Beispiele gefällig? Da wäre etwa der Bereich "Büro, Office, Verwaltung" mit Threads jeweils zu den Themen Barcode Scanner & Generatoren, Kalender, Statistiken für Anrufe, SMS, MMS und Datenvolumen u. a. m.; die "Lese-Ecke" mit den Themen eBook-Reader, Nachschlagen und Übersetzen sowie RSS-Reader. Weitere Rubriken umfassen Reise, Tools, Multimedia, Fernbedienungen... Einfach mal reinschauen!

Auszüge davon finden sich in den folgenden Kapiteln.

Telefonieren

Genau: Es ist kein Zufall, dass die Sektions-Überschrift hier heißt "machen das Phone smart" – und nicht "für das Smartphone". Eigentlich sollte der kleine Knochen ja ein Telefon mit Zusatzfunktionen sein. Auch wenn das bei einigen eher umgekehrt ist – oder sich zumindest die Waage hält. Doch definitiv sollte der Schwerpunkt sein: In Verbindung bleiben. Also das Wichtigste zuerst...

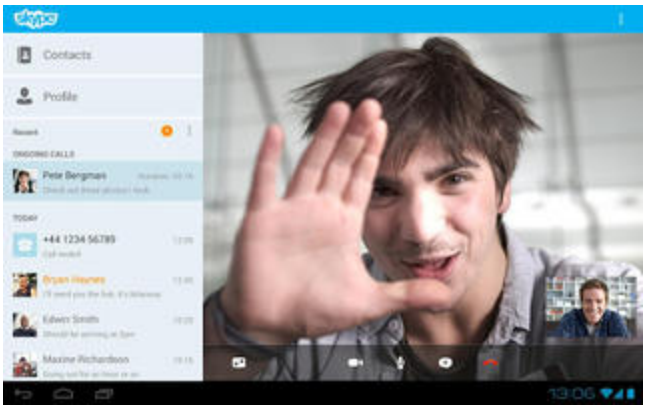
Telefon-Apps

Wie jetzt - braucht man dafür eine extra App? Nun: Genau genommen ist es ja eine App, mit der man das auf seinem Androiden von Anfang an gemacht hat. Auch wenn sie bereits vorinstalliert war, und zum Kernsystem gehört. Aber bei Android ist eigentlich alles, was man auf dem Bildschirm zu sehen bekommt (und alles, was irgendwelche Aktionen bearbeitet) eine App. Und da gibt es (fast) immer Alternativen; die Geschmäcker sind halt verschieden.

Auf meinem ersten Androiden hat mich die vorinstallierte Telefon-App von Anfang an genervt. Zum einen zu unübersichtlich: Die SIM-Kontakte ließen sich nicht ausblenden, jede Nummer wurde gefühlte zehn Mal wiederholt – für jede Aktion wie Anrufen, SMS schicken, separat. Auch wenn es recht wenig Sinn macht, eine SMS an eine Festnetz-Nummer zu schicken (vor allem, wenn zu dem Kontakt auch eine Mobilfunk-Nummer existiert). Und dann die "Fehlschüsse": Das Antippen eines Elements öffnet bei jeder anderen App die zugehörige Detailansicht. Die Telefon-App startete hingegen sofort einen Anruf. Wie oft das schon versehentlich losging – am besten mitten in der Nacht... Also musste dafür dringend eine Alternative her.

Die war zum Glück mit Dialer One (Bild links) schnell aufgetrieben. Diese App beseitigt alle vorgenannten "Pannen": Es wird übersichtlich, und sofern man nicht direkt auf das Telefon-Symbol am rechten Rand tippt, geht auch kein Telefonat los. Für die Aktionen gibt es ein Kontext-Menü. Schön auch die "automatische Suche": Beginnt man mit der Eingabe auf dem Ziffern-Feld, fängt die App im Hintergrund gleich zu suchen an: Ist das Eingegebene Bestandteil einer bereits gespeicherten Nummer? Oder entspricht es, in Buchstaben umgesetzt, dem Namen eines Kontaktes? Die gefundenen Treffer werden dann bereits während der Eingabe aufgelistet (siehe linkes Bild). Einzig zum Bearbeiten der Einträge wird auf die vorinstallierte Kontakte-App zurückgegriffen.

Neben der "herkömmlichen Telefonie" gibt es heutzutage natürlich auch VoIP (Voice-over-IP, also Internet-Telefonie). Die bekannteste Lösung in diesem Feld ist sicherlich Skype, das für nahezu jedes System verfügbar ist. So auch für Android. Wer über eine Front-Kamera verfügt, kann auch Video-Telefonate führen (siehe Bild). Vorausgesetzt, das Gegenüber hat auch diese Möglichkeit, sehen sich beide Gesprächsteilnehmer: Das große Bild zeigt das Gegenüber, man selbst wird als kleines Bild eingeblendet.



Anrufe von Skype-Teilnehmern untereinander (ebenso wie ihre Chats) sind kostenlos, auch Dateien können zwischen Clients gratis übertragen werden (im Mobilfunknetz können jedoch Kosten für die übertragenen Daten anfallen). Für Anrufe in "andere Netze" benötigt man allerdings ein Guthaben. Die Preise bewegen sich hierbei in üblichen VoIP-Regionen.

Setzt der VoIP-Dienstleister hingegen auf das offene SIP-Protokoll, können dessen Android-Kunden auf den seit Gingerbread im System integrierten SIP-Client zurückgreifen, dessen Konfiguration im Abschnitt Internet-Telefonie beschrieben wurde. Dies bietet den Vorteil, dass es komplett ins System integriert ist. Vor jedem Anruf kann man sich also fragen lassen, ob dieser über VoIP geführt – und auch festlegen, dass bei verfügbarer WLAN-Verbindung auf eingehende SIP-Anrufe geachten werden soll.

Alternativen finden sich natürlich im *Play Store*, oder in der passenden Forums-Übersicht – ähnliche, aber auch ganz andere...

Telefon-Widgets

Über *Shortcuts* und *Widgets* haben wir ja bereits im Zusammenhang mit dem Home-Screen gesprochen. Was aber sollen jetzt bitte "Telefon-Widgets" sein?

Klar, da hat Izzy wieder mal einen Begriff konstruiert. Da gibt es also Icons auf dem Home-Screen, die telefonieren können? Ja, so ungefähr. Unter Apps organisieren hatte ich ja bereits den *Folder Organizer* genannt, der die Permission zum Anrufen verlangt – genau hierfür: Es lassen sich damit nämlich auch *Shortcuts* zu Kontakten anlegen. Gibt es also Leute, die man öfter anruft, muss man deren "Kontakte" nicht erst lange im Adressbuch suchen – sondern legt gleich eine passende Verknüpfung auf dem Home-Screen ab. Manche Launcher (wie etwa der bereits genannte *GO Launcher EX*) bieten ebenfalls derartige Widgets an – was dann auch bei diesen die geforderte Anruf-Berechtigung erklären dürfte.

Werden die anderen Features von *Folder Organizer* nicht benötigt, und ist stattdessen eine Alternative gefragt? Der Markt hält davon etliche bereit. Viele davon heißen Speed Dial (nicht nur die verlinkte).

Die Kosten im Blick und unter Kontrolle

Ausführlicheres zu diesem Thema findet sich im Thread Statistiken für Anrufe, SMS/MMS und Datenvolumen.

Alleskönner

Was – schon wieder das gesamte Kontingent an Freiminuten aufgebraucht, und der Monat ist gerade mal zur Hälfte vorbei? Oder einen Schock beim Blick auf die Rechnung bekommen, weil das Datenvolumen hoffnungslos überschritten wurde? "Das muss nicht sein!" Nein, weder Geschirrspülmittel noch Palmolive helfen hier, und Du badest auch nicht gerade Deine Hände darin. Aber mit DroidStats (Bild rechts) wäre das nicht so schnell passiert.

Wie am Screenshot gut zu erkennen, bietet die Übersichts-Seite nicht nur die nackten Daten feil – sondern auch eine Schätzung, wie das Ganze wohl am Ende des "Abrechnungszeitraumes" (also i. d. R. des laufenden Monats) aussieht, wenn so weitergemacht wird wie bisher. Damit man dafür nicht immer erst die App aufmachen muss (das könnte man ja mal vergessen), lassen sich auch entsprechende Widgets auf den Home-Screens platzieren (siehe links).

Und das ist noch längst nicht alles: Will man wissen, mit wem man am meisten/ längsten telefoniert bzw. SMS ausgetauscht hat, teilt *DroidStats* das ebenfalls mit. Und mehr. Kurz: Solange man keinen zu komplizierten Tarif hat, ist *DroidStats* die erste Wahl!

Alternativen? Doch einen recht komplexen Tarif, so mit Sonderkonditionen von..bis, wenn..dann, und was einem noch so kompliziertes einfallen könnte – und *DroidStats* in Sachen Konfiguration überfordert? Dann hilft vielleicht ein Blick auf Call Meter 3G (bzw. dessen Vorgänger Call Meter NG). Die Konfiguration ist bei diesen naturgemäß weit komplexer (so mancher Einsteiger dürfte da leicht überfordert sein) – aber Forum und Support funktionieren hier eben so gut wie bei *DroidStats*.

Telefonie-Spezialisten

Spezialtarife für verschiedene Netze? Etwa *Base* mit 30min E+, Festnetz-Flat und 50min in alle Netze – oder ähnliches? Dann möchte man natürlich gern vorher wissen, in welchem Netz sich die anzurufende Nummer befindet – und stets, wie viele Minuten in welches Netz bereits "verbraten" sind. Und sollte einen Blick auf Zielnetz (Bild links) werfen. Die App bietet recht ausführliche Statistiken – mittlerweile auch für SMS und Daten, sodass diese App jetzt eigentlich in das vorige Kapitel gehört. Mit dabei sind übrigens auch Widget und Warnungen – letztere etwa bei teuren Rufnummern.

Die wichtigsten Features kurz im Überblick:

Zielnetzabfrage per Rufnummer, aus dem Telefonbuch oder mit einem Klick für alle Kontakte
automatischer Abruf neuer Nummern (Info wird als Notiz im Telefonbuch gespeichert)
akustische und optische Zielnetz-Info vor Anruf
zahlreiche Statistiken.

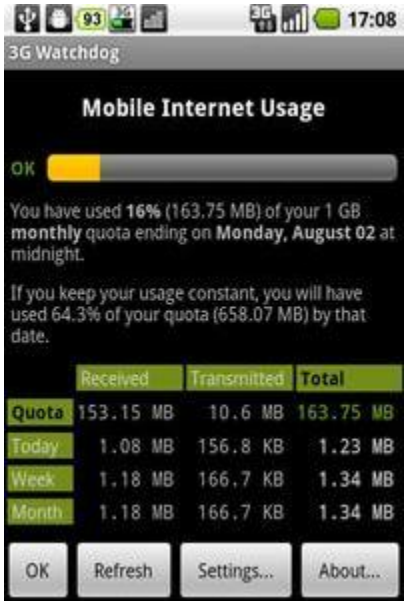
Natürlich lassen sich die Informationen zu Flatrates und Minutenpaketen für die Statistiken konfigurieren.

Nicht verschweigen darf ich aber die für Zielnetz selbst anfallenden Kosten. Hier besteht die Wahl aus verschiedenen Tarifmodellen:

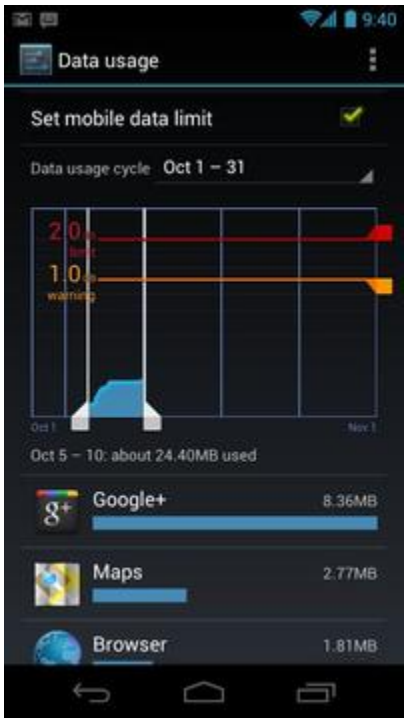
- OnDemand: 0.01 EUR pro Abfrage (25 Abfragen gratis)
- Flatrate: 3.99 EUR einmalig (Bezug über den *Play Store*)

Als Alternative zu *Zielnetz* wäre noch Welches Netz zu nennen. Der Funktionsumfang ist ähnlich (zusätzlich lassen sich noch Limits/Warnschwellen für Anrufe und SMS konfigurieren); laut Beschreibung im *Play Store* fallen jedoch keine "Abfrage-Kosten" an. Dafür bietet die Pro-Version (ca. 3 Euro) einige interessante Zusatz-Funktionalitäten.

Daten-Spezialisten



Der Spezialist für die Datenverbindungen wurde ja bereits zuvor erwähnt, und heißt 3G Watchdog. Diese App überwacht die mobile Datenverbindung (3G/Edge/GPRS) und deren Trafficverbrauch, zeigt ein Benachrichtigungssymbol (Grün, Orange, Rot) in der Statuszeile und gibt eine detaillierte Übersicht zum Verbrauch. Zwei Widgets stehen auch zur Wahl.



Aber *3G Watchdog* kann noch mehr. Sicher: Es warnt vor und bei erreichen der konfigurierten Limits – was für sich genommen schon eine gute Sache ist. So richtig interessant wird es, wenn außerdem die App APNdroid installiert ist: Kurz vor Erreichen des eingestellten Limits dreht *3G Watchdog* dann nämlich auf Wunsch einfach den Hahn zu! Der Zugangspunkt (in der Android-Konfiguration) wird dazu von *APNdroid* so verändert, dass er nicht mehr funktioniert. Und bevor jetzt Panik ausbricht: Selbstverständlich lässt sich diese Änderung rückgängig machen...

Gute Nachricht für alle Anwender (und weniger gute für das 3G-Watchdog-Team): Ab Android 4.0 ist diese App überflüssig. Denn hier ist die entsprechende Funktionalität bereits von Haus aus im System integriert: Eine Überwachung des Datenverbrauchs bis auf App-Ebene herab (sogar getrennt nach Verbrauch bei Vorder- und Hintergrundaktivität), mit Statistik-Graph, und einschließlich der Möglichkeit zum Festlegen eines Warn- und eines „harten" Limits (siehe linkes Bild). Natürlich getrennt nach WLAN und mobiler Datenverbindung.

Nachrichten verschicken und empfangen

Zum "Stay-in-Touch" gehören heutzutage natürlich auch die diversen Nachrichten. Nein, nicht Twitter, Facebook & Co – ich rede von Kurznachrichten (SMS), Multi-Media Nachrichten (MMS) und "richtigen" Mails. Die Erstgenannten gibt es schon seit den frühen Generationen der Mobiltelefone – aber da es mittlerweile auch die Letztgenannten auf unser mobiles Allzweck-Gerät geschafft haben, sollen diese hier ebenfalls mit behandelt werden.

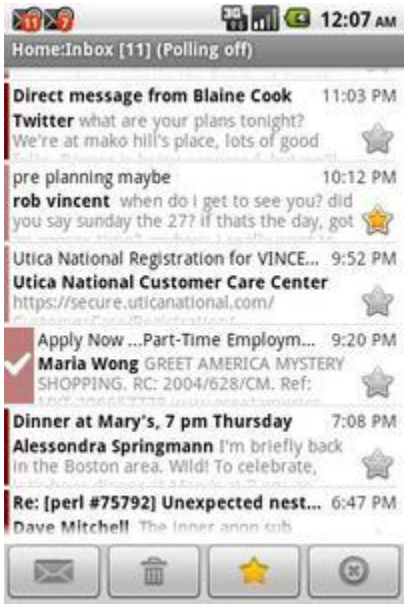
SMS & MMS

Wenn es ums "Texten" geht, scheint Handcent SMS (rechtes Bild) der absolute Favorit zu sein. Allein die Auflistung der "wichtigsten" Features füllt auf der Play Store-Page eine ganze Bildschirmseite (ja, auch aufgrund der vielen Leerzeilen): SMS und MMS werden gleichermaßen bedient, Nachrichten können an Empfängergruppen verschickt werden. Backup und Restore von SMS und MMS. Mehrsprachig (16 Sprachen unterstützt). Mit zahlreichen Plugins erweiterbar. Die ganzen bunten Features lassen sich ja bereits problemlos anhand des Screenshots erkennen.

Damit sollte hierzu das Wichtigste gesagt sein – aber vielleicht sollte ich ja auch noch kurz die gut 4,5★ bei fast 500.000 (!) Bewertungen erwähnen?

Wie – trotzdem ein Alternativ-Vorschlag gewünscht? Naja, da wäre noch chompSMS zu nennen. Bei ca. 4,3★ und über 100.000 Bewertungen kann es mit Handcent fast mithalten. Und was bietet diese App? Sie ist nicht ganz so "bunt", hat aber dafür Chat-Ansicht, Kontaktbilder, Quick Reply, Signaturen, Code-Sperre und auch ein Widget. Die Anwender meinen: Schaut gut aus, und ist umfangreich konfigurierbar. Besser? Schlechter? Das sind wieder sehr subjektive Entscheidungen, die jeder selbst treffen muss.

Mail



Auch die EMail ist aus unserem Alltag nicht mehr wegzudenken. Das hat man bei Android ebenfalls erkannt, und liefert eine passende App gleich mit. Welche das ist, ist aber teilweise auch noch Hersteller-spezifisch. Aber egal: Wer mit der bei sich installierten App ohnehin unzufrieden ist, braucht sich um selbige ja nicht weiter kümmern. Halten wir also besser nach einer guten Alternative Ausschau!

Eine der bekanntesten und beliebtesten Apps hierfür ist K-9 Mail (linkes Bild). Unterstützt mehrere Accounts, auf Wunsch auch mit "gemeinsamer Inbox" (quasi als "Zusammenfassung" der einzelnen Eingangs-Ordner; das einer Mail zugehörige Postfach erkennt man dort an einer farblichen Markierung – wobei sich die Farben dafür natürlich wählen lassen). Als Protokolle werden POP3, IMAP4, und Exchange unterstützt; auch das Google Mail Konto lässt sich natürlich einbinden. "IMAP-Push" lässt sich ebenfalls verwenden (d. h. der Mail-Server gibt der App Bescheid, wenn neue Mail da ist).

Natürlich ist dies nur ein Auszug aus dem Funktionsumfang – da könnte man noch weit mehr aufzählen. Zum Beispiel die Unterstützung für PGP (signieren/ verschlüsseln von Mails), konfigurierbare Benachrichtigungen in der "Notification Area" (dem "Balken" ganz oben auf Deinem Screen, den man nach unten "aufziehen" kann) sowie per Audio, Shortcuts für den Home-Screen, Signatur-Unterstützung...

Da jetzt sicher wieder auf eine Alternative gewartet wird, habe ich natürlich auch hier etwas herausgesucht: MailDroid wäre da eine Option. Zumindest von der Beschreibung her klingen die Features vergleichbar – und auch die Play Store-Bewertungen scheinen das zu unterstützen. Bei Interesse also einfach mal einen Blick darauf werfen! Und ansonsten, alternativ, einen Blick in die passende Übersicht...

Lektüre

eBook Reader

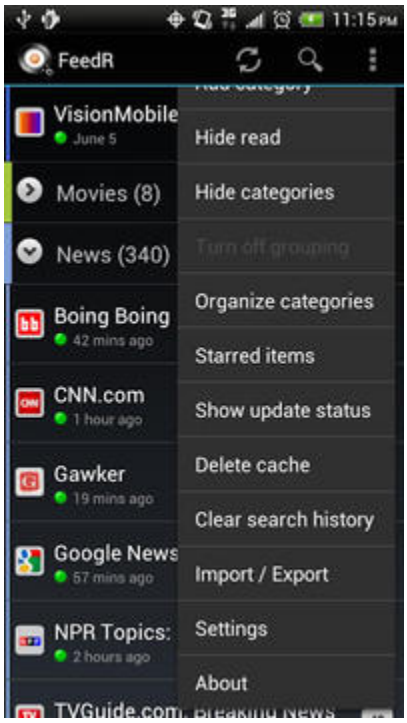
Bei den eBook-Readern ist Moon+ Reader (in der Pro-Version für ca. 4 Euro – es gibt auch eine werbefinanzierte Gratis-Version) mein klarer Favorit. Sofern man auf DRM-behaftetes Material verzichten kann, kann ihm keiner das Wasser reichen:

- Zugriff auf zahlreiche Online-Bibliotheken direkt aus der App (vorkonfigurierte wie z. B. Izzys Bibliothek mit über 5.000 gratis verfügbaren Büchern in deutscher Sprache, und eigene)
- Formate: txt, html, epub, mobi, pdf, cbr, umd, fb2, zip
- verschiedene Themes (u. a. "Tag" und "Nacht" – letzteres im rechten Screenshot)
- Unterstützung für Online und Offline Wörterbücher
- Highlighting, Annotations, Bookmarks, Share
- Scrolling, Vorlesen (Pro-Version)

Und damit sind nur die wichtigsten Funktionen kurz angerissen. Mehr Details gibt mein Testbericht (auf der App-Seite verlinkt). Und auch der zugehörige Forums-Thread.

Alternativen? Gibt es nicht wirklich. Der FBReader ist noch recht verbreitet – unterstützt aber weniger Formate, und möchte außerdem noch auf Konto-Informationen zugreifen (sicher für's Einkaufen von Büchern, welches er wohl unterstützt). txtr unterstützt neben ePub auch PDF – benötigt aber fünf mal soviel Platz für die Installation. Wiederum recht verbreitet und gut bedienbar ist Aldiko, der auf manchen Geräten bereits vorinstalliert ist (und zusätzlich DRM-geschütztes Lesematerial unterstützt). Wie bereits geschrieben: Ein Blick in die Übersicht im Forum gibt mehr Informationen: Dort ist u. a. eine Matrix enthalten, die einen allgemeinen Vergleich verfügbarer Lese-Apps ermöglicht.

RSS Newsreader



Auch hier habe ich mit FeedR meinen Favoriten. Alle Feeds lassen sich wunderbar kategorisieren, wobei Kategorien als Ordner fungieren (wie auch im Screenshot zu sehen), und mit dem Google-Reader synchronisieren (so man es braucht). Die App lässt sich sehr umfangreich konfigurieren: So kann man z. B. festlegen, dass *FeedR* automatisch jede Stunde aktualisieren soll, sofern man in einem WLAN Netz eingebucht ist. Natürlich lassen sich auch einzelne (oder alle) Feeds jederzeit manuell aktualisieren.

Die Feed-Sammlung kann man ebenfalls exportieren – oder die aus einem anderen Reader exportierte Einlesen, was einen Umstieg vereinfacht. Außerdem gibt es Sortierfunktionen für Feeds, Artikel und Ordner, sowie ein einfaches Widget.

Einziges Manko ist vielleicht, dass *FeedR* nur bis auf die Trailer-Ebene (den Vorspann vor dem Haupttext) die Inhalte selbst darstellt – für den eigentlichen Artikel wird der Browser aufgerufen. Das jedoch wahlweise über einen "Mobilizer", damit es schneller geht. Achja: Und seit Neuestem werden auch Podcasts unterstützt...

Alternativen? Ja, gibt es auch. Da wäre sicher zuerst NewsRob zu nennen. Und daneben gibt es noch eine ganze Reihe weiterer Kandidaten, von denen einige wieder in einer Forums-Übersicht aufgeführt und kurz vorgestellt sind.

Nachschlagewerke

Diese wurden ja bei den eBook-Readern schon einmal kurz erwähnt: Hier machen sie natürlich definitiv Sinn. Insbesonders bei der Lektüre fremdsprachlicher Texte. Was steht in diesem Bereich zur Verfügung?

Da wäre zunächst einmal mein Favorit: Fora. Diese App eignet sich vorzüglich für nahezu alle Einsatzgebiete. Sie unterstützt zahlreiche Online-Wörterbücher, und kann auch Google Translate zum Übersetzen heranziehen. Darüber hinaus wird zur Offline-Nutzung (also ganz ohne Datenverbindung) das StarDict Format unterstützt, für das es zahlreiche Wörterbücher frei zum Downloaden gibt. Ein Blick in den Testbericht gibt weitere Details preis.

Als Alternative mit ähnlichem Funktionsumfang wäre an dieser Stelle ColorDict zu nennen. Ein großer Vorteil bei ColorDict ist, dass sich diverse Wörterbücher direkt aus der App heraus herunterladen und lokal installieren lassen.

Darüber hinaus gibt es aber noch eine ganze Reihe weiterer Kandidaten, die einen Blick wert sind – zu finden wieder einmal in einem meiner Forums-Threads.

Schule & Studium

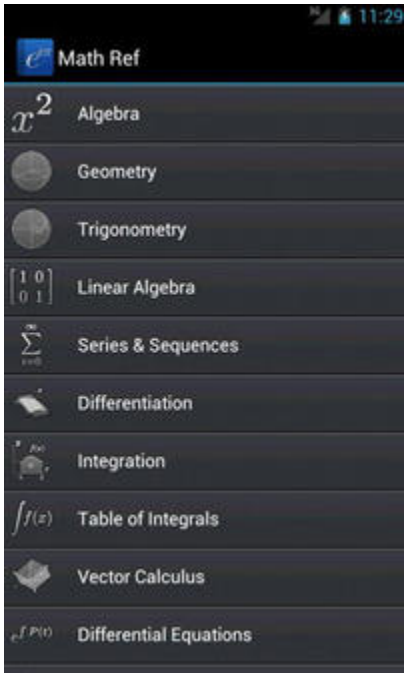
Auch Schülern und Studenten steht "Andy" hilfreich zur Seite: So passt z. B. der mit Formel- und Nachschlagewerken gefüllte Schulranzen früherer Tage heute bequem in die Jacken- oder Hosentasche.

Formelsammlungen und Übersichten

Da wäre als ***das*** Highlight zuerst die App Merck PSE zu nennen: Mit 4,8 von maximal möglichen 5 Punkten im *Play Store* absolut topp bewertet, kann sie mit Fug und Recht hier als Vorzeige-App herhalten.

Merck's Periodensystem gibt Schülern, Chemiestudenten und Lehrenden die Möglichkeit, sich umfassend und interaktiv über die Elemente des Periodensystems zu informieren. Damit steht Interessierten ein mehrsprachiges Nachschlagewerk zur Verfügung, das komplexe Inhalte intuitiv erfahrbar macht. So wird die App im *Play Store* beschrieben.

Jede Menge Informationen stehen zu den einzelnen Elementen zur Verfügung. In verschiedensten Ansichten. So lässt sich über einen "Zeitregler" recht einfach feststellen, welche Elemente zum Zeitpunkt X bereits bekannt waren. Oder anzeigen, wer sie entdeckt hat. Oder, oder, oder – der Möglichkeiten sind hier viele. Für weitere Details empfiehlt sich ein Blick in den Testbericht sowie auf die Projektseite – wobei man sich bei letzterer nicht davon irritieren lassen sollte, dass laufend von irgend einem iPhone die Rede ist...



Und natürlich gibt es auch entsprechende Referenzen und Nachschlagewerke für andere Fächer, etwa Physik oder Mathematik, wie z. B. das sowohl für Smartphones als auch Tablets optimierte Math Ref (Abbildung rechts), die für wenig Geld (etwa 0,75 Euro) eine große Menge Wissen in kompakter Form anbietet. Eine umfangreichere und detailliertere Übersicht findet sich wieder einmal im Forum.

Nachschlagen und Übersetzen

Nachschlagewerke haben wir ja bereits weiter oben behandelt. In der Regel werden Nachschlagewerke zur Begriffserklärung und Wörterbücher zur Übersetzung innerhalb ein und derselben App behandelt – schließlich ist das Prinzip ja auch in beiden Fällen das gleiche: Einen Begriff nachschlagen, und die zugehörige Information anzeigen.

Vokabeln & FlashCards

Wer nun nicht ständig zu Nachschlagewerken und Wörterbüchern greifen möchte, muss sich die Begriffe einprägen. Und da hören wir schon die Stimme unserer "Vorfahren": *Wir haben das früher mit kleinen Zetteln in einer Streichholzschachtel gemacht!*

Oh ja, das kenne ich aber auch noch – nur waren meine Streichholzschachteln aus Stabilitätsgründen schnell durch TicTac-Schachteln ersetzt. Das System ist geblieben: Damals stand auf der einen Seite des Zettels der Begriff, und die Bedeutung/Übersetzung auf der Rückseite. Heute nennt sich das "FlashCards", und statt umdrehen muss man antippen...

Die derzeit best bewertete, umfangreichste und noch dazu kostenlose App ist AnyMemo (linkes Bild). Sie bezeichnet sich selbst als *Vokabeltrainer mit dem adaptiven Lernalgorithmus* – was heißt, dass entweder die App sich dem Lernenden anpasst (was wohl gemeint ist), oder auch umgekehrt. Über 560 Datenbanken für Arabisch, Englisch, Chinesisch, Japanisch, Spanisch, Französisch uvm. stehen zur Verfügung – es lassen sich aber ebenso eigene erstellen: Import aus verschiedenen Formaten (u. a. auch CSV) wird unterstützt, Export ebenso (z. B. zur Datensicherung oder zur Weitergabe der eigenen Sammlung). *Keine Werbung*, verspricht der Entwickler auch bei der Gratis-Version. Dennoch: Der Preis der Pro-Version ist mit knapp zwei Euro mehr als gerechtfertigt – eigentlich sogar ein Schnäppchen, wenn alles so funktioniert wie beschrieben!

Wem die App nicht gefällt, oder wer sich zunächst nach Alternativen umsehen möchte – der wird, wie gewöhnlich, in einem speziellen Forums-Thread fündig.

Studentenfutter: Mensa-Pläne

Lernen macht hungrig. Also muss etwas zu essen her. Der Student lebt nicht vom Aldi allein, und auch – entgegen allen Vorurteilen – nicht vom Pizza-Bringdienst. Es gibt da so gewisse Einrichtungen, die sich "Mensa" nennen. Und einige davon sollen tatsächlich gesunde Nahrung servieren...

Wie aber diese ausfindig machen? Zum Glück gibt es Android, und jede Menge Apps. Viele davon ortsbezogen (dafür bitte im entsprechenden Forums-Thread nachschauen). Aber es sind auch einige dabei, die eine ganz respektable Abdeckung bieten. Und so lässt sich der Speiseplan der Stamm-Mensa z. B. mit Studentenfutter als Widget direkt auf dem Homescreen platzieren (linkes Bild).

Dies beherrscht auch MyMensa (rechtes Bild), zumindest in der Pro-Version. Aber auch schon in der gratis "Lite" Version ist der Funktionsumfang beachtlich: Wo ist die nächste Mensa? Zumindest die nächste unterstützte sollte sich mit dieser App leicht ausfindig machen lassen. Was gibt es da? Die Frage wird definitiv beantwortet. Taugt das was? Ein Blick in die Bewertungen der Kommilitonen sollte das klären. Wie schaut das aus? Mit etwas Glück hat's schon jemand fotografiert und hochgeladen.

Die Liste unterstützter Orte und Mensen ist bereits beachtlich lang. Sollte doch noch ein Ort oder eine Mensa fehlen, so freut sich der Entwickler über eine kurze Rückmeldung. Damit die Liste noch länger werden kann.

Unterwegs

Da es hier um *Mobil*telefone geht, sind wir natürlich auch mobil. Die Warte- und Reisezeit in Bahn, Bus und Flieger haben wir uns bereits mit Lektüre verkürzt – aber wohin soll es eigentlich gehen? Und wie kommen wir dahin? Das hätten wir doch fast vergessen...

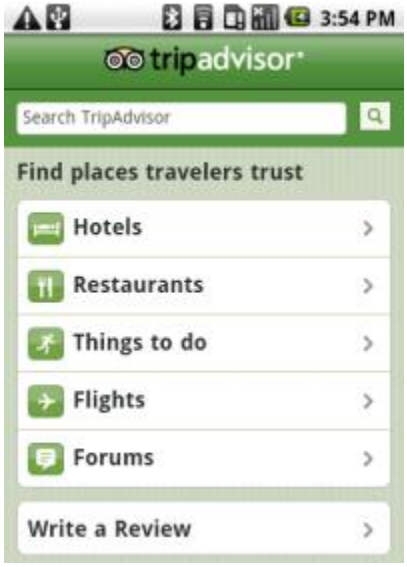
Fahrpläne

Für den ÖPNV (Öffentlichen PersonenNahVerkehr) ist sicher das sowohl für Smartphones als auch für Tablets optimierte Öffi (Bild links) der absolute und ungeschlagene Spitzenreiter unter den verfügbaren Apps. Nicht nur aufgrund seines Umfangs, sondern auch seiner Aktualität (ja, mehr als zwei Updates die Woche können manchmal schon ein wenig nerven). Aber wer irgendwo von A nach B möchte, liegt mit dieser App goldrichtig. Und zwar egal, ob in Berlin, München, Dresden, oder in Wien, Salzburg, Innsbruck, oder Graz, Basel... oder gar London, San Francisco, Melbourne oder Dubai (aha, daher die ständigen und vielen Updates). Öffi versorgt zielsicher mit Informationen wie nahegelegene Haltestellen (das Smartphone weiß ja, wo es ist - und dafür benötigt die App die Berechtigung für den Standort-Zugriff) inkl. Karte, den nächsten Abfahrtzeiten (inkl. etwaiger Verspätungen – hierfür und für die nächsten beiden Punkte wird der Internet-Zugriff benötigt), Verbindungen, und Netzplänen.

Warum Öffi auf die Kontakte zugreifen möchte? Damit es auch gezielt zu ihnen führen kann. Oder zu einem im Kalender eingetragenen Treffpunkt. Kalender schreiben? Klar doch, die Verbindung zum Termin. Laut Beschreibung kann es eine Verbindung auch per Mail an ausgewählte Kontakte verschicken – macht ja alles irgendwo Sinn, oder?

Alternativen? Nicht in dem Umfang von *Öffi*, aber klar gibt es sie. Unter anderem viele lokale Spezialitäten – wie etwa den ZVV-Fahrplan für Zürich und Umgebung. Wie gewohnt, finden sich in einer Forums-Übersicht wieder einmal ausführlichere Informationen.

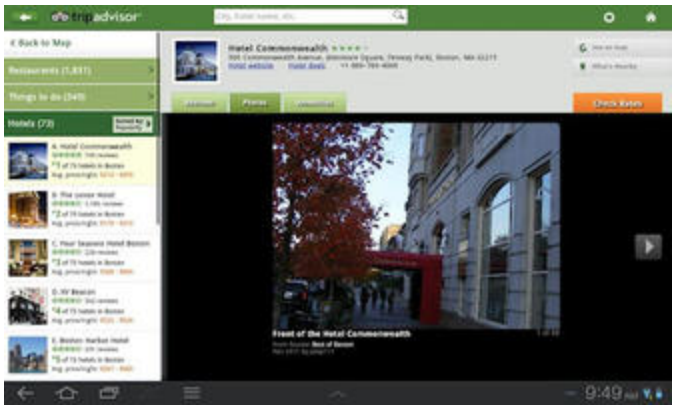
Und was, wenn die Reise ein wenig weiter gehen soll? So von Stadt zu Stadt, wo die S-Bahn nicht mehr fährt? Dann wird z. B. zum DB-Navigator (rechtes Bild) gegriffen. Klar gibt es gewisse Überschneidungen: Diese App bietet Fahrpläne für DB Bahn, S-Bahn, U-Bahn und Bus von VRR, VRS, RMV, VRN, VBB, VGN, VGM, MVV und NVV, Frankreich (SNCF), Österreich (ÖBB), Schweiz (SBB) und viele weitere. Sie berücksichtigt nicht den privatisierten Nahverkehr – zeigt aber bei allen anderen Verbindungen etwaige Verspätungen auch mit an. Sogar buchen soll man mit dieser App können.



Was denn, noch nicht weit genug weg? Möchte da wer "die Fliege machen", und sucht nach Flugverbindung mit Hotel und allem, was so dazu gehört? Dem soll auch hier geholfen werden – z. B. mit dem TripAdvisor (Bild links). Wie der Screenshot schon zeigt, findet man mit dieser App nicht nur Flüge und Hotels, sondern auch gleich noch das passende Restaurant. Und vorhandene Sehenswürdigkeiten. Das Ganze auch gleich mit Bewertungen von Leuten, die schon da waren – und der Möglichkeit, selbst eine Bewertung zu hinterlassen. Ein Zugriff aufs Forum lässt sich da auch am vorletzten Menüpunkt erahnen. Übrigens ist diese App ebenfalls sowohl für Smartphones als auch für Tablets optimiert, wie der Screenshot unten zeigt. Einziger Haken an der Sache: Die App funktioniert nur mit bestehender Netzverbindung – im Ausland können daher Roaming-Gebühren fällig werden, sofern man sich beim Einsatz nicht auf WLAN-Zugänge beschränkt.

Ein Kommentar weist bei dieser App noch auf einen Kniff hin: Man muss die App nicht unbedingt installieren – es gibt auch die zugehörige mobile Webseite, mit gleichem Funktionsumfang...

Und bevor ich es vergesse: Zu fliegenden Apps gibt es weitere Informationen in diesem Forums-Thread.



Navigation

Mit den Öffentlichen Verkehrsmitteln kommen wir nun also klar. Wie aber sieht es mit Auto, Rad und zu Fuß aus? Damit beschäftigt sich dieser Forums-Thread – und das aktuelle Kapitel.

Google Maps ist in diesem Umfeld sicher die bekannteste App, und auf den meisten Androiden bereits vorinstalliert. Das kleine Monster bietet eigentlich grundlegend alles, was zur Navigation benötigt wird: Kostenlose GPS-Navigation mit Sprachführung, Orte finden, Bewertungen, Empfehlungen – und bindet auch soziale Komponenten ein (Freunde auf der Karte sehen und bei Orten einchecken). Die Routenplanung eignet sich sowohl für die motorisierte als auch die unmotorisierte Fortbewegung.

Eine kleine Einschränkung könnte sein, dass man normalerweise dafür eine ständige Netzverbindung benötigt (es ist also eine sogenannte "offboard" Lösung, da nicht alles Material "onboard" ist). Aber selbst das lässt sich umgehen, indem man den Karten-Cache vorher entsprechend befüllt. Wem der Radius der von Google angebotenen Pre-Caching-Variante zu gering ist, der kann dies bequemer auch mit Maps(+) erledigen.

Natürlich gibt es auch hier wieder Alternativen, für die ich jedoch auf den genannten Forums-Thread verweise. Wer die aktuellste Version von Google Maps nutzt, braucht vielleicht auch keine Drittanbieter-App mehr für den Offline-Betrieb: Mittlerweile erlaubt die App, größere Kartenausschnitte vorab in den Cache zu laden. Abgesehen von der Routenberechnung selbst, lässt sich Google Maps somit ebenfalls als OnBoard (bzw. Offline) Lösung nutzen.

Daneben gibt es aber außerdem noch Spezial-Lösungen, die zumindest kurz erwähnt werden sollten. Wie etwa GPS Mate und OruxMaps (Outdoor Navigation für Radler, Wanderer, Skifahrer, Segler und Piloten - sowie Geo-Caching), GPS Compass Map (erstellen eigener Tracks – also Routen-Erfassung mit anschließendem Nachschauen, wie man gelaufen/gefahren ist), Ski Eagle GPS (für Ski-Fahrer und Pisten-Fans), diverse Location-Sharing Apps, GPS Toolboxen,

Speedometer, GPS Reminder (Wecker, die bei gewissen Koordinaten "klingeln": "Da ist die Post – jetzt gib endlich den Brief auf!" oder "Weindepot – da ist doch so ein Loch im Keller..."), und, und, und. Bei Interesse also wirklich mal einen Blick in den genannten Thread werfen.

Lokalkolorit

Was soll das denn jetzt sein? Wenn man reist, findet man viele lokale Gegebenheiten vor. Viele unterschiedliche. Touristen erkennt man häufig am (immer weniger um den Hals hängenden) Fotoapparat, am ständigen Knippsen, und oftmals auch am unkoordinierten Rascheln und Drehen des Stadtplans. Die Einheimischen ziehen höchstens einmal das Handy heraus – um zu schauen, wie spät es ist...

So wie der Typ da drüben. Hm, komisch: Der Kleidung nach ist der aber von ganz woanders. Scheint jedoch genau zu wissen, wo er hier was findet. Eben vertraut mit den lokalen Gegebenheiten. Und was hat er auf dem Handy geschaut? 10 Sekunden, und er wusste, wo die nächste Szene-Kneipe ist! Holla!

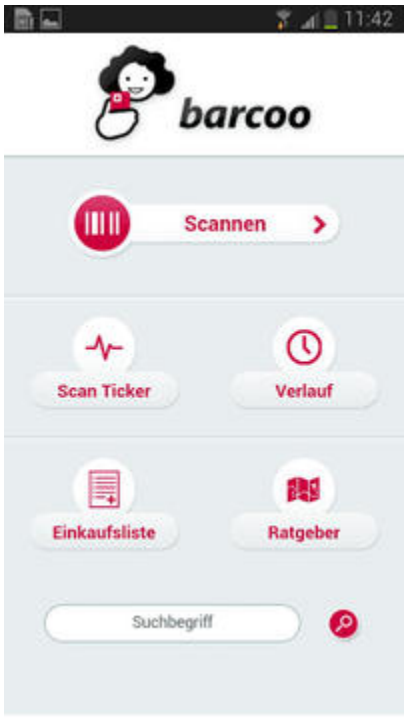
Man ahnt es schon: Da war eine App im Spiel. "Allways be a local" – mit diesem Slogan wirbt Aloqa. Die verfügbaren Informationen sind in sogenannten "Kanälen" organisiert, wie etwa Theater, Restaurants, Krankenhäuser, u. a. m. So kann jeder die Kanäle abonnieren, die ihn interessieren – und die anderen ignorieren.

Den aktuellen Standort ermittelt *Aloqa* via GPS – wie oft die App das tun soll (angefangen von alle 5 Sekunden bis hin zu "gar nicht", also manuell – per Default immer dann, wenn man die App in den Vordergrund holt), lässt sich nach eigenen Bedürfnissen konfigurieren, damit man den Akkuverbrauch ein wenig unter Kontrolle halten kann. Pro Kanal kann man auch einstellen, ob nach neuen Inhalten gesucht – und wie man auf selbigen aufmerksam gemacht werden soll. Die Möglichkeiten umfassen hier: Nicht aktualisieren, "still und heimlich" aktualisieren, vibrieren bei neuen Inhalten, oder einen Alarmton wiedergeben.

Da die Informationen somit immer recht aktuell sind, sind es in der Tat nur wenige Klicks bis zur nächsten Szene-Bar. Oder zum McDonalds. Oder zum Schuhladen... Weltweit. Und wem das nicht reicht, der erstellt einfach seinen eigenen Kanal...

Wer's lieber spezifischer und lokaler haben möchte, kann natürlich alternativ zu anderen Apps greifen. Etwa zu meinestadt.de...

Shopping



Jetzt hat uns das Navi also in die Shopping-Meile geführt – und da stehen wir nun, und haben dieses tolle XYZ in den Händen. Taugt das was? Stimmt der Preis? Gibt es das vielleicht nebenan günstiger? "Ja, ja, nein", wird der Verkäufer sagen, und einen vom Pferd erzählen. Denken wir jedenfalls. Und die Chance besteht ja, immerhin will er was verkaufen. Aber müssen wir ihm deshalb blind vertrauen? Gibt es Alternativen? Auch für Android? – "Nein, ja, ja..."

Der Klassiker schlechthin in diesem Bereich nennt sich Barcoo, ist gratis im *Play Store* erhältlich, und "scannt Dich glücklich". Äh – scannt? Na klar: Drehen wir doch mal das XYZ in der Hand, da ist bestimmt irgendwo ein Barcode drauf. Den scannen wir mit *Barcoo* ein – und *Barcoo* zeigt uns sogleich Details zum Produkt. Aha: Online also für diesen Preis. Und was es taugt, das könnten die Nutzer-Bewertungen aussagen. Gibt es Shops in der Nähe, die XYZ zu einem günstigen Preis anbieten, werden auch die angezeigt – sogar auf der Karte.

Sein volles Potential spielt Barcoo aber bei Lebensmitteln aus: Inhaltsstoffe werden hier ebenso aufgeführt wie die "Lebensmittel-Ampel", die unsere Politiker nach gründlichem Überdenken ja vielleicht 2057 einführen werden (oder auch nicht). Kurzum: Das wäre meine Empfehlung in diesem Bereich.

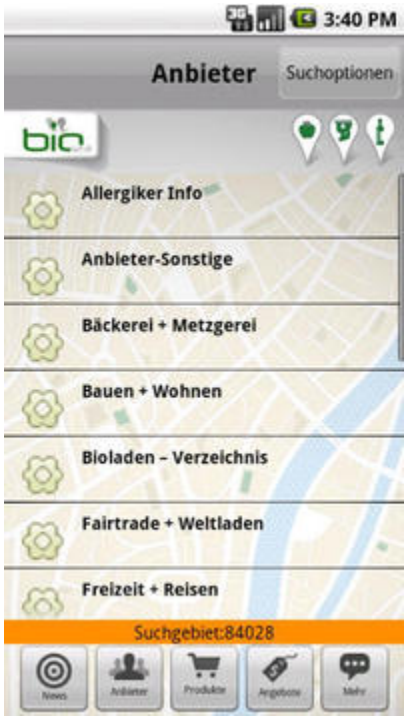
Dann wären da natürlich noch weitere Schnäppchen-Jäger-Apps, wie das beliebte myTopDeals. Oder Gutschein-Apps. Dinger, die auf Sonder-Aktionen ("Heute Friss-die-Hälfte zum doppelten Preis", oder umgekehrt?) hinweisen. Achtung – jetzt kommt der übliche Spruch: Einfach einen Blick in den passenden Forums-Thread werfen...

Gesundheit

Ernährung

Auf die "Ernährung" möchte ich hier in drei Schritten eingehen: Da wäre zuerst der Einkauf mit der Frage "Wo?", gefolgt von der Frage "Was ist drin in den Lebensmitteln?". Und schließlich die Frage: Was tun mit dem Einkauf?

Gesunder Einkauf



Was fällt einem zum Thema "gesunder Lebensmittel-Einkauf" als erstes ein? Klar: Bio. Und für Android? Bio123. Wie viele derartige Apps, ist die Einsatz-Eignung regional verschieden – und hängt nicht zuletzt von der vorhandenen Datenbasis ab. Einen Versuch wert ist es jedoch allemal, und zumindest der Bereich München ist, den auf der App-Seite im *Play Store* verfügbaren Screenshots zufolge, hier recht gut abgedeckt.

Postleitzahl und Umkreis in km eingegeben, und schon kurz darauf zeigt sich eine Liste mit Fundstücken und ihrer Anzahl: Bioläden, Bistros, Bäckereien, Cafés... Die gewünschte Kategorie angetippt, und die Details werden offenbar: Wie heißt der Laden, und wie weit ist er entfernt? Jetzt den gewünschten Eintrag noch ausgewählt, und es gibt die Öffnungszeiten, Telefon, ggf. auch Website (mit der Möglichkeit, selbige im Browser zu öffnen) und EMail (kann mit der Mail-App geöffnet werden). Und natürlich die Anschrift – mit der Möglichkeit, diese auch gleich auf der Karte anzuzeigen.

Als kleines Schmankerl wird auch gleich zu Schritt 3 gesprungen: Bei Bio brauchen wir ja nicht zu schauen, was drin ist – Bio natürlich. Also geht es gleich direkt zu den Rezepten. Und wem das noch nicht schnell genug ist: Es stehen ja auch Bistros, Cafés und Restaurants in der Liste...

Was ist drin?

Nicht immer kann alles Bio sein. Für den Einen ist das preislich nicht drin, beim Nächsten gibt es einfach keinen Bioladen in akzeptabler Entfernung, und der Dritte findet nicht alle benötigten Zutaten. Was also tun im "normalen Supermarkt"? Wie lässt sich da herausfinden, was drin ist?

Zunächst lässt sich da auf eine im Kapitel Shopping bereits genannte App zurückgreifen: Barcoo. Wie dort bereits genannt, soll sie ja im Bereich Lebensmittel ihr volles Potential ausspielen. Tut sie auch: Sie sagt nicht nur, wo es vielleicht günstigere Angebote gäbe – sondern zeigt die Lebensmittel-Ampel (rot-gelb-grün für viel/ akzeptabel/wenig Zucker, Fett und Co), Bewertungen anderer Kunden, und oftmals auch Hintergründe und soziale Kompetenz des Herstellers.

Etwas weiter geht da der das ist drin Scanner (siehe Bild rechts), der besonders für Allergiker interessant sein dürfte: Diese App zeigt an, welche Allergieauslöser in der Packung mit drin stecken (zusätzlich zum gewünschten Lebensmittel). Und da nicht immer alle Zutaten bekannt sind, steht auch noch dabei, welche Allergieauslöser bekanntermaßen *nicht* drin stecken.

Damit verbleiben noch die kryptischen E-Zutaten, die einem immer die Haare zu Berge stehen lassen: Manche Lebensmittel scheinen ja fast ausschließlich aus solchen zu bestehen! Dank sei der chemischen Industrie: Im Zeitalter von Rinderwahn, Schweinepest, Vogelgrippe, Atomfisch und EHEC-Gemüse wüssten wir ja ohne sie gar nicht mehr, was wir überhaupt noch essen könnten... Achso, für die E-Nummern hat der *das ist drin Scanner* auch ein Register integriert, das "Inhaltsstoffe-Lexikon".

Rezepte

Bio-Rezepte hatten wir ja bereits beim gesunden Einkauf als Dreingabe. Für "normale Rezepte" gibt es sicher auch viele Apps, die noch mehr Megabyte im Speicher belegen, und zum Teil auch seltsame Berechtigungen verlangen. Daher erlaube ich mir an dieser Stelle einmal einen kleinen Kunstgriff:

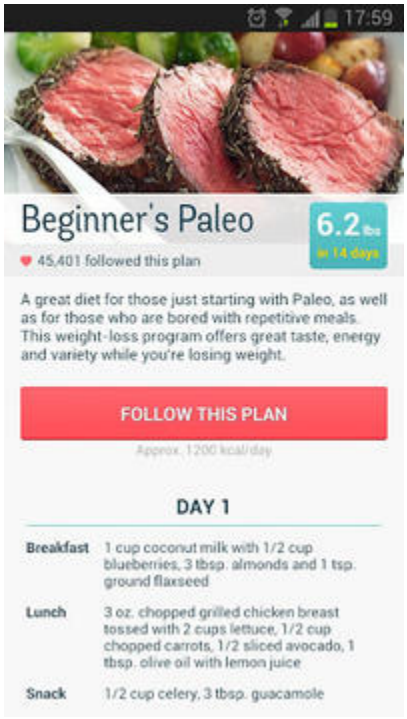
Wir greifen zum mobilen Browser, und legen ein Lesezeichen für http://m.essen-und-trinken.de/ an. Und schon haben wir eine recht umfangreiche Rezeptsammlung zur Hand!

Wer sich doch lieber eine App installieren möchte, wird wieder einmal im Forum fündig...

Abnehmen: Weg mit den Pfunden!

Die Hose geht nicht mehr zu? Der Gürtel ist zu kurz? Oder muss gar schon eine Schubkarre her, um den Bierbauch zu transportieren? Höchste Zeit, den Pfunden den Kampf anzusagen! Und welche Apps unterstützen uns dabei? Die "große Übersicht" findet sich wieder einmal im Forum – die "Kompakt-Ausgabe" gibt es hier:

Diät



Keine Lust auf Sport? Vielleicht tut es ja auch eine reine Diät. Dabei kann DietPoint (Bild links) helfen:

Die App ist zwar (noch) nicht komplett "eingedeutscht" – doch die deutschen Bewertungen im *Play Store* lassen darauf schließen, dass sie auch hierzulande gut verwendbar ist. Hier lassen sich Diät-Pläne verwalten, und auch gleich in einer Tag-für-Tag Diät aufreihen, eine passende Einkaufliste lässt sich ebenfalls erstellen. Der zu erwartende Gewichtsverlust wird anhand der hinterlegten (und stets gepflegten) Daten berechnet. Mit dabei sind auch BMI sowie BMR Rechner, Tipps und Ratschläge – und die direkte Einbindung eines Forums zum Austausch mit anderen interessierten.

Alarme weisen auf bevorstehende Mahlzeiten hin und fördern so eine dem Abnehm-Prozess und der Gesundheit förderliche Regelmäßigkeit. Da neben dem imperialen Maßsystem auch das metrische unterstützt wird, sollten Komplikationen in dieser Hinsicht minimiert sein. Kostenlos ist das Ganze obendrein – was gibt es also zu verlieren, außer den Pfunden?

Sport

Diät ist furchtbar? Sicher, aber vielleicht ja notwendig. Alternativen? Okay, die gibt es natürlich auch: (Mehr) Sport treiben!

Wer das für eine prima Sache hält, kennt wahrscheinlich die App CardioTrainer, und setzt sie auch bereits fleißig ein. Da kommt mein Hinweis vielleicht wie gerufen, dass es dafür eine Zusatz-App namens Noom - Die Abnehm-App gibt.

Während CardioTrainer für das Training gedacht ist, hängt sich diese Zusatz-App dort direkt ein, um die verbrauchten Kalorien zu zählen. Zuerst wird das Ziel der Aktion festgelegt (wieviel man in welchem Zeitraum abnehmen möchte – realistische Werte, bitte), und die geplanten Aktionen (welchen Sport, wie oft, ggf. weniger Kalorien aufnehmen?). Dann überwacht CardioTrainer die Ausführung – und zeigt schließlich die Resultate an.

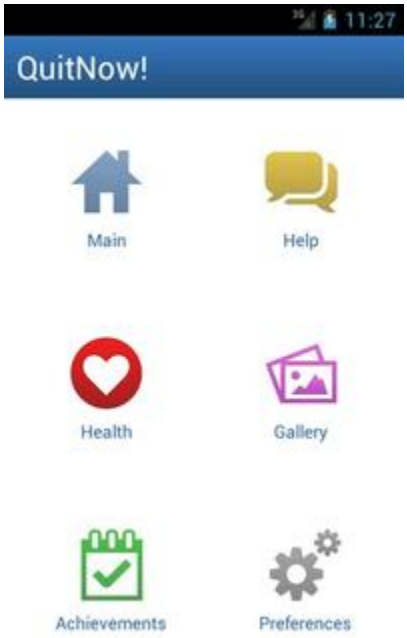
Wer *CardioTrainer* noch nicht benutzt, sollte allerdings einen Blick auf zweierlei werfen: Zum Einen ist die App mit ca. 7MB nicht unbedingt klein, was bei manchem Gerät bereits eine große Hürde darstellen könnte. Zum Anderen müssen auch die von der App verlangten Berechtigungen abgewogen werden: Die Verbindung "Kontaktdaten lesen" im Zusammenhang mit "uneingeschränktem Internetzugriff" würde sicher nicht nur mir Bauchschmerzen bereiten! Der Entwickler schreibt zwar zur Erklärung: *Die Einträge aus dem Adressbuch werden ausschließlich dazu verwendet, um mit anderen CardioTrainer-Benutzern in Verbindung zu treten.* (Oh – stehen die alle in meinem Adressbuch?) Aber vielleicht zieht er, wenn es oft genug gefordert wird, auch die Auslagerung dieser Funktionalität in ein Plugin in Erwägung...

BMI & Protokoll

Und dann waren da noch diejenigen, die das Thema auch so im Griff haben. Ohne Diät-App, ohne Sport-App. Aber es tut dennoch gut, den Erfolg "schwarz auf weiß" verfolgen zu können, oder? Und auch für diesen Fall ist mit Android gesorgt:

So wäre da zum Beispiel die App Droid Weight. Nicht vom englischen Namen irritieren lassen: Es ist eine deutschsprachige App aus deutschen Landen. Sie speichert Gewicht und BMI, und stellt ersteres als Graph über bis zu 6 Monaten dar. Darüber hinaus lässt sich das Zielgewicht hinterlegen. Man kann sich sogar daran erinnern lassen, regelmäßig die Werte einzugeben. Dabei versteht die App sowohl metrische als auch imperiale Maße. Die Datenbank lässt sich auf die SD-Karte ex- und auch von dort wieder importieren. Ebenso kann sie komplett zurückgesetzt (geleert) werden. Kurzum: Alles, was für Protokoll und Statistik nötig ist, hat *Droid Weight* mit an Bord.

Rauchentwöhnung



Die große Übersicht findet sich, wie gewohnt, wieder im Forum – was besagt, dass Android auch hier wieder eine ganze Reihe von Alternativen anbietet.

Aus dieser Reihe möchte ich QuitNow! herausgreifen – die in diesem Bereich mit Abstand am Besten bewertete App.

Laut Kommentaren im *Play Store* ist die App gut lokalisiert – auch wenn Name und Screenshot in Englisch sind, sie ist ebenso des Deutschen mächtig. *QuitNow!* bietet einige Statistiken – so zum Beispiel rauchfreie Tage und gesparte Zigaretten (letztere auch in Bares umgerechnet). Während des gesamten Prozesses können die Auswirkungen auf insgesamt neun gesundheitliche Aspekte beobachtet werden – es wird ja nicht einfach ein Schalter umgelegt; der Körper muss die ganzen Gifte erst nach und nach abbauen, und sich entsprechend regenerieren. Es lässt sich also verfolgen, wie er sich langsam erholt: Etwa, dass nach 48 rauchfreien Stunden so einige Geschmacks-Sensoren wieder erwachen...

Auch ein Widget ist mit dabei. So hat man den Erfolgsstand auch dann vor Augen, wenn die App gerade nicht im Vordergrund läuft.

Wie: Das war jetzt nicht so ganz ernst gemeint mit dem Aufhören? Geselligkeit und so? Macht nix, dann tauschen wir die App einfach aus, und die Beschreibung ebenso:

Mit der Mitrauchzentrale lassen sich raucherfreundliche Lokalitäten aufspüren. Nicht etwa nur Kneipen! Die Liste umfasst Clubs, Bars, Cafés, Restaurants, öffentliche Plätze, Privat, Parks, Raucherecken und Sisha-Lounges.

Mit einem Login gibt es darüber hinaus auch diverse Community-Features: Wie viele Raucher sind gerade an der Location angemeldet? Wie ist selbige bewertet? Selbst eine Bewertung abgeben ist natürlich ebenfalls möglich. Wo es "Raucherecken" gibt, zeigt die App auf der Karte an.

Für weitere Details lohnt sich auch ein Besuch des Headquarters...

Arzt und Apotheke

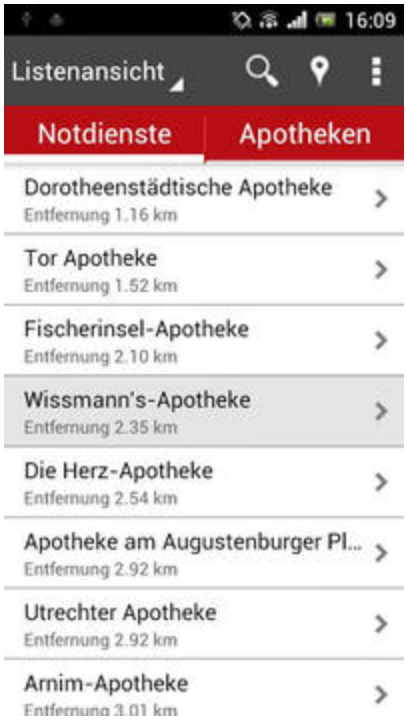
Arztsuche

Früher oder später trifft es jeden: Ein Arzt wird gebraucht. Entweder die Suche eines neuen Hausarztes nach dem Umzug, oder die Suche nach einem Spezialisten, den man sonst noch nie benötigt hatte. Klar: Die "Gelben Seiten" und auch andere Telefonbücher kennen Ärzte zuhauf. Doch man will ja schließlich nicht den erstbesten, sondern den ersten *und* besten: Gut soll er (oder sie) sein, natürlich vom Fach "etwas" verstehen – aber auch die "soziale Kompetenz" darf nicht zu kurz kommen. Alles Dinge, die uns das Telefonbuch nicht verrät.

Aber die jameda Arztsuche weiß an dieser Stelle weiter. Denn diese besteht nicht nur aus einem Telefonbuch mit Nummern – sondern auch aus einer Community, die ihre Bewertungen hinterlassen hat. Die folgen dem Schulnoten-Prinzip, wobei verschiedene Kriterien (u. a. Zufriedenheit, Vertrauensverhältnis, wurde sich Zeit genommen – oder war es eher eine "Massenabfertigung") separat ausgewiesen werden. Ein persönlicher Kommentar sagt schließlich etwas über die Dinge, die sich nicht in Zahlen fassen lassen.

Arzt, Tierarzt, Hebamme, Apotheke, Klinik, Augenoptiker oder auch Krankenkasse: Über 460.000 Adressen bundesweit sind in der Datenbank enthalten. Und Dank Umkreissuche findet man im Ernstfall auch den nächstgelegenen Arzt. Alternativ bietet sich die BundesArztsuche an, die von der Kassenärztlichen Bundesvereinigung herausgegeben wird – und zumindest in der Bewertung *Jameda* bereits den Rang abgelaufen hat.

Apotheken



Apotheken ist die einzige offizielle Anwendung im Auftrag der deutschen Apothekerschaft für ganz Deutschland. Und als solche darf man sich ja wohl auf die von ihr gelieferten Informationen getrost verlassen.

Wenn man eine Apotheke sucht, dann in der Regel keine, die gerade geschlossen hat. Macht ja keinen Sinn. Also eine offene – Sonntag früh um ein Uhr dreißig. Ja und? Kein Problem: Notfall-Apotheken haben auch an Sonn- und Feiertagen geöffnet. Und sind auch nachts bereit. Und *Apotheken* kennt sie natürlich, als offizielle App der Apothekerschaft. Und weiß auch, welche gerade Notdienst hat.

Also alles kein Thema: Schon nach wenigen Klicks ist die richtige Apotheke gefunden, und kann bei Bedarf auch telefonisch kontaktiert werden (na, hat sie wirklich geöffnet? Ist das gewünschte Medikament da – oder sucht man besser die übernächste Apotheke?). Auch eine Anzeige auf der Karte ist natürlich möglich. Inklusive Routenfunktion – wer jetzt immer noch nicht hingefunden hat, ruft besser ein Taxi...

Stopp einmal kurz: Und im Ausland? Gibt es da auch die "Deutsche Apothekerschaft" mit ihrer offiziellen App? Das vielleicht nicht, aber es gibt ja noch mehr Apps. Für diesen Fall wäre zum Beispiel Apotheken-Sucher einen Blick wert...

Medikamente

Fast jeder hat seine "Stamm-Medikamente", und sei es für die Reise-Apotheke: Aspirin für den Brummschädel, Iberogast für den Rumpel-Bauch, Voltaren für Verzerrungen & Co... Alles Sachen "für den Fall der Fälle", also nichts zeitkritisches. Oder Sachen, die man regelmäßig einnehmen muss: Im Moment noch genügend vorhanden, aber irgendwann braucht man wieder Nachschub.

Wenn es nicht akut ist, hat man Zeit zum Suchen nach dem besten Angebot. Und bei Dingen, die man immer wieder kauft, macht auch Kleinvieh mit der Zeit gehörig Mist. Und *wann* hat man die Zeit, so eine Suche durchzuführen? Genau: Wenn man ohnehin gerade zum Nichts-Tun verdonnert ist. Eine Stunde in der S-Bahn bietet sich da an – und die passende App auf dem Androiden:

MediPreis zum Beispiel. Wer das gesuchte Medikament gerade zur Hand hat, hält jetzt die Kamera seines Androiden auf den Barcode, bis es "Piep!" macht. Alle anderen geben brav den Namen in die Suchmaske ein. Und wenig später erscheint, eine Datenverbindung natürlich vorausgesetzt, eine Ergebnisliste – wie im rechten Bild zu sehen.

Keine Lust auf eine extra App? Oh... Dann tut es vielleicht auch ein Lesezeichen im mobilen Browser, welches auf handy.medipreis.de zeigt.

Notfall

110 & Co

Klar: Wem im Fall des Falles die Nummer 110 nicht mehr einfällt, der denkt auch nicht an eine auf dem Androiden installierte App. Doch kaum hat man die Nummer in der Hektik des Gefechts gewählt, geht das Stottern los: Wie sag ich's am Besten? Und was überhaupt? Welche Details sind wichtig?

Hier souffliert die Mobile Notruf-App für Notfälle (so der volle Name) mit den richtigen Stichworten – wie im linken Bild zu sehen. Frage 1 auch beantworten, selbst wenn es obsolet scheint: Natürlich hat das Smartphone im Hintergrund bereits die aktuelle Position per GPS ermittelt. Doch woher soll der CallCenter-Mitarbeiter am andern Ende der Leitung wissen, ob man selbst direkt am Ort des Geschehens ist – oder den Anruf aus "sicherer Entfernung" tätigt? "Ich sitze hier auf einer Bombe" ist wohl eher unwahrscheinlich...

Achja: Und dann wären da noch die Notruf-Nummern, die nicht jeder im Hinterkopf hat: Gift-Notruf? Frauenhaus? Oder, bei seelischen Notfällen: Telefon-Seelsorge? Die App kennt auch diese.

Mammi, ich muss mal!

Auch das ist ein "medizinischer Notfall" – gewissermaßen. Denn wenn jetzt nicht schnellstens reagiert wird, platzt am Ende die Blase. Oder das Kind wird von Mitte bis Unten ziemlich nass, und holt sich dadurch eine Erkältung. Beides nicht wirklich wünschenswert, oder?

Aber was tun – mitten in unbekanntem Terrain?

Zum Glück gibt es auch hier wieder eine tolle Android-App: GoToilet findet die passenden Örtchen. Und zwar weltweit! Sowohl die öffentlichen, als auch die von Cafés, Restaurants, oder Tankstellen (bei letzteren muss zur Rechtfertigung der hier getätigten Notdurfts-Verrichtung gegebenenfalls auch noch eine andere, kostenpflichtige Dienstleistung in Anspruch genommen werden).

Der Funktionsumfang beinhaltet nicht nur eine stumpfe Auflistung verfügbarer Notdurfts-Stätten (obwohl auch das, inklusive der Entfernung dorthin,

Bestandteil ist). Auf der Karte können sie ebenfalls eingeblendet werden (siehe Bild rechts). Sofern Bildmaterial dazu bei Streetview vorhanden ist, lässt sich die Umgebung des Wunsch-Ortes auch auf diese Weise vorab inspizieren. Mit etwas Glück gibt es sogar eine Bewertung – so dass unappetitliche Plätze gemieden werden können...

Büro, Office & Verwaltung

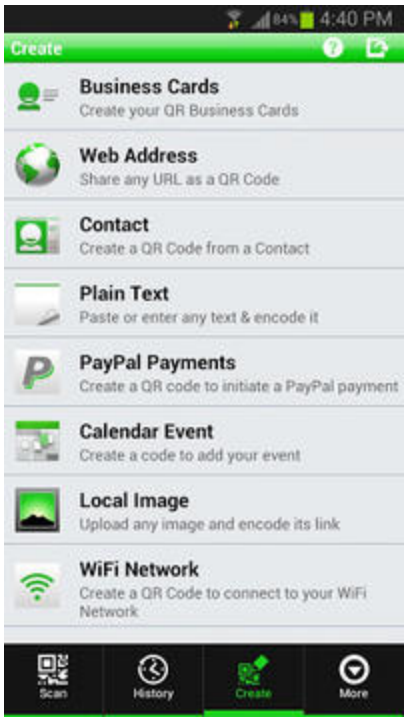
"Früher" sprach man von Büro-Gebäuden. Heute ist das Büro da, wo man gerade ist. Dummerweise auch nach Feierabend. Schauen wir uns also mal die Ausstattungs-Möglichkeiten an:

Barcodes

Barcodes sind aus unserem täglichen Leben ja nicht mehr wegzudenken – überall kleben die verschiedensten Fassungen drauf. Beim Thema Shopping sind wir ihnen ja bereits begegnet, und können jenen Teil (Produkt-Informationen) daher hier überspringen.

Am bekanntesten ist sicher der Barcode-Scanner (Bild links), den ja eigentlich jeder zweite auf seinem Androiden hat – und den so manch andere App für Barcode-Scan-Funktionen voraussetzt. Der erkennt z. B. die sogenannten QR-Codes, wie sie auch bei AndroidPIT benutzt werden: Draufhalten – "Piep" – und ab in den *Play Store*, auf die Seite der App, die man gerade "angepiept" hat. QR-Codes können verschiedenste Informationen enthalten: URLs (wie eben beschrieben), Adressen, kurze Texte, Termine (wäre nett, wenn die auf diversen Theater- und Kino-Plakaten mal Standard würden). Ein guter Reader öffnet dann jeweils die richtige App: Adressen lassen sich so gleich der Kontaktliste zufügen, Termine in den Kalender eintragen, und so weiter. Praktische Sache das. Und die genannte App beherrscht das auch weitgehend.

Natürlich gibt es gerade in diesem Bereich eine ganze Reihe von weiteren Apps, wie z. B. ixMAT, der besonders viele Formate kennen soll, i-nigma, oder lynkee. Besonders hervorheben möchte ich in diesem Zusammenhang die App QR Droid (rechtes Bild), die so ziemlich alles beherrscht, was sich mit Barcodes anstellen lässt. Dabei beschränkt sie sich nicht nur auf das Lesen – es lassen sich auch Barcodes erstellen: Von Kontakten, Terminen, dem Zugangscode zum WLAN-Router, URLs, PayPal Payments, Kurztexten, und mehr. Sogar kleine Bildchen lassen sich in die erstellten Barcodes einbetten.

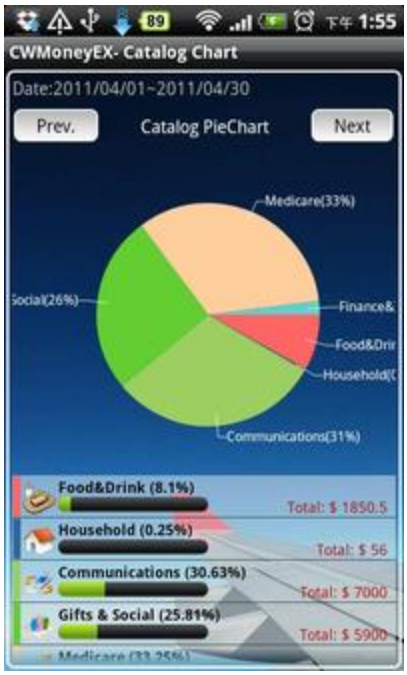


Für Details verweise ich daher wieder auf den zugehörigen Forums-Thread. Dort finden sich allerdings nicht nur die gerade beschriebenen Reader – sondern z. B. auch die Generatoren, mit denen man eigene Barcodes erstellen kann. Oder auch Apps wie Shelves, mit denen sich ein eigenes Inventory aufbauen lässt (also quasi eine Artikelverwaltung gleich mit dabei). Aber auch Buch-Manager gibt es (zur Verwaltung der eigenen Bibliothek), oder Buch-Infos (zur Nutzung im Buchladen: Taugt das was? Referenzen?)...

Finanzen

Auch einen Überblick über sein Budget kann man mit Hilfe seines Androiden behalten. Gerade in diesem Bereich stehen zahlreiche Apps zur Verfügung (für eine Übersicht siehe diesen Forums-Thread). Die Möglichkeiten reichen von der einfachen Erfassung von Ausgaben, über eine komplexe Budget-Verwaltung mit Export und Reporting, bis hin zu Online-Diensten, die alles aufbereiten, was man ihnen per Foto schickt (hochlädt).

In den vorangegangenen Kapiteln klang ja bereits mehrfach an, dass ich eher konservativ bin, was persönliche Daten auf dem Smartphone allgemein und speziell auf fremden Servern und in der Cloud betrifft. Das gilt natürlich insbesondere für so sensible Dinge wie Finanzdaten. Daher sei an dieser Stelle nochmals auf eines deutlich hingewiesen: Das Risiko eines Missbrauchs ist in diesem Falle größer, als wenn sich selbige Daten lediglich auf dem stationären Rechner daheim (oder gar nur in Papierform im verschlossenen Schrank) befinden. Der Anwender muss daher für sich selbst entscheiden, ob er derart sensible Daten überhaupt auf seinem mobilen Gerät haben, oder gar der Cloud (und somit fremden Rechnern – einige Apps ermöglichen oder erfordern gar den Upload der entsprechenden Dokumente) anvertrauen möchte.



Eine recht gute Wahl bei den etwas umfangreicheren Apps scheint CWMoney (Bild rechts) zu sein. Hier handelt es sich um die in diesem Bereich am besten bewertete App. Laut Beschreibung werden mehrere Accounts sowie verschiedene Währungen unterstützt. Einträge können mit GPS-Stamps, Fotos oder auch Sprachaufnahmen angereichert werden. Es gibt hierarchische Strukturen, Kataloge, Filter, Reports, Torten-Graphen, und mehr. u. a. auch einen Daten-Export als XML bzw. CSV.

Allerdings hat das Ganze auch seinen Preis: Ca. 7 Euro werden für die Vollversion fällig. Wer's lieber gratis haben möchte, greift dann z. B. zu Financisto. Ist fast genau so gut bewertet, aber vollständig Open Source.

Ist es interessanter, wie es praktisch auf dem Bank-Konto aussieht? Natürlich geht auch so "richtiges Homebanking" unter Android (die passende Übersicht im Forum findet sich hier). In Sachen Komfort und Sicherheit sind hier ganz klar die Produkte von StarMoney (die namensgleiche App ist links abgebildet) zu empfehlen. Je nachdem, ob es nur um ein Konto bei einer Sparkasse, oder mehrere Konten bei verschiedenen Banken geht, steht eine passende App gratis oder für ein bis vier Euro bereit.

Auch einige andere Banken stellen ihre eigene App bereit – Details dazu unter genanntem Link. Übrigens auch zum Thema "Börse" – sei es jetzt nur die Markt-Beobachtung, oder auch das "Broken" selbst...

Kalender

Oh, hier scheiden sich die Geister. "Die beste App" gibt es in dieser Kategorie nicht. Je nach Vorlieben und Bedürfnissen, gibt es immer mindestens zwei Kandidaten. Da fällt mir die Auswahl nicht leicht...

Also greife ich zuerst einmal den Business Calendar heraus. Der Name scheint ja bereits anzudeuten, wofür sich dieser besonders gut eignet. Unterstützt werden von der App sowohl der Google Kalender, Exchange, PC-Sync, und Facebook-Kalender – es besteht also die freie Wahl, wie öffentlich man gern sein möchte.

Die App lässt sich sehr angenehm bedienen. In der Übersicht (siehe Screenshot) kann man mit einem Slider (unten im Bild) frei einstellen, welchen Zeitraum man gern sehen möchte. Oder man nutzt die "Zwei-Finger-Geste" (auch als "Pitch-to-Zoom" bekannt), um den Zeitraum anzupassen. Kontext-sensitive Hilfe ist auch mit dabei.

Hm, alle Details können in der Monats-Ansicht sicher nicht angezeigt werden. Aber auch hier ist der Business Calendar clever: Termin antippen, und die Details erscheinen in einem extra Layer. Schön übersichtlich.

Als zweiten Kandidaten muss ich wohl zwangsläufig Jorte nennen – sonst bekomme ich Haue von der Community 😂. Also – linkes Bild, bitte!

Auch Jorte unterstützt sowohl Google, Exchange als auch PC-Sync Kalender. Wie bei der Größe (etwa 3MB Download) zu erwarten, kann man sich hier wirklich richtig austoben – alles mögliche lässt sich anpassen. Und da Jorte wirklich eine Unmenge an Widgets mitbringt, lässt sich die Widget-Auswahl des Homescreens ein wenig "handlicher" halten, indem man unerwünschtes einfach deaktiviert.

Eine wirklich gute Sache ist jedoch, dass Jorte die lokalen Feiertage importieren kann! Man muss in der Länderliste allerdings ein wenig suchen – das Sortierkriterium hat sich mir nicht erschlossen, sah eher etwas wild gewürfelt aus. Etwas kariert geschaut habe ich auch, dass es offensichtlich ein Land namens "Krawatte" gibt (da ist doch wohl nicht etwa Tie-Land gemeint?)... Leider sind die so importierten Feiertage offensichtlich nur in Jorte selbst zu sehen – oder ich habe etwas verpasst...

Für weitere Kandidaten sei wiederum auf den entsprechenden Forums-Thread verwiesen.

Und vielleicht gleich noch auf einen weiteren, bei dem es um die Synchronisation der Kalenderdaten geht. Was? Achso, ja klar, geht auch über Google. Aber nicht jeder möchte seine privaten Daten auf fremde Server schicken. Und deshalb gibt es Apps wie CalendarSync (sofern man einen passenden eigenen Webserver hat – bei Firmen ist das oftmals der Fall), SyncEvolution (zur Synchronisierung mit Evolution unter Linux), und andere.

Passwörter

Passwörter sollen möglichst sicher gespeichert werden. Apps dazu gibt es ja scheinbar wie Sand am Meer – sicher sind diese aber nicht unbedingt. Daher sollte bei der Auswahl unbedingt ein Blick in den entsprechenden Forums-Thread geworfen werden! Dort werden zwar nicht alle verfügbaren Apps ausführlich vorgestellt, doch die Liste im ersten Post hilft schon einmal, die "unsicheren Kandidaten" zu eliminieren.

Nach guter Tradition soll aber zumindest eine App hier kurz erwähnt werden. Sie nennt sich in diesem Fall KeePassDroid. Sieht zugegeben etwas spartanisch aus (siehe Bild rechts), ist aber sicher. Und es gibt eine PC-Version, mit der die App sogar kompatibel ist. Vorausgesetzt, man führt nicht zeitgleich in beiden Installationen Änderungen durch, hat man seine Passwörter somit an beiden Stellen parat. Gut verschlüsselt, versteht sich: Sollte ein "Fremder" das Smartphone (oder auch nur die Passwort-Datei) in die Finger bekommen, beißt er sich beim "Knacken" die Zähne aus.

Zu den anderen Kandidaten (und es sind einige) kann ich nicht viel sagen – ich kann mir ja nicht alle angucken

Office-Pakete

Mobiles Office? Kein Ding. Eine passende Übersicht gibt es in diesem Forumsthread. Ein paar Stichproben natürlich wieder hier.

Allerdings gibt es eine traurige Nachricht gleich vorab: Ich konnte kein Office-Paket finden, das auch freie Formate (wie das OpenDocument Format, welches u. a. bei OpenOffice/LibreOffice zum Einsatz kommt) unterstützt. Alle sind voll und ganz auf Microsoft konzentriert...

Als prominenteste App wäre hier Documents To Go (rechtes Bild) zu nennen. Wie auch Office Suite Pro unterstützt die App Word, Excel und Powerpoint in den gängigen Versionen: Dokumente können geöffnet oder neu erstellt, bearbeitet, und natürlich wieder gespeichert werden. Darüber hinaus ist außerdem ein PDF-Viewer mit an Bord. Jeweils ungefähr 10 Euro kostet der Spaß – wobei es bei den kleineren Displays eher weniger Spaß machen wird. Aber dafür kann die jeweilige App nichts. Auf Tablets sieht es schon ein wenig anders aus...

Einziger Kandidat mit Unterstützung für ein offenes Format ist scheinbar Androffice, das im Playstore allerdings nicht mehr auffindbar ist (der Link führt daher zum Aptoide-Store). Wer sich nicht vom Wort "Office" irritieren lässt, findet in dieser App eine Tabellenkalkulation, die sowohl Excel als auch OpenDocument Spreadsheet unterstützt.

Für Spartaner und Entwickler sind sicher auch noch reine Text-Editoren, wie TxtPad (Bild links) interessant: Hiermit lassen sich reine ASCII-Texte bearbeiten. Das spart nebenbei auch Ressourcen, denn sowohl App als auch Dokumente benötigen weniger Platz.

Nicht verschweigen möchte ich an dieser Stelle die ganz speziellen Notizen-Apps, von denen ich besonders Note Everything hervorheben möchte.

Der Name ist wörtlich zu nehmen. Der Name ist Programm. Hiermit kann man wirklich alles notieren: Natürlich Textnotizen: Schnell ein paar Stichpunkte zum Vortrag, eh es wieder vergessen ist. Oder mal was skizzieren - kein Thema. Auch eine Foto-Notiz stellt Note Everything nicht vor ein Problem. Zu faul zum Schreiben? Dann diktier doch einfach was. Und schreib am Ende doch was dazu. Auch Widgets sind mit von der Partie: Für die schnelle Notiz zwischendurch...

Wem das nicht reicht, der greift für ca. 3 Euro zur Pro-Variante – und erhält zusätzlich Abhak-Listen, Video-Notizen, Foto-Notizen (oops), und mehr.

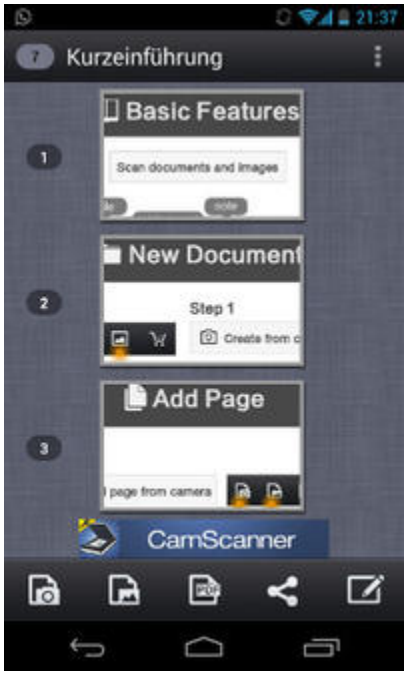
Natürlich gibt es wieder eine Reihe von Alternativen, wie z. B. ColorNote, das auch bunte "Stickies" auf den Home-Screens ablegen kann. Einfach mal in den Forums-Thread schauen.

PDF-Dateien Anzeigen und Erstellen

PDF (das "portierbare Dokumenten-Format" oder, im O-Ton "portable document format") wurde 1993 von Adobe auf den Markt gebracht – und stellt seitdem einen gewissen Standard dar. Die Besonderheit dieses Dokumentenformates ist, dass der Inhalt überall gleich dargestellt werden soll: Ob unter Windows, Mac, oder Linux, auf dem Bildschirm oder gedruckt... Auf dem Androiden? Die Frage ist sicher nicht unberechtigt! Also habe ich ein wenig im *Play Store* gestöbert, ob ich auch zu diesem Thema passende Apps nennen kann.

Und: "Yes, we can!". Der unvermeidliche Forums-Thread gibt eine ganze Liste an die Hand – gegliedert nach einfachen Betrachtern, Generatoren, und Tools. Klar sind da auch wieder die "Original-Produkte" von Adobe vertreten, auch wenn sie nicht unbedingt die Apps sind, die am besten abschneiden...

Bei den Betrachtern ist das vielmehr der ezPDF Reader (Bild rechts). Kostet zwar einen knappen Euro – ist aber nicht nur topp bewertet, sondern kann auch eine ganze Menge: Nicht nur das Anzeigen einer PDF-Datei. Das setze ich mal bei einem PDF-Reader als gegeben voraus. Mit dieser App lassen sich jedoch ebenso Markierungen anbringen, Texte unter- oder durchstreichen, Bereiche umrahmen (Rechteck oder auch Kreis/Ellipse), Notizen oder gar Freihand-Zeichnungen einfügen. Da bleibt eigentlich nichts mehr übrig, oder?



Wie jetzt – PDF-Dateien erstellen? Kommt ganz auf die Quelle an. Relativ viele Formate unterstützt Document Converter: nahezu alle MS-Office und OpenOffice/LibreOffice Formate kann diese App umwandeln. Etwa 800 kB bringt die App auf die Waage – benötigt für die Umwandlung jedoch eine Netzverbindung, da diese auf dem Server des Anbieters stattfindet. Mit privaten/vertraulichen Daten sollte man daher Vorsicht walten lassen...

Ganz interessant sind in diesem Zusammenhang aber auch "Hosentaschen-Kopierer" wie der im linken Bild dargestellte CamScanner Phone PDF Creator. Nein, diese Apps kopieren keine Hosentaschen – auf dem Smartphone installiert, passen sie aber bequem in selbige. Und man hat sie quasi immer zur Hand. Eben mal schnell ein paar Seiten aus einem Buch in der Bibliothek, die man zu Hause nochmal genauer anschauen möchte? Kein Thema. Schnell gemacht – und auf der SD-Karte gespeichert, zu Google Docs hochgeladen, oder per

Mail verschickt. Ist mit etwa 10 MB ein wenig größer als zuvor genannte App, arbeitet dafür aber auch mehr lokal.

Achja: Dann lassen sich natürlich auch noch Webseiten zum Offline-Lesen konvertieren. Hierfür bietet sich z. B. die App UrlToPDF an. Mit ihren 300 kB dient auch diese App natürlich nur als Frontend, welches die eigentliche Konvertierarbeit einem Webdienst überlässt – aber wenn die Quelle ohnehin öffentlich zugänglich ist, fällt dies weit weniger ins Gewicht, oder?

Zeiterfassung

Sicher nicht nur für Freiberufler interessant ist das Thema Zeiterfassung: Wieviel Zeit habe ich an welchem Projekt verbracht? Xpert Timer (Bild links) beantwortet mehr als nur diese Frage. Die Bedienung ist denkbar einfach, wie eine Stempeluhr: Bei Beginn der Tätigkeit auf Start, bei eventuellen Pausen auf Pause, und bei Feierabend auf Stop gedrückt. Natürlich müssen vorher einmal Kunde und Projekt erfasst sein – aber dann bekommt man neben zahlreichen Statistiken und Übersichten auch eine Stundenübersicht, die man sogar direkt aus der App heraus verschicken kann. Stundensatz eingetragen? Dann zeigt sich auch gleich, wie es ums Finanzielle bestellt ist.

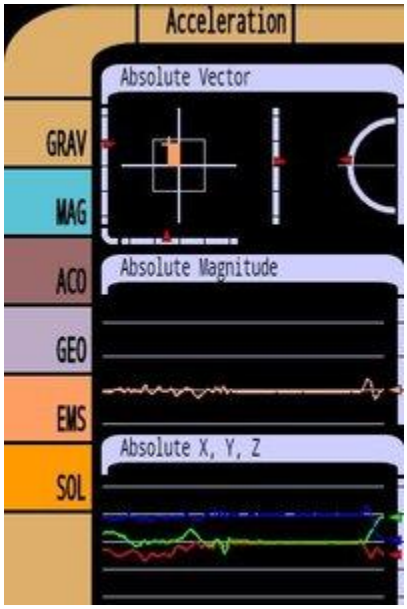
Xpert-Timer bietet außerdem einen Barcodescanner. In der App lassen sich eigene Barcodes erstellen, diese dann auf Maschinen oder Akten anbringen und eine Tätigkeit durch einfaches scannen starten.

Wie beschrieben: Verschicken lassen sich die Reports direkt aus der App heraus. Aber auch einfach exportieren (als HTML oder CSV), und dann am PC weiter verarbeiten. A propos arbeiten: An einem Desktop-Client (leider nur für Windows) wird ebenfalls fleißig gearbeitet. Zusätzlich ist ein Plugin zum direkten Export im PDF-Format (kostenpflichtig) verfügbar.

Fairerweise seien die Mitbewerber hier aber noch kurz erwähnt: Da wäre z. B. Workaholic, dem man seine Arbeitsorte derart beibringen kann, dass er einen per Lokalisierung automatisch ein- und wieder ausstempelt. Oder Time Tracker, der die Daten auch noch per Passwort schützen kann.

Wollte ich jetzt hier alle Alternativen aufzählen, würde es ein wenig lang. Also verweise ich wieder einmal auf den passenden Forums-Thread für die weitere Lektüre.

Sensoren



Es ist ja ein offenes Geheimnis, dass unsere kleinen Androiden mit Sensoren gespickt sind. Kaum jemand denkt darüber nach. Und wer weiß eigentlich im Detail, was da so beteiligt ist?

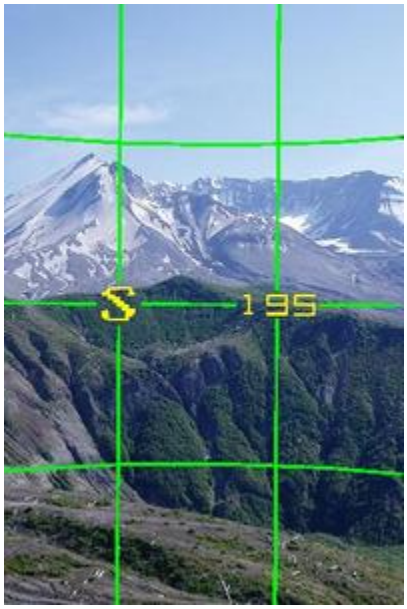
Entdeckerfieber geweckt? Dann lohnt sich ein Blick auf die App Tricorder (Bild rechts). Ja, sieht auf den ersten Blick nach einem Startrek-Spielzeug aus. Aber das hat es in sich. Am linken Rand finden sich die verfügbaren Sensoren: Gravity (Beschleunigungs-Sensor), Magnetfeld (Kompass), Akkustik (Mikrofon), Geografisch (GPS), EMS (Elektro-Magnetisches Spektrum – also Funknetz), und schließlich Solaraktivitäten. Häh? Nein, für letzteres gibt es nicht wirklich einen Sensor – die Daten kommen übers Internet.

Die Anzeigen sind hier keinesfalls Fake, sondern spiegeln in der Tat die Sensoren-Daten wieder. Die Tricorder-App ist ein gutes Beispiel dafür, wie Praktisches sich mit Spielerischem verbinden lässt – weswegen ich es in meinem Buch auch unbedingt erwähnt haben wollte.

Leider hat Google den Tricorder auf Druck seitens Rechtsanwälten der CBS aus dem Markt entfernen müssen (obiger Link führt daher in den Aptoide-Store) – der Name war hier weniger der Grund, Stein des Anstoßes war wohl vielmehr das Design. Nachzulesen ist diese Misere auf der Projektseite. Als Ausweichmöglichkeit sei daher hier auf My Sensors verwiesen...

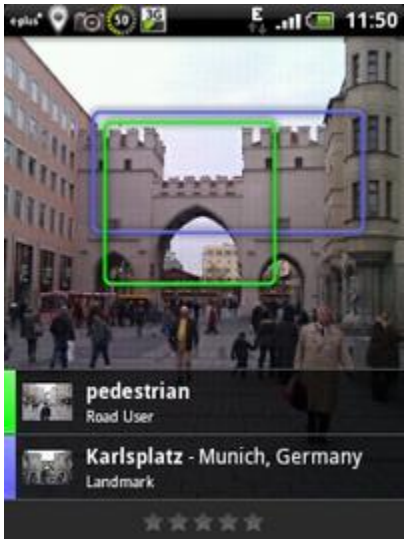
Wie lassen sich die Sensoren denn nun noch sinnvoll einsetzen? Da gibt es einige Möglichkeiten. Zum Beispiel als Compass, oder mit Bubble als Wasserwaage. Diverse Logger und Monitore sind ebenfalls im *Play Store* verfügbar. Und (Geschicklichkeits-) Spiele. Und mehr. Details finden sich wieder einmal in einem Forums-Thread...

Augmented Reality



Hier wird die Realität erweitert – denn nichts anderes bedeutet die Übersetzung des Begriffs "Augmented Reality". Dazu werden mehrere Dinge gemischt: Das Kamera-Bild wird mit weiteren Informationen versehen. Meist mit Daten eines oder mehrerer Sensoren. Oder mit Karten-Informationen. Oder weiteren Informationen zu auf dem Bild ersichtlichen Objekten. Oder einer Mischung mehrerer Komponenten...

Eine der einfacheren (aber dennoch wirkungsvollen) Varianten stellt hier Compass Ball dar: Nicht einmal 30kB Download erfordert dieses kleine Tool. Und prompt sitzt man im Kompass und schaut heraus auf die Umgebung. Nette Sache!



Etwas komplexer wird es da schon bei Google Goggles. Hier ist *Augmented Reality* eigentlich nur ein Teilaspekt der App, wie im rechten Screenshot zu sehen: Wo bin ich eigentlich, und was schaue ich da gerade an? Auf Wunsch kann *Goggles* entsprechende Informationen einblenden. Auch ohne aktiviertes GPS (wie hier im Bild); mit GPS sind die Informationen natürlich etwas genauer. Und manche scheint die App auch nur preiszugeben, wenn GPS aktiviert ist.

Wenn ich schon *Goggles* hier erwähne, dann möchte ich auch noch kurz einige weitere Features der App nennen – im übertragenen Sinne lassen sie sich ja alle in dieser Kategorie unterbringen: Man macht Fotos von realen Dingen – und Goggles sagt einem, was man da fotografiert hat: DVDs und Bücher (Goggles nennt Titel, Preis, und Erwerbsquellen), Logos, Kunstwerke (geniale Sache zum Angeben: Kurzes Foto machen und dann wissend tun, dass van Gogh dieses Gemälde namens ... im Jahre...), Barcodes (Produkt-Infos und Kaufangebote), Visitenkarten (Übernahme der Daten in die Kontaktliste), und mehr.

Damit ist das Thema aber noch lange nicht ausgeschöpft. Zu nennen wären da noch Apps wie Wikitude und Mixare, die nicht nur mitteilen, was man unmittelbar sieht – sondern auch auf der Karte einblenden, was es in Blickrichtung (und in welcher Entfernung im eingestellten Radius) noch interessantes zu sehen gibt. Oder wenn es jemanden nicht auf der Erde hält: Mit Google Sky Map oder Satellite AR den Sternhimmel erkunden – was ist da gerade im Blickfeld? Sternbilder, Satelliten? Und wer ohnehin schon ein wenig Balla-Balla ist, kann auch gleich virtuelle (oder echte) Objekte jagen und abschießen (im Falle von "echten" á là Paintball) – genug Spielmaterial gibt es auch dafür. Nähere Informationen und mehr Details natürlich wieder im passenden Forums-Thread...

Fernbedienen und Überwachen

Kommen wir uns nicht alle hin und wieder etwas fremdgesteuert vor? Und was fällt uns dazu bei unserem Androiden ein? Das logischste und naheliegendste ist, ihn als Fernsteuerung zu benutzen:

Den PC fernsteuern

Achso – dachte da jemand eigentlich an etwas anderes? Kommt auch noch, weiter unten... Aber zunächst schauen wir mal, wie wir unseren PC fremdsteuern können. Natürlich mit unserem Androiden. Und da gibt es Apps für alles Mögliche: Androide als Maus- oder Tastaturersatz, zur Bedienung von Powerpoint-Präsentationen, zur Steuerung verschiedener MultiMedia-Software wie Winamp, iTunes, VLC & Co. Auch Torrents im Blick behalten ist kein Problem.

Will man gar den gesamten PC fernsteuern, so ist auch das möglich. Auf den Mini-Displays so mancher Smartphones wird das aber sicher alles andere als bequem sein – und den meisten Tablets fehlt dafür die Netz-Verbindung... Aber es gibt hier zahlreiche Lösungen sowohl für Windows, Mac, Linux, als auch systemübergreifend.

Für letztgenanntes hat sich in letzter Zeit Teamviewer etabliert, und funktioniert sogar durch Firewalls hindurch. Hierfür installiert man auf den zu steuernden PCs den passenden Client. Und natürlich auf dem Androiden. Der Verbindungsaufbau erfolgt nun über einen Server von Teamviewer: Steckt der zu steuernde Rechner hinter einer Firewall, wird die Kommunikation vom Teamviewer-Server gemanagt. Andernfalls reicht dieser die Verbindung einfach durch.

Für den Privatgebrauch ist dies kostenlos – Firmen können entsprechende Lizenzen erwerben.

Wer bedenken hat, dass da der "Man-in-the-Middle" zu sehr mithorchen könnte, der greift halt zu einer der anderen Lösungen (über VNC oder RDP). Mit Firewall dazwischen wird es allerdings schwierig...

Und wem jetzt eine Liste möglicher Apps zu diesem Thema fehlt, der werfe bitte einen Blick auf diesen Forums-Thread.

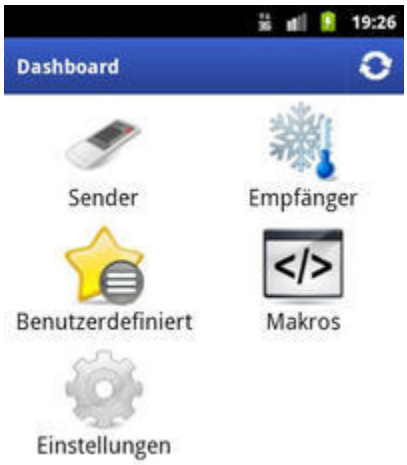
Multimedia-Geräte fernsteuern

Ohja, der Wust an Fernbedienungen auf dem Tisch oder Sofa. Und genau die, die man gerade benötigt, natürlich nicht dabei. All-in-Ones? Entweder zu teuer, oder nicht passend von der Belegung (welche Taste war's doch gleich nochmal?). Aber der Androide, der ist doch immer an der Frau (grabbel – oops... oder am Mann), kann man den nicht gleich... Aber klar doch, man kann!

Auch hier steht gleich wieder eine ganze Armee von Helferlein zur Verfügung. Aber eben wieder nicht für alles. Der große Haken: Die meisten gängigen Fernbedienungen funktionieren über Infrarot. Dafür haben "moderne Smartphones" aber weder Empfänger noch Sender (warum eigentlich nicht? Hallo, Herr Steller vom Hersteller?). Bleibt natürlich das IP-Netzwerk und daran angeschlossene IP-fähige Geräte, sofern man keinen passenden Adapter hat (oha, sowas gibbet also auch – in der Tat.). Dreamboxen können das – und die guten alten DM70x0 (aber auch neuere) lassen sich z. B. mit Controloid bequem steuern. Und man sieht schon vor dem Umschalten, was einen da erwartet (siehe Bild links). Voraussetzung ist lediglich Enigma1 oder 2. Im Zusammenspiel mit einem Streaming-fähigen Videoplayer (z. B. VPlayer) kann man damit auch direkt auf seinem Androiden das aktuelle Programm verfolgen (oder die Konserven abspielen).

Eine ganze Reihe weiterer Geräte lassen sich ähnlich fernbedienen: Etwa verschiedene Blueray-Player von LG und Sony, netzwerkfähige Receiver von Denon, Marantz und Yamaha, diverse TVs, und mehr. Wo sich dazu weitere Informationen finden, ist sicher nicht schwer zu erraten: Ja, auch hierfür gibt es einen Thread im Forum...

Hausautomation & Überwachung



Bei Multimedia ist natürlich noch lange nicht Schluss – wir können mehr! Auch das Licht zum Beispiel. Oder andere Dinge. Mit der richtigen Hardware und z. B. der App EzControl (Bild rechts) lässt sich so einiges steuern. Dazu braucht es allerdings in diesem Beispiel auch eine *EzControl XS1*, die verschiedene Hersteller und Standards unterstützt. Andere Apps wiederum unterstützen wieder andere Standards, wie etwa KNX Controller für EIB/KNX, oder AutoHTN für ZWave. Also für (fast) jeden etwas dabei.

Und wer jetzt noch wissen will, wann man das Licht ausmachen muss, damit der Einbrecher auf die F...lurtüre (geschlossen) rennt, der greift zur passenden Video-Überwachung. Je nach Geldbeutel ist diese mit WebCams oder "richtig guten" IP-Cams ausgestattet. IP Cam Viewer unterstützt eine lange Liste von Kameras. HomeMonitorViewer verspricht gar gleich, aus einer am heimischen PC angeschlossenen Webcam ein vollwertiges Surveillance-System zu machen. Und natürlich gibt es wiederum spezielle Apps für spezielle Kameras.

Nachdem der Einbrecher nun aufgelaufen ist, soll er vielleicht mit einer mobilen Kamera verfolgt werden? Mit AndRovio und der dazugehörigen Hardware ist auch das kein Problem.

Übrigens, nicht nur James Bond, sondern auch jeder Normalo kann sein Auto fernsteuern. Nein, nicht das kleine Spielzeug-Auto – das große. Zum Beispiel mit CarLink oder OnStar. Die Apps gibt es gratis – das dazu passende Auto eher nicht...

So – und die Gesamtübersicht hierzu findet sich in diesem Forums-Thread.

Server überwachen

Vom Haus zum Housing: Irgendwo steht der/stehen die Server, und keiner weiß, was auf ihnen eigentlich abgeht. Natürlich können wir auch diese überwachen. Und wenn es um Server-Überwachung geht, fällt uns wahrscheinlich als erstes Nagios ein. Genau dafür ist die App uNagi gedacht. Alles grün? Prima, dann gibt es auch keine Probleme. Oder der "problematische Service" ist halt einfach noch nicht in Nagios eingebunden... Doch *uNagi* beschränkt sich nicht auf einfache Status-Meldungen – bei Bedarf können auch weitere Details (etwa Statistik-Graphen) abgerufen werden. Sogar konfigurierte Aktionen lassen sich vom Androiden aus damit auslösen. Zu viele Services konfiguriert, oder zu viele Maschinen überwacht? Die Ausgabe lässt sich auch filtern. Widgets befinden sich ebenfalls im Lieferumfang.

Nagios ist "zu fett" für den eigenen Bedarf – es gilt ja nur zu wissen, ob der Webserver läuft bzw. wann er Probleme hat? Dann wären vielleicht Apps á là Site Alert Widget oder der HTTP Server Monitor eine Alternative.

Weitere mögliche Apps sind in diesem Forums-Thread aufgeführt. Natürlich ist auch hier die Liste keinesfalls vollständig – wer weitere Apps kennt, kann sie dort aber jederzeit gern vorschlagen...

Anders herum: Den Androiden fernsteuern

Huch? Wo isser denn? Piep doch mal! Ja, das geht nicht nur mit dem HTC-Sense Web Service. Das kann man auch haben, ohne seine Daten einem fremden Service anzuvertrauen. Auch wenn es dann wahrscheinlich nicht überall greift; aber meist hat man das "kleine Ding" ja eher im eigenen Zuhause verlegt...

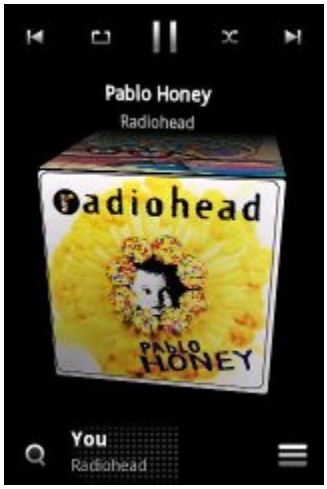
Das mächtigste Werkzeug in diesem Bereich ist sicher der bereits im Kapitel Das Android-Gerät vom PC aus verwalten vorgestellte PAW Server. Ja, die App möchte einige Berechtigungen haben – aber sie muss schließlich auf all das zugreifen können, was gesteuert werden soll. Etwa SMS. Oder ein Foto machen. Oder irgendwelche Daten vom Phone zotteln. Alles kein Thema; sogar ein Plugin für *Tasker* und *Locale* wird bereitgestellt. Bei laufendem *PAW Server* verwaltet man sein Phone dann bequem aus dem Web-Browser heraus.

Als Alternative dazu wäre MyPhoneExplorer zu nennen – der allerdings ein Windows-System mit dort installiertem Desktop-Client voraussetzt. Dann kümmert er sich aber u. a. auch um den Datenabgleich mit Outlook, Thunderbird, Sunbird, Lotus Notes, Tobit Davis, Windows Kontakte, Windows Kalender und anderen, um Backups, das Verwalten von SMS-Nachrichten, Anruflisten, Dateien, Anwendungen...

Multimedia: Alles, was Krach macht

Zur Vielseitigkeit unserer kleinen Dauer-Begleiter gehört auch die Wiedergabe multimedialer Inhalte. Im allgemeinen Sprachgebrauch meint das: Audio und Video. Im übertragenen Sinne halt: Alles, was Krach macht. Also:

Musik: Jukeboxen und mehr



Dies ist wohl die gefragteste Gruppe: Warum noch einen MP3-Player zusätzlich mitschleppen? Allenfalls aufgrund der Akku-Laufzeit (sonst läuft am Ende nur noch der Träger und schnauft, während das restliche Equipment keinen Ton mehr von sich gibt).

Im "normalen Einsatz" ist ³ (sprich: Cubed, linkes Bild) sehr beliebt. Wo der Name herrühren mag, lässt sich dem Screenshot leicht entnehmen: Die Auswahl der Musikstücke erfolgt hier über einen Würfel. Senkrecht scrollt man durch die Alben, waagerecht geht es alphabetisch vor- bzw. zurück. Auch last.fm wird (laut Play Store-Kommentaren) unterstützt. Lädt Album-Art aus dem Internet, und bringt auch ein Lockscreen-Widget mit.

Dann wären sicher noch die "Hands Free" Player für Auto und andere passende Plätze zu nennen (z. B. Car Tunes). Und Player, die mit der Zeit den Musikgeschmack des Hörers lernen, oder sich nach Farben bedienen lassen, Musik automatisch nach "Ähnlichkeit" verknüpfen. Oder solche, die man über den Bewegungssensor steuert (Schüttelt es einen bei einem Titel – schüttelt es den Androiden gleich mit, und weiter geht's zum nächsten Titel). Player mit Timer zum Einschlafen. Radios. Streaming-Services mit den zugehörigen Abos. Und, und, und. Sollten diese Themen jemanden interessieren, schaut er einfach wieder im zugehörigen Forums-Thread vorbei.

Video-Player

Mucke alleine reicht nicht – es soll auch auf dem Screen zucken? Kein Thema, auch Video-Player für Android sind nicht gerade dünn gesät. Ein richtiger Alleskönner in diesem Bereich ist der MoboPlayer: Große Format-Vielfalt, Unterstützung für Untertitel und multiple Audio-Streams, Playlisten, Streaming aus dem Netz, sortieren, Thumbnails... Auf den ersten Blick scheint nichts zu fehlen. Auch eine spezielle Vorbereitung der Videos (Konvertierung) soll nicht nötig sein: Zum Einsatz kommt hier die FFMpeg-Engine; alles, was die versteht, kann also abgespielt werden. Und das ist nicht gerade wenig...

Ebenfalls auf eine große Formatvielfalt greift VitalPlayer Neon zurück. Also, falls der eine nicht will, einfach den anderen probieren! Oder den ganz anderen: No Video Player erlaubt, das Bild einfach wegzulassen. Damit bleibt das Display aus (spart Akku), und man kann das Musik-Video ohne Bild genießen...

Habe ich jetzt etwas vergessen? Oh, vielleicht etwa die offizielle YouTube App? Iwo, die ist in den meisten Fällen ja ohnehin bereits vorinstalliert. Wenn nicht, findet sie sich natürlich im *Play Store* – und man kann damit das allseits bekannte Portal durchsuchen, sowie die Funde abspielen. Und mehr.

Mehr? Ja, das gibt es natürlich. Wie immer, im passenden Forums-Thread.

Wecker und Erinnerer

Das Klingeln des Aufzieh-Weckers ist "sowas von Out"? Naja, zumindest braucht der keinen Akku. Dafür kann man natürlich das Aufziehen mal vergessen haben... Also gut: Ja, auch der Androide kann wecken. Hat sogar ab Werk eine entsprechende App dabei. Zu öde? Da ist aber jemand anspruchsvoll! Macht nix, Hilfe gibt es trotzdem. Und zwar umfangreich. Wenn jemand in diesem Forums-Thread nicht fündig wird, sollte mich das doch stark wundern!

Neben "schnöden" allgemeinen Weckern gibt es hier eine ganze Reihe von Spezialitäten. So berücksichtigen Wecker wie Sleep as an Droid (Bild links) die Tatsache, dass wir nicht immer gleich tief schlafen, sondern in Phasen (Die meisten haben sicher schon einmal von der "Tiefschlaf-Phase" gehört: Wer da vom Wecker rausgerissen wird, steht meist "mit dem falschen Bein" auf). Diese Spezialisten warten also darauf, dass man in den "Halbschlaf" fällt – und wecken dann. Vielleicht 10 Minuten vor der Zeit, die eingestellt war; aber dennoch fühlt man sich ausgeruhter.

Das Gegenstück dazu sind die "Wellness Wecker", die uns abends sanft einlullen (z. B. mit Natursounds, oder einem selbst zusammengebrauten Mix). Ob sie einen dann morgens per Polizeisirene aus dem Bett werfen, habe ich nicht probiert... Aber vielleicht mag man dazu ja einen anderen Wecker nehmen, der ordentlich Radau macht – und damit erst aufhört, wenn eine knifflige Mathe-Aufgabe gelöst, eine Quiz-Frage beantwortet, oder (besonders ausgefallen: Morning Routine) das passende Produkt zu einem zuvor eingescannten Barcode gefunden wurde. Wie, das war jetzt die Milch – und die ist gerade alle, der Müll auch schon runtergebracht? Nachschub gibt es im Supermarkt. Und von da zurückgekehrt, den Barcode eingescannt, ist man sicher wach. Wer das nicht schafft, sondern den Task-Killer rausholt: Ja, auch wenn diese Aufgabe erledigt ist, ist man wach...

AlarmDroid mag zwar optisch eher ein wenig schlicht wirken (siehe Bild rechts), hat es aber durchaus in sich: Die App vereint das Beste aus den genannten Dingen, arbeitet zuverlässig, und nimmt noch einiges vorweg. Mich weckt sie jeden Morgen pünktlich mit einem persönlichen Gruß: "Guten Morgen, Izzy!". Es folgen Uhrzeit, aktuelles und erwartetes Wetter. Umdrehen des Androiden löst die "Snooze"

Funktion aus – und 5 Minuten später geht das Ganze von vorn los. Bis ich den Androiden kräftig durchschüttel. Oder den Mini-Androiden auf dem Display mit meinen Wurstfingern erwische...

Alternativ ließe sich natürlich auch ein Internet-Radio-Stream abspielen. Oder das "Sanfte Wecken" (beginnt leise und wird immer lauter) zuschalten. Und die Mathe-Aufgabe integrieren. Wird alles von *AlarmDroid* unterstützt.

Nicht verrückt genug? Es gibt auch Wecker, bei denen man seine Freunde das Weck-Video bei Youtube raussuchen lässt. Kann eine schöne Überraschung sein. Oder möchte jemand mal zurück-brüllen, damit der Wecker Ruhe gibt? Haben wir auch. Für Leute im "Winterschlaf" gibt es sogar einen Wecker, der bei passendem Schnee auf der Piste losgeht.

A propos losgeht: Reisewecker sind was Feines, gelle? Und was, wenn Bus oder Zug wieder einmal Verspätung haben? Achso, das war bereits einkalkuliert, weil es die Regel ist... Nagut: Also was, wenn sie versehentlich mal pünktlich sind? Ohja, wir haben auch ortsbasierte Wecker. Die gehen nicht "wann" los, sondern "wo". Und man definiert statt der Uhrzeit Weckort und Radius. Sobald der Zug also 10km vorm Ziel ist, ist es soweit...

Tools

Einige Tools habe ich ja bereits vorgestellt – z. B. für die Verwaltung bzw. Organisation der Apps auf dem Androiden, oder für Backups. Einige weitere sollen in diesem Kapitel folgen:

Dateimanager

Wo ist jetzt diese dumme Datei gelandet? Und wie bekomme ich mal eben die Datei von A nach B? Oder einfach weg? Datei-Manager gehören eigentlich zur Grundausstattung. Nur leider kommt bei Android nicht wirklich etwas brauchbares mit. Aber zum Glück gibt es da genügend im *Play Store* – wie z. B. der ES Datei Explorer (Bild links). Neben dem Linda File Manager und dem Astro Datei Manager gehört er zu den drei beliebtesten Apps in dieser Kategorie.

Und das nicht ohne Grund: Der *ES Datei Explorer* ist nicht nur intuitiv bedienbar, sondern kann auch gleich von Haus aus auf entfernte Dateisysteme (wie etwa den heimischen PC, oder auch einen FTP-Server) via SMB (alias Samba alias Windows-Freigabe) oder FTP zugreifen. Somit steht einem Datenaustausch nichts im Wege – auch wenn einmal kein USB-Kabel zur Hand ist. Im lokalen Netzwerk werden SMB-Freigaben automatisch gefunden – auch hier also wieder einfache Bedienung und Laientauglichkeit.

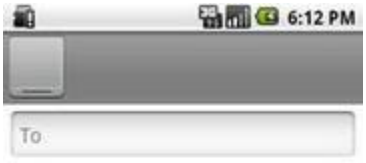
Mit ZIP-Archiven kann diese App ebenfalls von Haus aus etwas anfangen. Sogar ein kleiner Bildbetrachter sowie Video-Abspieler sind integriert. Und wem das noch nicht ausreicht, der findet auch Plugins für einen "Bookmark Manager" (Lesezeichen für Dateien, Verzeichnisse, etc. verwalten), einen "Sicherheits-Manager" (Apps mit Passwort schützen, Thread Detector, Gerät aus der Ferne sperren, Standort des Gerätes ermitteln) sowie einen "Task-Manager" (Task-Killer, Apps löschen – mit Widget).

Die Szene könnte durchaus in absehbarer Zeit ein wenig aufgemischt werden – denn einer der bekanntesten Dateimanager aus der Windows-Welt hat den *Play Store* betreten. Die Rede ist vom Total Commander – und der kann sich offensichtlich in Sachen Funktionsumfang mit den beiden anderen vorgestellten Kandidaten durchaus messen. Wie der Screenshot erkennen lässt, kann man durch das lokale Dateisystem ebenso navigieren wie durch SMB-Freigaben. Ein Lesezeichen- sowie ein App-Manager sind zu erkennen, ebenso die Möglichkeit zum Download weiterer Plugins. Die Archiv-Unterstützung (ZIP, RAR) entspricht der des *ES Datei Explorers*; an Netzwerk-Protokollen stehen neben SMB offensichtlich noch FTP und FTPS zur Verfügung (SFTP ist unter Windows eben nicht so verbreitet). Ebenso soll ein Text-Editor direkt integriert sein. 4,9 Sterne bei über 6.000 Bewertungen (vor allem in so kurzer Zeit) legen nahe, dass der *Total Commander* sicher keine schlechte Wahl darstellt.

Weitere und ähnliche Apps sind wieder im zugehörigen Forums-Thread aufgeführt und – teilweise – auch kurz näher beschrieben.

Tastaturen

Zumindest in diesem Bereich ist bei Android bereits ein brauchbares Bordwerkzeug dabei. Was natürlich nicht heißt, dass es nicht vielleicht besser ginge. Wobei: Was da besser ist, ist doch meist recht subjektiv – und so gibt es da auch die verschiedensten Ansätze für die Verbesserungen...



So gibt es mit ThickButtons (Bild rechts) eine Tastatur für Wurstfinger, die automatisch die wahrscheinlich passendsten Tasten (gemäß der vorigen Eingabe, also quasi Worte-raten) vergrößert, damit man sie besser trifft. Finger noch dicker? Viele Tastaturen bieten auch "T9" an – tippen wie SiMSen in den "guten alten Zeiten".

Eine andere Möglichkeit der Texteingabe ist das "Swypen": Hier tippt man nicht jeden Buchstaben einzeln an, sondern "wischt" über die Tastatur, ohne

abzusetzen. Und wäre es nicht schön, wenn man auch die lustigen Smileys immer gleich zur Hand hätte? Oder Funktionen zum Kopieren und Einfügen? Ultra Keyboard vereint alle diese Möglichkeiten in einer App, für den Preis von ca. 2 Euro.

Nostalgiker aus Palm-Zeiten greifen vielleicht lieber zu Graffiti (ja, das gibt es auch für Android!). Und wer es futuristischer mag, holt sich einen Assistent, und gibt seine Anweisungen verbal: "SMS an Peter: Komme heute später." Geht natürlich auch ohne Reim: "Suche nächste Sushi-Bar!". Der Assistent führt dann (hoffentlich) die richtige Aktion durch: Schickt dem Peter die SMS, und navigiert schließlich zur Sushi-Bar. Das sind nur einige Beispiele – da geht bestimmt noch mehr.

Mehr? Ja, wieder im Forums-Thread...

System-Info

Wer belegt da eigentlich schon wieder den ganzen Speicher? Und wer frisst die ganze CPU? Und wo ist die Bandbreite der Netzwerk-Verbindung abgeblieben? Diese Frage beantworten Apps wie OS Monitor (links) oder SystemPanel (rechts).

Die Details sind da recht unterschiedlich (und weitere in diesem Bereich verfügbare Apps mögen wieder eine andere Zusammenstellung bieten). *OS Monitor* bietet u. a. einen Task-Manager, in dem man laufende Prozesse nach Kriterien wie CPU- oder Speicherverbrauch sortieren (und bei Bedarf auch beenden) kann, versorgt mit Informationen über vorhandene Netzwerk-Interfaces sowie offene Verbindungen (welche App und wohin – mit "whois" und Karten-Ansicht), und bietet auch Zugriff auf die System-Logs. *SystemPanel* hingegen eignet sich gut zum "Monitoring" – also zur Langzeit-Beobachtung der Verbraucher.

Natürlich sind das noch nicht alle Kandidaten dieser Kategorie: Da wären noch Android System Info, welches allgemeine System-Informationen, TaskManager, AppManager, und ein farbiges SystemLog zur Verfügung stellt. Auch eine ganze Reihe von Widgets mit SystemInfos gibt es. Mehr Informationen dazu natürlich wieder im entsprechenden Forums-Thread...

Verschlüsselung

Vertrauliche Daten auf dem Smartphone sind heute sicher keine Seltenheit mehr. Was aber, wenn das Gerät in falsche Hände gerät? Wie sicher sind die Daten?

Wer also unbedingt sensible Dinge auf seinem Androiden haben muss, sollte sich vielleicht auch über Verschlüsselung derselben Gedanken machen. Apps wie FilesCrypter oder Encryption Manager sind in der Lage, sowohl einzelne Dateien als auch ganze Verzeichnisse zu Verschlüsseln. Ein gut gewähltes Passwort, kombiniert mit einer sicheren Verschlüsselungsmethode – das macht das "knacken" nahezu unmöglich.

Die App Droid Crypt bietet noch etliche zusätzliche Möglichkeiten: Etwa die Prüfung, ob irgendwo verschlüsselte Dateien auch noch unverschlüsselt vorliegen (das wäre gar nicht gut!). Oder die Möglichkeit, Dateien zusätzlich zum Verschlüsseln auch gleich zu komprimieren (um Platz zu sparen). Alternativ zu Passwörtern lassen sich übrigens mit dieser App auch die Bewegungs-Sensoren nutzen: Schwenken und Schütteln als Passwort, das ist doch mal was anderes!

Wer hingegen gleich das ganze Gerät verschlüsseln möchte: Diese Möglichkeit bietet Android ab Version 4.0 von Haus aus...

Automatisieren von Aufgaben

Wozu hat man eigentlich einen Hosentaschen-Computer, wenn man dann doch jede Kleinigkeit selber machen muss? Und Mensch ist ja so vergesslich: Wieder einmal das Telefon auf dem Schreibtisch liegen lassen, zum Mittagessen gegangen, und die Kollegen hat das dauernde Klingeln "erfreut"? Oder vergessen, vor dem Starten des Navis GPS anzuschalten? Oder...

Was kann man also tun? Mein Forums-Thread zum Thema zeigt da etliche Möglichkeiten auf. Da gibt es einfache Apps für einfache Möglichkeiten (und einfache Leute) – und auch richtig komplexe Dinge, die schon ein wenig Einarbeitungszeit benötigen. Egal, was die Wünsche hier sind – dort sollte sich eine passende App finden.

Hat man einen sehr geregelten Tagesablauf, und möchte lediglich zeitgesteuert ein paar "kleine Dinge" erledigt haben – wie nachts in den Flugzeugmodus, morgens wieder an, und von 9-17 Uhr leise? Dann reicht eine zeitgesteuerte App wie Timeriffic oder Android Audio Profile völlig aus. Geht jemand oft ins Kino, aber zu unterschiedlichen Zeiten – und da soll der "kleine Quälgeist" gefälligst still sein? Dann greift dieser eher zu einer "ortsgesteuerten" App wie Llama. Beides wird gebraucht, und vielleicht noch ein paar Aktionen mehr – doch zu kompliziert soll es auch nicht werden? Dann sind Apps wie EasyProfiles oder PhoneWeaver vielleicht das Richtige.

Wer das Ganze aber richtig ausreizen will, greift zu Apps wie Locale oder besser noch Tasker (Bild links). Gerade bei letzterem kann man sich so richtig austoben – den Möglichkeiten sind hier (fast) keine Grenzen gesetzt: Bei Ankunft zu Hause das WLAN aktivieren. Um Mitternacht in den Flugmodus schalten, morgens um 7 wieder zurück, und dann auch gleich den Audio-Stream der Lieblings-Internet-Radio-Station (oder ein Random-MP3 von der Karte) auf die Ohren. Wenn der Kopfhörer angeschlossen wird, gleich den Musikplayer starten – und wenn die Navi-App gestartet wird, GPS anmachen.

Das waren noch die harmlosen Sachen. Wie wäre es damit: Während der Autofahrt eingehende Anrufe und/oder SMS automatisch beantworten lassen? Auch noch zu einfach. Anruf stummschalten, wenn das Handy auf das Display gelegt wird? Jaaa... Wifi Abschalten wenn Signal zu schwach? Geht auch. Automatische Freisprech-Einrichtung (Ton auf Lautsprecher legen, wenn Telefon nicht am Ohr)? Auch das.

Ich könnte noch eine ganze Weile so weiter machen. Alternativ kann aber auch in der "Rezepte-Sammlung bei Android-Hilfe.DE (Deutsch), oder in der Profil-Liste des Tasker Wikis (Englisch) nachgeschaut werden. Natürlich gibt es auch bei AndroidPIT zahlreiche Tasker-Threads, etwa mit Vorschlägen für neue Profile." Mit *Tasker* wird uns da kaum jemals der Stoff ausgehen...

TIEFERGEHENDES FÜR FORTGESCHRITTENE

Nachdem sich die ersten beiden Teile dieses eBooks 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 man sich jedoch an die Umsetzung der "schweren Kost" macht, sollte man mit seinem Android-Gerät schon recht gut vertraut sein.

Dennoch heißt das nicht, dass diese 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 "verscheißert" vorkommen könnte). Dies verschafft zumindest einen Überblick über sich bietende Möglichkeiten. Und als Seiten-Effekt 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:

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" (bei einem Mac sicher ähnlich). 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."

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). Eine EU-Richtlinie stellt hier sicher, dass der Gewährleistungs-Anspruch trotz root nicht erlischt.

Braucht man den root-Zugang nun wirklich? Ja und nein. Wer mit seinem Gerät, dessen Funktionen, sowie der verwendeten Software bereits rundum zufrieden bist, alles so läuft, wie gewünscht, und "eigentlich" nichts vermisst – der braucht auch keinen root-Zugang. Er hat ja bereits alles, was er braucht. Hat man hingegen ein Problem, was 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 ggf. verbunden?

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 de-installierter Apps; siehe Unnütze Apps raus!)
- App2SD bei Android < 2.2 (siehe Tuning)
- Aufspielen alternativer Firmware (AKA Custom ROM)
- Ändern der Systemschriftart(en)
- Erstellen eines wirklich vollständigen Backups Deines Android-Systems (erst ab Android 4.0 ohne root möglich)
- Einrichten einer Firewall (z. B. 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:

Risiken des root-Zugangs

Die Risiken sind schnell mit einem Satz beschrieben: Falsch angewendet, kann man sich mit root-Zugang 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 eingesetzt, 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...

Oder sich schlicht vor unnötigen Rückgaben und Garantie-Einforderungen von sich selbst überschätzenden Anwendern zu schützen. Ein nachvollziehbarer Grund – denn solche Anwender gibt es leider zu viele. Da es somit keinen root-Zugang ab Werk gibt, liegt für Anwender mit Sinn und Verstand das größere Risko eher in der Erlangung eines solchen. Je nach Gerät und Verfahren ist dieses größer oder fast gar nicht vorhanden. Da die Höhe des Risikos jedoch vom verwendeten Verfahren abhängt, lässt sich hier keine allgemeingültige Aussage treffen. Für weitere Details bietet ein Artikel bei StackExchange einen guten Einstieg.

Noch ein Wort zu vermeintlichen Risiken: "Wenn ich mein Gerät gerootet habe, können dann alle Apps mit Superuser-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.

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. Und natürlich findet man auch StackExchange treffsichere Hilfe.

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 "SuperUser, 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 "su" voranstellt. Also "su <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 SuperUser-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.

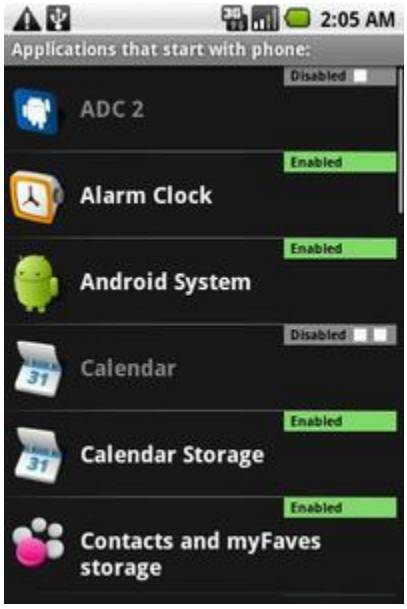
Bei jedem weiteren Aufruf findet der SuperUser die App in seiner Datenbank mit dem Vermerk "die darf das immer" (sofern der Haken beim ersten Aufruf entsprechend gesetzt war), und führt den Befehl direkt aus. Zur Sicherheit wird dieser Fakt jetzt nochmals als Hinweis eingeblendet (siehe Screenshot rechts). 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.

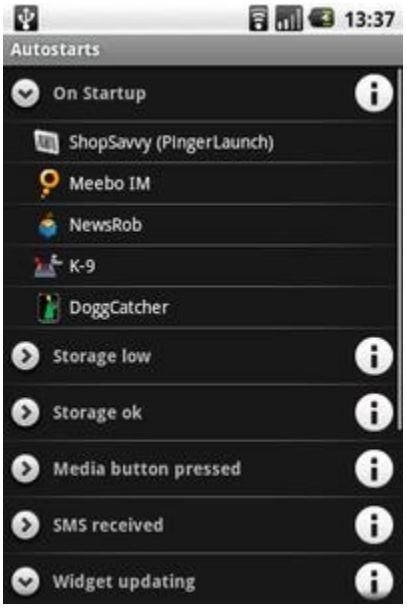
Apps am automatischen Starten hindern

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 auf einer Ausschluss-Liste stehender Apps) 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).

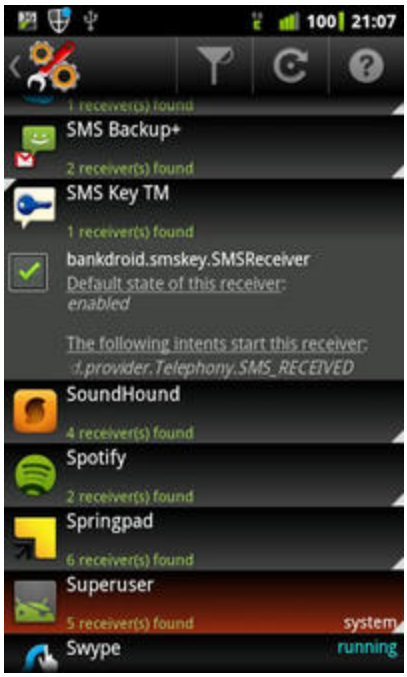
Für Details gleich an dieser Stelle den Verweis zum zugehörigen Foren-Thread.





Ja, es gibt sie: Apps wie Startup Auditor (linkes Bild) und AutoStarts (rechts). 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.

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 kann dann in einen Kreislauf ausarten, der alles andere als Ressourcen-schonend ist! Es gibt allerdings eine App, die so etwas selbst erkennt: Autorun Manager (Bild rechts) 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 "unregistriert" die jeweilige App vom jeweiligen Event. Hier muss man dann vor einer eventuellen De-Installation daran denken, ***vorher*** die ursprünglichen "Defaults" wieder herzustellen (geht allerdings einfach: "Rescue-Mode", und fertig).

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 werd ich "den Schrott" los? Jetzt kommt das böse Wort: "Ohne *root*? Gar nicht." Da wären wir also wieder. Zum Glück lassen sich ab Android 4.0 Apps zumindest auch ohne root "einfrieren" (deaktivieren).

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 anbietet). Damit taucht die App in keiner Liste (außer hier 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 wieder herstellen, und die System-Dinge nicht anfassen).

Wer da noch einfrieren und auftauen kann, und noch einiges mehr, ist SuperBox, das sich selbst auch als "Schweitzer Taschenmesser" bezeichnet. Definitiv auch einen Blick wert. Kann nämlich auch den Cache aufräumen, und solche Dinge – die im nächsten Kapitel zur Sprache kommen...

Tuning – Das Android-System auf Trab bringen

...und nicht nur das: Auch mehr Stabilität kann ein durchaus willkommener Nebeneffekt dieser Maßnahmen sein.

Ein altbekannter Effekt: mit der Zeit wird unser Androide immer träger. Oder kommt uns das nur so vor? Doch spätestens dann, wenn jemand seinen "guten alten" Freund aus der ersten Generation neben einen Kameraden aus der aktuellen Mittel- oder gar Oberliga legt, liegt die Antwort auf der Hand: Ja klar, der neue ist definitiv schneller. Diesen großen Schritt werden wir mit unseren "alten kleinen Gurken" kaum vollständig bewältigen – aber wir können die Lücke kleiner machen. Und darum soll es hier gehen, in mehreren Schritten. Nicht jeder wird alle Schritte durchführen können/wollen (ich sage nur, da kommt Herr Root ins Spiel) – dennoch ist sicher für die meisten etwas passendes dabei. Auch, wenn das Gerät bereits neuer und schneller ist: Ein wenig Finetuning kann ja nicht schaden, gelle?

Auch hier wieder, gleich zu Beginn, der Hinweis: Die ausführlichere Variante dieses Textes, ggf. mit weiteren Informationen und Benutzer-Diskussionen, findet sich im zugehörigen Forums-Thread.

Schnellwaschgang

Bevor ich ein wenig in die Details einsteige, hier ein paar Schnelltipps für Ungeduldige – sozusagen das Wichtigste auf einen Blick (eine Übersicht über Verbrauchsdaten gibt es im Anhang):

Akku-Laufzeit verlängern

- WLAN komplett abschalten, wenn es nicht gebraucht wird. Das spart enorm, und lässt sich auf Wunsch auch automatisieren
- Wer kein mobiles High-Speed benötigt: 3G aus, das frisst auch ganz nett (siehe auch 2G versus 3G: Spart 2G wirklich so viel Akku?)
- Dito ggf. für GPS (spart aber nur wenig, da es im Standby so gut wie nix frisst)
- Helligkeit des Displays weitmöglichst herunterregeln. "Aufdrehen" dann im Bedarfsfall.
- Live-Wallpaper und sonstige "animierte Dauerrenner": Wer drauf verzichten kann, sollte das tun!
- root und Modder: CPU nicht über-, sondern ggf. eher untertakten. Ich weiß, das klingt nicht besonders "cool" – spart aber Akku.
- Apps, die nicht benötigt werden, deinstallieren. Was nicht da ist, macht keinen Stress.
- Apps, die man *nur gelegentlich* braucht, müssen *nicht ständig* im Hintergrund laufen. Tun sie das doch, verbietet man ihnen ggf. das Automatische Starten.
- Die Datensynchronisierung muss evtl. auch nicht ständig laufen. Bei vielen Apps, die eine solche benötigen (z. B. RSS-Reader, Mail-Apps) lassen sich die Intervalle entsprechend anpassen – oder gar der Abgleich auf Zeiträume mit WLAN-Empfang beschränken (das spart nebenbei gleich noch Datenvolumen)

Mehr Speed

- RAM Bereinigen (Android-interne Einstellungen optimieren)
- Eventuell Swap-Space nutzen (braucht root)
- Nur für bestimmte Situationen, wo es darauf ankommt: CPU ggf. leicht übertakten. Frisst aber auch mehr Akku.
- Apps, die nicht benötigt werden, deinstallieren. Was nicht da ist, macht keinen Stress.
- Die Datensynchronisierung muss evtl. auch nicht ständig laufen. Bei vielen Apps, die eine solche benötigen (z. B. RSS-Reader, Mail-Apps) lassen sich die Intervalle entsprechend anpassen – oder gar den Abgleich auf Zeiträume mit WLAN-Empfang beschränken (das spart nebenbei gleich noch Datenvolumen)

Mehr Platz im internen Speicher schaffen

- Apps, die nicht benötigt werden, deinstallieren. Was nicht da ist, frisst kein Brot.
- Apps aus dem internen Speicher auf die SD-Karte auslagern
- Cache bereinigen

Apps auslagern

Normalerweise werden Apps im Telefonspeicher installiert – und der ist nicht immer unbedingt üppig ausgestattet. Ein paar "größere Knaller" installiert, und voll ist er: Vor der Installation der nächsten App muss man sich also entscheiden, auf welche bereits installierte App man hier verzichten kann...

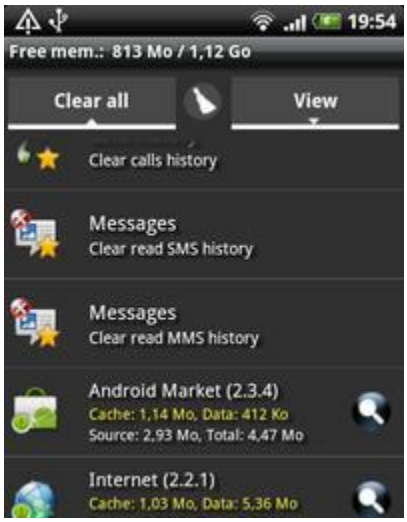
Mit Froyo (Android 2.2) und neuer, lässt sich bereits von Haus aus App2SD nutzen – größere bzw. seltener benutzte Apps können so auf die SD-Karte ausgelagert werden. Damit hat man wieder freien internen Speicher – u. a. auch für die Apps, die kein *App2SD* unterstützen. Fertig – der Rest dieses Kapitels kann nun übersprungen werden!

Hm, noch hier? Also noch Android < 2.2 am Laufen, ja? Kein root? Naja, dann hat das Folgende eher informativen Charakter. Um die hier beschriebenen Möglichkeiten zu nutzen, muss der Androide zuvor gerootet werden...

Die App Link2SD (Bild rechts) ermöglicht das Auslagern von Apps auf die SD-Karte auch unter "älteren" Android-Versionen. Und zwar sogar "besser" als *Apps2SD*: Es wird eine separate Partition auf der Karte angelegt (äh, falsch: *der Anwender* muss diese Partition im ersten Schritt anlegen). Auf diese verschiebt man dann die gewünschten Apps, und am ursprünglichen Speicherort werden sogenannte "symbolische Links" auf die neue Location angelegt. Schließt man nun den Androiden per USB-Kabel an den PC an, wird nur die andere Partition dorthin exportiert – und die ausgelagerten Apps bleiben weiterhin lokal verfügbar. Das ist bei *App2SD* nicht der Fall.

Was hierfür benötigt wird, und welche Schritte nötig sind, beschreibe ich ausführlich im Forum – und auch bei der App-Beschreibung finden sich die entsprechenden Informationen.

Cache bereinigen



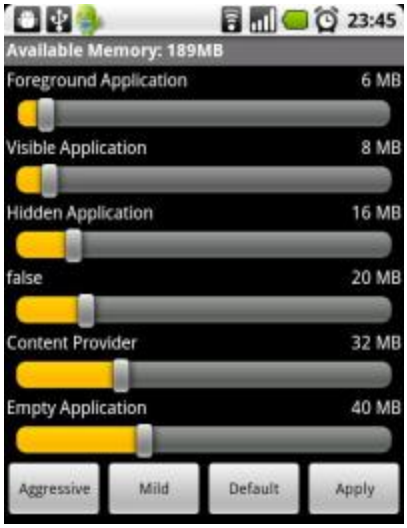
Und weiter geht's mit der Bereinigung des internen Speichers. ***Dieser Schritt benötigt kein root*** – kann also von jedem genutzt werden.

Cache ist schon eine feine Sache, und soll so manche Dinge ja schneller machen. Zum Beispiel, indem man Daten aus dem Internet im lokalen Dateisystem ablegt, damit man sie nicht jedes Mal neu laden muss, wenn sie wieder gebraucht werden. Der letzte Teilsatz ist aber genau der Knackpunkt: Braucht man sie überhaupt noch? Und was, wenn dummerweise mal gerade eine "kaputte Variante" im Cache landet? Oder der Platz im internen Speicher knapp wird?

Kurz: Wird der Cache gelöscht, geht dabei nix kaputt. Die Daten müssen im schlimmsten Fall neu (z. B. aus dem Internet) geladen, oder neu generiert werden. Dafür ist aber anschließend aufgeräumt – und so manches Problem nebenbei mit behoben.

Und wie erledigt man das? Mit Bordmitteln: In den Einstellungen in die Anwendungs-Verwaltung gehen, jeden Eintrag einzeln durchforsten (ob die App überhaupt Cache nutzt), und für jede betroffene App den Cache von Hand löschen. Da geht schon mal gern ein Stündchen bei drauf – und bequem ist es auch nicht gerade. Zum Glück gibt es zahlreiche Alternativen, wie z. B. Quick App Manager (rechts), Quick Cache Cleaner, und weitere.

RAM bereinigen



Nachdem wir uns nun um den internen Speicher gekümmert haben, geht's ans Eingemachte: Das RAM ist fällig!

Wer aber nun an Task-Killer denkt – voll daneben. Kontrovers diskutiert, verteufelt, hochgejubelt... Aus meiner Sicht ist die Aufgabe eines Task-Killers nicht, freien Speicherplatz im RAM zu schaffen (das ist eher ein Nebeneffekt) – sondern vielmehr, "hängende" Apps zu beenden, die andernfalls z. B. Amok laufen, oder das System lahmlegen (z. B. mit hoher CPU-Last). Details finden sich weiter oben unter Von Taskkillern und anderen bösen Buben.

Nächstes Argument: "Android kümmert sich doch selbst um die Speicherbereinigung". Jetzt kommen wir der Sache näher: Ja, das stimmt – die Frage ist nur: Wann? Wie oft? Und wie? Darum geht es in erster Linie: Die zugehörigen Einstellungen für diesen sogenannten "OOM-Killer" (**O**ut **O**f **M**emory Killer)

anzupassen. Ihm beizubringen, wie viel freien Speicher wir benötigen – und wann er zuschlagen darf.

Auch hierfür gibt es wieder zahlreiche Helferlein. Da es sich um System-Einstellungen "unter der Haube" handelt, wird hier i. d. R. root benötigt. Eine rühmliche Ausnahme ist da Auto Memory Manager (Bild links), der es angeblich auch ohne schafft. Selbst getestet habe ich den AutoKiller Memory Optimizer, der recht gut funktioniert.

Swapspace nutzen

Kommen wir zum nächsten Punkt dieser Reihe: Wenn das RAM nicht reicht, wie schaut es mit "virtuellem RAM" – also dem Auslagern auf einen anderen Datenträger – aus? ***Hier brauchen wir definitiv wieder root***.

Klar: Wenn der Speicher im RAM knapp wird, kommt Android (genauer: o. g. OOM-Killer) daher und beendet "überflüssige" Prozesse. Geht ja auch nicht anders. Aber was in diesem Augenblick überflüssig ist, war das vielleicht vor 10 Minuten noch nicht – und wird u. U. in weiteren 10 Minuten doch wieder benötigt. Ja, es lässt sich neu starten – aber das ist naturgemäß nicht so schnell wie das "aufwecken" bestehender Strukturen.

Mehr RAM ist (in bestehender Hardware) schwer realisierbar – es lässt sich ja nicht, wie etwa beim PC, einfach ein zusätzlicher Speicher-Riegel einstecken. Somit kommen wir zur Auslagerung, dem sogenannten Swapping. Hierbei wird ein Bereich eines Datenträgers (gewöhnlich einer Festplatte – im Falle unserer Androiden muss dafür die SD-Karte herhalten) genutzt, um Teile des RAM (natürlich die gerade am wenigsten benötigten) dort temporär unterzubringen. Werden diese wieder benötigt, liest das System sie halt wieder ein. Das ist zwar nicht so schnell, als würde ausschließlich im RAM gearbeitet – aber i. d. R. immer noch schneller und besser, als hätte man diese Möglichkeit überhaupt nicht.

Wie realisieren wir das nun – sofern wir nicht ein Custom-ROM einsetzen, bei dem es bereits "fertig eingerichtet" ist? Auch hier greift uns wieder eine geniale App hilfreich unter die Arme: Swapper (Bild rechts). Die App kümmert sich in jeder Hinsicht um das Bereitstellen der Funktionalität (sofern der eingesetzte Betriebssystem-Kernel das unterstützt):

- Neuanlegen einer Swap-Datei beim Boot
- sauberes Abschalten des "Swapping", wenn der Datenträger per USB gemountet wird
- Neu-Aktivierung nach Lösen des USB-Mount
- gezieltes Einstellen der "Swap-Prioritäten"

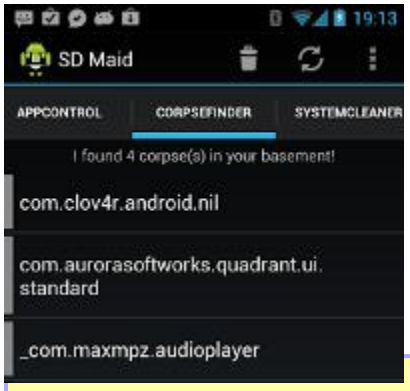
Sind nur die wichtigsten Punkte – und jeder davon ist optional. Es lässt sich auch eine Swap-Partition nutzen (das erübrigt dann auch das Abschalten bei

USB-Kontakt, sowie das spätere wieder Aktivieren). In der Regel ist eine Swap-Partition ein wenig schneller als eine Datei – aber aufgrund der begrenzten Schreibzyklen von SD-Karten hat man länger etwas von selbigen, wenn Swapper sich darüm kümmert, die Datei bei jedem Neustart an anderer Stelle der Karte wieder anzulegen.

Nebenbei: Übertreiben sollte man es auch nicht, ein gutes Mittelmaß ist gefragt. Ist zuviel "Krams" ausgelagert, bremst das am Ende doch wieder. Gute Anfangswerte sind 32..64MB Swap sowie eine "Swappiness" von 10..20.

Unnütze Apps raus!

Das sollte eigentlich sowas von klar sein: Apps, die man überhaupt nicht mehr braucht, belegen unnütz Speicher – und können auch bei Nicht-Benutzung das System (leicht) ausbremsen. Also runter damit! Die notwendigen Details hierzu finden sich bereits weiter oben unter Apps verwalten. Und was man nicht deinstallieren kann/möchte, kann man ja zumindest noch am automatischen Starten hindern.



Noch Leichen im Keller? Im Laufe seines Androiden-Lebens hat unser Gerät so manche App "einmal kurz gesehen", die dann wieder entfernt wurde – etwa weil wir etwas besseres gefunden haben, oder die App aus anderen Gründen nicht mehr benötigen. Nicht jede dieser Apps wurde restlos entfernt – manch eine App ließ noch ein paar "Leichen" zurück. Und dann wären da noch diverse "core dumps" von "Force Closes" ("Schließen erzwingen"), System-Logs, und mehr.

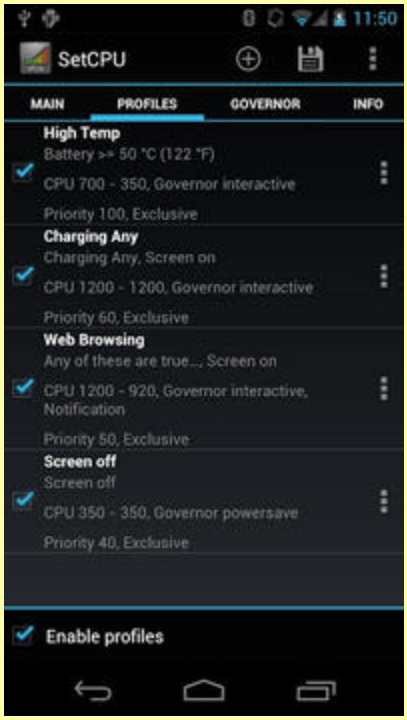
Eine App verspricht, sich genau darum zu kümmern: SD Maid (Bild links). Die App ***braucht allerdings root***. Was sie tut: Sie durchsucht die typischen Verzeichnisse (`/data/data` und `/mnt/sdcard/Android/data` bzw. bei Samsung-Geräten `/dbdata/databases` für erstere Location) und vergleicht die dortigen Einträge mit der Liste tatsächlich installierter Apps. Auf diese Weise wird überflüssiges identifiziert, und kann entweder einzeln (Eintrag antippen) oder gleich in einem Rutsch ("Clean All") entfernt werden. Im Reiter "Clean System" lassen sich weitere Plätze und Dinge bereinigen – etwa System-Logs, Core-Dumps oder – huch? – auch Cache.

CPU Taktung anpassen

Wiedermal nur für gerootete Geräte.

Hier gibt es generell eigentlich zwei Richtungen:

- Höhere Taktung → Schnellere Reaktion & Arbeitsgeschwindigkeit – aber auch der Akku wird so schneller leer
- Niedrigere Taktung → Langsamere Reaktion & Arbeitsgeschwindigkeit – aber der Akku hält (teilweise deutlich) länger durch



Eigentlich klar soweit – auch wenn die meisten beim Thema "CPU Taktung" nur/zuerst ans Übertakten denken, auch Untertakten kann seine Vorteile haben. Beim Übertakten sollte man überdies vorsichtig sein, dass man aus seinem Androiden nicht zuerst eine Warmhalteplatte, dann eine Kaffeemaschine, und schließlich einen Ziegelstein macht – nicht übertreiben!

Sinnvolle Szenarien beinhalten u. a.:

- Wenn das Gerät nicht benutzt wird (Bildschirm aus, Nachtschlafene Zeit, ...) → runter mit dem Takt
- Wenn das Gerät benutzt wird (Bildschirm an) → Auf "normalen" Takt schalten (was immer das für den einzelnen ist)
- Wenn eine bestimmte (hungrige) App im Vordergrund läuft → Hoch mit dem Takt (Vorsicht – nicht zu hoch)

Viele der CPU-Taktveränderer decken die ersten beiden Punkte ab. Der dritte Punkt ließe sich z. B. mit Tasker sicher realisieren.

Wiederum gibt es etliche Apps, die beim Drehen an der CPU-Schraube behilflich sein wollen. Die bekannteste ist sicherlich SetCPU (rechtes Bild), der bekannteste Mitbewerber dazu heißt CPU tuner. Weitere Kandidaten sind im Forums-Thread benannt, oder finden sich auf den jeweiligen Seiten der Apps als Alternativen aufgeführt.

Durststrecke – mehr aus dem Akku herausholen

Wenn der Akku mit einer Ladung länger durchhalten soll, müssen wir den Energieverbrauch senken. Soweit klar. Also stellen sich die Fragen:

- Was verbraucht Energie?
- Was ist dafür verantwortlich?
- Wie können wir dem beikommen?

Schauen wir uns diese Fragen also einmal nacheinander an.

Was verbraucht Energie?

Gleich von vorn herein auf den Aspekt des "können wir dem beikommen" betrachtet, lassen sich die Verbraucher schnell auf wenige Punkte reduzieren:

- CPU
- Speicherzugriffe
- Netzwerkzugriffe
- "Peripherie-Geräte" (hier: Kamera, Display)

Dafür verantwortlich sind natürlich die Apps, welche die Ressourcen beanspruchen – und natürlich nicht zuletzt der Benutzer, der einen gewissen Einfluss auf diese Apps hat. So ergeben sich einige Lösungsansätze schon von selbst:

Wie können wir dem beikommen?

Zum größten Teil sind diese Punkte bereits in den vorigen Kapiteln behandelt worden. Diese Kandidaten seien daher hier nur noch einmal kurz aufgezählt:

- Apps, die nicht benötigt werden: Weg damit! Was nicht da ist, kann auch nichts verbrauchen.
- Was man nur selten braucht, muss nicht ständig laufen – diese Apps sollte man also am automatischen Starten hindern! Das gilt auch für auf den Homescreens installierte Widgets: Hier handelt es sich ja ebenfalls um laufende Apps, die automatisch gestartet werden. Daher sollte man diese möglichst sparsam einsetzen.
- Wenn im RAM genügend freier Platz existiert (also der "OOM-Killer" gut konfiguriert ist), wird dieser als Cache genutzt – und dafür weniger auf die Speichermedien zugegriffen.
- Exzessive Nutzung von Task-Killern verbraucht zusätzliche Energie – da viele Apps gleich nach dem Kill vom System wieder nachgeladen werden
- Ist der Androide gerootet, lääst sich die CPU untertakten (zumindest dann, wenn man sein Gerät ohnehin nicht benutzt).
- Das Display muss auch nicht unbedingt als Scheinwerfer herhalten – die Helligkeit lässt sich entsprechend anpassen.

Die meisten Dinge haben wir bereits besprochen. Ein paar jedoch noch nicht:

Speicherzugriffe: Ja, klar: mehr Cache mit sauberem Speicher – stand doch da schon. Richtig, aber das ist noch nicht alles. Die Frage ist auch: Was für eine SD-Karte steckt in meinem Gerät? Im Allgemeinen verbrauchen "ältere Karten" (also die langsameren Teile – erkennbar u. a. an ihrer kleineren "Klasse") mehr Strom als neuere, da die Lesezugriffe hier ja länger brauchen. Eine neue Karte verschafft uns also u. U. nicht nur mehr Speicher, sondern ist auch schneller – und der Akku hält länger. Steht also ohnehin ein Neukauf an, sollte man nicht zu knauserig sein: Lieber einen Euro mehr ausgeben, und was vernünftiges holen! "Class-6" sollte es heutzutage schon sein – unter "Class-4" sollte man nicht mehr gehen.

Netzwerk-Zugriffe: Auch diese kosten Energie – manche mehr, manche weniger. 3G (UMTS) knabbert i. d. R. stärker am Akku als 2G (GPRS/EDGE). Wer also (wie ich) nicht unbedingt auf "HighSpeed" an dieser Stelle angewiesen ist, schaltet 3G einfach komplett ab (schaut aber sicherheitshalber zuvor noch unter 2G versus 3G: Spart 2G wirklich so viel Akku? nach). Die passenden Schalterchen finden sich in *Einstellungen→Drahtlos und Netzwerke→Mobile Netzwerke* (Netzwerkmodus: "Nur GSM", bzw. "Nur 2G"). Weitere Kandidaten sind Bluetooth

und WLAN, die man bei Nichtgebrauch auch deaktivieren kann (siehe dazu unter Helferlein).

In die Rubrik *Netzwerk-Zugriffe* gehört übrigens auch der **mobile Datenabgleich** – hier kann man ebenfalls einschränken: Wetterinformationen müssen nicht alle fünf Minuten aktualisiert werden (hier genügen in der Regel 3-6 Stunden als Intervall). Bei RSS-Feeds kommt es auf die Ansprüche an; normalerweise ist ein stündlicher Abgleich aber ausreichend. Bei vielen RSS-Readern lässt sich das sogar noch auf die Zeiträume beschränken, in denen eine WLAN-Verbindung verfügbar ist; das spart dann nebenbei auch noch Datenvolumen. Bei Mails empfiehlt sich ein Anbieter (und eine App), die das "IMAP Idle" Protokoll unterstützen: Dann stößt der Server nämlich den Abgleich an, wenn neue Mail eintrifft – und man muss nicht alle paar Minuten unnötig nachschauen lassen ("Pollen"). Letzteres gilt jedoch nur, wenn man wirklich "ständig auf dem Laufenden" sein muss; wem eine Aktualisierung alle 30 (oder mehr) Minuten genügt, für den ist "Polling" sparsamer.

Kamera: Natürlich braucht auch diese "Saft", und nicht unbedingt wenig. Das betrifft nicht nur das Fotografieren, sondern auch die Barcode-Scanner. Von letzteren sind etliche dafür bekannt, dass sie auch nach "beenden" noch fleißig weiter nuckeln (was an einem Bug in der betreffenden Google-API zu liegen scheint). Hier könnte also ausnahmsweise ein Task-Killer-Einsatz gerechtfertigt sein. Oder aber die Wahl eines alternativen Barcode-Scanners.

Zu letzterem Fall gibt es sicher noch Parallelen, wo eine alternative App sparsamer wäre als die gerade eingesetzte. Um solche Kandidaten aufzuspüren, kann man z. B. die Statistiken unter *Einstellungen→Telefoninfo→Akku→Akkuverbrauch* nutzen, die besonders hungrige Apps auflistet. Aber aufpassen: Die Statistik zählt seit dem letzten Boot – lief eine hungrige App also nur mal eben ein Minütchen, fällt sie hier (noch) nicht so ins Gewicht. Mehr Details liefert dann, je nach eingesetzter Android-Version, auch noch ein "Anruf" bei der magischen Nummer **#*#4636#*#*...

Helferlein

Nicht verschweigen möchte ich hier einige Helferlein, die dem Nutzer beim Energiesparen "unter die Arme greifen" können. Grob gesehen wären dies zwei Kategorien von Apps: Schnellumschalter (finden sich in diesem Forumsthread ausführlicher behandelt), und im Hintergrund laufende, auf "Events" reagierende Apps.

Schnellumschalter sind meist Widgets auf dem Home-Screen, mit denen man "toggeln" (also zwischen zwei Zuständen wechseln) kann. z. B. "WLAN an/aus", "Bluetooth an/aus", etc. Einige dieser Widgets stehen schon "von Haus aus" zur Verfügung – aber damit kann man sich den Home-Screen schnell "zupflastern", wenn mehrere benötigt werden. Daher gibt es auch Apps, die mehrere Schalterchen sinnvoll vereinigen, und so platzsparend mehr anbieten können. Als Beispiele seien hier nur Dazzle (rechtes Bild) und Extended Controls genannt.

Hintergrund-Aufpasser steuern den Energieverbrauch "ereignisgesteuert", wobei der Anwender die Ereignisse meist selbst festlegt. Zum Beispiel: Wenn weniger als 20% Akkuleistung verbleibt, schalte Bluetooth und WLAN aus. Die bekannteste App in dieser Kategorie nennt sich JuiceDefender (Bild rechts); ein vergleichbarer Kandidat wäre Green Power.

Nicht vergessen werden sollten an dieser Stelle auch spezielle Helferlein wie APNdroid (mit dem man sein Telefon – temporär – daran hindern kann, Netzwerk-Verbindungen aufzubauen) oder 3G Watchdog (passt nicht so ganz hier, da es eher über das Datenvolumen wacht – aber es nutzt *APNdroid*, wenn man möchte, um bei einem bestimmten Volumen "abzuschalten").

Sicher gibt es noch etliche mehr – und ich gebe auch frei heraus zu, nicht alle zu kennen. Aber ich hoffe, hier zumindest einen Einblick in die Möglichkeiten gegeben zu haben: Nun ist jedenfalls bekannt, wonach man Ausschau halten kann. Und zum Glück werden ja sowohl im Google Playstore als auch bei AndroidPIT zu (fast) jeder App ja eine Reihe vergleichbarer Apps genannt, sodass man sich da weiter "durchhangeln" kann.

Den Akku Kalibrieren

Die Kapazität eines Akkus kann nicht einfach über ein Messgerät erfasst werden – das ist aus technischen Gründen leider nicht möglich. Daher sind angezeigte Kapazitäten und Laufzeiten lediglich Schätzwerte auf Basis zurückliegender Beobachtungen, die der im Akku befindliche Ladeprozessor aufgezeichnet hat. Damit das Gerät nicht "plötzlich und unerwartet" bei einem angeblichen Akku-Stand von über 30% "das Zeitliche segnet", oder aber die Anzeige schnell von 100% auf 1% fällt, um dann noch ein paar Stunden dort stehen zu bleiben, bevor der Akku wirklich leer ist, muss dieser Prozessor also lernen, wie sich der Akku verhält – und seine Berechnungen auf Grundlage dieses Verhaltens neu ausrichten.

Dies geschieht durch einen sogenannten "vollständigen Ladezyklus". Bildlich gesprochen, wird der Akku dabei einmal von 100% auf 0% und wieder auf 100% gebracht – wobei während des gesamten Zyklus das Ladegerät exakt ein Mal mit

dem Gerät verbunden wird (oder auch umgekehrt; auf jeden Fall eine volle Ladung ohne Unterbrechung).

Diesen Vorgang nennt man die "Kalibrierung" des Akkus. Optimalerweise werden zu Beginn dieses Zyklus noch die Akku-Statistiken gelöscht, was in der Regel jedoch root-Rechte voraussetzt. Doch dieser Schritt scheint eher einem Mythos gezollt, wie Android-Entwicklerin Diane Hackborn laut XDA-Developers erklärt: In der `batterystats.bin` Datei werden laut ihrer Aussage keine Daten der Batterie, sondern ausschließlich die (auch unter *Einstellungen → Akku-Verbrauch* einsehbaren) Verbrauchsdaten gespeichert. Somit erübrigt sich eigentlich der Einsatz der folgenden Apps, mit deren Vorstellung ich dem Mythos dennoch meine Referenz erweisen möchte:

Ein hilfreiches Tool zur Kalibrierung präsentieren die XDA Developers mit Battery Calibration (Bild links). Nach dem Start der App gibt diese genaue Anleitungen für das Vorgehen: Ladekabel anschließen und Akku vollaufen lassen wird empfohlen. Damit man nun nicht alle paar Minuten nachschauen muss, wie weit das Ganze gediehen ist, kann die App auch mit einem "Piep" benachrichtigen – wenn man nicht ein QVGA-mini-Display hat und somit übersieht, nach dem "Tapp" auf den "Piep" Button auch den links daneben für das "Wait" noch zu betätigen...

Akku voll? Dann geht's los: Per Druck auf den entsprechenden Button veranlasst man die App, die alten Akku-Statistiken zu löschen. Dem System bleibt nun keine Alternative mehr: Es muss neue erstellen. Womit die "Leichen" aus dem Keller wären. Empfohlen wird, den Akku nun einmal bis zur Erschöpfung zu leeren (am Besten komplett, unter 20% sollte es sein), und dann mit einem ununterbrochenen Ladezyklus wieder auf 100% hoch. Muss nicht sein, aber desto akkurater wird die Sache.

Bleibt die Frage: Wie oft sollte man dies tun, und wie sollte man vorgehen? Eine gute Zusammenfassung verlässlicher Quellen findet sich in einem Artikel bei StackExchange. Das Wichtigste kurz zusammengefasst: Keinesfalls öfter als einmal im Monat (alle drei Monate sollte völlig ausreichend sein) sollte man seinen Akku so weit als möglich entladen. Die 5% Marke sollte dabei auch definitiv nicht unterschritten werden. Anschließend das Gerät ohne Unterbrechung vollständig aufladen. Und immer daran denken: Vollständige Entladungen sind für einen Lithium-Ionen-Akku schädlich und verkürzen seine Lebensdauer, weshalb man eine "Kalibrierung" so selten wie möglich durchführen sollte.

Wenn wir uns die Praxis anschauen: Oft genug kommt es vor, dass der Akku des Android-Gerätes nahezu vollständig entladen wird, ohne dass dies beabsichtigt war (Warum ist am Ende des Akkus noch so viel Tag übrig?). Hier sollte man anschließend sogleich eine "vollständige Aufladung ohne Unterbrechung" durchführen, womit sich die Kalibrierung nebenbei erledigt hat.

Alternative Apps? Aber klar doch, wie immer in einem speziellen Forums-Thread...

Wer saugt da meinen Akku leer?

Soso, irgendwer saugt da also plötzlich den Akku leer – und der Anwender hat keinen blassen Schimmer, wer oder was das sein könnte? Da gibt es zunächst ein paar Bordmittel für die Analyse. Zum Beispiel die Übersicht der "größten Verbraucher", die sich unter Menü→Telefoninfo→Akkuverbrauch finden. Und auch ein paar mehr Details, wenn man mal bei **#*#4636#*#** "anruft".

Allerdings bieten beide Stellen nur einen groben Überblick über längere Zeiträume. Ein "Dauerläufer" sollte so zwar aufspürbar sein – doch manchmal hätten wir gern ein paar mehr Details zur Hand. Aber auch kein Thema: Einen passenden Kandidaten habe ich ja bereits unter System-Info benannt, das SystemPanel App (Bild rechts).

Für die detaillierte Analyse muss es allerdings in der Tat die Kaufversion sein – denn nur diese bietet das Monitoring im Hintergrund. Sobald sie für eine Weile Daten gesammelt hat, können diese dann ausgewertet werden. Wie das in etwa aussieht, zeigt der Screenshot am Beispiel eines bereits beendeten Google-Maps: Der obere Graph lässt erkennen, dass diese App etwa von 18 Uhr bis 20 Uhr lief. Ein Ladekabel war offensichtlich nicht angeschlossen (kein grüner Balken bei "Charging"), dafür wurde der Akku aber permanent entladen (dritter Graph von oben). Auch die CPU war derweil gut beschäftigt (unterster Graph), obwohl das Gerät nicht selbst durchgehend aktiv genutzt wurde (blauer Graph). Während dieser zwei Stunden leerte sich der Akku von knapp 100% auf gut 50% – ohja, das hat gut geschluckt! Und der Schuldige am "plötzlich leeren Akku" ist mit ziemlicher Sicherheit identifiziert...

Wie jetzt: Alternativen? Na gut, auch hier gibt es natürlich einen passenden Forums-Thread...

2G versus 3G: Spart 2G wirklich so viel Akku?

Eine Empfehlung, die man häufig zu hören und zu lesen bekommt: 2G geht viel sparsamer mit dem Akku um als 3G (oder gar 4G). Schaut man sich die nackten Zahlen an (siehe Leistungsaufnahme verschiedener Komponenten), scheint das auch zu stimmen. Aber ist das in der Praxis auch wirklich der Fall?

Vor dem Hintergrund dieser Frage habe ich den Selbstversuch gemacht. Als wenig telefonierender Wenigsurfer, hatte ich bislang alle meine Geräte auf 2G/GSM fixiert. Zum Test habe ich diese Sperre für ein paar Tage deaktiviert, und mein *LG Optimus 4X* per 3G (UMTS) ins Netz gelassen. Eigentlich hätte ich nun einen sich schneller leerenden Akku erwartet – aber das Ergebnis war ein anderes: Die minimalen Unterschiede, welche ich über die Tage feststellen

konnte, lassen sich durchaus als "Mess-Fehler" interpretieren. Schließlich hatte ich nicht gerade Laborbedingungen. Wie aber ist das zu erklären?

Man darf sich nicht ausschließlich den "Verbrauch pro Zeiteinheit der Aktivität" betrachten. Es muss auch darauf geachtet werden, wie lange diese Aktivität ausgeführt wird! Genau das will ich an einigen praktischen Beispielen im Folgenden tun. Dabei habe ich aus den genannten Daten im genannten Anhang Mittelwerte gebildet. Gleichzeitig habe ich 2G/GSM ein wenig "schön gerechnet" (also recht optimale Bedingungen zugrunde gelegt), während ich 3G/UMTS etwas pessimistischer betrachtete (weniger optimale Bedingungen, geringere Bandbreite). Dies sollte m. E. der Praxis recht nahe kommen, da nicht jeder Anbieter auch die neueste Technologie voll ausreizt.

Der wenig telefonierende Wenigsurfer

Hier habe ich ja bereits im Selbstversuch (siehe oben) festgestellt, dass sich nichts geändert zu haben scheint. Legen wir einmal 150–300 Minuten Telefonie und 50 MB Daten monatlich zugrunde, so kommen wir auf ca. 5–10 Minuten Telefongespräche sowie 1,5 MB Daten pro Tag. Beides Werte, die nahezu vernachlässigbar sind; es verbleibt daher der "Standby Verbrauch". Und der beträgt bei UMTS ca. 15 mW, bei GSM ca. 10 mW. Bedenkt man, dass das Display durchschnittlich mit 700 mW zu Buche schlägt, dürfen die 5 mW Differenz getrost ignoriert werden: Für diese Anwendergruppe spielt es also keine Rolle, ob die Datenverbindung auf 2G fixiert wird oder nicht.

Der Vieltelefonierer mit minimalem Datenverbrauch

In diesem Fall schaut die Sache ganz anders aus: Für Telefonate benötigt UMTS ca. 800 mW, während GSM mit gerade einmal der Hälfte (also ca. 400 mW) auskommt. Die Länge eines Telefonats verändert sich dabei nicht (man spricht mit UMTS ja nicht schneller) – der Verbrauch ist also mit UMTS in diesem Fall tatsächlich doppelt so hoch. Diese Anwender-Gruppe fährt also in der Tat mit 2G/GSM besser bzw. Akku-sparender.

Der wenig telefonierende Dauersurfer

Für diesen darf der Telefonie-Anteil wieder vernachlässigt werden, wie der erste Fall bereits zeigte: Im Standby sind die Unterschiede schließlich marginal. Bleibt der Datendurchsatz. Die "nackten Zahlen" zeigen auch hier nicht viel Differenz: Etwa 1.200 mW bei UMTS stehen etwa 1.000 mW bei 2G gegenüber. Schaut also gar nicht so wesentlich aus. Aber haben wir da eventuell etwas vergessen?

Werfen wir einmal einen Blick auf die Übertragungs-Geschwindigkeiten: UMTS schafft mit HSDPA/HSUPA einen Durchsatz von ca. 7 MBit für Downloads sowie 1 MBit für Uploads. 2G kommt mit EDGE lediglich auf ca. 300 kBit beim Download sowie 100 kBit beim Upload. Der Download einer Datenmenge von 1 MB benötigt somit ca. 1 Sekunde mit UMTS – jedoch ca. 30 Sekunden mit EDGE. Gemessen an der übertragenen Datenmenge, ist der Stromverbrauch also bei EDGE fast um den Faktor 30 größer!

Ergebnis der Berechnung: Diese Anwender-Gruppe sollte besser auf 3G/UMTS setzen.

Der viel telefonierende Dauersurfer

Für diesen hängt es maßgeblich davon ab, was er unter "viel Telefonieren" und "Dauersurfen" versteht. Je nachdem, was von beidem überwiegt, muss er sich in eine der drei obigen Gruppen einordnen; eine generelle Aussage lässt sich hier nicht treffen.

Der "Grashüpfer"

Ein spezieller Fall, besonders in ländlichen Gegenden, in denen die Netzabdeckung ein wenig "wackelig" ist: Muss das Gerät ständig zwischen den Netzen hin und her hüpfen, geht das anständig auf den Akku. GSM und UMTS verwenden verschiedene Frequenzbänder. Wird das Signal daher schwach, sucht das Gerät auch im jeweils anderen Band nach "besseren Konditionen". Ist man von diesem Missstand betroffen, sollte man sich ggf. ebenfalls für entweder 2G oder 3G entscheiden.

Fehlt da noch etwas?

Sofern jemand in obigen Ausführungen 4G/LTE vermisst hat, dies hat gute Gründe: Zum Einen habe ich kein Gerät, mit dem ich das Testen könnte – und zum Anderen fehlen mir zu 4G auch die "nackten Daten". Zu erwarten ist jedoch ein ähnliches Ergebnis: Es müsste für obige Ausführungen also lediglich "3G" durch "4G", "2G" durch "3G", "UMTS" durch "LTE", und "EDGE" durch "UMTS" ersetzt werden, während man die Zahlen entsprechend ignoriert...

ROMs: Stock, Vendor, und Custom

ROM – was ist das denn nun wieder? Klar, eine Abkürzung. ROM steht für **R**ead-**O**nly **M**emory. Also eigentlich Speicher, auf den nur lesend zugegriffen werden kann. Im Falle einer CD oder DVD ist das klar – im Falle unserer Androiden eigentlich glatt gelogen: Hier gehörte dann noch ein "m" davor, für "mostly" ("meistens"). Denn natürlich kann man da auch Schreiben: Irgendwie müssen die Updates ja da rein kommen...

Wie dumm von mir: Ich sollte erst einmal sagen, was da bei Android eigentlich drin ist. Nämlich das Betriebssystem, sowie die "Core Apps" (*Google Play Store*, Telefon & Co.). Manchmal auch noch mehr – kommt auf das ROM an. Da gibt es nämlich verschiedene: Stock, Vendor, Custom...

Stock ROM

Als "Stock" ROM bezeichnet man eigentlich das, was direkt aus der Google-Schmiede kommt (und für bessere Eindeutigkeit auch "Vanilla" genannt wird). Wörtlich eigentlich aus dem "Lager". Also das "nackte Original", so wie es von Google eigentlich gedacht war. Naja, die meisten verstehen darunter auch (noch) das Folgende:

Vendor ROM

Das vom Hardware-Hersteller vorinstallierte ROM. Also das, was aus dem gleichen Lager kommt wie das Gerät – weshalb es meist auch als "Stock ROM" bezeichnet wird. Obwohl das so nicht korrekt ist: Es gibt kaum einen Geräte-Hersteller, der hier nicht noch seine Modifikationen einbaut. Ich denke da nur an HTCs Sense, Motorolas Moto-Blur, oder Samsungs TouchWiz Oberfläche. Oder an das ganze Gesocks an vorinstallierten Apps, die "Otto Normalbenutzer" gar nicht und "Super User" auch nur mit Mühe wieder los wird. Genau genommen fehlt jetzt gar noch eine Kategorie, denn auch die Provider spielen nochmals dran rum, und pappen ihren Brandy, pardon, ihr Branding noch oben drauf...

Während Updates von Google natürlich recht regelmäßig, und Updates vom Hersteller noch "relativ zügig" kommen, bremst das Branding natürlich ein weiteres Mal: Denn auch hier muss erst das Zusammenspiel getestet werden. So kommt ein Hersteller-Update in der Regel frühestens im Quartal nach dem Google-Update. Und das Update fürs gebrandete Gerät kann sich durchaus noch zusätzlich um ein halbes Jahr verspäten. Zu diesem Zeitpunkt ist unter Garantie schon wieder mindestens ein neues Stock-ROM-Update draußen...

Custom ROM

Kostümiert? Zugegeben, auch das gewissermaßen. Aber eigentlich steht "Custom" für "customized", also auf den Kunden (customer) angepasst. Im Gegensatz zum Hersteller, oder Provider, zu sehen. Hier stehen meist eingespielte Teams von Entwicklern dahinter – und ein neues Custom-ROM steht häufig schon kurz nach der "Vanilla"-Stock-Version (nicht selten auch mal vorher) zur Verfügung.

Das AndroidPIT Wiki schreibt zu diesem Thema:

> *Eine auf Open Source basierende Software ist zur Entwicklung durch Dritte freigegeben.*
> *Somit haben Entwickler die Möglichkeit die original Software zu modifizieren, zu optimieren, Elemente hinzu zu fügen oder auch zu entfernen mit dem Ergebnis für den Verbraucher das bestmögliche Ergebnis zu bieten in den Bereichen Performance, Energie, Effizienz etc.*

Womit auch bereits die zahlreichen Vorteile geklärt wären. Haken an der Sache: Um ein Custom ROM installieren zu können, muss der Androide i. d. R. gerootet sein.

Die bekanntesten Custom-ROMs bzw. ihre Entwickler sind wahrscheinlich MoDaCo und Cyanogen. Aber es gibt noch zahlreiche Spezial-ROMs, die speziell auf bestimmte Geräte zugeschnitten sind (wie etwa *WildPuzzle* und *OpenFire* im Falle des HTC Wildfire). Hier informiert man sich am besten bei AndroidPIT im root-Forum des betroffenen Gerätes.

Selbst installieren?

Kann man sich nun selbst ein ROM eigener Wahl installieren? Klar doch – denn außer vielleicht einem "guten Kumpel" nimmt einem das kaum jemand ab. Am wenigsten der Hersteller. Mit den richtigen Werkzeugen (wie z. B. dem ROM Manager, Bild rechts) ist das auch recht problemlos bewerkstelligt – die App bietet u. a. eine Übersicht der für das jeweilige Gerät verfügbaren ROMs, lädt diese herunter, und führt durch den Installationsprozess. Einschließlich Backups, und was so dazu gehört.

Besonders vorbildlich ist das Ganze im Falle von *Cyanogen*: Hier stellt das Wiki für jedes unterstützte Gerät eine Anleitung bereit. Wie das Ganze in der Praxis aussieht, und ob es wirklich so "schwierig" ist, wie es beim ersten Mal klingt – lässt sich übrigens für das Beispiel "HTC Wildfire bekommt Gingerbread" in diesem Blog nachlesen.

Wie bereits im vorigen Kapitel beschrieben, ist allerdings das rooten des Androiden i. d. R. eine Grundvoraussetzung, ohne die man kein Custom ROM installieren kann...

Ortsdaten-Cache einsehen (und verwalten)

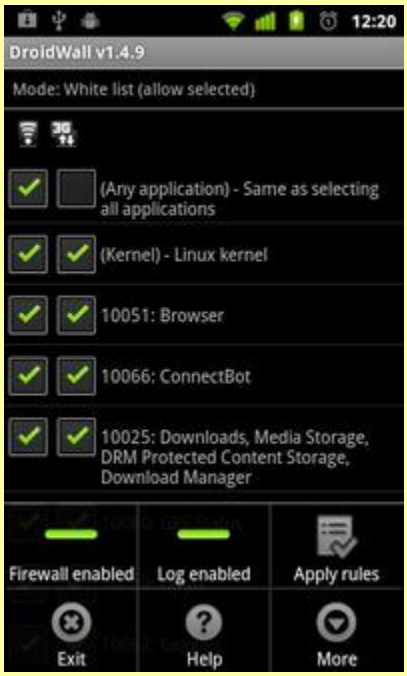
Im April 2011 geisterte es durch die Presse: Der böse Apfel-Konzern sammelt Bewegungsprofile seiner Kunden! Und speichert diese ein ganzes Jahr! Da liegt es natürlich nahe zu schauen, was Android in diesem Zusammenhang treibt.

Und ja, auch hier wird "gesammelt". Das Ganze nennt sich "Cache". Laut Informationen des Entwicklers von Android Location Cache Viewer sind das die letzten 50 Mobilfunk-Zellen sowie die letzten 200 Wifi-Locations. Ein ganzes Stück weniger als Daten eines ganzen Jahres – auch wenn sich damit, zugegebenermaßen, durchaus auch bereits so einiges anfangen ließe.

Doch nun die gute Nachricht: Wie Forums-Mitglied Frank feststellen durfte, bleibt der Cache komplett leer, wenn man das "Datensammeln" in den Netzwerk-Einstellungen einfach abschaltet (Huch? So einfach?). Und aus die Maus. Einziger Haken an der Sache: Der Androide benötigt dann beim ersten Aufruf einer "Location-based App" (Google Maps etc.) ein wenig länger, um die Position festzustellen. Und bei einigen ROMs (bzw. Android ab Version 2.2) schaltet man damit die Positions-Ermittlung über WLAN und Mobilfunknetz gleich ganz ab...

Wer nur mal eben kurz nachschauen wollte, wo er so gewesen ist – für den bietet sich (neben gerade benannter App) Location Cache (Bild rechts) an – sofern der Androiden gerootet ist. Diese App zeigt (bis Android 4.0) die im Cache gespeichert Koordinaten als Liste oder auch auf der Karte an, bietet die Möglichkeit, die Daten im GPX-Format auf die SD-Karte zu exportieren, und kann überdies auch den Cache löschen sowie deaktivieren.

Zugriffe Sperren: Firewalls & Permission-Blocker



So mancher App möchte man kräftig auf die Finger hauen: Was will das Teil ständig im Internet? Dieser Teil der App-Funktionalität lässt sich leider auch nicht separat abschalten. Oder man weiß nicht, wann eine App ins Internet will, und wozu schon gar nicht. Nur die entsprechende Permission hat die App halt (jaja, das haben sie fast alle – in der Regel zum Laden von Werbung). Kurz und gut: Sie soll das nicht! Ist das hinzubekommen?

Na, wenn der Izzy das hier so dumm fragt, hat er bestimmt auch... Richtig. Eine mögliche Antwort ist im Bild zur Linken zu sehen und nennt sich DroidWall. Dabei handelt es sich um ein FrontEnd für iptables, welches im System integriert sein muss. Dies ist bei den vom Hersteller gelieferten Geräten von Haus aus leider nur selten der Fall, sodass die App in der Regel ein Custom ROM voraussetzt. Was root natürlich gleich impliziert...

Sind diese Voraussetzungen jedoch gegeben, hat man mit *DroidWall* ein gutes Werkzeug zur Hand: Entweder, man verbietet einzelnen Apps den Zugriff auf's Internet (erstellt also eine sogenannte "Blacklist" der "schwarzen Schafe") – oder man verbietet den Internet-Zugriff generell für alle Apps außer denen, die auf eine sogenannte "Whitelist" (die Apps mit der "weißen Weste") gesetzt wurden. Noch besser: Dies lässt sich auch getrennt nach "Netzwerk Interface" tun – was sich z. B. anbietet, wenn nur ein begrenztes Datenvolumen im Mobilfunk-Vertrag enthalten ist: So kann man einer App verbieten, die "mobile Datenleitung" zu benutzen – ihr aber gleichzeitig den Internet-Zugriff per WLAN erlauben.

Darüber hinaus lassen sich Zugriffe auch protokollieren. So weiß man anschließend zumindest, was "abging"...

Okay, prima – aber das betrifft ja nur Internet-Zugriffe. Klar, schon eine gute Sache: Eine App, die nicht ins Internet kommt, kann auch nicht meine privaten Daten dorthin übertragen. Aber wie schaut das mit den anderen Dingen aus? Zugriff auf meinen aktuellen Standort, meine SMS, meine Adressdaten?

Das sah lange schlecht aus. Seit einer Weile gibt es jedoch dafür LBE Privacy Guard (siehe rechtes Bild). Der passt im Hintergrund auf – und sobald eine App auf etwas "kritisches" zugreifen will, erhält der Benutzer eine entsprechende Warnung. Nun kann dieser entscheiden: Darf, darf nicht? Nur diesmal – oder ist es eine dauerhafte Entscheidung? Im letzteren Falle setzt man das entsprechende Häkchen, und erhält in der gleichen Situation beim nächsten Mal keine Warnung mehr.

Vorsicht ist jedoch geboten, wenn auf dem Androiden bereits Jelly Bean läuft: Keinesfalls die Version aus dem Playstore installieren, sonst hängt das Gerät anschließend in einem Boot-Loop fest! Eine Alternative wäre der *LBE Security Master*, der im Playstore allerdings lediglich in einer chinesischen Version verfügbar ist. Zum Glück haben sich unsere Freunde bei den *XDA Developers* bereits mächtig ins Zeug gelegt, und bieten lokalisierte Versionen der App zum Download an.

Achja: Versteht sich von selbst, dass eine solche App natürlich root voraussetzt...

ANHANG

Begriffserklärungen

An dieser Stelle möchte ich einige Begriffe kurz erklären, da ich danach desöfteren gefragt wurde. Wie gewohnt, versuche ich mich dabei kurz zu fassen – und verweise für Details auf "externe Quellen".

2G

Gemeint ist damit die Datenübertragung der "zweiten Generation" (die erste ist bereits nicht mehr verfügbar). Hierzu gehören sowohl GPRS als auch EDGE.

3G

Da dies ein Android-Handbuch ist, denken wir jetzt mal nicht an das iPhone 3G. Obwohl der Zusatz auch hier bedeutet: Dritte Generation. Gedacht ist in unserem Fall jedoch an die Datenübertragung mittels UMTS bzw. CDMA.

ADB

Die **A**ndroid **D**ebug **B**ridge ist Bestandteil des Android-SDK. Anders als der Name es nahelegt, ist ADB für mehr als nur das Debuggen gut. so lässt sich hiermit ein Android-Gerät steuern und kontrollieren, Dateien können übertragen, installiert oder auch gelöscht werden, und mehr.

Android

Hierfür zitiere ich einmal kurz das Wesentliche aus dem passenden Wikipedia-Artikel:

> *Android ist ein Betriebssystem wie auch eine Software-Plattform für mobile Geräte wie Smartphones, Mobiltelefone, Netbooks und Tablets, die von der Open Handset Alliance entwickelt wird. Basis ist der Linux-Kernel 2.6. Android ist freie Software und quelloffen.*
> *[...]*
> *Als erstes Gerät mit Android als Betriebssystem kam am 22. Oktober 2008 das HTC Dream unter dem Namen T-Mobile G1 in den Vereinigten Staaten auf den Markt. Dass bereits dieses erste Gerät auf das Global Positioning System zugreifen konnte und mit Bewegungssensoren ausgestattet war, gehörte zum Konzept von Android.*

Also grob zusammengefasst: Speziell für mobile Geräte – Linux unten drunter, "eine Art Java" obendrauf, und ganz zuoberst laufen unsere lieben Apps.

Android Versionen

Der kleine Andy (der grüne ~~Roboter~~ Androide) ist ein Süßer. Entsprechend hat Google auch die Namen der Android-Versionen recht süß gewählt. Kommen also entsprechende Kuchen-Varianten ins Spiel, zielt das i. d. R. auf eine Android-Version:

Version	Name	wichtigste Neuerungen
1.1		(Full Version notes)

Version	Name	wichtigste Neuerungen
1.5	Cupcake	AutoRotate, Bildschirmtastatur, Videos (Full Changelog)
1.6	Donut	VPN, Verbesserungen bei der Energieverbrauchssteuerung, TTS, Gesten (Full Changelog)
2.0	Eclair	Digitalzoom, Blitzlicht, Exchange, Bluetooth 2.1 (Full Changelog)
2.1	Eclair	Webkit-Erweiterungen (HTML5, GeoLocation, u. a.) (Full Changelog)
2.2	Froyo (Frozen Yoghurt)	sparsamerer Kernel, mehr RAM nutzbar, Tethering, App2SD, Bluetooth-Sprachwahl (Full Changelog)
2.3	Gingerbread	DualCore, NFC, SIP (Full Changelog)
3.0	Honeycomb	Optimierungen für Tablets (Full Changelog)
3.1	Honeycomb	USB Host-Modus (Full Changelog)
3.2	Honeycomb	Optimierungen für Tablets (Full Changelog)
4.0	Ice Cream Sandwich	Data-Tracking, Screenshots (Full Changelog)
4.1	Jelly Bean	Offline-Sprachsteuerung, Notification Bar Actions (Ursprung ermitteln, direkter Rückruf...) (Full Changelog)
4.2	Jelly Bean	Daydream (interaktiver Bildschirmschoner mit API), Unterstützung für "Secondary Screens" (gleicher Inhalt auf zwei Bildschirmen), Lockscreen-Widgets, MultiUser, Swype (Full Changelog)

Wen die Unterschiede zwischen den einzelnen Versionen interessieren, der schaue doch einfach mal bei Wikipedia vorbei...

AndroidPIT

AndroidPIT ist eine Community, in der sich Android-Nutzer austauschen. Wo sie aber auch in Blogs, Wiki, Foren und Testberichten fundierte Informationen erhalten. Kurzum: Eine Anlaufstelle für alle Fragen rund um Android. Aber was verbirgt sich hinter diesem seltsamen Namen?

Da steckt der Name "Android" drin, den wir ja gerade geklärt haben. Bleiben die drei Großbuchstaben am Ende: PIT. Was heißen die denn nun? **P**rogramme, **I**nformationen, **T**ests? **P**izza **I**m **T**iefkühlfach? (Unserem Apple-Stevie zufolge müsste das "P" ja sicher für "**P**orno" stehen – doch findet sich eh kein Regisseur, der einen solchen **i**m **T**iefkühlfach dreht). Ich bin sicher, daraus ließe sich eine Preisfrage machen – und der Gewinner bekommt dieses Buch...

Na? Erraten? Ich helfe mal ein wenig nach: Denken wir mal an Autos. Ganz schnelle. F1 (Hilfe? Nee, Formel-1 meine ich). Und genau: "Pit stop", der Boxen-Stopp. Auftanken, und weiter geht's!

Weitere Informationen gibt es u. a. in der FAQ.

API

Kurzform (oft gesprochen, wie man es schreibt – aber auch als Abkürzung buchstabiert) steht für **A**pplication **P**rogrammers **I**nterface. Gemeint ist hier eine definierte Schnittstelle, über die Informationen bezogen werden können.

Die Android-API bietet auf diese Weise z. B. Informationen über Akkustand u. a. m. So muss nicht jeder Programmierer das Rad neu erfinden.

APK-Datei

Die Abkürzung steht für **A**ndroid **P**ac**k**age, und da drin befindet sich in der Regel eine App zur Installation unter Android. Da diese Apps ja in Java geschrieben sind, verwundert es sicher nicht, dass das APK Format eine "Abwandlung" des JAR (**J**ava **AR**chive) ist, und sich somit mittels WinZip & Co. ein Blick in selbige werfen lässt...

Datei-Manager unter Android erkennen diese Packages natürlich, und bieten an, die enthaltene App zu installieren.

APN

Kürzel für **A**ccess **P**oint **N**ame (zu Deutsch: Name des Zugangspunkts). Gemeint ist in der Praxis mitnichten nur der Name, sondern vielmehr der komplette Datensatz. Siehe auch mobiles Datennetz für eine detailliertere Beschreibung, sowie APNs für eine nach Netzanbietern sortierte Liste von APN-Definitionen.

App

Kurzform für *Application*. Wird auch im Deutschen ("Neudeutsch": Applikation) verwendet, da "Anw" einfach blöd klingt. Denn nichts anderes bedeutet das englische Wort *Application*: Anwendung.

Im Zusammenhang mit Smartphones aller "Coleur" (also Früchte wie auch KGMs, kleine grüne Männchen) hat sich die Kurzform "App" eingebürgert – "Application" (oder im Deutschen "Anwendung") wird hier eher selten verwendet.

App2SD

Das hat nix mit dem abendlichen "Jezz abba App ins Bett" zu tun – sondern vielmehr mit der Frage: "Wie kann ich mehr Apps installieren, als in den internen Speicher passen?". Dazu gibt es mehrere Ansätze, die unter dem Begriff "App2SD" zusammengefasst sind:

App2SD: Mit Froyo eingeführt. *App2SD* verschiebt Teile der App auf die (einzige) Partition der SD-Karte, wobei die App dies unterstützen muss. Mit Widgets klappt dies in der Regel nicht – hier kommt es zu Abstürzen, da die SD-Karten-Partition bei Anschluss an den PC via USB auf dem Androiden nicht mehr zur Verfügung steht.

App2SD+: Gibt es mit einigen Custom-ROMs. Hier wird das Widget-Problem dadurch umgangen, dass eine eigene Partition auf der SD-Karte verwendet wird. Android gibt bei USB-Anschluss lediglich die erste Partition frei, die zweite mit den Apps bleibt somit unangetastet. Wie bereits geschrieben: Benötigt root und Custom-ROM, wobei auch nicht jedes Custom-ROM App2SD+ anbietet (Cyanogen zum Beispiel nicht).

Link2SD: Im Prinzip wie App2SD+ – nur bedarf es keines Custom-ROMs: Die App wird dabei zunächst auf die zusätzliche Partition verschoben, und sodann ein sogenannter "symbolischer Link" dorthin im internen Speicher angelegt. Somit wird die App gefunden, als wäre sie im internen Speicher – obwohl sie ganz woanders steckt... Benötigt root und eine zweite Partition auf der SD-Karte.

Baseband

Auch "Radio-ROM" bzw. "Radio-Image" wird es gern genannt. Das ist quasi die eigentliche Geräte-Firmware. Hat weniger direkt mit Android, als vielmehr mit der Hardware zu tun – und initialisiert letztere, so dass sie von ersterem genutzt werden kann. Also sowas ähnliches wie das BIOS beim PC. Und genau wie dieses, befindet es sich i. d. R. auf einem separaten Chip.

Das Teil bootet also die Hardware, und übergibt dann an den eigentlichen Bootloader, der sich dann um Android kümmert. Daher muss das Radio-Image auch zum verwendeten SPL passen. Flasht man das falsche Image, hat man einen Ziegelstein (engl.: "Brick") oder Briefbeschwerer, aber kein brauchbares Telefon mehr...

Bloatware

Vom Hersteller und/oder Provider zusätzlich auf dem Gerät fest vorinstallierte, und oftmals völlig unerwünschte (oder gar unnötige) Apps. Da diese Installation i. d. R. Im ROM erfolgt, kann Otto Normalnutzer diese Apps auch nicht einfach de-installieren (ab Android 4.0 aka Ice Cream Sandwich allerdings zumindest deaktivieren). Das Vorhandensein dieser Apps stellt für sich nicht das große Problem dar – nur lassen diese häufig Hintergrunddienste laufen, die natürlich Systemressourcen verbrauchen.

Bootloader

Sozusagen der "zweite Teil" nach dem Baseband (daher auch "SPL" oder "Secondary Program Loader" genannt). Bleiben wir weiter bei den Hinke-Vergleichen, sind wir hier etwa im "Boot-Manager" (Lilo, Grub) gelandet (davor wäre noch der "MBR" oder "Master Boot Record" auf dem PC – das wäre in diesem Fall der "IPL", der "Initial Program Loader" – der ist bei Androiden in Hardware gegossen, und daher nicht veränderbar).

Aber das wäre jetzt nur sehr grob und ungenau, denn hier steckt mehr drin: Der Android-Bootloader, sowie weitere Boot-Optionen wie das Recovery-Menü, Fastboot, u. a. m.

Branding

Provider-spezifische Anpassungen am ROM. Das kleinste Ärgernis dabei ist evtl. noch die Boot-Animation, die ggf. das Provider-Logo anzeigt. Haarsträubender sind oftmals die zusätzlich installierten Apps (Bloatware), die der Benutzer ohne root-Rechte nicht entfernen kann. Darüber hinaus stellt das Branding gelegentlich wünschenswerte zusätzliche Funktionalitäten bereit – wie etwa das Bezahlen von Apps im Playstore über die Mobilfunkrechnung (Vodafon, T-Mobile).

Brick

In der Regel das Lebensende eines Androiden – der dann nur noch als Briefbeschwerer o. ä. herhalten kann. Wörtlich heißt das zwar "Ziegelstein", aber das würde im Deutschen u. U. zu meilenweisen Verwechslungen mit gewissen Androiden aus dem Hause Motorola führen...

Was sich Google dabei dachte, als es die gleichnamige Permission einführte, sei der Fantasie anheim gestellt...

Wie verwandelt man einen Androiden nun in einen "Brick"? Dazu werde ich keine Schritt-für-Schritt-Anweisung geben (da wenig sinnvoll). Nur soviel sei gesagt: In etwa 95% aller Fälle hängt das mit dem Flashen eines zum

Gerät inkompatiblen RUU zusammen. Vermeiden lässt sich solches also durch gründliches Lesen der Anleitungen und prüfen des "Zubehörs" ***vor*** dem "Brutzeln".

CDMA

CDMA (**C**ode **D**ivision **M**ultiple **A**ccess) ist ein Mobilfunkstandard der dritten Generation (3G), der primär in Amerika und Teilen von Asien und Afrika für den Betrieb von Mobilfunknetzen Anwendung findet. Die maximal möglichen Datenraten reichen hier fast bis an die 5 MBit/s.

CupCake

Eine Tasse Kuchen, klar. Oder doch eher eine Android-Version? Genau, nämlich 1.5.*.

Dalvik

Dafür muss ich ein klein wenig ausholen: Android besteht, vereinfacht gesagt, aus einem Linux-Kernel, auf dem eine spezielle Java-Version läuft. Letzteres ist die sogenannte *Dalvik VM* (wobei "VM" für "Virtual Machine" steht). Android Apps sind also in Java geschrieben.

Für die Ausführung der App wird der Java Code in einen sogenannten "Byte Code" übersetzt, der optimal auf die Hardware (und Android-Version) angepasst ist. Damit dies nicht bei jeder Ausführung der App geschehen muss, passiert diese "Übersetzung" unmittelbar nach der Installation der App – und der Byte-Code wird im sogenannten *Dalvik Cache* abgelegt. Da dies nach der Installation eines "neuen Systems" für alle Apps geschehen muss, dauert auch der erste Start nach der Neuinstallation (bzw. bei Erst-Inbetriebnahme) ein wenig länger (dafür geht die Ausführung der Apps nachher entsprechend schneller).

Bei der Installation eines neuen ROMs muss aus genannten Gründen (optimale Anpassung ans System) der *Dalvik Cache* neu aufgebaut werden. Dafür gibt es im Recovery-Menü einen extra Menüpunkt – aber das ist im entsprechenden Kapitel auch erklärt.

Debuggen

Wörtlich "entkäfern". Ein Computer-antiker Begriff, der noch aus einer Zeit stammt, in der "Programmierung" durch das Ziehen von Drähten, Stecken von Röhren und Löten von Leiterbahnen stattfand. Da war der "Bug" im "Programm" nämlich durchaus wörtlich zu nehmen – wenn ein verbrutzelter Käfer für einen Kurzschluss sorgte...

Die Käfer sind mittlerweile zu groß geworden (oder vielmehr die Chips zu klein), trotzdem haben sich beide Begriffe gehalten: "Bug" für einen Fehler im Programm, und "Debuggen" für die Suche nach und das Entfernen desselben.

Derivat

Eine Abspaltung (auch Fork; englisch fork = Gabel, üblicherweise als Maskulinum verwendet) ist in der Softwareentwicklung ein Entwicklungszweig nach der Aufspaltung eines Projektes in zwei oder mehr Folgeprojekte, wobei Teile des Quelltextes und seiner Historie kopiert werden und dann unabhängig von dem ursprünglichen Projekt weiterentwickelt werden. Mit Bezug auf das Urheberrecht wird auch von einem Derivat (derivativ, lat.: derivare = ableiten) gesprochen. (Wikipedia).

DLNA

Die DLNA (**D**igital **L**iving **N**etwork **A**lliance) *ist eine internationale Vereinigung von Herstellern von Computern, Unterhaltungselektronik und Mobiltelefonen mit dem Ziel, die Interoperabilität von informationstechnischen Geräten unterschiedlicher Hersteller aus dem Bereich Heim- und Eigengebrauch sicherzustellen.* (Wikipedia). Klingt nach viel ("Oh, da kann ich meine Waschmaschine, das Licht, den Rollladen...") – beschränkt sich meist jedoch auf die Steuerung von Bild- und Tonkonserven kompatibler Geräte (auf denen dann auch "DLNA" steht).

Donut

Die Lieblingsspeise eines gewissen Homer Simpson – aber was soll das hier? Na klar, süßes Backwerk, und daher folgerichtig eine Android-Version (1.6).

Downgrade

Kurz und schmerzlos: Das Gegenteil eines Upgrades. Also ein (oder mehrere) Versionsschritt(e) rückwärts.

Warum man so etwas tun sollte/möchte? In der Regel natürlich gar nicht. Aber wenn man nach einem Upgrade wesentlich schlechter dran ist als davor, und auch kein Update zur Abhilfe in Sicht – dann bleibt einem nicht viel anderes übrig.

Ein weiterer Grund ist häufig, dass man sein Gerät rooten möchte, das aber mit der aktuellen Firmware nicht möglich ist...

DroidDream

DroidDream ist ein Trojaner, der eine Sicherheitslücke in Android-Versionen vor Froyo ausnutzt. Er sendet private Daten an einen Server im Netz und installiert eine "Hintertür" im Android-Gerät, durch die Code aus dem Netz nachgeladen werden kann.

Bekannt wurde dies Anfang März 2011: Etwa 50 infizierte Apps wurden im *Google Play Store* aufgespürt und aus diesem entfernt. Dies war auch einer der seltenen Fälle, dass Google von der Möglichkeit Gebrauch machte, diese Schadsoft aus der Ferne von betroffenen Android-Geräten zu löschen.

Weitere Informationen finden sich im Netz – u. a. hier.

DroidSheep

DroidSheep ist eine Android-App zur Sicherheitsanalyse des verbundenen WLAN und zum Abfangen offener Facebook, Twitter und anderer Sitzungen. Wie häufig, lässt sich eine derartige Lösung allerdings auch missbrauchen – wogegen man sich unter Android z. B. mit DroidSheep Guard schützen kann.

Eclair

Klingt nach einem süßen Backwerk – und lässt daher korrekt auf eine Android-Version (2.0.*/2.1.*) schließen.

EDGE

EDGE steht für **E**nhanced **D**ata Rates for **G**SM **E**volution. Als Erweiterung zu GPRS dient es der Datenübertragung, wobei es die maximal mögliche Datenrate auf 384 kbit/s mehr als verdoppelt. Dennoch gehört es noch zur Kategorie 2G. In der Statusleiste von Android-Geräten macht es sich durch ein "E" bemerkbar.

FaceNiff

FaceNiff ist ein Tool ähnlich DroidSheep. Sein Name setzt sich zusammen aus "Facebook" und "Sniff" (schnüffeln) – obwohl sich das "Schnüffeln" dieser Android-App nicht auf Facebook allein beschränkt. Schutz bietet auch hier bereits benannter DroidSheep Guard.

Fastboot

Der Name ist zunächst ein wenig irreführend – handelt es sich dabei doch nicht um die Möglichkeit, das Android-Gerät schneller einsatzbereit zu haben. *Fastboot* hat eigentlich mit dem installierten Android-Betriebssystem nicht einmal direkt etwas zu tun...

Zu finden ist ein Fastboot-Eintrag gelegentlich im Boot-Menü. Und gedacht ist es in erster Linie zum schnellen Bearbeiten von Partitionen via USB. Dazu wählt man am Android-Gerät diesen Punkt aus, und kann dann vom PC aus mit der entsprechenden Software passende Befehle absetzen – etwa um die Daten auf einer Partition zu löschen, mit einer Image-Datei zu überschreiben, oder schlicht das Gerät neu zu starten.

Flaschen

A: Behälter für Bier, Cola, Wein, u. a. m.

B: Taugenichtse, Tagediebe, Apfeldiebe...

C: Gesucht war bestimmt eher der Begriff Flashen, gelle?

Flashen

Foto: Benutzung des Blitzlichts (engl.: flash)

Android: Den Androiden mit einem neuen ROM versehen, indem entweder ein reguläres Update, oder ein Custom-ROM installiert wird. Der Name rührt daher, dass hier die Daten größtenteils im "internen Speicher", dem sogenannten "Flash Speicher", landen.

FOTA

Ein OTA-Update der Firmware. Auf einigen Custom-ROMs läuft auch ein Prozess namens *FOTA kill*, der eben selbiges (insbesondere seine Verfügbarkeits-Meldungen) verhindern soll. Die machen ja da auch keinen Sinn...

Froyo

Eigentlich *Frozen Yoghurt*: Eine Android-Version (2.2.*)

GingerBread

Eine Android-Version (2.3.*)

GingerBreak

In Anlehnung an den Namen GingerBread ist dies zum einen der Name eines Algorithmus als auch einer App zur Erlangung von Root-Rechten unter Android > 2.2.1.

GPRS

GPRS steht für **G**eneral **P**acket **R**adio **S**ervice. Es dient der Datenübertragung, und ist aktuell wohl die langsamste Fassung davon. GPRS gehört in die Kategorie 2G, zusammen mit der Erweiterung EDGE. Die maximal mögliche

Datenrate beträgt bei *GPRS* 171,2 kbit/s. Zeigt die Statusleiste eines Androiden ein "G", muss sich dessen Besitzer hiermit begnügen...

Hardreset
Auch *Rücksetzen auf Werkseinstellungen* genannt: Wiederherstellung des Auslieferungs-Zustandes. Stimmt natürlich nicht so ganz, denn die ursprüngliche Firmware wird dabei nach einem Update nicht wieder hergestellt; es werden lediglich alle Nutzerdaten einschließlich vom Anwender installierter Apps etc. gelöscht.

HBoot
So nennt HTC seinen Bootloader.

HSDPA
HSDPA (**H**igh **S**peed **D**ownlink **P**acket **A**ccess) ist eine Erweiterung des 3G Mobilfunkstandards UMTS, der Datenraten von bis zu 14 MBit/s ermöglicht. Wird manchmal auch gern als "3,5G" oder "3G+" bezeichnet, und macht sich in der Statusleiste eines Androiden durch ein "H" bemerkbar.

HTTPS
Dieses Kürzel steht für **H**yper**T**ext **T**ransport **P**rotocol **S**ecure, was sich auf Deutsch am besten mit "sicheres Hypertext-Übertragungsprotokoll" wiedergeben lässt. Sämtliche Daten werden hierbei verschlüsselt über das Netzwerk übertragen. Nähere Details finden sich u. a. bei Wikipedia.

Ice Cream Sandwich
Hmmm, wieder etwas Süßes? Richtig: Eine Android-Version, nämlich 4.0

Image
Die Fotos, die mit der Kamera des Androiden gemacht wurden, sind damit *nicht* gemeint. Die nennt man nämlich *Pictures*.

Ein **Image** nennt man das Speicher-Abbild einer Partition (für Windows-User: Das, was sich hinter einem Laufwerks-Buchstaben verbirgt; eine Partition kann schließlich wie ein eigenständiges Laufwerk behandelt werden). Im Zusammenhang mit Android werden Images häufig in folgenden Kontexten genannt:

- **Nandroid-Backup:** Erstellt Images von allen Partitionen
- **Update.zip:** Enthält nicht selten ein (oder mehrere) Image(s)
- **Custom-ROMs** kommen auch oft als Images daher
- **Fastboot** kann zum Flashen verschiedener Images verwendet werden

IMEI
Die International Mobile Station Equipment Identity (IMEI) ist eine eindeutige 15-stellige Seriennummer, anhand derer jedes GSM- oder UMTS-Endgerät eindeutig identifiziert werden kann. (Wikipedia). Diese Nummer ist also Geräte-spezifisch, und wird von diversen Werbe-Modulen gern zur Identifizierung herangezogen. Mit ihr lässt sich aber auch ein Gerät beim Netzanbieter sperren, sodass ein Dieb es nicht mehr verwenden kann (zumindest nicht im gesperrten Netz – dies weltweit durchzusetzen, dürfte ein wenig aufwendig sein). Genauere Details finden sich u. a. bei den XDA-Developers.

IMSI

Abkürzung für *International Mobile Subscriber Identity*. Diese aus 15 Ziffern bestehende interne Teilnehmerkennung dient in GSM- und UMTS-Mobilfunknetzen der eindeutigen Identifizierung von Netzteilnehmern, und wird auf der SIM-Karte gespeichert.

Jelly Bean

Code-Name der Android-Versionen 4.1 & 4.2

Kernel

Da steckt das Wort "Kern" drin, genau. Wenn wir hier vom "Kernel" sprechen, meinen wir den "Betriebssystem-Kern", den "Linux-Kernel". Das ist, vereinfacht ausgedrückt, eine Abstraktions-Schicht: Unten speziell an die jeweilige Hardware angepasst, stellt der *Kernel* "oben" eine einheitliche Schnittstelle (API) für die Software zur Verfügung.

Bei Android läuft auf dem *Linux-Kernel* die Dalvik-VM (eigentlich je eine pro App), und in der *Dalvik-VM* sodann die App.

Launcher

Der *Launcher* ist sozusagen die "Grafische Benutzeroberfläche" (GUI) von Android – das, was nach dem Entsperren des Bildschirms angezeigt wird. Anders als bei Windows (und eher ähnlich wie bei Linux) gibt es bei Android nicht *den* Launcher, sondern eine ganze Reihe von Alternativen: Angefangen von "besonders Ressourcen-schonend" bis hin zu "mit allen (un)möglichen Features". Mehr Details dazu finden sich im Kapitel zum Home-Screen.

Nandroid Backup

Ein vollständiges System-Backup, welches sich z. B. aus dem Custom-Recovery-Menü heraus erstellen und auch wieder herstellen lässt. Hier werden nicht einzelne Dateien gesichert, sondern ein Abbild ("Image") des gesamten Systems wird angelegt. Es ist also ein "Alles-oder-Nichts": Die Wiederherstellung einzelner Dateien ist hier nicht vorgesehen (und auch nicht ohne weiteres möglich).

Insbesondere bevor man ein Custom-ROM einspielt, aber auch generell vor einem System-Update sollte ein Nandroid-Backup angelegt werden. Es ist natürlich auch sonst immer eine gute Idee, ein komplettes Backup zur Hand zu haben.

NFC

Nein, nicht **N**ashville **F**ried **C**hicken, sondern **N**ear **F**ield **C**ommunication. Dient zum Ultra-Kurzstrecken-Datenaustausch (Reichweite also noch kleiner als bei Bluetooth), und soll u. a. zum "Bezahlen mit dem Handy" genutzt werden. Aber auch Dinge wie "Handy als Autoschlüssel" oder "Handy als Fahrkarte" etc. sind denkbar (und schon gedacht worden).

OTA

Da liegt was in der Luft... Denn OTA steht für "**O**ver **T**he **A**ir". Ja was denn? Beim Rundfunk ist es "On The Air" und heißt Musik. Bei Phil Collins "In The Air Tonight". Und bei Android ein "(komplettes) Over The Air Update" – also ein Kotau, sozusagen. Die Frage wäre da nur, wer dabei der Kaiser ist...

Also, kurz gefasst: Beim *OTA* werden Software-Updates des Herstellers/ Providers über das Funknetz des letzteren verteilt.

Partition

Eine Partition ist ein zusammenhängender Bereich auf einem Datenträger (unter Windows häufig mit einem Laufwerksbuchstaben verbunden).

Auf einem Android-System sind immer mehrere Partitionen in Benutzung, auch wenn nur der interne Speicher zur Verfügung steht (und keine SD-Karte eingelegt ist): So ist das "`/system`" in der Regel nur lesend eingebunden (um Änderungen im Betrieb zu verhindern), während für Apps und Daten eine eigene Partition ("/data") bereitsteht.

Die SD-Karte beinhaltet meist nur eine (in der Regel unter "/sdcard" eingebundene) Partition. Es sind aber auch hier mehrere Partitionen möglich (und werden z. B. mit App2SD+/Link2SD verwendet) – wobei Android bei Anschluss an den PC via USB nur jeweils die erste Partition davon freigibt.

Weitere Details können z. B. bei Wikipedia nachgelesen werden.

Provider

In der Regel ist damit der "Netzanbieter" gemeint (also E-Plus, T-Mobile, A1 & Co).

Zum anderen könnte aber auch ein Dienst des Android-Systems gemeint sein: So stellt etwa der *Location Provider* über eine API den Apps die aktuelle Position bereit...

RAM

Diese drei Buchstaben stehen für **R**andom **A**ccess **M**emory – also Speicher, auf den man nach belieben an beliebiger Stelle zugreifen kann. Im Gegensatz nicht etwa zu ROM, sondern zu Dingern wie Bandlaufwerken (jaja, so alt ist der Begriff schon), bei denen man sich erst mühsam vom Start zur gewünschen Position (linear) vortasten muss.

Sowohl auf PCs wie auch auf unseren Androiden ist damit meist der Arbeitsspeicher gemeint, in den die Programme/Apps zur Ausführung geladen werden. Üblicherweise ist dies der Bereich, der generell zu klein ist... oder von dem man halt nie genug haben kann...

Recovery Menü

Ein separater Bereich des Boot-Menüs (siehe Bootloader), aus dem heraus verschiedene Operationen wie Nandroid-Backup oder auch das Bereinigen des Dalvik-Caches möglich sind.

In das *Recovery Menü* gelangt man in der Regel durch eine spezielle Tasten-Kombination beim Einschalten. Diese ist aber zumindest von Hersteller zu Hersteller unterschiedlich. Bei HTC ist es üblicherweise das Halten der "Leiser-Taste" während des Einschaltens. Bei Motorolas Milestone muss die Kamera-Taste beim Einschalten gedrückt gehalten, und anschließend die "Lauter-Taste" betätigt werden. Und so weiter. Bei Bedarf also am besten im Forum erlesen/erfragen.

Einfacher geht es mit dem bereits im Kapitel Custom-ROM genannten *ROM Manager*: Diese App erlaubt auch einen direkten Boot ins Recovery-Menü. Ebenso integrieren einige Custom-ROMs einen entsprechenden Punkt in dem Menü, welches sich bei langem Drücken der Power-Taste öffnet.

Repository

Ein Repository (engl. für Lager, Depot, Quellen oder Archiv), auch Repositorium, ist ein verwaltetes Verzeichnis zur Speicherung und Beschreibung von digitalen Objekten. Bei den verwalteten Objekten kann es sich beispielsweise um Programme (Software-Repository), Publikationen (Dokumentenserver), Datenmodelle (Metadaten-Repository) oder betriebswirtschaftliche Verfahren handeln. Häufig beinhaltet ein Repository auch Funktionen zur Versionsverwaltung der verwalteten Objekte. (Wikipedia)

Reset

Je nachdem: Siehe Softreset, Hardreset, sowie Wipe.

ROM

Richtig **o**ffensichtlicher **M**ist ist diese **r**eal **o**fferierte **M**ehrdeutigkeit: Manchmal hat man den Eindruck, er wurde nur zur Verwirrung der Massen eingeführt. Wer einmal den Namen für eine Android-Komponente nicht kennt, sagt einfach "ROM". Klingt, als wüsste man voll Bescheid – und die Chance, dass das auch noch Sinn ergibt, ist verdammt hoch...

Aber im Ernst: Worum geht es hier? Eigentlich steht der Begriff "ROM" für **R**ead **O**nly **M**emory – also Speicher, auf den ausschließlich lesend zugegriffen werden kann. Ja, richtig: So wie bei CD-ROM, da steckt das ja auch drin. Nur bei Android, da kann das alles mögliche sein. Nicht selten sachlich falsch – aber wen kümmert's? Schauen wir uns also die einzelnen Bedeutungen einmal an:

Systemspeicher: Teile des Android-Systems werden in der Tat "nur lesend" eingebunden. Unter anderem eine Schutzmaßnahme, um Veränderungen zu erschweren (damit wir die dusseligen Apps, mit denen uns die Hersteller/ Provider "beglücken", nicht einfach löschen können). So heißt es z. B. in den Spezifikationen des HTC Wildfire: "384 MB RAM; 512 MB ROM". Nonsens(e): Ein Blick hinter die Kulissen offenbart, dass nur 250MB read-only (/system) eingebunden sind. Die restlichen 250MB "ROM" stehen zur Installation von Anwendungen zur Verfügung. Read-only? Mitnichten. De facto kann der ganze Bereich jederzeit schreibbar gemacht werden, sofern man root hat. Also eher irreführend – richtiger müsste es hier heißen: "interner Speicher", oder – in Abgrenzung vom RAM – "interner Flash-Speicher".

Das System selbst: Um die Verwirrung komplett zu machen, wird auch hier gern von "ROMs" gesprochen (siehe Custom ROMs). Das hat schon Tradition: Auch bei älteren Spiele-Konsolen sprach man davon, "ein ROM zu laden". Dabei handelte es sich aber "seinerzeit" tatsächlich um eine Cartridge – also einen Speicher-Chip, den man an das Gerät ansteckte. Später kamen dann die Emulatoren, welche die "antiken Geräte" auf moderner Hardware emulieren können. Und bei diesen kommt die "Cartridge" natürlich in Form einer Datei daher. Den Begriff "ein ROM laden" hat man beibehalten. Und schließlich weiter übertragen...

ROM Kitchen

ROM-Knast? Nein, gemeint ist der englische Begriff "Küche" (also wenn man schon "Knast" hat). In einem *ROM Kitchen* kann der Anwender sich sein eigenes ROM kochen. Natürlich setzt dies root voraus (sonst kann

man das fertige "Gericht" nicht servieren/installieren), und ist etwas Geräte-spezifisches.

Neben "vollständigen ROM-Küchen" gibt es auch noch welche, die sich auf Elemente der Gestaltung beschränken, wie z. B. das UOT (Ultimate Online Kitchen, Beschreibung und Video findet sich bei den XDA-Developers). Hier tauscht man lediglich einzelne Elemente (Batterie-Anzeige in der Statusbar, Icons, etc.) eines bereits installierten ROMs aus. Natürlich braucht auch dieses root, da sonst kein Austausch von Systemdateien möglich ist.

root

Aus Herstellersicht: Die Wurzel allen Übels. Objektiv betrachtet: Der Administrator (auch "SuperUser") eines Linux-Systems. Der darf alles, und kann alles (kaputtmachen auch, ja). Näheres ist im Kapitel root ausführlicher beschrieben.

RUU

Radio **U**nit **U**pdate: Eine Art update.zip für das Radio-Image, also ein "Firmware-Upgrade".

ROM **U**pgrade **U**tility: Wie der Name bereits sagt, ein Utility zum Upgrade des ROM, welches entweder vom Hersteller oder von Drittanbietern zur Verfügung gestellt und vom PC aus installiert wird.

Wenn nicht ganz klar ist, was von beidem gemeint ist, ist es in der Regel das erste – wobei das durchaus mit dem zweiten identisch sein kann, da die Begriffe oftmals gleichbedeutend verwendet werden. Was mancherorts als "ROM Upgrade Utility" bezeichnet wird, ist nämlich nichts anderes als das Update des Radio-Images...

Safe Mode

Vielen aus der Windows-Welt als "Abgesicherter Modus" bekannt. Bootet man in diesen, werden beim Systemstart alle Anwender-Apps ignoriert. Dies ist beispielsweise hilfreich, wenn das Gerät bei einem normalen Start in einer Force-Close-Schleife festhängt.

SDK

Das SDK (**S**oftware **D**evelopment **K**it) ist die Grundlage für die Android App Entwicklung und liegt für die jeweilige Version von Android vor. Es ist aber nicht nur dafür verwendbar, sondern bringt auch einige brauchbare Tools wie Fastboot, den Dalvik Debug Monitor sowie ADB mit.

Ergänzt man das Ganze noch um Eclipse, kann es mit der Entwicklung von Apps losgehen!

SIP

Das Kürzel SIP steht für Session Initiation Protocol. In unserem Zusammenhang kann es quasi als Alias für "Internet-Telefonie" bzw. "IP-Telefonie" betrachtet werden, da es bei dieser zum Einsatz kommt.

S-OFF

Mit S-OFF (kurz für Security off) ist der volle Zugriff (lesen und schreiben) auf die System-Partition während des Betriebs des Android-Gerätes gemeint. Üblich ist dieses "secu_flag" nur bei HTC, somit kann man es bei nicht-HTC-Geräten ignorieren.

Softreset
Ein "weiches" herunterfahren des Systems, wenn nichts mehr geht – vergleichbar mit Strg-Alt-Entf am PC. Siehe Weiches Zurücksetzen für Details.

Tethering
Die Leinen los! Ja, so kam es einigen vor, als das mit *Froyo* zur Standard-Funktionalität wurde: Mittels Tethering lässt sich die mobile Internet-Verbindung mit anderen Geräten teilen.

UMTS
UMTS (**U**niversal **M**obile **T**elecommunications **S**ystem) ist ein Mobilfunkstandard der dritten Generation, und wird deshalb umgangssprachlich auch einfach als 3G genannt. Seine maximale Datenrate liegt – wie übrigens auch die der 2G-Erweiterung EDGE – bei 384kBit/s. Schneller wird es mit der Erweiterung HSDPA.

Unroot
Rückgängigmachen des sogenannten "rootens" (siehe root), also das System wieder vom root-Zugang befreien (und in den Hersteller-konformen Zustand zurücküberführen). Dies geschieht in der Regel durch das Flashen eines RUU (sauberste Variante) – wobei mittlerweile auch etliche rooting-Tools eine entsprechende "Undo-Funktion" anbieten.

Update
Das Ersetzen etwas Bestehenden durch etwas Neueres. Meist handelt es sich hier um eine Fehlerbereinigung von System oder Apps, aber auch neue/ zusätzliche Features können damit einhergehen.

Update.Zip
Ganz offensichtlich eine Datei. Und ebenso offensichtlich will diese etwas aktualisieren – nur was?

Es handelt sich hier um ein "flashbares Update". Offizielle Firmware-Updates kommen meist unter diesem Namen daher. Und da das System eine solche Datei, so sie im Wurzel-Verzeichnis der SD-Karte liegt, als ein solches betrachtet, lässt sich auf diese Weise auch so einiges anderes ins System mogeln. Das nutzt z. B. Titanium Backup aus, wenn es ein update.zip erstellt.

Einspielen lässt es sich zum Beispiel über das Bootmenü.

Upgrade
Ist mit einem Update ein Versionssprung verbunden (etwa von Eclair auf Froyo, oder von Froyo auf Gingerbread, oder gleich von Eclair auf Gingerbread), spricht man von einem Upgrade.

VoIP
Abkürzung für **V**oice **o**ver **IP**, oder auch "Internet-Telefonie". Aber so wie man heute simst (SMS schickt), googelt (mit Google sucht), und skypet (mit Skype chattet oder telefoniert), so voipt man auch.

VPN
Steht für Virtual Private Network – zu Deutsch: Virtuelles Privates Netzwerk. Hier wird von Client eine verschlüsselte Verbindung zu einem VPN-Server aufgebaut, der ersteren sodann in sein eigenes Netz integriert. Aller Datenverkehr lässt sich dann über diese verschlüsselte Strecke leiten –

sodass die übertragenen Daten vor Schnüfflern (etwa in offenen WLANs) relativ sicher sind.

Wipe

Wörtlich übersetzt: Löschen. Das "was" ist hier allerdings die Frage. Und da kommt es darauf an, wen man fragt bzw. wie man den Wipe initialisiert.

Hardreset: Eine Form des Wipe ist mit diesem gleichbedeutend, denn sie löscht lediglich die "/data" Partition. Das ist der Bereich, in dem die selbst installierten Apps sowie die Daten abgelegt werden.

Dalvik-Cache: Mit dem Wipe/Löschen des Dalvik-Caches erzwingt man eine Neu-Übersetzung des Programmcodes aller Apps. Damit geht kein Datenverlust einher: Lediglich der nächste Gerätestart dauert etwas länger.

Komplett-Wipe: Den gibt es in verschiedenen Versionen des Recovery-Menüs. Sollte nur ausgeführt werden, wenn man auch wirklich weiß, was man da tut: Der löscht nämlich alle Daten von allen Partitionen, auch von "/system". Danach geht dann nichts mehr – es lässt sich lediglich ein neues ROM einspielen.

Fragen aus Alltag und Praxis

Google Account

Wozu brauche ich einen Google-Account?

Klar kann man seinen Androiden auch ohne Google-Account benutzen. Bei vielen Tablets hat man zunächst nicht einmal eine andere Wahl. Doch manche Dinge funktionieren einfach nicht ohne. Zum Beispiel der *Google Play Store*, über den die meisten Apps kommen. Auch die Synchronisation von Kontakten und Terminen ist an einen Google-Account gebunden – zumindest, wenn man die Bordmittel benutzen möchte.

Kann ich einen Account mit mehreren Geräten nutzen?

Das ist problemlos möglich. Und das Schöne dabei: Auch die mit dem Account gekauften Apps lassen sich auf all diesen Geräten parallel nutzen, denn der Kauf ist ja an den Account gebunden.

Darüber hinaus zeigt der neue Web-Markt bei jeder App an, mit welchem Gerät selbige kompatibel ist – und gibt dem Anwender dann die Möglichkeit, sie dort zu installieren. Auch Kalender und Kontakte lassen sich auf allen mit diesem Account verknüpften Geräten synchronisieren (so man diese Funktion aktiviert hat). Kurzum: Die Sache scheint geradezu dafür ausgelegt.

Aufpassen sollte man allerdings mit Datensicherungen (auch diese lassen sich ja auf den Google-Servern speichern) – hier bin ich nicht sicher, wie diese auseinandergehalten werden.

Wie kann ich meinen Google-Account ändern?

Offensichtlich soll der Anwender dies nicht tun – denn die entsprechende Stelle in der Konfiguration lässt es nicht zu. Natürlich klappt das nach einer "Werksrückstellung", da dann ohnehin alles neu eingerichtet werden muss. Das ist aber nicht immer gewünscht: Auch alle Apps müssen dann nämlich neu installiert und konfiguriert werden.

Mit einem kleinen Trick geht es aber auch ohne "Werksrückstellung": Vom Home-Screen aus geht man dazu in die Maske *Einstellungen→Anwendungen→Anwendungen verwalten*, und wählt nacheinander folgende Anwendungen an, um deren Daten und Caches zu löschen: GMail, Google Apps, GTalk (Google Talk), GTalk Services, IM und evtl. noch Google+ und Google Storage (auch "Speicherplatz bei Google Mail" genannt; was nicht da ist, überspringt man halt). Jetzt hat der Androide seine "Kontoverbindung" vergessen, und man kann diese wieder neu einrichten – mit den gewünschten "anderen Daten", oder indem man einen neuen Account erstellt.

Kann ich die Youtube App mit einem alternativen Account verwenden?

Wer über mehrere Accounts verfügt (z. B. einen für GMail und Android, sowie einen anderen für Youtube), und diese gern getrennt halten möchte, kann dies auf recht einfache Weise tun:

1. Youtube-App starten
2. Aus dem Menü "Abmelden" ("Sign out") wählen
3. Aus dem Menü "Anmelden" ("Sign in") wählen
4. Es sollte an dieser Stelle eine Box zur Account-Auswahl erscheinen. Sofern der gewünschte Account aufgeführt ist, kann er nun gewählt werden. Alternativ lässt sich von hier aus auch ein neuer Account anlegen.

Google Play Store

Ich finde den *Play Store* auf meinem Gerät nicht!

Dies ist oftmals insbesondere bei Tablets "normal": Ein Android-Gerät muss bestimmte Voraussetzungen erfüllen, damit es mit den Google-Apps ausgeliefert werden darf (z. B. muss es über eine Kamera und ein GPS-Modul verfügen). Das heißt jetzt aber nicht, dass "Hopfen und Malz verloren" sind: Eine Suche in den einschlägigen Foren (z. B. im für das fragliche Gerät zuständige Hardware-spezifische Unterforum bei AndroidPIT), oder auch bei Google mit den Begriffen *"Google Apps" <Gerätename>*, führen nicht selten zu einer Lösung. Diese heißt dann in der Regel: Die gapps.apk händisch herunterladen, und auf dem Gerät installieren. Was jedoch (zumindest für die Playstore-App) wiederum root voraussetzt.

Warum finde ich die App im *Play Store* nicht?

Hier ist die Antwort ähnlich zur vorigen – nur dass es diesmal einen direkten Bezug zur App hat. Entweder hat der Entwickler etwas vergessen anzugeben (das ist nicht gerade selten), oder aber das fragliche Android-Gerät wird tatsächlich nicht unterstützt: Zu kleines Display (auf einem Motorola Flipout HD-Videos abspielen? Macht bestimmt Spaß), zu schwacher Prozessor (CPU-intensive Spiele wie *Asphalt* überfordern so manches kleine Gerät), oder die installierte Android-Version ist zu niedrig. Eine Anfrage beim Entwickler schafft häufig Abhilfe, sofern letztere möglich ist.

Hilfe, der *Play Store* spinnt!

Sowas tut der in der Tat: Downloads starten nicht oder werden nicht abgeschlossen, Installationen schlagen fehl, oder die Server des *Play Store* werden erst gar nicht erreicht (Anmelde-Probleme). In der Regel liegt das in der Tat am *Play Store* bzw. den Google Servern, daher lohnt sich in solchen Fällen ein Blick auf deren Monitor, das so genannte "Dashboard". Steht dort alles auf „grün“, zur Sicherheit noch im Forum vorbeigeschaut (bei AndroidPIT gibt es da auch eine

Sektion für Play Store-Fragen), ob gerade wieder eine Epidemie ausgebrochen ist (und auch andere betroffen sind).

Ist auch das nicht der Fall, ist ein lokales Problem naheliegend. Jetzt gibt es mehrere Möglichkeiten, die einfach in dieser Reihenfolge abgearbeitet werden können. Nach jedem Schritt ist natürlich zu Prüfen, ob das Problem damit schon beseitigt ist – dann kann man sich die folgenden Schritte nämlich sparen:

- In der *Play Store* App auf die "Downloads" Seite gehen, lange (mindestens ein bis zwei Sekunden) auf die Fortschrittsanzeige "drücken", und aus dem sich nach dem Loslassen öffnenden Menü "Download abbrechen" auswählen. Dann erneut versuchen, die App zu installieren.
- Ein Geräteneustart (Herunterfahren, Ausschalten, evtl. zur Sicherheit noch den Akku rausnehmen, kurz warten, ggf. Akku wieder rein, neu Starten.
- Datum, Uhrzeit und Zeitzone manuell einstellen (kann später wieder auf Automatik zurückgestellt werden)
- Google Talk starten, sich dort abmelden, es wieder starten (und dann beenden)
- Unter *Einstellungen→Anwendungen→Anwendungen verwalten* der *Play Store App* den Cache leeren
- An gleicher Stelle: "Stoppen erzwingen", dann "Daten löschen" (damit sind aber auch die Einstellungen für Auto-Updates zurückgesetzt).
- Letzter Ausweg: Zurücksetzen auf Werkseinstellungen

Unbekannter Fehler: -18

Dieser Fehler tritt nur im Zusammenhang mit App2SD auf, wenn eine zu aktualisierende App auf der SD-Karte installiert ist (oder eine neue dort installiert werden soll). Die einfachste Lösung ist hier: App wieder in den internen Speicher zurück verschieben, das Update erneut versuchen (sollte jetzt funktionieren), und anschließend optional wieder auf die SD-Karte damit.

Schlägt das Update noch immer fehl, oder handelt es sich um eine neu zu installierende App, kann auch folgendes helfen: Androiden per USB-Kabel an den PC anschließen, und die Karte im Modus "USB Massenspeicher" (nicht MTP/PTP) als Laufwerk freigeben. Damit steht sie dem Android-System nicht mehr zur Verfügung, was eine Installation in den internen Speicher erzwingt.

Eine letzte Möglichkeit ist mit Vorsicht zu genießen: Mit einem Datei-Manager auf der SD-Karte den Ordner `.android_secure` (mit Punkt vorne!) suchen, und die darin befindliche Datei namens `smdl2tmp1.asec` löschen, dann die Installation bzw. das Update noch einmal versuchen.

Wie kann ich de-installierte Apps aus der Übersicht *Andere Apps in meiner Bibliothek* entfernen?

Google merkt sich alles. Das gilt insbesondere auch für die Apps: Alles, was man je installiert hatte, findet sich auf der Playstore-Seite unter *Meine Android Apps* wieder. Auch, wenn man es schon lange wieder von allen seinen Geräten entfernt

hat – unter *Andere Apps in meiner Bibliothek* bleibt es stehen. Zumindest auf der Webseite ist auch nicht ersichtlich, wie man da einmal aufräumen kann.

Die Apps sind in diesem Segment auf maximal 20 Seiten zu je 9 Einträgen eingeteilt. Wer nun häufiger neue Apps testet, hat die Begrenzung von 180 Einträgen recht schnell überschritten. Was im Alphabet weiter hinten steht, lässt sich dann nicht mehr anzeigen. Dumm nur, wenn man eine (zeitweilig) deinstallierte App zu einem späteren Zeitpunkt doch wieder installieren möchte, sich aber nicht mehr an den Namen erinnert!

Hilfe findet sich hierzu in der Playstore App. Zumindest ab Version 3.10.* lässt sich mit selbiger an dieser Stelle Ordnung schaffen. Dazu sucht man zunächst die Seite mit den eigenen Apps auf (entweder über *Menü → Meine Apps*, oder über das Download-Symbol in der Titelseite). Hier wählt man den Tab "Alle". Neben nicht-installierten Apps taucht in der Liste nun ein Symbol mit einem durchgestrichenen Kreis ("Parkverbot") auf. Tippt man dieses an, erfolgt eine Abfrage: "<AppName> aus meine Apps entfernen?" Einfach auf "Ja" tippen, und sie ist verschwunden – auch von der zugehörigen Playstore-Webseite.

Dummerweise springt die Liste anschließend automatisch wieder ganz an den Anfang zurück. Wer also richtig aufräumen (und mehrere Apps von der Liste entfernen) möchte, greift zu einem kleinen Trick: Die erste zu entfernende App einfach etwas länger drücken. Nun ist sie markiert. Am oberen Seitenrand sollte ein Balken auftauchen, der Links mit "1 App markiert", und rechts mit "Entfernen" beschriftet ist. Jetzt einfach die übrigen zu entfernenden Apps markieren, und dann alles in einem Rutsch aufräumen lassen – fertig.

Kann ich auf einem Gerät mehrere Google-Accounts für den Playstore verwenden?

Sinnvoll wäre dies für verschiedene Szenarien: Geschäftliches von Privatem trennen, oder der Wechsel zu einer neuen GMail-Adresse ohne Verlust der gekauften Apps wären nur zwei davon. Und glücklicherweise ist dies mittlerweile auch recht einfach möglich.

Einen neuen Account kann man beispielsweise unter *Einstellungen → Konten & Synchronisation* erstellen, auch wenn dort bereits ein Google-Account besteht. Eine weitere Möglichkeit ist, dies gleich direkt in der Playstore-App zu erledigen: Unter *Menü → Konten* findet sich dafür der Punkt „Konto hinzufügen". Beides führt zum Einrichtungs-Wizard, in dem sich entweder ein bereits bestehendes Konto eintragen, oder ein neues anlegen lässt.

An besagter Stelle in der Playstore-App lässt sich dann auch das für die jeweilige Einkaufstour zu verwendende Konto auswählen.

Wie kann ich im Playstore das Land wechseln?

Nein, es geht nicht um das Aushebeln regionaler Beschränkungen, sondern vielmehr um einen Umzug: Da gibt es Apps, die beispielsweise in Österreich verfügbar sind, in Deutschland jedoch nicht. Hat nun jemand seinen Wohnort von Deutschland nach Österreich verlegt, ist der Wunsch der entsprechenden Umstellung im Google Playstore also völlig legitim. Nur wie wird er bewerkstelligt?

Zuerst müssen die in Google Wallet hinterlegten Adressdaten aktualisiert werden. Dazu gehört auch die mit dem Google-Konto verknüpfte Kreditkarte, die in unserem Beispiel nun aus Österreich stammen sollte.

Soweit scheint alles nachvollziehbar – dennoch werden besagte österreichische Apps ggf. noch immer als "in Ihrem Land nicht verfügbar" angezeigt: Google Play hat vom Adresswechsel offensichtlich noch nichts mitbekommen. Was hier hilft, ist der Kauf einer beliebigen App (wenn man sie nicht braucht, kann man sie ja binnen 15 Minuten wieder retournieren). Durch den Kauf muss Google Play seine Daten mit Google Wallet abgleichen, und weiß nun Bescheid: Jetzt sind besagte österreichische Apps verfügbar, der "Länderwechsel" ist erfolgreich vollzogen.

Backup

Welche Arten von Backups gibt es eigentlich, und was wird da jeweils gesichert?

Auf dieses Thema geht ein Artikel bei den XDA-Developers ein, der auch Links zu weiterführenden Informationen beinhaltet. Das Wesentlichste sei hier kurz zusammengefasst:

Backup-Typ	Was wohin gesichert wird
Google Sync (aka "Google Cloud Backup")	Kontakte, Kalender, Docs / Drive, Gmail, Google Photos, Google Reader, "Internet & Instant" (Lesezeichen u. a.), WLAN Passwörter, und mehr werden in der Google Cloud abgelegt. Es soll auch die Daten der installierten Apps in der Cloud speichern und zwischen Geräten synchronisieren – in der Praxis hat es sich aber als extrem unzuverlässig erwiesen.
Dropbox & Co.	Vom Anwender speziell vorgegebene Dateien und Verzeichnisse. Der Umfang variiert je nach Cloud-Service. Etliche Apps verfügen zudem über Dropbox-Support. So können z. B. auch mit *Titanium Backup* erstellte Datensicherungen hier abgelegt werden.
Titanium Backup	Apps und ihre Daten, sowie Systemeinstellungen und mehr werden auf die SD-Karte gesichert. Ebenfalls möglich ist die Speicherung in der Cloud – so wird z. B. Dropbox direkt unterstützt. Benötigt root-Rechte.
ADB Backup	Apps und ihre Daten werden auf das System gesichert, welches den Backup-Prozess ausgelöst hat (i. d. R. ist dies der PC, an den das Android-Gerät per USB-Kabel angeschlossen wurde – es gibt aber auch Implementierungen dieses Backup-Typs direkt in einer App, z. B. *Helium*, ehemals als *Carbon Backup* bekannt). Erst ab Android 4.0 verfügbar.
Samsung Kies (und andere herstellerspezifischen PC-Suites)	Nur für die Geräte des jeweiligen Herstellers verfügbar, und sowohl im Umfang als auch in Sachen Zuverlässigkeit durchaus verschieden.
Nandroid Backup	Erstellt 1:1 Sicherungen der meisten (und aus Anwendersicht wichtigsten) Partitionen des Android-

Backup-Typ	Was wohin gesichert wird
	Gerätes in so genannten "Image Dateien". Auf diese lässt sich u. a. auch mit *Titanium Backup* zugreifen. Benötigt root und ein Custom Recovery.
Diverse datenspezifische Backups	Je nach Backup-App werden hier SMS, MMS, Anruflisten, Lesezeichen, Kontakte, Termine, oder andere Daten (ggf. auch Kombinationen der genannten Auswahl) auf die SD-Karte oder in die Cloud gesichert.

Wie kann ich vom Android-Gerät auf ein Nandroid-Backup zugreifen?

Am einfachsten kann dies geschehen, wenn man dafür ein kleines Helferlein aus dem Google Play Store verwendet. Dort finden sich mindestens zwei Apps, die bei dieser Aufgabe dienlich sein sollen:

Nandroid Browser versteht sich sowohl auf das bei älteren Geräten häufig zum Einsatz kommende YAFFS2 Format, als auch auf das aktuellere EXT4. Mit der App lässt sich in Nandroid-Backups stöbern, einzelne Dateien können extrahiert, geöffnet, und auch über das Share-Menü geteilt werden.

Mit Nandroid Manager ist ähnliches möglich. Zusätzlich lassen sich damit auch einzelne Komponenten wie WLAN APNs, Kurznachrichten, Anrufprotokolle, oder Apps einschließlich ihrer Daten wieder herstellen – was übrigens auch von *Titanium Backup* unterstützt wird.

Kann ich Backups auf einem anderen Gerät wieder herstellen?

Das hängt u. a. von der Art des Backups ab. Mit einem Nandroid Backup sollte man dies besser nicht versuchen (es sei denn, es handelt sich um identische Geräte). Bei "datenspezifischen Backups" (wie sie von verschiedenen Apps im Playstore angeboten werden) sollte es hingegen keinerlei Probleme geben. Geht es um das "Google Cloud Backup", lässt sich ohnehin keine Auswahl treffen (es klappt, oder auch nicht, oder nur teilweise – der Anwender hat darauf keinen Einfluss).

Mit von *Titanium Backup* erstellten Sicherungen sollte es keinerlei Probleme geben, sofern man nur Benutzer-Anwendungen (sowie ihre Daten) wieder herstellt. Vorsicht ist geboten, sobald System-Anwendungen und -daten ins Spiel kommen: Zwar bietet *Titanium Backup* hierfür einen speziellen Migrations-Modus – Garantien gibt es jedoch keine.

Ähnlich steht es um "ADB Backups". Bei deren Wiederherstellung lässt sich bekanntermaßen keine Auswahl treffen: Es wird immer die gesamte Backup-Datei wiederhergestellt. Enthielt diese nur (eine) einzelne User-App(s), sollte dies keine Probleme bereiten – schließlich synchronisiert auch Helium Apps und Daten auf diese Weise geräteübergreifend. Von der Wiederherstellung einer Komplettsicherung auf einem anderen Gerät sollte man jedoch, wie bereits beim Nandroid Backup, Abstand nehmen.

Medien

Wie kann ich Dateien in der Mediengalerie ausblenden?

Einzelne Verzeichnisse (einschließlich deren Unterverzeichnisse) lassen sich "ausblenden", indem man in ihnen eine Datei mit dem Namen `.nomedia` (also mit Punkt vorne) anlegt. Dies lässt sich am einfachsten mit einem Dateimanager bewerkstelligen. Damit werden diese Verzeichnisse vom Medien-Scan ausgeschlossen – und ihre Inhalte somit in der Galerie nicht mehr angezeigt.

Wie kann ich eigene Töne als Klingelzeichen, Benachrichtigung, oder für den Wecker nutzen?

Dafür gibt es spezielle Verzeichnisse auf der SD-Karte:

Verzeichnis	Verwendung
alarms	Alarm-Töne
notifications	Benachrichtigungstöne
ringtones	Klingeltöne
ui	Tastatur-Klick-sounds etc.

Wo genau diese anzulegen sind, unterscheidet sich offensichtlich bei verschiedenen Android-Geräten. Der Wahrscheinlichkeit nach geordnet, sollte dies an folgenden Stellen geschehen:

- /sdcard/media/audio
- /sdcard/media
- /sdcard

In den in der Tabelle genannten Unterverzeichnissen werden die gewünschten Sound-Dateien dann platziert. Damit das System sie auch findet, muss der Medien-Scanner sie aber zunächst erfasst haben – also nicht wundern, wenn sie nicht sofort auftauchen!

Eine sichere Möglichkeit, einen Medien-Scan anzustoßen, besteht im Neustart des Androiden: Nach jedem Booten wird der Scanner nämlich automatisch ausgeführt. Wer nicht so lange warten will, lädt sich das kleine Tool SDRescan aus dem *Play Store*, und stößt den Scan damit manuell an. Anschließend sollten sich die neuen "Töne" als Klingelzeichen usw. auswählen lassen.

Wie kann ich aufgenommene Fotos und Videos automatisch auf der SD-Karte speichern lassen?

Bei den meisten Geräten ist gar nichts anderes vorgesehen, als selbst gemachte Fotos und Videos auf der Speicherkarte abzulegen – der interne Speicher ist oftmals ohnehin schon zu knapp bemessen. Sollte dies jedoch einmal anders sein, lässt es sich i. d. R. in der Kamera-App selbst konfigurieren. Dazu öffnet man selbige, und dort das Einstellungsmenü (sofern kein entsprechendes Icon angezeigt wird, einfach einmal die Menü-Taste betätigen). Hier sollte nun ein Menüpunkt "Speicher" zu sehen sein – unter dem man zwischen "Telefonspeicher" (dem internen Speicher) und "Speicherkarte" wählen kann.

Umgang mit der SD-Karte

Wo finde ich die SD-Karte im lokalen Dateisystem?

Die meisten Geräte binden sie unter `/sdcard` ein. Leider jedoch ist dies kein Standard, sodass insbesondere bei Geräten mit zusätzlicher "interner SD-Karte" Abweichungen gelten. So findet sich die „externe" SD-Karte beispielsweise beim Motorola Xoom unter `/mnt/external1` – andere Geräte binden die Karte unter `/sdcard/external_sd` ein, wiederum andere legen sie auf `/mnt/sdcard` oder gar `/mnt/sdcard/external_sd`... Sollte sich die Karte an keiner der genannten Stellen auffinden lassen, hilft ggf. ein Blick ins Handbuch – oder eine Frage im Forum.

Wie kann ich vom PC auf die SD-Karte zugreifen?

Eine Möglichkeit wäre natürlich, sie aus dem Gerät zu entnehmen und (ggf. mittels eines Adapters) über einen Kartenleser an den PC anzuschließen. Das ist natürlich ein wenig umständlich – insbesondere dann, wenn man (wie bei einigen Geräten der Fall) nur an sie heran kommt, nachdem man den Akku entfernt hat. Daher gibt es eine einfachere Möglichkeit: Man verbindet das Gerät mittels eines USB-Kabels mit dem Computer. Oftmals wird sie dabei automatisch auf letzterem angezeigt. Ist dies nicht der Fall, zieht man auf dem Androiden kurz die Benachrichtigungsleiste auf: Bei angeschlossenem USB-Kabel sollte sich nun hier ein Punkt finden, über den man die Karte an den PC freigeben kann. Als Symbol trägt dieser meist ein USB-Icon.

Wie kann ich meine SD-Karte wechseln?

Banale Antwort: Alte Karte raus, neue rein. Aber die Frage gilt sicher in erster Linie der Tatsache, dass man die darauf enthaltenen Daten auch gern auf die neue, größere Karte mitnehmen möchte. Auch das stellt aber kein Problem dar – solange auf der Karte nur eine einzige Partition ist (wer das jetzt von seiner Karte nicht weiß, bei dem ist dies mit ziemlicher Sicherheit der Fall).

Das Vorgehen ist in etwa folgendes:

1. Über *Einstellungen→SD-Karte und Telefonspeicher* zunächst die SD-Karte trennen (alternativ: Das Telefon abschalten)
2. Die "alte" SD-Karte entnehmen, und mit einem Kartenleser am PC anschließen
3. Sämtliche Daten in ein leeres Verzeichnis auf der Festplatte kopieren
4. Die Karte wieder sauber vom PC trennen, und die "neue" Karte mit dem Kartenleser anschließen
5. Die Daten wieder 1:1 auf die neue Karte kopieren
6. Karte sauber vom PC trennen, dem Kartenleser entnehmen, und in den Androiden einlegen.

Wer ganz auf "Nummer sicher" gehen möchte, macht das an einem Linux-PC (z. B. mit einer Live-CD wie Knoppix).

Fertig. Testen ob alles klappt. Das sollte es in 99% aller Fälle – und falls nicht, hat man bis zu einer Problemlösung ja noch immer die "intakte alte" Karte...

Ich kann App xyz nicht auf die SD-Karte verschieben!

Bei einem „Factory Reset" (zurücksetzen auf Werkseinstellungen, siehe Hardreset) gehen bekanntlich alle selbstinstallierten Apps (und Daten) verloren. Also müssen sie neu installiert werden. War eine App zuvor auf der SD-Karte installiert, kann es nun beim Versuch, die neu installierte App wieder dorthin zu verschieben, zu folgender Fehlermeldung kommen: "App kann nicht verschoben werden". Aber es ging doch zuvor auch?

Das Problem ist hier oftmals, dass Reste der App noch auf der SD-Karte verblieben sind – diese gilt es nun zunächst aufzuräumen. Das geht nicht am Gerät selbst, da Android (ohne root) den Zugriff auf das entsprechende Verzeichnis nicht zulässt. Daher muss die SD-Karte entnommen, und mittels eines Kartenlesers am PC eingebunden werden.

Zuerst gilt es, den Paketnamen der betroffenen App zu ermitteln. Dies geht am einfachsten, indem man sie auf der Website des Play Store (also mit dem Browser) aufsucht: Die URL nennt den Paketnamen sodann in der ID (Beispiel: Google Goggles findet sich unter `https://play.google.com/store/apps/details?id=`**`com.google.android.apps.unveil`** – der Paketname lautet hier also `com.google.android.apps.unveil`). Mit dieser Information bewaffnet, sucht man auf der SD-Karte im Verzeichnis `.android_secure` nun nach der passenden `.asec`-Datei, die bei unserem Beispiel etwa `com.google.android.apps.unveil-1.asec` heißen könnte – und löscht sie. Jetzt die Karte sauber vom PC trennen, zurück damit ins Gerät – und die App sollte sich nun wieder auf die SD-Karte verschieben lassen.

Auf meinem Android-Gerät kann ich keine Option zum Verschieben von Apps auf die SD-Karte finden!

Apps2SD wurde mit Android 2.2 eingeführt. Ist auf dem Gerät noch eine ältere Android-Version installiert, gibt es diese Möglichkeit schlicht nicht. Aber auch ab Android 4.0 haben sich einige Hersteller offenbar dazu entschlossen, ihren Kunden diese Funktionalität nicht anbieten zu wollen. Beispiele dafür sind das *Samsung Galaxy S Duos*, oder auch das *LG Optimus 4X:* Auf beiden Geräten sucht man die passende Option vergeblich. Abhilfe schafft in diesen Fällen nur das Rooten des Gerätes, um auf alternative Möglichkeiten wie beispielsweise Link2SD auszuweichen.

Interne und externe SD-Karte vertauschen

Verfügt ein Android-Gerät sowohl über eine so genannte "interne SD-Karte" als auch über einen Micro-SD Slot, verwenden die meisten Apps per Default die interne Karte. Dies ist besonders ärgerlich, sofern selbige nicht gerade üppig mit Speicher versehen ist. Da wünscht man sich oftmals, die Speicherplätze austauschen zu können.

Leider ist das nicht so ohne weiteres möglich. Alle mir bekannten Möglichkeiten erfordern zumindest ein gerootetes Gerät. Die meisten Anleitungen beschreiben zu diesem Zweck die manuelle Bearbeitung der entsprechenden System-Datei, was nicht jedem gefallen dürfte (näheres dazu findet sich u. a. in einem Stackexchange-Artikel). Eine einfachere Alternative bietet die App External 2 Internal SD, die ursprünglich für das *Samsung Galaxy S3* geschrieben wurde. Sie funktioniert allerdings nicht auf jedem Gerät; es empfiehlt sich daher in jedem Fall, zunächst die Kommentare nach Erfolgsmeldungen zum eigenen Gerät zu durchforsten.

Netzwerk

Die Netzwerk-Icons in der Statusbar sind plötzlich weiß. Was hat das zu bedeuten?

Die Farbe der Netzwerk-Icons in der Statusbar (WLAN, Signalstärke, mobile Daten) zeigt an, ob eine Verbindung zu den für Synchronisation etc. benötigten Google-Servern besteht. Sind die Icons Grau oder Weiß, besteht keine Verbindung. Grün (bis Gingerbread) bzw. Blau (ab Honeycomb) weisen auf eine bestehende Verbindung hin. Nachlesen lässt sich dies u. a. im Android 2.3 Users Guide:

> *Network status icons turn green if you have a Google Account added to your phone and the phone is connected to Google services, for syncing your Gmail, Calendar events, contacts, for backing up your settings, and so on. If you don't have a Google Account or if, for example, you're connected to a Wi-Fi network that is not connected to the Internet, the network icons are white.*
>
> Zu gut Deutsch:
>
> *Die Icons für den Netzwerkstatus werden Grün, wenn ein Google-Konto auf dem Android-Gerät konfiguriert, und das Gerät mit den Google-Services zur Synchronisation von GMail, Kalenderdaten, Kontakten, zum Backup der Einstellungen etc. verbunden ist. Ist kein Google-Konto konfiguriert, oder das Gerät beispielsweise mit einem WLAN verbunden, welches keinen Zugang zum Internet bietet, sind die Netzwerk-Icons Weiß.*

Ich kann mit dem Browser auf Webseiten zugreifen – aber meine Apps kommen nicht ins Netz?

Die Ursache kann trivial sein. So ist dieses Verhalten normal, wenn die Zeiteinstellungen des Gerätes zu weit von der Realität abweichen (falsches Datum). In diesem Fall ist der Zugriff auf unverschlüsselte Websites ("http") zwar problemlos möglich, nicht aber der auf verschlüsselte Ressourcen ("https"). Bei letzteren kommt es dann nämlich zu einem Fehler mit dem verwendeten Zertifikat, welches entweder noch nicht (Geräte-Datum zu weit in der Vergangenheit) oder nicht mehr (Gerätedatum zu weit in der Zukunft) gültig ist. Abhilfe schafft in diesem Fall die Korrektur der Systemzeit des Gerätes.

Tritt das Problem jedoch ausschließlich bei mobiler Datenverbindung auf, könnte die Ursache auch mit dem verwendeten APN zusammenhängen, wie Anwender bei StackExchange beschreibt. In diesem Fall überprüft man die konfigurierten

Zugangspunkte. Stehen für den Anbieter mehrere APNs zur Verfügung, verwendet man testweise einen anderen. Lässt sich das Problem damit nicht beheben, hilft eine Nachfrage beim Provider.

In seltenen Fällen hat sich einfach nur etwas "verhakt", sodass ein Wechsel in den Flugzeugmodus und wieder zurück das Problem bereits behebt.

Wie bediene ich Webseiten, die ein "Mouse-Over" Menü verwenden?

Offensichtliches Problem: Hat man keine Maus, kann auch kein Mauszeiger über einen Menüpunkt bewegt werden. Wie lässt sich ein solches Menü also auf "mauslosen Geräten" wie Smartphones und Tablets bedienen?

Ein Ansatz ist wieder bei StackExchange beschrieben: Langes Drücken der Stelle, über die man sonst die Maus bewegen soll, öffnet häufig das entsprechende Menü. Eventuell muss anschließend noch die "Zurück-Taste" betätigt werden, um das Kontext-Menü der Browser-App zu schließen.

Telefonie

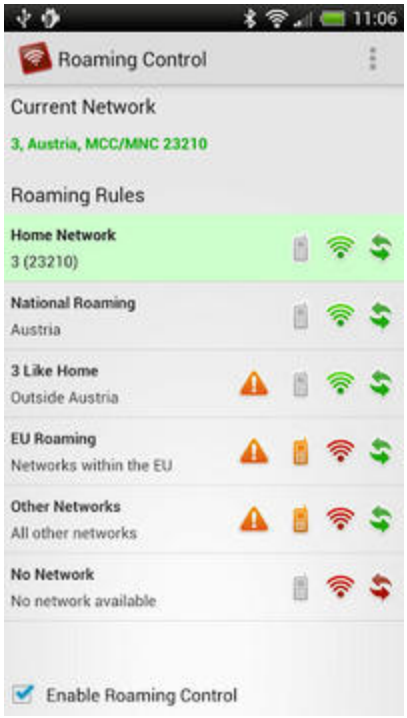
Rufumleitungen lassen sich nicht deaktivieren

Das Gepäck ist bereits aufgegeben, der Check-In absolviert, und der Aufruf zum Boarding erfolgt – ab geht es in die Sonne! Da fällt es einem siedend heiß ein: Die Rufumleitung zum Anrufbeantworter ist noch aktiviert! Das kann im Ausland teuer werden. Also schnell ins Android-Menü, und unter *Anrufe* → *Rufumleitungen* die entsprechende Rufumleitung abschalten. Und schon kann dem ahnungslosen Telefonie-Kunden ein neuer Schreck drohen, der in Form einer Fehlermeldung daher kommt: "Diese Funktion wird vom Diensteanbieter nicht unterstützt." Was nun?

Zeit für einen Anruf beim Service bleibt nicht mehr, das Boarding ist ja bereits eingeläutet. Auf diese Situation scheinen manche Anbieter zu hoffen, um noch ein paar zusätzliche Einnahmen generieren zu können: Nimmt man im Ausland einen Anruf nicht an, wird er nämlich nun kostenpflichtig (zum Auslands-Tarif) auf die Mailbox weitergeleitet! Schließlich musste man das (nicht geführte) Gespräch zunächst zum Roaming-Partner, und von dort zur Mailbox zurück durchstellen.

Die schnelle Abhilfe: Ein Anruf bei der magischen Nummer `##002#` deaktiviert sämtliche Rufumleitungen auf einen Schlag – also sowohl die bei Nichtannahme, als auch die bei Nichterreichbarkeit. Pech gehabt, gieriger Anbieter!

Ich fahre ins Ausland / Grenzgebiet. Wie vermeide ich Roaming-Kosten?



Die einfachste Möglichkeit ist natürlich, den Flugzeugmodus zu aktivieren – und ggf. bei Bedarf WLAN zu nutzen. Nicht immer ist dies aber das, was einem vorschwebt. Für das Datennetz gibt es einen einfachen Schalter in den Einstellungen unter "Drahtlos & Netzwerk": Hier lässt sich das Roaming für die Datendienste deaktivieren (per Default ist dies in der Regel auch die Voreinstellung). Darüber hinaus kann man an dieser Stelle auch den Netzbetreiber fest voreinstellen (manuell auswählen, anstatt automatisch wählen zu lassen). Somit bucht sich das Telefon auch für Gespräche nicht in ein fremdes Netz ein.

Besonders für Geschäftsleute ist es aber tragisch, wenn sie dadurch zeitweilig nicht erreichbar wären. Abhilfe verspricht für diesen Fall die App Roaming Control: Mit dieser App lässt sich für jedes Netz separat festlegen, ob ausgehende Anrufe erlaubt sein sollen, die Synchronisation deaktiviert bzw. die mobile Datenverbindung gekappt, oder gar in den Flugzeugmodus gewechselt wird. Auch allgemeine Regeln sind möglich, etwa für "EU Roaming" oder unbekannte Netzwerke. Die App kostet zwar etwa dreieinhalb Euro – kann aber ein kleines Vermögen sparen helfen. Wer das zunächst prüfen möchte, findet auch eine gratis Testversion im Playstore.

Weiteres

Ich habe mein Entsperr-Muster/Passwort vergessen!

Besteht gerade eine Netzwerk-Verbindung über 3G/2G (WLAN genügt eventuell nicht), gibt es noch Hoffnung: Einfach die Adresse des primären Google-Accounts (benutzername@googlemail.com – wobei "benutzername" natürlich entsprechend zu ersetzen ist) und das dazugehörige Passwort eingeben. Andernfalls (oder falls das fehlschlägt), muss etwas tiefer in die Trickkiste gegriffen werden:

Die Zugangsdaten werden nicht akzeptiert, obwohl sie korrekt eingegeben wurden:

Manchmal scheint die Entsperrung fehlerhaft zu arbeiten. Ist dies der Fall, helfen folgende Schritte:

1. Den richtigen Benutzernamen, aber als Passwort "null" (also genau diese vier Buchstaben) eingeben
2. Den Benutzernamen ohne `@gmail.com` (bzw. `@googlemail.com`) eingeben
3. Schritte 1 und 2 kombinieren

4. Per Browser das Passwort-Recovery bei Gmail verwenden, dann ggf. nochmals von 1. beginnen

(Quelle: Einartysen)

Die Bildschirmsperre mit einer speziellen App umgehen:

1. Mit dem Web-Browser den Google Playstore aufsuchen
2. Mit den auf dem gesperrten Gerät verwendeten Zugangsdaten anmelden
3. Die App Screen Lock Bypass installieren
4. Das Gerät booten

Diese App umgeht die „zu viele Fehlversuche" Sperre, und hebelt somit den Sperrbildschirm komplett aus – es kann also direkt wieder auf das Gerät zugegriffen werden. Allerdings nur so lange, wie diese App installiert ist. Da das natürlich keine Sicherheit darstellt, sollte dieser Zustand nur eine kurze Zwischenlösung sein, um das eigentliche Problem ohne Datenverlust beheben zu können. Als allererstes sollte jetzt natürlich ein Backup erstellt werden – zumindest, sofern man nicht über ein aktuelles verfügt. Die nächsten möglichen Schritte wären sodann:

1. Zu *Einstellungen → Konten & Synchronisation* gehen
2. Unter *Konten verwalten*, alle Konten außer dem Google-Konto entfernen (dies sollte die Verwendung des Google-Benutzernamens und Passwortes wieder aktivieren)
3. Unter *Einstellungen → Anwendungen → Anwendungen verwalten* die App *Screen Lock Bypass* aufsuchen und deinstallieren (dies setzt den Sperrbildschirm mit dem Fehler "zu viele Fehlversuche" sofort wieder in Kraft).
4. Den originalen Google Benutzernamen und das zugehörige Passwort zum Entsperren des Gerätes verwenden
5. Ein neues Sperrmuster festlegen (zwei Mal das gleiche eingeben), um den Vorgang abzuschließen

Dieser gesamte Prozess setzt natürlich voraus, dass das Gerät über eine aktive Netzwerk-Verbindung (WLAN oder mobil) verfügt. (Quelle: UltraTechy)

Über das Web entsperren:

Dies setzt zweierlei voraus: Zum einen wieder eine bestehende Netzwerk-Verbindung auf dem gesperrten Gerät – und zum Anderen die Kenntnis des korrekten Sperrmusters (vielleicht hat ja nur der kleine Bruder zu oft versucht, sich Zugang zu verschaffen). Sind diese Voraussetzungen erfüllt, kann man folgendermaßen vorgehen:

1. Mit dem Google-Benutzernamen und zugehörigem Passwort bei Google anmelden
2. Entweder direkt den Link https://accounts.google.com/IssuedAuthSubTokens eingeben – oder in der rechten oberen Ecke des Browserfensters auf die eigene Mail-Adresse klicken, *Konto* auswählen, auf der nächsten Seite rechts auf *Sicherheitseinstellungen verwalten* klicken, und schließlich den Button *Bearbeiten* neben dem Schriftzug *Autorisierung von Anwendungen und Websites* betätigen.
3. Unter *Verbundene Websites, Apps und Dienste* die Zugriffsrechte für den Android-Account widerrufen.

3. Alternativ: Wer sein Google-Konto bereits für die Zwei-Schritt-Autorisierung eingerichtet hat und in der Lage ist, am Ende der Seite

ein anwendungsspezifisches Passwort einzurichten, kann dies hier tun, und selbiges zum Entsperren des Gerätes verwenden.

4. Jetzt auf dem Gerät mit den Zugangsdaten für Google Mail anmelden. Die Zugangsdaten sollten nun akzeptiert werden, und der Sperrbildschirm wird wieder angezeigt. Das "korrekte" Sperrmuster zum Entsperren eingeben, und der Homescreen sollte wieder angezeigt werden.

(Quelle: UltraTechy)

Weitere Möglichkeiten:

Hat nichts von obigem Erfolg gezeitigt, bleiben nur noch technisch tiefer greifende Tricks – die für dieses Buch ein wenig zu weit gehen. Zu finden sind sie u. a. bei StackExchange.

Wie kann ich ohne root Screenshots vom Android Handy erstellen?

Dies lässt sich am einfachsten bewerkstelligen, indem man eines der im Kapitel "Das Android-Gerät vom PC aus verwalten" benutzt, wie etwa den *PAW Server*. Screenshots erstellt man dann einfach vom PC aus.

Wer jedoch bereits Android 4.0 oder neuer auf seinem Gerät hat, kann das viel einfacher haben: Hier gibt es häufig eine Tasten-Kombination, um einen Screenshot auszulösen. Leider unterscheiden sich diese bei Geräten unterschiedlicher Hersteller. Bei Geräten von Samsung sind meist die Power- und die Home-Taste gleichzeitig zu drücken. Bei Geräten von Motorola (und einigen anderen Herstellern) hält man dazu die Power- und die Leiser-Taste gleichzeitig gedrückt.

Was passiert mit einer App, wenn sie aus der Liste zuletzt genutzter Anwendungen gewischt wird?

Vor Android 4.0 erreichte man die Liste zuletzt genutzter Apps durch langes Drücken auf die "Home" Taste, und konnte so zu einer dieser Apps zurückkehren – mehr ging da nicht. Mit Android 4 wurde die "Multi-Tasking-Taste" eingeführt, und zeigt nun Screenshots der zuletzt genutzten Apps. Beiden Varianten ist gemein, dass an dieser Stelle aufgeführte Apps nicht zwangsläufig noch im Hintergrund laufen (selbst über einen Task-Killer beendete Apps sind hier noch aufgeführt). Doch durch eine Wisch-Bewegungen lassen sie sich nun aus der Liste entfernen. Was aber passiert dabei eigentlich?

Das offensichtliche zuerst: Die betroffene App wird aus der Liste zuletzt genutzter Apps entfernt, taucht also bis zu ihrem nächsten Start hier nicht mehr auf. Doch das ist natürlich nicht alles: Sie wird gleichzeitig auch "beendet". Und zwar in etwa so, als hätte man in der App selbst so oft die "Zurück"-Taste gedrückt, bis sie sich schließt. Mit anderen Worten: Die App wird höflich gebeten, sich doch zu beenden – sie wird jedoch nicht "gekillt". Soll sie vollständig beendet werden, drückt man stattdessen länger auf den betreffenden Eintrag, wodurch man zu den App-Details gelangt. Hier kann man nun den "Beenden" Button betätigen.

Wer sich für genauere Einzelheiten interessiert, findet diese u. a. in einem Artikel bei StackExchange.

Ich bekomme plötzlich Werbung in der Benachrichtigungsleiste eingeblendet!

Airpush und Kollegen lassen grüßen. Klar, dass sich auch Programmierer von etwas ernähren müssen – aber das geht definitiv zu weit. Es gibt jedoch mehrere Möglichkeiten, sich zu wehren. Eine Übersicht bei AndroidPIT gibt detailliert Auskunft darüber. So lässt sich die verursachende App ermitteln (ab Jelly Bean geht das von Haus aus, und kann dann auf per-App-Basis unterbunden werden), und der Unsinn abstellen. Letzteres am einfachsten, indem man auf der Airpush Website vorbeischaut, und "Nein, Danke!" sagt (Opt-Out – "Ich will das nicht mehr!").

Mein Gerät hängt in einer Force-Close-Schleife

Das Gerät bootet. Unmittelbar nach dem Hochfahren startet eine App, die aufgrund eines Fehlers abstürzt und sich gleich wieder neu startet – um wieder abzustürzen und neu zu starten, um wieder... Das nennt man einen "Force Close Loop". Das Schlimme daran: Während dieses Loops ist das Gerät auf keine Weise bedienbar, es reagiert auf keinerlei Eingaben – man kommt aus dieser Schleife also nicht heraus.

Für Fälle wie diesen gibt es bei Android den "Safe Mode" (vielen von Windows als "Abgesicherter Modus" bekannt). Startet man in diesen, so ignoriert das Android-Gerät alle Benutzer-Apps – so, als wären sie gar nicht installiert. Die Force-Close-Schleife sollte damit umgangen werden. Nun kann der Anwender die "missratene App" deinstallieren, und das Gerät wieder im normalen Modus starten – das Problem sollte gebannt sein.

In den "Safe Mode" gelangt man auf den meisten Geräten mit folgenden Schritten:

- Gerät ausschalten, Akku herausnehmen und wieder einsetzen
- Menü-Taste drücken und gedrückt halten
- Bei gedrückter Menütaste das Gerät einschalten
- Sobald der Sperrbildschirm erscheint, kann die Menü-Taste wieder losgelassen werden. In der unteren linken Ecke sollte nun der Schriftzug "Safe Mode" zu sehen sein.

Hat man das Problem beseitigt, möchte man natürlich gern wieder den "Safe Mode" verlassen:

- Gerät ausschalten, Akku herausnehmen und wieder einsetzen
- Gerät wieder normal einschalten. Dabei nur die Power-Taste benutzen, und keine weiteren Tasten gleichzeitig betätigen.

In seltenen Fällen kann es passieren, dass das Gerät den "Safe Mode" nicht wieder verlassen möchte. Hier helfen folgende Schritte:

- Gerät ausschalten, Akku und SIM-Karte entnehmen, sowie für mindestens 20 Sekunden entfernt lassen (damit keine eventuelle Restladung verbleibt). Anschließend SIM-Karte und Akku wieder einsetzen, und neu starten. Natürlich sollte während dieses Vorgangs auch kein Ladekabel angeschlossen sein.

- Ist der "Safe Mode" noch immer aktiv, bootet man in den Recovery-Modus und bereinigt die Cache-Partition ("Wipe Cache"). Wie man in den Recovery-Modus gelangt, ist von Gerät zu Gerät unterschiedlich. Meist geschieht dies, indem man bei ausgeschaltetem Gerät die "Leiser" und "Power" Taste gleichzeitig drückt und gedrückt hät, bis das Recovery-Menü zu sehen ist.
- Hat auch das nicht geholfen, bleibt als letzte Möglichkeit der Factory Reset (Zurücksetzen auf Werkseinstellungen).

Mein Touchscreen spinnt, wenn das Gerät am Ladekabel hängt!

Hierfür kann es verschiedene Ursachen geben, wie auch ein Artikel bei StackOverflow ausführt. In der Regel liegt dabei aber weder ein Software-Problem, noch ein Fehler am Gerät selbst vor. Vielmehr sind entweder das Kabel oder das Netzteil die Verursacher.

So kann beispielsweise ein Billig-Netzteil schlecht abgeschirmt sein, und damit für Störungen des auf elektromagnetische Störungen empfindlich reagierenden Touchscreens sorgen.

Wahrscheinlicher ist hingegen, dass eine unterschiedliche Pin-Belegung für die Probleme verantwortlich ist. Eine Beschreibung der Pin-Belegung von USB-Adaptern findet sich beispielsweise bei PinOuts. Ins Deutsche übertragen, sieht diese etwa folgendermaßen aus:

Pin	Name	Beschreibung
1	VCC	+5V DCC
2	D-	Data -
3	D+	Data +
x		Dieser Pin kann zur Kabelerkennung in einigen Fällen mit GND verbunden sein
4	GND	Masse

Zu beachten ist hier der "x" Pin, der mit GND verbunden sein *kann* – aber nicht *muss*. Während der eine Hersteller diese Belegung also sauber auswertet, kann sie bei Geräten eines anderen Herstellers durchaus Probleme hervorrufen.

Da ich selbst einen solchen konkreten Fall erlebt habe, bin ich der Sache nachgegangen. Beteiligt waren drei Kabel verschiedener Hersteller, drei Netzteile, sowie ein HTC und ein Motorola Smartphone (das dritte Kabel sowie Netzteil waren "generisch"). Fazit: Lediglich das Motorola-Gerät "spann", sobald das HTC-Netzteil ins Spiel kam – alle anderen Kombinationen liefen problemlos.

Google Permissions – und was sie bedeuten

Normalerweise sieht man eine Kurzbeschreibung der Permission (z. B. bei der Installation einer App). Die technische Bezeichnung taucht selten im Klartext für den Anwender auf – man kann aber z. B. auch einen Blick auf das Manifest werfen, und da stehen sie im Klartext.

Nun werde ich aber hier nicht alle Permissions aufführen, das wäre einfach zu viel. Die findet man bei Interesse im Entwickler-Handbuch (allerdings auf Englisch). Ein Wiki zum Thema, an dem sich jeder beteiligen kann, existiert ebenfalls, und zwar bei StackExchange (wiederum auf Englisch). Ein paar ausgewählte, die doch häufiger einmal auftauchen könnten, möchte ich aber hier kurz erklären:

Permission	Erklärung
ACCESS_COARSE_LOCATION	*Ungefährer (netzwerkbasierter) Standort*. Hier kommt kein GPS zum Einsatz, sondern die Informationen von Funkmasten (Cell-ID) sowie WLANs
ACCESS_FINE_LOCATION	*Genauer (GPS-) Standort*. Exakte, per GPS ermittelte Standortdaten.
ACCESS_MOCK_LOCATION	*Falsche Standortquellen für Testzwecke*. Fake Location (falsche Standortdaten vom System anfordern). Für Testzwecke gedacht (z. B. im Emulator); wird aber scheinbar auch benötigt, um ein externes GPS Gerät nutzen zu können. Hier geht es nicht darum, einer anderen App eine Fake-Location unterzujubeln – das ginge allenfalls in Verbindung mit INSTALL_LOCATION_PROVIDER.
ACCESS_NETWORK_STATE	*Netzwerkstatus anzeigen*. Informationen über Netzwerke (besteht eine Verbindung, und wenn ja zu welchem Netzwerk?)
ACCESS_SURFACE_FLINGER	Zugriff auf die API des "Surface Flinger" (Teil des Medien-Frameworks unter Android: Stellt einen systemweiten "Oberflächen-Kompositor" bereit, der sich um das Rendering in Framebuffer-Devices kümmert - also Grafik, Grafik-Beschleunigung und so).
ACCESS_WIFI_STATE	*WLAN-Status anzeigen*. Informationen über WiFi-Netzwerke (besteht eine Verbindung, und wenn ja zu welchem Netzwerk? Welche Netzwerke sind verfügbar?)
ACCOUNT_MANAGER	*Als Konto-Manager fungieren*. App darf mit Konto-Authentifizierern interagieren. (für Systemanwendungen reserviert).
AUTHENTICATE_ACCOUNTS	*Als Kontoauthentifizierer fungieren*. Konto-Authentifizierungsfunktionen verwenden, Konten erstellen, Abrufen und Einstellen der zugehörigen Passwörter.

Permission	Erklärung
BIND_APPWIDGET	*Widgets auswählen*. Erlaubt einer App dem AppWidget-Service mitzuteilen, welche App auf die AppWidget-Daten zugreifen darf. Mit dieser Berechtigung kann anderen Anwendungen Zugriff auf persönliche Daten gewährt werden. Laut API-Referenz sollten nur sehr wenige Apps diese Permission benötigen.
BLUETOOTH	*Bluetooth-Verbindungen herstellen*. Zugriff auf bereits "autorisierte" Bluetooth-Geräte
BLUETOOTH_ADMIN	*Bluetooth-Verwaltung*. Bluetooth-Geräte "autorisieren" (also "pairen" und so). Eine mit dieser Permission ausgestattete App darf selbständig Bluetooth-Verbindungen aufbauen und etablieren – auch zu "wildfremden" Geräten.
CALL_PHONE	*Telefonnummern direkt anrufen*. Anruf *ohne Bestätigung durch den Anwender* tätigen. Wird z. B. für Kontakt-Widgets benötigt, wenn ein "Tapp" auf selbige direkt einen Anruf auslösen soll – macht aber bei einer Mal-App herzlich wenig Sinn. Gilt nicht für Notruf-Nummern.
CALL_PRIVILEGED	*Alle Telefonnummern direkt anrufen.* Wie CALL_PHONE, aber inklusive Notruf-Nummern ("Hallo, Polizei – Anwender ist gerade in Bank eingebrochen... Bitte Fußboden reparieren...")
CAMERA	*Fotos aufnehmen*. Vollzugriff auf die Kamera. Nebenwirkung: Diese App lässt sich nicht auf Geräten installieren, die über keine Kamera verfügen. Die API-Referenz schreibt sinngemäß: "Wenn die App auch ohne Kamera bedienbar ist, diese Permission nicht anfordern." Da sei die Frage erlaubt: Braucht man sie dann überhaupt, wenn es auch ohne geht?
CHANGE_CONFIGURATION	*UI-Einstellungen ändern*. Änderungen an der Umgebung durchführen. API-Ref nennt als Beispiel "Locale", also Ländereinstellungen wie Währung und Zeitformat. Beschreibung sehr vage.
CHANGE_NETWORK_STATE	*Netzwerkkonnektivität ändern*. Netzwerk-Status ändern (also z. B. Verbindung trennen)
CHANGE_WIFI_MULTICAST_STATE	*WLAN-Multicast-Empfang zulassen*. WiFi MultiCast aktivieren. Damit können Datenpakete an mehrere Empfänger zeitgleich verschickt werden, ohne dass dies

Permission	Erklärung
	zusätzliche Bandbreite erfordert. Macht z. B. Sinn bei einem Streaming-Server, der mehrere Clients bedient ("Radio"). Gleichzeitig ermöglicht dies auch den Empfang von Netzwerk-Paketen, die nicht an das eigene Gerät gerichtet sind (Netzwerk-Sniffer).
CHANGE_WIFI_STATE	*WLAN-Status ändern*. CHANGE_NETWORK_STATE für WiFi. Kann auch Änderungen an konfigurierten WLAN-Netzen vornehmen.
CLEAR_APP_CACHE	*Alle Cache-Daten der Anwendung löschen*. Cache beliebiger/aller Anwendungen leeren
CLEAR_APP_USER_DATA	*Alle Cache-Daten der Anwendung löschen*. Benutzerdaten beliebiger/aller Apps löschen (siehe Einstellungen→Anwendungen verwalten, der Button "Daten löschen" bei jeder Anwendung) – richtiger wäre also *Anwendungsdaten* löschen oder CLEAR_APP_DATA, das "User" verwirrt hier ein wenig.
DELETE_CACHE_FILES	(einzelne) Dateien aus dem Cache löschen
DELETE_PACKAGES	*Anwendungen löschen*. Apps entfernen/ löschen/deinstallieren/wegmachen
DEVICE_POWER	Tiefgreifender (low-level) Eingriff in die Energieverwaltung (Power Management). Hat nicht direkt etwas mit "Power Off" zu tun, könnte aber bei Missbrauch durchaus zu selbigem führen...
DIAGNOSTIC	*Lese-/Schreibberechtigung für zu Diagnosegruppe gehörige Elemente*. Lese- und Schreibzugriff auf "diagnostic ressources" – die API-Referenz beschreibt leider nichts genaueres.
DISABLE_KEYGUARD	*Tastensperre deaktivieren*. Tastensperre (inkl. deren Passwort-Schutz) deaktivieren, sodass der Bildschirm nicht mehr automatisch gesperrt wird. Sinnvoll z. B. bei Video-Apps und insbesondere bei Navis – und bei eingehenden Telefonaten.
EXPAND_STATUS_BAR	*Statusleiste ein-/ausblenden*. Status-Bar (Notification?) erweitern/kollabieren. Wohl die Lite-Version von STATUS_BAR
GET_ACCOUNTS	*Bekannte Konten suchen*. Liste konfigurierter Accounts abrufen (nur die Accounts, nicht die Zugangsdaten selber). Mit dieser Permission kann lediglich festgestellt werden, welche Accounts existieren.

Permission	Erklärung
GET_TASKS	*Laufende Anwendungen abrufen*. Informationen über laufende Anwendungen abrufen. Wird natürlich von Task-Managern und -Killern, aber auch von Akku-Statistik-Apps benötigt. "Böse Apps" können dies nutzen um auszukundschaften, wo sich lohnende Daten zum Klauen finden lassen.
INJECT_EVENTS	*Tasten und Steuerungstasten drücken*. "Generieren" und "ausführen" bestimmter Events, wie z. B. Benutzer-Eingaben. Die App kann also vermutlich andere Apps "fernbedienen".
INSTALL_LOCATION_PROVIDER	App will selber Ortsdaten bereitstellen ("Du bist jetzt *hier*"). Woher sie die nehmen will? Naja, vielleicht von einem Bluetooth-GPS o. ä.
INSTALL_PACKAGES	*Anwendungen direkt installieren*. Andere Apps installieren. Kann OK sein (App-Manager), muss aber nicht (Wallpaper etc. wollen vielleicht eher Schadsoft nachladen, wenn sie diese Permission anfordern)
INTERNET	*Uneingeschränkter Internetzugriff*. Öffnen von Netzwerk-Sockets. Die App kann also beliebige Internet-Verbindungen herstellen. Wird von allen Apps gebraucht, die Werbung anzeigen wollen.
KILL_BACKGROUND_PROCESSES	*alle Anwendungen im Hintergrund schließen*. Hintergrund-Prozesse "töten", also beenden. Dabei kann es sich um die eigenen Prozesse handeln (was dem Anwender die Möglichkeit gibt, das Programm tatsächlich zu beenden, statt es nur in den Hintergrund zu schieben) – es können aber eben so gut fremde Prozesse beendet werden. i. d. R. handelt es sich dann um einen Task-Manager oder Task-Killer.
MANAGE_ACCOUNTS	*Als Konto-Manager fungieren*. Accounts/ Zugangsdaten *verwalten* – also auch verändern. Die Doku ist leider wieder einmal sehr vage – aber hier würden bei mir die Alarmglocken läuten.
MODIFY_PHONE_STATE	*Telefonstatus ändern*. *Status* der Telefonie anpassen: Power, MMI-Codes (z. B. Rufumleitung [de]aktivieren, Rufnummernübermittlung ein/ausschalten) etc. – jedoch nicht Anrufe tätigen. Allerdings kann das Netzwerk (zu einem anderen Anbieter, Roaming) gewechselt oder die Mobilfunkverbindung ein- bzw. ausgeschaltet

Permission	Erklärung
	werden, ohne dass der Benutzer davon informiert wird. Auch können mit dieser Permission eingehende Anrufe abgefangen werden.
MOUNT_FORMAT_FILESYSTEMS	*Externen Speicher formatieren*. Externe Dateisysteme (SD-Karten etc.) *formatieren* (Vorsicht! Nach dem Formatieren ist das entsprechende Dateisystem leer, die (vorher) darauf befindlichen Daten sind weg!). Nix für Wallpaper, Spiele, etc.!
MOUNT_UNMOUNT_FILESYSTEMS	*Dateisysteme bereitstellen oder Bereitstellung aufheben*. Dateisysteme ein- und ausbinden. Toll für externe Festplatten am Telefon – gilt aber ebenso für SD-Karten.
PROCESS_OUTGOING_CALLS	*Abgehende Anrufe abfangen*. Ausgehende Anrufe beobachten, verändern oder abbrechen. Hm, könnte das einen Anruf bei der Mailbox ins Ausland weiterleiten? Für eingehende Anrufe siehe MODIFY_PHONE_STATE.
READ_CALENDAR	*Kalenderdaten lesen*. Sollte klar sein: Alle Termine können damit gelesen werden.
READ_CONTACTS	*Kontaktdaten lesen*. Damit ist das Adressbuch fällig.
READ_FRAME_BUFFER	Zugriff auf die Frame-Buffer Daten (vereinfacht gesagt: Den Inhalt des Bildschirms). Erlaubt u. a. das Erstellen von Screenshots. Da stellt sich die Frage: Warum gibt es dann keine App zur Erstellung von Screenshots, die keine root-Rechte benötigt?
READ_HISTORY_BOOKMARKS	Erlaubt lesenden Zugriff auf Lesezeichen und Browserverlauf (Chronik).
READ_LOGS	*System-Protokolldateien lesen*. Lesender Zugriff auf die Log-Dateien des Systems. Hier werden allgemeine Informationen zu durchgeführten Aktionen gespeichert, i. d. R. jedoch keine vertraulichen Informationen (es sei denn, ein Programmierer hat etwas verbockt).
READ_OWNER_DATA	*Eigentümerdaten lesen*. Auslesen der auf dem Gerät gespeicherten Eigentümerdaten.
READ_PHONE_STATE	*Telefonstatus lesen und identifizieren*. Zugriff auf die Telefonfunktionen des Gerätes. Eine Anwendung mit dieser Berechtigung kann unter anderem die Telefon- und Seriennummer dieses Telefons ermitteln und feststellen, ob ein Anruf aktiv ist oder mit welcher Nummer der Anrufer verbunden ist. Ein Media-Player kann so z. B. bei

Permission	Erklärung
	eingehenden Anrufen automatisch auf "Pause" schalten. Bei Werbung (z. B. AdMob) wird dies häufig zum Auslesen der IMEI/IMSI genutzt um festzustellen, welche Werbung auf dem Gerät bereits angezeigt wurde (eindeutige Identifizierung, Tracking). Apps, die auch für Android 1.6 und früher kompatibel sein sollen, wird diese Permission automatisch gesetzt.
READ_SECURE_SETTINGS	Lesezugriff auf Systemeinstellungen (u. a. Umschalter für die mobile Datenverbindung). Eigentlich dem System vorbehalten.
READ_SMS	*SMS oder MMS lesen*. Damit lassen sich bereits gespeicherte Kurznachrichten lesen. Darunter können natürlich auch vertrauliche Informationen sein...
READ_SYNC_SETTINGS	*Synchronisierungseinstellungen lesen*. Lesezugriff auf die Einstellungen der Synchronisation – etwa um festzustellen, ob selbige für Kontakte aktiviert ist. Ein gutes Zeichen: Die App möchte vielleicht wissen, ob der Anwender eine Datensynchronisation im Hintergrund erlaubt, und sich (hoffentlich) entsprechend verhalten.
READ_SYNC_STATS	*Synchronisierungsstatistiken lesen*. Beispielsweise den Verlauf bereits durchgeführter Synchronisationen einsehen.
REBOOT	Erlaubt den Neustart des Gerätes. Wie der Name es bereits andeutet: Diese App kann mal eben einen Reboot veranlassen.
RECEIVE_BOOT_COMPLETED	*Automatisch nach dem Booten starten*. App möchte benachrichtigt werden, wenn der Bootvorgang abgeschlossen ist. i. d. R. heißt das: Sie möchte nach dem Booten automatisch gestartet werden.
RECEIVE_MMS, RECEIVE_SMS	*MMS empfangen, SMS empfangen*. Eingehenden MMS/SMS abfangen – da möchte wohl jemand mitlesen. Kann aber durchaus OK sein, wenn die App auf MMS/ SMS reagieren *soll*. Auf der anderen Seite kann man damit eingehende Nachrichten auch "im Nirvana" verschwinden lassen...
RECORD_AUDIO	*Audio aufnehmen*. Tonaufnahmen erstellen. Das kann sowohl für ein "Diktaphon" genutzt werden – als auch zum Mitschneiden von Telefonaten.
RESTART_PACKAGES	*Anwendungen neu starten*. Laufende Apps neu starten. Wird z. B. verwendet, um von selbigen ein Backup erstellen zu können. (In

Permission	Erklärung
	der API-Referenz mittlerweile auf "deprecated" gesetzt, sollte also in neueren Versionen nicht mehr genutzt werden)
SEND_SMS	*Kurznachrichten senden*. Und zwar ohne Zutun des Benutzers, auch an richtig teure Premium-Dienste (womit klar ist, wozu "böse Apps" das gern hätten). Es gibt aber auch "gute" Gründe für diese Permission: Natürlich die SMS-Apps, aber teilweise auch In-App-Käufe, die nicht über Google Checkout abgewickelt werden.
SET_ACTIVITY_WATCHER	Die Ausführung von Systemaktivitäten beobachten. Wird meist für Debugging benutzt. Wenn es also keine Beta ist, hat der Entwickler vielleicht nur vergessen, das wieder raus zu nehmen.
SET_ALWAYS_FINISH	App kann sich selber *beenden* – also wirklich beenden, nicht nur in den Hintergrund gehen.
SET_ANIMATION_SCALE	*Allgemeine Animationsgeschwindigkeit einstellen*. Anpassung der Animationsgeschwindigkeit (schnellere/ langsamere Animationen).
SET_PREFERRED_APPLICATIONS	App kann jeder Aktivität eine Default-App zuweisen (etwa den Browser zum Öffnen einer URL). In neueren Android-Versionen ohne Auswirkung.
STATUS_BAR	Kann die Status-Bar (Notification?) öffnen, schließen, und ausblenden. Meist will die App wohl letzteres, um einen "Vollbild-Modus" zu ermöglichen.
SUBSCRIBED_FEEDS_READ	*Abonnierte Feeds lesen*. Abrufen von Details zu den derzeitig synchronisierten Feeds.
SUBSCRIBED_FEEDS_WRITE	*Abonnierte Feeds schreiben*. Änderungen an kürzlich synchronisierten Feeds vornehmen.
SYSTEM_ALERT_WINDOW	*Warnungen auf Systemebene anzeigen*. Fenster mit Systemwarnungen einblenden. Eine böswillige App kann so den gesamten Bildschirm blockieren. Sollte eigentlich nicht benutzt werden, da dies für System-Meldungen gedacht ist. Erlaubt das anzeigen von "Alert Windows", d. h. Nachrichtenfenstern, die immer im Vordergrund angezeigt werden.
USE_CREDENTIALS	*Authentifizierungsinformationen eines Kontos verwenden*. Möchte die konfigurierten Zugangsdaten verwenden. Das heißt nicht unbedingt, dass es sie "zu sehen bekommt" –

Permission	Erklärung
	aber die App kann sich quasi "im Namen des Anwenders" anmelden.
USE_SIP	App kann Internet-Telefonie nutzen (SIP ist das Protokoll dafür)
VIBRATE	*Vibrationsalarm steuern*. Wird gern genutzt, um beispielsweise auf die Beendigung (oder auch den Start) einer Aktivität hinzuweisen – oder generell, um die Aufmerksamkeit des Anwenders zu wecken. Laute Töne sind ja nicht immer erwünscht. „Vibrieren" heißt: Lass das Gerät zittern und summen...
WAKE_LOCK	*Standby-Modus deaktivieren*. App kann das System daran hindern, einen Ruhezustand einzunehmen (also den Bildschirm zu dimmen, die CPU "schlafen" zu lassen, etc.) Wäre doch blöd, wenn die Navi-App läuft und plötzlich der Bildschirm ausgeht.
WRITE_APN_SETTINGS	*Einstellungen für Zugriffspunktname schreiben*. App kann die Zugangsdaten zum Internet etc. (siehe APN) verändern. Meist geht es der App nur darum, den Namen des APN zu ändern – um die Verwendung des mobilen Datenverkehrs zu steuern (Beispiel: APNDroid).
WRITE_CALENDAR	*Kalenderdaten schreiben*. Diese Permission erlaubt lediglich den Schreib-, nicht aber den Lesezugriff auf den Kalender. Die damit versehene App kann also Termine hinzufügen, nicht aber lesen oder ändern.
WRITE_CONTACTS	*Kontaktdaten schreiben*. Wie WRITE_CALENDAR, nur in Bezug auf die Kontaktdaten bzw. Browser-History (Chronik) und Lesezeichen.
WRITE_HISTORY_BOOKMARKS	
WRITE_EXTERNAL_STORAGE	App darf beliebige Daten auf der (externen) SD-Karte lesen, schreiben, verändern und auch löschen – prinzipiell auch die Daten anderer Apps. Diese Permission ist aber beispielsweise essentiell für diverse Backup- und Kamera-Apps, die natürlich Daten auf der Karte manipulieren müssen.
WRITE_OWNER_DATA	*Eigentümerdaten schreiben*. Schreiben/ verändern der auf dem Gerät gespeicherten Eigentümerdaten.
WRITE_SECURE_SETTINGS	*Allgemeine Systemeinstellungen ändern*. Lesen und Schreiben von Systemeinstellungen. "Secure Settings" können nur von Systemanwendungen (also solchen, die ins "ROM" integriert wurden) angefordert werden.
WRITE_SETTINGS	

Permission	Erklärung
WRITE_SYNC_SETTINGS	*Synchronisierungseinstellungen schreiben*. Schreibzugriff auf die Einstellungen der Synchronisation. Eine mit dieser Permission ausgestattete App kann u. a. die Synchronisation von Kontakten und Kalendern aktivieren bzw. deaktivieren.
com.android.vending.BILLING	In-App Payment (in der App integrierte Bezahldienste, die über den *Play Store* abgewickelt werden)

Weniger gebräuchliche sowie offensichtlich klingende Permissions (was heißt wohl *BRICK*? Ja, genau: Phone in Sachen Brauchbarkeit mit einem Ziegelstein vergleichbar zu machen, also unbrauchbar. Nicht lachen – diese Permission gibt es wirklich! So, jetzt lachen...) habe ich hier ausgelassen; die müssen also bei Bedarf unter eingangs genanntem Link selber nachgeschlagen werden. Oder man wirft einen Blick auf die App AllPermissions (bei AndroidPIT – aus dem *Play Store* wurde sie entfernt). Wie der Name bereits suggeriert, handelt es sich hier um eine dummy-App, die alle (unter Android 2.1 verfügbaren) Permissions verlangt. Da AndroidPIT bei "Mouse Over" kurze Erklärungen anzeigt, lernt man dabei auch einiges.

APN-Einstellungen ausgewählter Netzbetreiber

APN steht für **A**ccess **P**oint **N**ame (Name des Zugangspunktes). Es sind also die Zugangspunkte gemeint, die den Androiden ins Internet bringen – oder erlauben, MMS zu verschicken. Diese Zugangspunkte sind, verständlicherweise, Anbieter-spezifisch. Eine kleine Auswahl (entnommen aus dem AndroidPIT Wiki und von Android-Hilfe.DE, unserem sogenannten "Parallel-Universum"; einen Blick Wert ist auch die APNList von CyanogenMod, da gut gepflegt) finden sich hier:

Netzanbieter	Einstellungen
Deutschland	
Aldi Talk	Name: Tagesflat APN: tagesflat.eplus.de Username: eplus Passwort: gprs *Die 30-Tages-flat muss erst bei 1155 (Konto-Hotline) gebucht werden:* Name: Monatsflat APN: internet.eplus.de Username: eplus Passwort: gprs
Alice (O2-Netz GPRS, UMTS und MMS)	Name: Alice GPRS APN: internet.partner1 Proxy: nicht festgelegt Port: nicht festgelegt Nutzername: nicht festgelegt Passwort: nicht festgelegt Server: nicht festgelegt MMSC: http://10.81.0.7:8002 MMS-Proxy: 82.113.100.41 MMS-Port: 8080 MCC: 262 MNC: 07 APN-Typ: nicht festgelegt
Blau DE	Name: blau DE MMC: 262 MNC: 05 APN: internet.eplus.de Username: blau Password: blau APN-Typ: default,supl *MMS:* Name: blau DE MMS MCC: 262 MNC: 05 APN: mms.eplus.de Username: mms Password: eplus MMSC: http://mms/eplus

Netzanbieter	Einstellungen
	MMS proxy: 212.23.97.153 mmsport: 5080 APN-Typ: mms
e-plus	Name: Eplus Internet APN: internet.eplus.de Username: eplus Passwort: eplus MCC: 262 MNC: 03 APN type: default *Für MMS:* Name: Eplus MMS APN: mms.eplus.de Username: mms Passwort: eplus MMSC: http://mms/eplus MMS proxy: 212.023.097.153 MMS port: 5080 MCC: 262 MNC: 03 APN type: mms *WAP:* Name: E-Plus WAP GPRS MMC: 262 MNC: 03 APN: wap.eplus.de Proxy: 212.23.97.9 Port: 8080 APN-Type: default,supl,mms
netzclub	Name: netzclub APN: pinternet.interkom.de MCC: 262 MNC: 07 APN Typ: default *Für MMS:* Name: netzclub MMS APN: pinternet.interkom.de MMSC: http://10.81.0.7:8002 MMS Proxy: 82.113.100.5 MMS Port: 8080 MCC: 262 MNC: 07 APN Typ: mms
O2	Name: o2-de (frei definierbar) APN: pinternet.interkom.de Proxy: nicht festgelegt

Netzanbieter	Einstellungen
	Port: nicht festgelegt Nutzername: nicht festgelegt Passwort: nicht festgelegt Server: nicht festgelegt MMSC: http://10.81.0.7:8002 MMS-Proxy: 82.113.100.6 MMS-Port: 8080 MCC: 262 MNC: 07 APN-Typ: internet + mms Authenthfizierungstyp: None (ggf. nicht festgelegt testen!) *Alternativ (O2 Prepaid):* Name o2-de (frei definierbar) APN internet Proxy Nicht festgelegt Port Nicht festgelegt Nutzername Nicht festgelegt Passwort: Nicht festgelegt Server Nicht festgelegt MMSC http://10.81.0.7:8002 MMS-Proxy 82.113.100.5 MMS-Port 8080 MMS-Protokoll WAP 2.0 MCC 262 MNC 07 Authenthfizierungstyp CHAP APN-Typ Nicht festgelegt
Simyo	Name: simyo Internet APN: internet.eplus.de username: simyo passwort: simyo MCC: 262 MNC: 03 APN Typ: default *Für MMS:* Name: simyo MMS APN: mms.eplus.de username: simyo passwort: simyo MMSC: http://mms/eplus MMS Proxy: 212.023.097.153 MMS Port: 5080 MCC: 262 MNC: 03 APN Typ: mms
Solomo	Name: solomo.de Internet MMC: 262

Netzanbieter	Einstellungen
	MNC: 03 APN: internet.vistream.net Username: web Password: web APN-Typ: default,supl *MMS:* Name: solomo.de MMS MMC: 262 MNC: 03 APN: mms.vistream.net Username: mms Password: mms MMSC: http://172.30.66.40:20080 MMS proxy: 172.31.43.21 mmsport: 8080 APN-Typ: mms
Tchibo (O2-Netz)	Name: Tchibo APN: webmobil1 proxy: port: username: passwort: server: MMSC: http://10.81.0.7:8002 MMS Proxy: 82.113.100.8 MMS Port: 8080 MCC: 262 MNC: 07 APN Typ:
T-Mobile	APN: internet.t-mobile Benutzername: t-mobile Passwort: tm Authentifizierungstyp: PAP *MMS:* Name: T-Mobile MMS APN: internet.t-mobile Nutzername: t-mobile Passwort: tm MMSC: http://mms.t-mobile.de/servlets/mms MMS-Proxy: 172.28.23.131 MMS-Port: 8008 Authentifizierungstyp: PAP APN-Typ: mms
Vodafone	APN: web.vodafone.de primärer DNS: 139.7.30.125 sekundärer DNS: 139.7.30.126 Benutzername: -

Netzanbieter	Einstellungen
	Passwort: - *MMS:* Name: Vodafone DE-MMS MMC: 262 MNC: 04 APN: event.vodafone.de MMSC: http://139.7.24.1/servlets/mms MMS proxy: 139.7.29.17 mmsport: 80 APN-Typ: mms
Österreich	
A1	Name: A1.net APN: A1.net Benutzer: ppp@A1plus.at Kennwort: ppp MCC: 232 MNC: 01 APN-Typ: Internet *Für MMS:* Name: free.A1.net APN: free.A1.net MMSC: http://mmsc.a1.net Proxy: 194.48.124.71 Port: 8001 APN-Typ: MMS
bob	APN: bob.at Benutzername: data@bob.at Passwort: ppp
Drei	APN: drei.at Benutzername: leer Passwort: leer MNC: 10
One Orange	APN: web.one.at Benutzername: web Passwort: web MNC: 05
Telekom-at	name: gprsinternet apn: *99# *Alle anderen Felder bleiben leer*
tele.ring	Name: tele.ring web APN: web Benutzer: web@telering.at Kennwort: web MCC: 232 MNC: 07
Yesss!	APN: web.yesss.at Benutzername: leer

Netzanbieter	Einstellungen
	Passwort: leer MNC: 12
Schweiz	
Orange-CH	MMC: 228 MNC: 3 APN: internet *MMS:* MMC: 228 MNC: 03 APN: mms MMSC: http://192.168.151.3:8002 MMSProxy: 192.168.151.002 MMSPort: 8080 APN-Typ: mms
Swisscom	Name: Swisscom GPRS APN: gprs.swisscom.ch username: gprs passwort: gprs MCC: 228 MNC: 01 APN Typ: default *Für MMS:* Name: Swisscom MMS APN: event.swisscom.ch MMSC: http://mms.natel.ch:8079 MMS Proxy: 192.168.210.2 MMS Port: 8080 MCC: 228 MNC: 01 APN Typ: mms

Secret Codes oder Magische Nummern

Klar kann man mit einem Telefon telefonieren. Dazu gibt man eine Ziffernfolge ein, und drückt die Taste für "Abheben". Was aber passiert, wenn man noch ein paar Sonderzeichen hinzufügt?

Beschränken wir uns dabei auf die Zeichen `#` und `*` erhalten wir – richtig kombiniert – so genannte GSM-Codes. Der verlinkte Wikipedia-Artikel beschreibt ganz gut, worum es dabei geht (kurz gefasst: Steuer-Codes für diverse Netzanbieter-Funktionen, die eigentlich auf allen Geräten gleich funktionieren sollten, aber nicht bei allen Anbietern in gleichem Umfang verfügbar sind). Unterteilen lassen sich diese Codes grob in mehrere Untergruppen:

USSD-Codes:

Diese folgen dem Muster `*1nn#` – also der * Taste, gefolgt von einer 1 und weiteren zwei Ziffern, abgeschlossen durch eine Raute (optional mit Parametern: `*1nn*<Parameter>#`). Dabei handelt es sich um

Zugangsnummern für einfachere Mobilfunkdienste, die zum Beispiel Zugang zu vorkonfigurierten Diensten bereitstellen, welche für den Betreiber des jeweiligen Mobilfunknetzes spezifisch sind. Gibt man einen solchen USSD-Code auf dem Mobilfunk-Gerät ein, wird die Antwort des Betreibernetzes normalerweise innerhalb weniger Sekunden auf dem Bildschirm dargestellt.

Erweiterte Service-Codes:

Diese werden für erweiterte Service-Dienste wie etwa Anrufweiterleitungen oder die (De-)Aktivierung der Rufnummernübermittlung, aber auch zum Ändern bzw. Entsperren der PIN genutzt.

Geräte-, Hersteller- und Systemspezifische Codes:

Diese dienen i. d. R. dem zuständigen Service-Personal zur Abfrage/ Anpassung diverser Geräte-Parameter, für Status-Tests, u. a. m.

Disclaimer: Naturgemäß kann es sein, dass einige dieser Codes nicht auf allen Geräten bzw. nicht bei allen Mobilfunkanbietern funktionieren. Sofern sie nicht im Handbuch des Gerätes aufgeführt sind, mag das durchaus seine Gründe haben: So kann der eine oder andere Punkt, unsachgemäss angewendet, u. U. Schäden verursachen. Ich übernehme keinerlei Garantien dafür, dass folgende Codes a) funktionieren, b) das tun, was da steht, oder c) "folgenfrei" genutzt werden können. Insbesondere übernehme ich keinerlei Verantwortung für etwaige negative Folgen! Für etwaige positive Folgen stelle ich natürlich gern mein Bankkonto zur Verfügung...

Ebenso kann es vorkommen, dass nach Eingabe des einen oder anderen Codes nichts passiert. Es kann aber auch sein, dass dies nur so scheint (bei meinen Tests fand ich anschließend – am nächsten Tag – einige der "magischen Nummern" in der "Verbraucherliste" wieder). Es können durchaus Hintergrund-Dienste gestartet oder aber "versteckte Klassen/Menüs" in Apps freigeschaltet werden, was sich u. U. nur durch einen Werksreset wieder rückgängig machen lässt ...

USSD Codes

Code	Bedeutung
*100#	Prepaid-Guthaben anzeigen
*135#	Eigene Rufnummer anzeigen

Erweiterte Service-Codes

Code	Bedeutung
**21*<Rufnummer># / *21# / #21# / *#21#	Anrufweiterleitung einrichten / aktivieren / deaktivieren / überprüfen
##002#	alle Rufumleitungen deaktivieren
*30# / #30# / *#30#	CLIP: Eingehende Rufnummern anzeigen / unterdrücken / Status
#31#<Rufnummer>	CLIR: Mit unterdrückter Rufnummer anrufen
*43# / #43# / *#43#	Anklopfen aktivieren / deaktivieren / Status abfragen

Code	Bedeutung
*76# / #76# / *#76#	COLP: Wenn der ausgehende Anruf weitergeleitet wird, Zielrufnummer anzeigen
*77# / #77# / *#77#	COLR: Bei eingehendem umgeleiteten Anruf die Ursprungsnummer anzeigen
*N# (TCom: *T#)	Wird eine SMS mit dieser Zeichenfolge begonnen, erfolgt eine SMS Empfangsbestätigung

Obige Tabelle ist keinesfalls vollständig. Weitere "GSM Codes" finden sich u. a. bei:

- MobileMania.DE
- GSMCodes-Online.DE

Geräte-, Hersteller-, und Systemspezifische Codes

Die fett gedruckten Codes sollten nach Informationen bei StackExchange auf allen Android-Geräten (zumindest mit Android Version 4.1) gleichermaßen funktionieren. Ob das "Spielen" damit deswegen unbedingt ratsam ist (zumal wenn man nicht genau weiß, was sich dahinter verbirgt), steht auf einem anderen Blatt. Daher habe ich die Codes, die mir als "absolut harmlos" bekannt sind, einmal kursiv hervorgehoben.

Code	Bedeutung
##0*#*#*	Test des LCD-Displays
*#0011#	GSM-Infos
*#0228#	ausführliche Infos zum Batteriestatus
##0283#*#*	Loopback-Test
**05*<PUK Code>*<neue PIN>*<neue PIN zur Bestätigung>#	Entsperren des Telefons aus dem Notruf-Modus
##0588#*#*	Test des Annäherungs-Sensors
#06#	IMEI
##0673#*#* *#*#0289#*#*	Einer der beiden Codes führt zu einem Audio-Test
*#0782#	RTC (Real-Time-Clock) auslesen und anzeigen
##0842#*#*	Test für Vibrator (oh ja!) und Hintergrund-Beleuchtung
##1111#*#*	FTA Software Version
##1234#*#*	Firmware-Info
##1472365#*#*	ein kurzer GPS-Test (und Einstellungen)
##1575#*#*	ein weiterer GPS-Test
##197328640#*#*	Service-Menü mit verschiedenen Test-Möglichkeiten
##2222#*#*	FTA Hardware Version
#*#225#*#	Kalender-Debug
*#2263#	Bandnutzung
##232331#*#*	BlueTooth-Test
##232337#*#	MAC-Adresse des BlueTooth-Interfaces
##232338#*#*	MAC-Adresse des WLAN-Interfaces anzeigen

Code	Bedeutung
##232339#*#* *#*#526#*#* *#*#528#*#*	Einer dieser Codes führt zu den WLAN-Tests...
##2432546#*#* (*#*#CHECKIN#*#*)	Nach OTA-Updates suchen
##2663#*#*	Touch-Screen Version anzeigen
##2664#*#*	Touch-Screen Test
##273283*255*663282*#*#*	angeblich für eine schnelle Sicherung der Medien-Dateien (Fotos, Videos..) gut. Von wo und nach wo? Habe ich nicht probiert...
*2767*3855#	Factory Format (Wipe). Vorsicht damit!!!
##3264#*#*	RAM Test / RAM-Version anzeigen
##3424#*#*	HTC Function Test
##34971539#*#*	Kamera-Menü mit folgenden Punkten: Update mit Firmware aus Bild (keinesfalls! Sonst futsch!); Update mit Firmware von SD-Karte; Versions-Info; Update-Counter
##36245#*#*	EMail Debug
##44336#*#*	Herstellungszeitpunkt und Laufende Nummer
#*#4636#*# ***(*#*#INFO#*#*)***	Öffnet ein Menü, aus dem sich wählen lässt: Telefon-Infos, Akku-Infos, Akku-History, Verbrauchsstatistiken.
#4646#	Feldtest (Details zu Akkustand + Funknetz, Wechsel UMTS/GSM)
##4986*2650468#*#*	Diverse Hardware-Infos
##564#*#*	QXDM (Qualcomm eXtensible Diagnostic Monitor) Logging FrontEnd
##7262626#*#*	Ein Bett im Kornfeld... äh, Feld-Test
##7269#*#*	Standard Device-Logging (Device [logcat?], AT-Befehle, Kernel [dmesg?] -- HTC?)
##7378423#*#* *#*#SERVICE#*#*	Ein weiteres Service-Menü: Service-Information, Service-Settings, Service-Tests...
*#7465625#	Netz- und Subnetzsperre, Simlook, Service Provider und Corporate Lock (Galaxy-S?)
#*#759#*#	GooglePartnerSetup
##7594#*#*	Verhalten des Einschalt-Knopfes ändern (z. B. direktes Abschalten ohne Menü)
##7780#*#*	Zurücksetzen auf Werkseinstellungen
#*#8255#*#	GoogleTalk Service Überwachung
#*#8350#*#	Logging der Anrufe deaktivieren
#*#8351#*#	Logging der Anrufe aktivieren
*#9090#	Service-Modus UART/USB
##9696#*#*	FTP Test

Weitere spezielle magische Nummern gibt es für Geräte von...

- ...LG
- ...Motorola
- ...Samsung

- ...Samsung (SGS)

Und dann wären da noch diverse Listen mit GSM und USSD Codes...

- ...bei den XDA-Developers
- ...bei SMSMich.DE (auch Provider-spezifische Codes)
- ...und sicher noch an vielen anderen Stellen.

Leistungsaufnahme verschiedener Komponenten

Heise hat für seinen Artikel Energiesparplan ein Motorola Milestone angepasst und ausführlich getestet, was welche Komponente so verbraucht. Und wie man das Einschränken kann (das war jetzt eine klare Empfehlung, den Artikel zu lesen!). Die Daten davon werden einerseits ein "war ja klar", aber bei einigen Daten auch ein "oh, das hätte ich jetzt nicht gedacht" hervorrufen. Passende Angaben zum Galaxy S3 hat die c't in ihrer Ausgabe vom August 2012 gesammelt – und dabei den Test gleich noch ein wenig ausgeweitet.

Anmerkungen zum Galaxy S3 (*): Der Energieverbrauch des Displays hängt hier auch stark von den dargestellten Inhalten ab, was auf das verwendete Amoled-Display zurückzuführen ist: Bei vollständig schwarzem Display entspricht der Verbrauch auf allen Stufen nicht mehr als das Minimum.

Weiterhin sollte man beim Vergleich der Werte auch die unterschiedliche Hardware-Ausstattung im Hinterkopf behalten: So werkelt beispielsweise im Galaxy S3 ein mit 1,4 GHz getakteter Quad-Core Prozessor, und zur Anzeige dient ein 4,8 Zoll Display – im Milestone waren es noch eine Single-Core CPU mit 550 MHz und ein 3,7 Zoll Display.

Betriebszustand	zusätzliche Leistungsaufnahme	
	Motorola Milestone	**Samsung Galaxy S3**
Videoaufnahme[1]	1557 mW	1683 mW
UMTS Upload	1410 mW	1033 mW
UMTS Download	1349 mW	1074 mW
EGDE Upload	1179 mW	
WLAN Download	1158 mW	549 mW
Video abspielen (fullscreen)[1]	1135 mW	597 mW
UMTS-Telefonat	983 mW	637 mW
Kamera[1]	934 mW	1460 mW
EGDE Download	853 mW	
Bluetooth empfangen	751 mW	487 mW
Display (höchste Stufe)	730 mW	1568 mW*
GPS Suche	550 mW	263 mW
GSM-Telefonat	511 mW	297 mW
Bluetooth senden	487 mW	454 mW
WLAN Upload	479 mW	488 mW
Display (niedrigste Stufe)	310 mW	567 mW
WLAN Tether [2]		372 mW
MP3 abspielen über Bluetooth		296 mW
MP3 abspielen	160 mW	153 mW
UMTS Standby	18,3 mW	13,8 mW
GSM/EDGE Standby	11,6 mW	9.5 mW
WLAN Standby 2,4 GHz	7,8 mW	9.3 mW
WLAN Standby 5 GHz	N/A	14.6 mW
NFC Standby	N/A	4 mW
Bluetooth Standby	2,8 mW	1.8 mW
GPS Standby	0,4 mW	0.7 mW
WLAN Tether Download[3]		1254 mW

1 Leistungsaufnahme des Displays bereits abgezogen

2 Tethering aktiv, 1 Benutzer

3 Download vom Notebook per WLAN-Tether

Für die Gesamt-Leistungsaufnahme muss natürlich noch die Grundlast hinzugerechnet werden (was das Gerät verbraucht, wenn alles in der Tabelle genannte abgeschaltet ist; also "Flugmodus"). Das wären ganze fette 6,4mW. Wird das Gerät also des Nachts in diesen versetzt, spart das bereits enorm (Werte des Motorola Milestone):

Betriebszustand	**zusätzliche Leistungsaufnahme**	
	Motorola Milestone	**Samsung Galaxy S3**
Flugmodus	6,4 mW	6,4 mW
GSM Bereitschaft	18 mW	9,5 mW
GSM Bereitschaft + WLAN Standby	25,8 mW	18,8 mW
GSM Bereitschaft + WLAN Standby + Bluetooth Standby	28,6 mW	20,6 mW
UMTS Bereitschaft	24,7 mW	10,9 mW
UMTS Bereitschaft + mobile Daten aktiv		13,8 mW
UMTS Bereitschaft + WLAN Standby	32,5 mW	20,2 mW
UMTS Bereitschaft + WLAN Standby + Bluetooth Standby	35,3 mW	22,0 mW

Die Werte sind natürlich alle spezifisch für o. g. Motorola Milestone bzw. das Samsung Galaxy S3, und können auf anderen Geräten abweichen. Die Größenordnungen sollten aber zumindest ähnlich sein.

Nur so nochmal gesagt: Selbst wenn WLAN etc. alles aus sind, und nur Telefonate (und SMS) noch durchkommen (den Datenverkehr also mal ganz außen vorgelassen), reduziert sich der Verbrauch im Flugmodus auf ein Drittel (GSM) oder gar ein Viertel (UMTS). Einmal 6 Stunden angenommen (von 0 Uhr bis 6 Uhr), hält der Akku damit (theoretisch) für bis zu gut 2 Stunden länger. Natürlich wieder nur, wenn man dann anschließend auch nichts damit macht – also wieder so ein "Laborwert". Trotzdem kann man sich leicht ausrechnen: Sechs Stunden Flugmodus (statt GSM Bereitschaft) schaffen Raum für zusätzliche ca. 8 Minuten GSM Telefonat...