

Virenschutz gratis: **1 Jahr ESET Mobile Security**

ct Android

# ct Android

Mehr aus Smartphones und Tablets rausholen

## Privat und Beruf clever trennen

Daten sicher verwalten  
Rechtsfallen vermeiden  
Sparen mit Dual-SIM

Display kaputt, Akku platt?  
Reparatur-Shops im Test

Tests: Smartphones  
MicroSD, Powerbanks

Finger weg von Tuning-Tools  
Bessere Bilder mit Foto-Apps  
Android kindgerecht einrichten

Test und Beratung

## Android, aber sicher!


Befall erkennen • Viren vernichten • Verschlüsselung aktivieren



www.ctspecial.de

# Werden Sie zum Hardware-Profi!



 [shop.heise.de/ctguide](http://shop.heise.de/ctguide)  [service@shop.heise.de](mailto:service@shop.heise.de)  
Auch als eMagazin erhältlich unter: [shop.heise.de/ctguide-pdf](http://shop.heise.de/ctguide-pdf)

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 15 €

 **heise shop**

[shop.heise.de/ctguide](http://shop.heise.de/ctguide) 



## Liebe Leserin, lieber Leser,

Android dominiert den Smartphone-Markt mehr denn je, rund 80 Prozent der Kunden entscheiden sich mittlerweile für ein Gerät mit Googles mobilem Betriebssystem. Aus gutem Grund, kein anderes System ist so vielfältig, so mächtig und so erweiterbar wie Android. Zudem ist es in den vergangenen Jahren spürbar erwachsener geworden, denn viele Anfangsprobleme konnte Google mittlerweile ausmerzen. Perfekt ist es deswegen aber längst noch nicht. Gerade in Sachen Sicherheit eilt Android ein schlechter Ruf voraus – manchmal zu Recht.

In unserer Auswahl der besten Android-Artikel aus der c't zeigen wir, wie man sich leicht vor Schädlingen schützen kann und die Plagegeister im Ernstfall wieder loswird, was Security-Suiten taugen und wie man Berufliches und Privates auf einem Gerät sicher trennen kann. Darüber hinaus geben wir Tipps, wie Sie Smartphone und Tablet kindersicher machen, und checken, wie die Hersteller mit Android-Updates umgehen.

Wir vergleichen außerdem die besten Smartphones miteinander und schauen uns an, was die neuesten Android-Smartwatches taugen. Der Reparatur-Check verrät, wie gut sich freie Werkstätten beim Beheben von Schäden und beim Austausch von schlappen Akkus schlagen.

Wer mehr aus seinem Smartphone herausholen will, findet im Heft zudem jede Menge Tests und Beratung zu interessantem Zubehör, passenden Tarifen und praktischer Software. Unter anderem haben wir uns angeschaut, welche Speicherkarte sich am besten für den Einsatz im Smartphone eignet, wie die Geräte mit der richtigen Powerbank länger durchhalten und wie man dank Dual-SIM-Smartphones Geld sparen kann.

Viel Spaß beim Lesen



Alexander Spier





## Android-Überblick

- 6 Was Android 7 besser macht
- 8 CyanogenMod wird zu LineageOS
- 10 Updates und Sicherheitspatches im Check

## Android, aber sicher!

- 14 Sieben Security-Suiten im Test
- 22 Schädlinge aufspüren und loswerden
- 28 Erpressungs-Trojaner werden mobil
- 32 Geräteverschlüsselung aktivieren
- 36 Probleme bei der Android-Verschlüsselung
- 37 WebView-Irrtum verhindert Updates
- 38 Android für Kinder absichern
- 42 Tablets für Kinder im Vergleich

## Beruf und Privat trennen

- 46 Datenschutz trotz Handy
- 52 Berufliche und private Daten voneinander abschotten
- 58 Android ohne Google auf dem Fairphone 2
- 60 Zwei Sim-Karten optimal kombinieren
- 62 Smartphones mit zwei Sim-Karten-Slots

## Tarifgeschichten

- 66 Schnelles mobiles Internet: LTE ausreizen
- 70 LTE-Tarife fürs Smartphone
- 74 Kaufberatung: Smartphones mit LTE



## Hardware

- 76 Die besten Android-Handys im Vergleich
- 82 Die Google-Smartphones Pixel und Pixel XL im Test
- 84 Sony Xperia X im Test
- 86 Mit zwei Sim-Karten-Slots: Motorola Moto G4 und Moto G4 Plus im Test



# Inhalt



## Wissenswertes, Praxis und Tipps

- 88 Freie Smartphone-Werkstätten im Test
- 92 Systemoptimierer-Apps auf den Zahn gefühlt
- 96 Smartphone-Hersteller Fairphone und das Fairtrade-Gold



## Software

- 98 Apps für die Bildbearbeitung
- 104 Apps zum Schreiben, Rechnen und Präsentieren
- 110 Kostenlose Filemanager ohne Werbe-Overkill
- 113 Gute Weine finden: Vivino
- 113 Selfie-App: MSQRD
- 113 App für die Reiseplanung: Google Trips
- 116 Zeiterfassung für PC und Smartphone

## Zubehör

- 120 Schnelle MicroSD-Karten im Test
- 125 Kameragriff für LG G5
- 125 Zeitraffer-Stativauflauf Flow-Mow
- 126 Test: Powerbanks von 15 bis 65 Euro
- 130 Test: Outdoor-Powerbanks im Vergleich
- 132 Smartwatches für jeden Geschmack

## Android-Programmierung

- 138 Android-Apps dekompileieren
- 142 Force Touch in eigenen Apps nutzen
- 146 Nachrichtenzähler am Homescreen-Icon einblenden

## Aktion

- 9 Virenschutz gratis: Security Suite von Eset

## Zum Heft

- 3 Editorial
- 137 Impressum

Alexander Spier

# Was Android 7 besser macht

**Android 7 Nougat ist endlich fertig und wird verteilt. Zeit, sich die Verbesserungen genauer anzuschauen: Läuft das Smartphone mit dem neuen Doze-Modus länger, eignen sich Android-Tablets dank Splitscreen besser zum Arbeiten und lohnt sich die Vorfreude, während man mal wieder aufs Update warten muss?**

**D**as Beeindruckende an Android 7 sind nicht die offensichtlichen großen Neuerungen. Überraschend ist vielmehr, wie gereift das System nach dem Update wirkt. Viele Funktionen sind einen entscheidenden Fingertipp näher, die Oberfläche legt keine spürbaren Denkpausen ein und das ganze System wirkt viel häufiger wie aus einem Guss. Die siebte Version von Googles mobilem Betriebssystem hat mehr denn je das Zeug dazu, den Ruf eines bisweilen hakeligen Systems mit einer oft inkonsequent gestalteten Oberfläche abzulegen. Spannenderweise entwickelt sich iOS 10 gerade in eine andere Richtung und zerfärbt stärker.

Ob der gute erste Eindruck insgesamt hält, lässt sich erst in ein paar Monaten sagen. Noch gibt es Android 7.0 nur für wenige Geräte, und selbst hier dauert die Verteilung lange. Wir haben uns das Nougat getaufte System auf Nexus 5X, Nexus 6P und dem Tablet Nexus 9 näher angeschaut.

## Flotter Auftritt

Lahm ist Android auch in den Vorgängerversionen nicht, bei frisch aufgesetztem Smartphone laufen Lollipop und Marshmallow ebenfalls geschmeidig. Doch auf vielen Geräten schleicht sich gerade bei einer umfangreichen App-Sammlung nach einiger Zeit eine gewisse Behäbigkeit ein – trotz Mehrkern-CPU's und jeder Menge Arbeitsspeicher.

Google hat viel unter der Haube getan, um dieser schleichenden Verlangsamung entgegenzuwirken. So können sich Apps nicht mehr vom System wecken lassen, wenn sich die Netzwerkverbindung ändert oder ein Bild beziehungsweise Video

geschossen wird. Sie müssen nun von sich aus den Status abfragen, damit Android solche Abfragen besser bündeln und die Prozessorlast verringern kann.

Statt ein Programm vorab zu kompilieren, erweitert ein JIT-Compiler (Just in Time) die Laufzeitumgebung ART. Er sorgt einerseits dafür, dass Apps besser an die aktuellen Bedingungen auf dem Gerät angepasst werden, und kompiliert zudem Teile der App erst dann, wenn sie genutzt werden. Hängt das Gerät am Strom, werden Anwendungen aber auch vorkompiliert, um Zeit und Akkulaufzeit zu sparen. Ein Cache erspart doppelte Arbeit bei häufig genutzten Programmteilen.

Auf dem nominell schwächeren Nexus 6P mit Android 7 brauchte ein größeres Spiel rund 10 Sekunden zum Installieren, auf einem Samsung Galaxy S7 mit Android 6 trotz schnellerer CPU und Speicher über 15 Sekunden. Beim ersten Start direkt danach gab es dennoch keine Unterschiede, das Spiel erschien bei beiden Geräten genauso schnell auf dem Schirm. Zudem spart das neue Verfahren Speicherplatz: Statt 280 MByte brauchte die Facebook-App nur 160 MByte auf dem Nexus 6P – allerdings kommt da noch der Cache hinzu.

## Geteilte Ansichten

Lange erwartet ist die Möglichkeit, zwei Apps parallel auf dem Bildschirm anzuzeigen – das klappt anders als bei iOS nicht nur auf Tablets, sondern auch auf Smartphones. Läuft ein Programm im Vordergrund, startet ein langer Druck auf den Taskwechsler die geteilte Ansicht. Nun kann man sich je nach Bildschirmorientierung auf der rechten oder unteren Hälfte die zweite App aus den kürzlich verwendeten heraussuchen. Die zuerst gestartete

App lässt sich in der geteilten Sicht nicht wechseln. Die gleiche App zweimal aufzurufen klappt bislang nicht – bisher erlaubt nur Chrome den Start einer zweiten Instanz aus dem Programm heraus.

Die Aufteilung ist begrenzt wählbar: Eine App darf ein Drittel, die Hälfte oder zwei Drittel des Schirms einnehmen. Den Rest nutzt das andere Programm. Das Ändern der Aufteilung läuft bis zu einem gewissen Grad erstaunlich flott und geschmeidig, hin und wieder bauen sich die Apps aber auch komplett neu auf. Schiebt man den Trenner weiter Richtung Bildschirmrand, wechselt die größere App ins Vollbild.

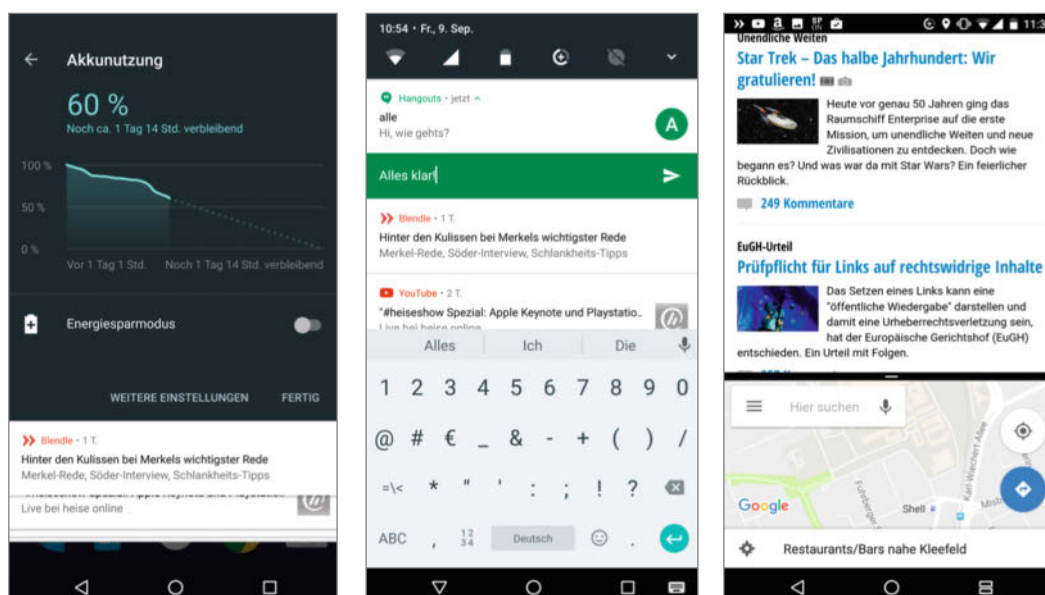
In der Praxis hakt die geteilte Ansicht noch. Elemente von einem ins andere Fenster zu verschieben klappt derzeit nicht, bei vielen Apps warnt das System vor Problemen und einige sind gar nicht auswählbar. Beim Aufwachen aus dem Standby dauert es deutlich zu lange, bis die Inhalte wieder erscheinen. Einige Apps stürzen hin und wieder bei der Größenanpassung ab. Auch ist nicht erkennbar, welche App gerade den Fokus hat. Besonders beim Tippen auf der Tastatur ist das lästig.

## Dösen für unterwegs

Trägt man das Smartphone mit abgeschaltetem Display in der Tasche, nutzt es nun den verbesserten Doze-Modus. Hintergrundaktivitäten und Netzwerkzugriffe werden dann reduziert und den Apps nur hin und wieder kurze Zeitfenster zum Synchronisieren gewährt. Dabei geht das System nicht so weit wie im stationären Schlafmodus: Apps können etwa weiterhin den Standort abfragen. Die ersten praktischen Erfahrungen zeigen eine etwas verlängerte Akkulaufzeit, wenn das Gerät un-



Android 7 rüstet mit den verbesserten Schnelleinstellungen, erweiterten Benachrichtigungen und der geteilten App-Ansicht viele hilfreiche Funktionen nach.



benutzt in der Tasche steckt. Hier nähert es sich dem Grundbedarf im Flugmodus an. Wer alle paar Minuten zum Smartphone greift, wird jedoch kaum eine Änderung bemerken.

Auffällige Verzögerungen beim Empfang von Nachrichten konnten wir dabei nicht feststellen, WhatsApp und Co. bekamen ihre Infos auch bei aktivem Doze-Modus. Wie gehabt können einzelne Apps aber auch komplett vom Stromsparmodus ausgenommen werden.

## Datensparsamkeit

Um unterwegs Energie und Datenvolumen zu sparen, konnten Android-Nutzer bisher nur die Option „Hintergrunddaten“ deaktivieren. Apps können dann keine Daten mehr abgleichen, wenn sie nicht aktiv im Vordergrund genutzt werden. Der neue Datensparmodus macht das alltagstauglicher: Ist er aktiv, dürfen Apps wie gehabt im Hintergrund keine Daten mehr übertragen. Dies wird nun deutlich in der Statusleiste angezeigt, zudem kann der Modus über eine Schaltfläche in den Schnelleinstellungen einfach ein- und ausgeschaltet werden.

Die Auswirkungen sind bisher die gleichen wie beim Abschalten der Hintergrunddaten: Teilweise kommen Nachrichten verzögert an und Apps haben beim Start nicht die neusten Einträge vorgeladen. Einzelne Apps können in den Einstellungen des Datensparmodus ausgenommen werden, bei Android 6 war die Blockade nur pauschal für alle möglich. Zudem signalisiert der aktive Datensparmodus Apps im Vordergrund, dass sie möglichst wenig Bandbreite nutzen sollen. Ob sich die App daran hält, bleibt allerdings weiter ihr überlassen.

## Praktischere Benachrichtigungen

Das neue Benachrichtigungssystem erweitert die Möglichkeiten der kleinen Info-Häppchen beträchtlich. So können bei vielen Apps Infos ausführlicher angezeigt und besser gruppiert werden sowie Nachrichten direkt aus der Benachrichtigungsleiste heraus beantwortet werden. Der Play Store beispielsweise zeigt Update-Benachrichtigungen zunächst gebündelt an und klappt beim Tippen auf die Betreffzeile alle Einträge aus. Das Erweitern und Durchscrollen der Benachrichtigungen klappt endlich verlässlich und ohne Knoten im Finger.

Allerdings hängt es vom App-Entwickler ab, wie gut er die Möglichkeiten nutzt. WhatsApp erlaubt zwar das direkte Antworten an den Kontakt, zeigt aber nur noch die zuletzt empfangene Nachricht. Prinzipiell bietet Android aber einen guten Kompromiss aus Kürze und Funktionsumfang und macht das übersichtlicher als die Widgets von iOS. Benachrichtigungen einzelner Apps können zudem feiner differenziert werden: Sie lassen sich nicht mehr nur komplett blockieren, sondern auch stumm schalten. So sind sie weiterhin sichtbar, erzeugen aber keine Vibrationen und Töne mehr.

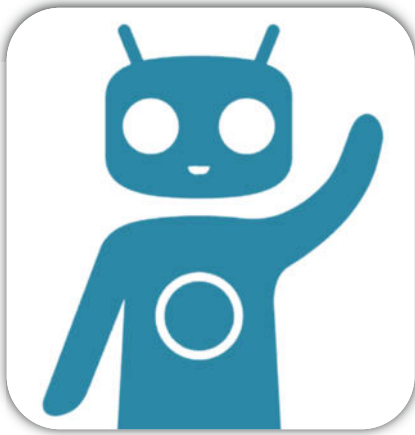
Auch sonst tut Google einiges für mehr Bedienkomfort. Der schnelle Wechsel zur vorher angezeigten App über einen Doppeltipp auf den Taskwechsel-Knopf ist ebenso praktisch wie die nun mit einem Wisch zugänglichen Schnelleinstellungen im Benachrichtigungsmenü. Einige der Schaltflächen geben beim kurzen Antippen mehr Informationen preis, etwa die verbrauchte Datenmenge oder den Akkuverlauf. In den Android-Einstellungen

geben die Kategorien bereits auf der Übersichtsseite mehr Informationen zum jeweiligen Zustand, ein ausziehbares Menü erlaubt einen flotten Wechsel dazwischen.

## Fazit

Google geht mit Android 7 konsequent den Weg hin zu mehr Benutzerfreundlichkeit. Das System war in dieser Hinsicht noch nie näher an iOS – ohne dabei seine Stärken wie Anpassbarkeit und Offenheit einzuschränken. Ja, Google bedient sich der Ideen von Apple und anderen Herstellern. Funktionen wie Doze, den Datensparmodus oder die geteilte App-Ansicht haben Samsung, Sony und Co. teilweise seit Jahren in ihre Android-Versionen eingebaut. Dass sie nun direkt in Android stecken, rüstet aber nicht nur nützliche Funktionen für alle Nutzer nach, es reduziert auch die Notwendigkeit für die Hersteller, eigene Lösungen zu pflegen.

Zu verbessern gibt es immer noch genug. Die Multitasking-Funktionen sind ausbaufähig und wirken teilweise nicht richtig fertig, weil die App-Unterstützung lahmte. Die Rechteverwaltung und Möglichkeiten für wirksamen Datenschutz sind weiterhin umständlich gelöst und teils nicht vorhanden. Zeitnah Android-Updates für alle anderen als die Nexus-Geräte bereitzustellen gelingt immer noch nicht: Wenn erneut Monate vergehen, bis alle Hersteller wenigstens ihre aktuellen Top-Geräte aktualisiert haben, sind all die schönen Verbesserungen für die Mehrheit gar nicht relevant – das klappt bei iOS weiterhin besser. Zumal Google es selbst schlimmer macht: Das Google Pixel lief schon mit Android 7.1, während die anderen Nexus-Geräte darauf warten mussten. (asp) **ct**



Alexander Spier

## Cyanogen ist tot, lang lebe LineageOS

Wer für sein Smartphone keine aktuelle Android-Version vom Hersteller mehr bekam, der konnte bisher immer noch auf CyanogenMod hoffen. Doch das größte Projekt für alternative Android-ROMs ist mit dem Absturz der kommerziellen Abspaltung Cyanogen ebenfalls in schwere Turbulenzen geraten.

Die von Freiwilligen entwickelte Android-Distribution CyanogenMod wird ab sofort als LineageOS weitergeführt. Dafür muss das Projekt allerdings seine jahrelang gewachsene Infrastruktur in wesentlichen Teilen neu aufbauen. Die Auswirkungen auf die aktive Szene für alternative Android-ROMs sind bisher nicht komplett abzuschätzen, doch der Neustart als LineageOS dürfte auch viele weitere darauf aufsetzende Projekte betreffen.

Hintergrund ist der Niedergang der Firma Cyanogen. Diese ging ursprünglich aus dem Freiwilligen-Projekt hervor und war für die von der freien Variante CyanogenMod unabhängige kommerzielle Vermarktung und Weiterentwicklung zuständig. Nachdem zunächst die dort angestellten Entwickler für das Betriebssystem entlassen wurden, stellte man Ende 2016 sämtliche Dienstleistungen für das Custom-ROM ein. Das macht die Weiterentwicklung des Systems durch die zahlreichen unabhängigen und freiwilligen Entwickler nahezu unmöglich.

### Ungewisse Zukunft

Das trifft besonders Besitzer von älteren Geräten, die ein aktuelles Android und dessen weiterentwickelte Funktionen nutzen wollen. Denn viele Hersteller machen in der Regel nur ein und höchstens zwei Versionssprünge mit, bei billigen Smartphones gibt es oft nicht einmal das. Die CyanogenMod-Community lieferte dagegen für viele beliebte Geräte auch nach drei und mehr Jahren noch Updates.

Einen Schlag bedeutet das Aus auch für die restliche Entwicklerszene von Custom-ROMs unter Android. Denn CyanogenMod war nicht nur das größte und umfangreichste Projekt, es war auch Grundlage und Anstoß für viele Alternativen sowie spezielle Anpassungen für eine große Anzahl exotischer Geräte. Aufgrund der vielen unterstützten Smartphones und des

meistens sehr stabilen Systems ist CyanogenMod auch bei vielen unserer Artikel die Empfehlung, wenn man vom Hersteller-ROM weg will oder Google von seinem Gerät verbannen möchte.

Die abgeschalteten Server haben auch für bestehende CyanogenMod-Nutzer spürbare Auswirkungen: Regelmäßige OTA-Updates wie bisher dürften kaum mehr möglich sein. Da sich auch die genutzten Domains im Besitz von Cyanogen befinden, müssen auch die URLs in der Update-Software auf den Geräten geändert werden; was unter Umständen ein manuelles Aufspielen eines neuen Images erforderlich macht.

Das CyanogenMod-Team zog aus dem Ende der Unterstützung Konsequenzen: Es forkte den Quellcode von CyanogenMod und benannte das acht Jahre alte Projekt in LineageOS um. Denn die Markenrechte liegen weiter bei Cyanogen, obwohl Gründer Steve Kondik das Unternehmen bereits im November 2016 verließ. Auf seinen Nutzernamen cyanogen gingen der Name für Projekt und Firma ursprünglich zurück. Lineage bedeutet so viel wie Abstammung, Geschlecht oder Stammbaum.

### Namenswechsel soll für Klarheit sorgen

Der neue Name soll mehr als ein Markenwechsel sein. So will man laut den Verantwortlichen mit dem neuen Fork zu den gemeinschaftlichen Anstrengungen der Basis zurückkehren, die CyanogenMod ausmachten, während man die professionelle Qualität und Verlässlichkeit erhalten will. Auch hatten die PR-Aktionen und markigen Sprüche von Cyanogen gegenüber Google für einige Verstimmung gesorgt, zumal kommerzielles Cyanogen OS und CyanogenMod häufig als ein und dasselbe System gesehen wurden.

Der Weg zu alter Größe wird jedoch steinig: Auf ihrer Webseite lineageos.org baten die Entwickler Anfang 2017 noch um

Unterstützung beim Aufbau einer professionellen Server-Infrastruktur. Auch sonst muss im Hintergrund vieles neu aufgebaut werden, damit die vielen Entwickler weiterhin ihren Teil zum Custom-ROM beitragen können. Mit dem Kompilieren von offiziellen Betriebssystem-Dateien hat LineageOS noch nicht begonnen. Unterdownload.cyanogenmod.org standen zumindest bis Redaktionsschluss aber noch alle Daten von CyanogenMod bereit. Wie lange, das bleibt ungewiss.

### Kein Android mehr von Cyanogen

Die Firma Cyanogen versucht davon unabhängig weiter zu agieren und mit Entlassungen aus der heftigen Krise zu kommen: Im Juli wurde einem Fünftel der Belegschaft gekündigt, im November wurde dann auch das Büro in Seattle geschlossen. Ein Strategiewechsel soll die Rettung bringen: Man werde kein komplettes Betriebssystem auf Android-Basis mehr entwickeln, hieß es. Vielmehr stehen nun Software-Module für Hardware-Hersteller im Fokus. Die nutzt allerdings bisher kein Anbieter. Hersteller, die bisher auf Cyanogen OS gesetzt haben, müssen sich Ersatz suchen. So wird Smartphone-Anbieter Wileyfox seine Geräte auf ein eigenes Android-ROM aktualisieren und dessen Entwicklung vorantreiben. Außer dem bekannten Namen bleibt also wenig vom ursprünglichen Gedanken erhalten, als alternatives Android-System Google Konkurrenz zu machen. (asp) **ct**



**Neuer Name und neues Logo:**  
Das CyanogenMod-Team macht unter dem neuen Namen LineageOS weiter, muss aber vieles neu aufbauen.





## ESET Mobile Security & Antivirus für Smartphones und Tablets

**Aktion:** Eset Mobile Security ist eine Art Allround-Security-Werkzeugset für Android-Geräte. Die Sicherheits-Suite schützt unter anderem vor Phishing und hilft, gestohlene oder verlorene Smartphones wiederzufinden.

**A**uf Smartphones und Tablets liegen viele vertrauliche Informationen wie Kontakte, E-Mails oder Passwörter – häufig ohne ausreichenden Schutz. Solche Daten sichert die App Eset Mobile Security vor verschiedenen Angriffsszenarien ab. Zum Umfang der Android-Software gehört beispielsweise ein Virens Scanner, der den lokalen Speicher sowie die von Webseiten heruntergeladenen Daten in Echtzeit überprüft – wichtig, wenn man beispielsweise APK-Installationsdateien aus unbekannten Quellen herunterladen möchte. Darüber hinaus blockiert Eset den Aufruf von Phishing-Seiten. Praktisch vor allem für ältere

Android-Geräte ist das Sicherheits-Audit: Es fasst in mehreren Punkten potenzielle Risiken zusammen – zum Beispiel, ob das Smartphone das Installieren von Apps abseits des Play Store erlaubt oder welche Anwendungen SMS verschicken dürfen. Zwar bietet Android von Haus aus einen Diebstahlschutz an, Eset geht aber über die Standard-Funktionen hinaus. So macht das Smartphone Fotos von einem potenziellen Dieb, wenn er zu häufig falsche Passwörter eingibt, und sperrt das Gerät, wenn die SIM-Karte ausgetauscht wird.

Viele Funktionen der im Google Play Store erhältlichen App sind kostenlos, manche erfordern ein Premium-Abo – etwa die

automatische Virensuche oder das Löschen der Smartphone-Daten aus der Ferne.

Leser von c't Android bekommen das Premium-Paket im Wert von knapp zehn Euro kostenlos und erhalten ein Jahr lang Updates dafür. Die Software kann über den c't-Link heruntergeladen werden. Der 1-Jahres-Zeitraum startet nach der Aktivierung mit dem eingetragenen Registrierungscode. Dieser ist bis zum 31. Juli 2017 gültig. Leser der digitalen Ausgabe erhalten den Aktivierungscode nach Zusage einer Kopie des Kaufbelegs per E-Mail an [android@ct.de](mailto:android@ct.de). (tir) **ct**

Download: [www.ct.de/wqu6](http://www.ct.de/wqu6)

# WIR TRINKEN DEN KAFFEE #000000.

ix. WIR VERSTEHEN UNS.



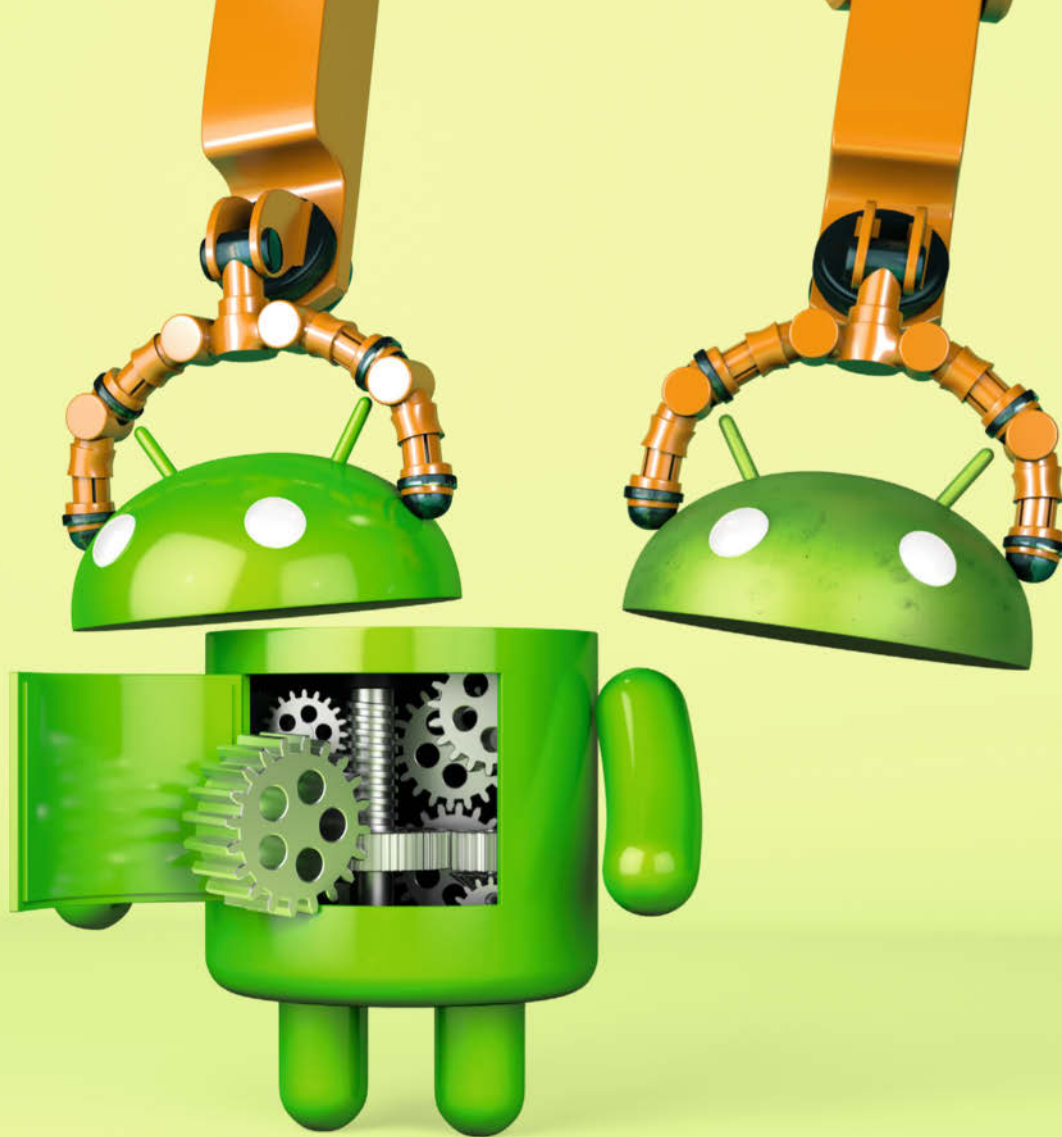
3 x als Heft

Jetzt Mini-Abo testen:  
3 Hefte + ix-Kaffeebecher nur 13,50 €  
[www.ix.de/test](http://www.ix.de/test)

ICH TRINKE  
DEN KAFFEE  
#000000.

Sie mögen Ihren Kaffee wie Ihr IT-Magazin: stark, gehaltvoll und schwarz auf weiß! Die ix liefert Ihnen die Informationen, die Sie brauchen: fundiert, praxisnah und unabhängig. Testen Sie 3 Ausgaben ix im Mini-Abo + ix-Kaffeebecher für 13,50 Euro und erfahren Sie, wie es ist, der Entwicklung einen Schritt voraus zu sein.

Bestellen Sie online oder telefonisch unter +49 (0)541 800 09 120.



Alexander Spier, Christian Wölbert

# Updates und Sicherheitspatches im Check

Immer wieder nagten Sicherheitsprobleme an Android. Doch mit zügigen System-Updates können die meisten Gerätehersteller nicht dienen. Monatliche Sicherheitspatches von Google sollen das Problem eindämmen, doch wie bei den großen Updates gibt es in der Umsetzung deutliche Unterschiede.

**A**ndroid-Updates bleiben für viele Nutzer ein hoffnungsloser Fall. Seit über einem Jahr gibt es nun bereits Android 6.0, doch gerade mal 25 Prozent der aktiv genutzten Geräte arbeiten mit der inzwischen nicht mehr al-

terneuesten Version. Auf über der Hälfte der Smartphones und Tablets laufen mindestens zwei Jahre alte Android-Versionen, und die am weitesten verbreiteten Varianten sind deutlich über ein Jahr und älter. Das Fehlen neuer Funktionen ist nur ein Teil

des Problems. Bedenklicher sind die ausbleibenden Sicherheits-Updates. Viele nicht einmal drei Jahre alte Modelle sind über die veraltete Browser-Engine in Android 4.3 und früher verwundbar. So können Angreifer Inhalte anderer Webseiten abgreifen,



Apps installieren und die Kamera anzapfen. Da auch Apps diese Komponente nutzen, um Webinhalte und Werbebanner anzuzeigen, kann das Smartphone auf vielen Wegen angegriffen werden. Für die Lücke gibt es weder Patches noch passenden Ersatz von Google. Hier würde nur eine neue Android-Version helfen, doch gerade für billige Geräte liefert die kaum ein Hersteller.

Die vor einem Jahr aufgetauchte „Stagefright“-Lücke hat Google zwar längst repariert, trotzdem fanden wir immer noch zahlreiche Geräte, bei denen die dazugehörigen Löcher nicht gestopft waren. Über diese Lücken kann ein Angreifer sich erhöhte Rechte verschaffen und Schadcode auf dem Gerät ausführen. Dafür reicht bei komplett ungepatchten Geräten sogar eine einzige MMS. Selbst wenn einem das alte Smartphone für den Alltag noch völlig ausreicht, muss man ein erhöhtes Risiko in Kauf nehmen oder zähneknirschend ein neues Gerät bestellen.

## Sicherheitspatch-Ebenen

Dass es keine gute Idee ist, Sicherheits-Updates nur mit neuen Android-Versionen auszuliefern, hat Google inzwischen eingesehen. Zwar schloss Google entdeckte Lücken schon immer zeitnah im Android-Sourcecode (AOSP), die Patches kamen aber oft erst mit der nächsten Android-Version beim Nutzer an. Der konnte auch nicht einfach nachvollziehen, welche Lücken gestopft wurden und welche nicht.

Seit einem Jahr veröffentlicht Google daher monatlich einen Sicherheitsbericht und führt darin die eingepflegten Patches auf. Für seine aktuellen Nexus-Geräte gibt man zeitgleich ein Update heraus und

bringt sie auf den neuesten Stand. Dazu nennt Google die „Android-Sicherheitspatch-Ebene“ mit dem Datum des Berichts. Deshalb kann jeder Nutzer einfach in den Einstellungen sehen, ob sein Gerät verwundbar ist. Das Patch-Level ist unabhängig von der Android-Version, die Sicherheitspatches werden in den Sourcecode aller Versionen ab Android 4.4 eingepflegt.

Prinzipiell steht diese Methode auch den anderen Herstellern offen. Bereits zuvor pflegten die Gerätehersteller oft Pflaster für Sicherheitslücken in ihre Software ein, ohne gleich eine neue Android-Version auszurollen. Aufwendige Anpassungen der Oberfläche und Herstellersoftware wie bei einer neuen Hauptversion konnte man so vermeiden. Durchschaubar war das mangels ausführlicher Changelogs jedoch oft nicht. So ließ ein Update zwischendurch zwar einen Fix vermuten, aber nicht immer verlässlich feststellen. Mittlerweile zeigt die große Mehrheit der Smartphones mit Android 5.0 und höher das Patch-Level in den Geräteinformationen an.

Generell auf monatliche Sicherheits-Updates hoffen darf man trotzdem nicht. Auch wenn sich viele Hersteller wie BlackBerry, HTC, Huawei, LG, Motorola, Samsung und Sony zu dem System bekennen, erhalten nur die aktuellen Top-Geräte tatsächlich regelmäßig Updates. Selbst hier kann es auch mal länger dauern, bis der Patch beim Nutzer ankommt. So übersprang das Samsung Galaxy S7 in Deutschland bei vielen Nutzern das Mai-Update, bei einigen blieb es sogar monatelang auf dem Stand vom April stehen.

Denn an der grundlegenden Problematik ändert die neue Methode nichts: Der Code muss unter Umständen angepasst und optimiert, das Update danach getestet und vom Provider freigegeben werden. Oft kommen zu den Google-Fixes auch noch weitere, vom Hersteller eingepflegte Fehlerbehebungen. Abgesehen von Samsung führt kein anderer Hersteller diese im Detail auf und selbst bei den Koreanern gilt das Security Bulletin nur für die Top-Geräte.

Ältere und billige Geräte dürfen weiterhin höchstens alle Jubeljahre einen Patch erwarten und drei Jahre nach dem Verkaufsstart ist für die meisten Geräte ganz Schluss. Google pflegt inzwischen das Nexus 4 und das Nexus 7 aus dem Jahr 2012 nicht mehr, obwohl auf beiden Android 5.1.1 läuft. Die theoretische Möglichkeit, Android 4.4 monatlich zu aktualisieren, nutzt kein Hersteller.

Um ohne Anzeige des Patch-Levels zu erkennen, ob ein Gerät auffällig ist, muss man auf Apps aus dem Play Store zurückgreifen. Der „Stagefright Detector“ von Zimperium, dem Entdecker der Lücke, etwa prüft auf diverse Patches. Der „Vulnerability Checker“ von Avira schaut auf eine Anfälligkeit durch Fernwartungstools. Ob die Android-Browser-Komponente WebView veraltet und angreifbar ist, prüft der UXSS-Test auf der c't-Webseite (siehe c't-Link).

Absolut verlässlich sind solche Tools nicht. Bei einigen Geräten wurden zum Beispiel bei aktivem WLAN offene Sicherheitslücken angezeigt, obwohl sie bereits eine aktuelle Android-Version besaßen. Zudem werden die Apps bei neuen Lücken häufig nicht erweitert. So patcht Google den mit dem Stagefright-Bug verbundenen Mediaserver inzwischen jeden Monat, die Tools zeigen aber nur ältere Fixes an.

## Update-Frust bleibt

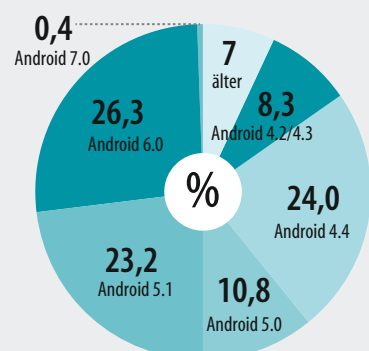
Die von uns in den vergangenen Jahren immer wieder bemängelte Zwei-Klassen-Gesellschaft bei System-Updates besteht weiterhin. Sieht man von den Nexus-Geräten von Google ab, dauert es wie gehabt meistens mehrere Monate, bis Android-Updates von den Herstellern ausgeliefert werden und neue Features zur Verfügung stehen. Je teurer und neuer das Gerät, desto größer die Chance auf ein zeitnahes Update. Nur Google verspricht für alle seine Geräte rasche System-Updates bis zu 2 Jahre nach der Veröffentlichung und stopft 3 Jahre lang Sicherheitslücken.

Andere Hersteller geben solche allgemeinen Garantien nicht ab, doch zumindest bei ihren Flaggschiffen halten sich Hersteller wie Samsung, Sony und HTC an einen ähnlichen Zeitraum. So haben die gut zwei Jahre alten Samsung Galaxy S5, Sony Xperia Z2 und HTC One M8 ein Update auf 6.0 erhalten. Die jeweiligen Vorgänger müssen mit Android 5.1 vorliebnehmen. Ein Galaxy S4 beispielsweise erhält aber durchaus noch Patches für Sicherheitslücken.

Bei der großen Masse der Geräte kommen diese hingegen immer noch nicht an, denn verpflichtend sind weder Sicherheits-Updates noch neue Android-Versionen. Je geringer die Gewinnmarge und exotischer ein Gerät, desto unwahrscheinlicher werden Updates. Die Macht, sie zu erzwingen, hätte Google durchaus: Für neu entwickelte Geräte fordert man von seinen Partnern mittlerweile eine Mindestversion, sodass es

## Aktueller Stand

Google zufolge läuft fast ein Viertel der aktuell genutzten Android-Geräte noch mit Version 4.4.



kaum noch Geräte mit Android 4.4 oder älter zu kaufen gibt. Viele Bestandteile des Systems (z. B. WebView, Google Verbindungsdienste oder die umfangreichen Play Dienste) werden längst über den Google Play Store gepflegt und benötigen keine langwierigen Updates mehr.

Mit Android One wurde zudem ein Programm für Billig-Smartphones aufgelegt, das das Update in die Hände von Google legt. Das folgt dann oft auch wenige Tage nach den Nexus-Geräten und meist vor den Top-Smartphones der großen Hersteller. Doch Modelle aus dem Android-One-Programm gibt es nur in Schwellenländern, in Deutschland sucht man vergeblich danach.

## Zukunftsaussichten

Bei aller berechtigten Kritik an Android, mit den Sicherheit-Patches geht Google zumindest in die richtige Richtung. Denn die lassen sich prinzipiell leichter pflegen und einbinden als die großen System-Updates. Dass die Hersteller das neue System unterstützen und zumindest für einige Geräte auch regelmäßig Updates veröffentlichen, ist ein gutes Zeichen. Durch das leicht abrufbare Patch-Level wirkt das Vorgehen nun deutlich transparenter und erhöht den Druck, den Patchday auch konsequent umzusetzen.

An der grundlegenden Problematik mit neuen Android-Versionen hat Google

aber wenig geändert. Aktualisierungen des Systems liegen weitgehend in den Händen der Hersteller und diese führen sie genauso langsam und stückhaft durch wie in den letzten Jahren. Auch die Abhängigkeit von den Providern konnte Google bisher nicht wesentlich reduzieren. Dass Android 7.0 Updates nahtlos einspielen kann und Apps danach deutlich schneller kompiliert, ist zwar erfreulich. Doch auch 2016 profitieren zunächst nur die Nexus-Geräte von der neuen Version. Erst zum Jahresende tröpfelten die Updates für einige Geräte nach. (asp) **ct**

Tests für Sicherheitslücken: [www.ct.de/wbnu](http://www.ct.de/wbnu)

## Android-Updates und die Sicherheit (Stand Juli 2016)

Wenn Sicherheitslücken bekannt werden, versprechen die Hersteller stets schnelle Updates. Unsere Stichprobe mit Geräten aus dem Redaktionsfundus zeigt allerdings: Nicht einmal die seit langem bekannten Stagefright- und UXSS-Lücken wurden überall behoben. Auch Updates auf neue Android-Versionen blieben oft aus. Von Android 7 können diese Geräte nur träumen.

			Update erhalten / nicht verwundbar			kein Update erhalten			offene Sicherheitslücke		
Hersteller	Modell	Verkaufsstart	Android 4.1 (Juli 2012)	Android 4.2 (November 2012)	Android 4.3 (Juli 2013)	UXSS-Lücke/WebView	Android 4.4 (Oktober 2013)	Android 5.0 (November 2014)	Android 5.1 (März 2015)	Stagefright-Lücken	Android 6.0 (Oktober 2015)
Asus	Memo Pad HD7	Jul 13		ab Werk						9 kritische Lücken	
Dell	Venue 8	Mrz 15					ab Werk			2 kritische Lücken	
Fairphone	Fairphone 1	Dez 13		ab Werk			Update angekündigt			2 kritische Lücken	
Google	Nexus 4	Nov 12		ab Werk							
Google	Nexus 10	Nov 12		ab Werk							
HTC	One	Feb 13	ab Werk								
Huawei	Ascend G7	Okt 14					ab Werk			1 kritische Lücke	
Motorola	Moto G	Nov 13			ab Werk					9 kritische Lücken	
Motorola	Moto G (2. Gen.)	Sep 14					ab Werk				
OnePlus	One	Apr 14					ab Werk				
Samsung	Galaxy S4	Apr 13		ab Werk							
Samsung	Galaxy S4 Active	Jul 13		ab Werk						9 kritische Lücken	
Samsung	Galaxy Note 10.1 2014	Nov 13			ab Werk						
Samsung	Galaxy Tab 3	Aug 13	ab Werk								
Sony	Xperia Z1 Compact	Jan 14			ab Werk						
ZTE	Grand Memo	Nov 13	ab Werk							9 kritische Lücken	

Stagefright-Lücken getestet mit dem Stagefright Detector von Zimperium (kostenlos im Play Store). UXSS-Test: <http://m.heise.de/uxss-check>. Details zu den Sicherheitslücken: siehe c't-Link



# NO ROCKET SCIENCE



Jetzt für  
12,90 €  
bestellen!



shop.heise.de/ix-cloud16 ✉ service@shop.heise.de  
Auch als eMagazin erhältlich unter: shop.heise.de/ix-cloud16-pdf

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten  
oder ab einem Einkaufswert von 15 €

 **heise shop**

shop.heise.de





Stefan Porteck, Alexander Spier

## Sieben Security-Suiten

**Android steht in Verruf, besonders einfach angreifbar zu sein. Jede Menge Security-Suiten im Play Store versprechen, das Smartphone bequem abzusichern, und das oft sogar kostenlos. Doch im Test ergeben sich nicht nur erhebliche Unterschiede bei der Erkennung von Schädlingen und Adware. Die Ergebnisse lassen auch Zweifel am tatsächlichen Nutzen der Tools aufkommen.**

**E**in falscher Klick hier: Die Festplatte ist verschlüsselt. Eine Unachtsamkeit dort: Die Kreditkartendaten sind geklaut. Erpressungs-Trojaner wie Locky und Co. haben in der Vergangenheit für so viele Schlagzeilen gesorgt,

dass praktisch jeder weiß, wie wichtig ein Virens Scanner ist.

Dieses Sicherheitsbedürfnis überträgt sich so langsam auch auf Nutzer von Mobilgeräten. Schließlich lagern darauf besonders sensible Daten: Fotos, Chats,

Adressbücher und vieles mehr. Nachdem Sicherheitslücken wie Stagefright und Warnungen vor gefälschten und schädlichen Apps Android den Ruf eines unsicheren Betriebssystems eingebracht haben, sind mittlerweile viele Nutzer bereit, für



einen Virens scanner oder eine Security-Suite ein paar Euro auszugeben.

Entsprechend tummeln sich in Googles Play Store etliche Sicherheits-Tools. Wir haben uns aus der Masse der Angebote die Sicherheits-Apps von Avast, Avira, G-Data, Kaspersky, McAfee sowie Norton herausgepickt und getestet, welchen Schutz sie bieten.

Alle Apps spüren eindeutige Malware ähnlich zuverlässig auf. Die regelmäßig von unabhängigen Instituten wie AV-Test durchgeführten Kontrollen ergeben Werte von deutlich über 98 Prozent bis 100 Prozent bei allen Kandidaten. Auch unsere eigenen Stichproben mit bekannten und offensichtlichen Schädlingen ergaben keine Auffälligkeiten. Eine gefälschte Pokémon-Go-App, die kostenpflichtige Premium-SMS verschickt, erkannten alle Suiten. Zudem mussten sie sich alle daran messen, ob sie den Download der standardisierten und harmlosen Eicar-Virus-Testdatei bemerken. Doch wie früh sie eingriffen, unterschied sich im Test erheblich: Die meisten warteten erst nach der Installation einer verdächtigen App zuverlässig vor dem Schädling.

Deutliche Abweichungen gibt es auch bei Apps, die mit Werbung nerven, aber im engeren Sinne keine Schadfunktionen mitbringen. Einige Tools warnten ausdrücklich

vor Apps mit dubiosen Werbenetzwerken, andere ignorierten die Programme völlig.

## Gemeinsame Sache

Reine Virens scanner findet man selten im Play Store. Bei unseren Testkandidaten handelt es sich vielmehr um Security-Suiten, die einen breiten Schutz vor verschiedenen Gefahren versprechen. Außer Virens scannern haben sie beispielsweise Web- und Phishing-Filter an Bord, die beim Surfen vor schädlichen Webseiten warnen. Ebenfalls zum Repertoire gehören bei einigen Probanden ein Diebstahlschutz nebst Ortung und Fernlöschen sowie Tools zum Schutz der Privatsphäre, die Apps mit einem Passwort sperren und Kontakte oder Nachrichten verstecken.

Viele dieser Funktionen erschienen uns überflüssig, denn sie lassen sich oft auch mit Android-Bordmitteln erledigen: Der Android-Gerätemanager erlaubt es von jedem PC oder Mobilgerät aus ein verlorenes Smartphone oder Tablet zu orten. Liegt es nur unter einem Stapel Zeitungen, hilft er bei der Suche, da selbst stummgeschaltete Geräte auf Knopfdruck klingeln. Sollte das Gerät wirklich verloren oder gestohlen sein, lässt es sich aus der Ferne löschen, damit

die Daten nicht in falsche Hände fallen. Erweiterte Funktionen wie die Überwachung der eingesetzten SIM-Karte, die ein weiteres Tool tatsächlich rechtfertigen würden, bekommt man meist nur im teuren Abo.

Lästig wird es, wenn die Suiten zusätzlich noch Akkuoptimierer und Reinigungswerkzeug sein wollen und Probleme suggerieren, wo meist gar keine sind. Der Nutzen solcher Tools hält sich in Grenzen und das Ergebnis wäre ebenfalls mit Bordmitteln erreichbar. Besonders auffällig ist dabei McAfee Mobile Security: Es pflanzt ungefragt ein Widget an den Bildschirmrand, das den „Systemstatus“ ausgibt.

Von den Funktionen zum Schutz der Privatsphäre hatten wir uns ebenfalls mehr versprochen. Seit Android 6 kann sich jeder Nutzer die Rechte einer App anzeigen lassen und bei Bedarf einzelne davon wieder entziehen. Letzteres schafften unsere Testkandidaten nicht. Häufig sind auch die Einschätzungen des Risikos eher irreführend, mal zu lasch und mal deutlich übertrieben. Zudem warnte uns keines der getesteten Tools vor Apps, die sich als Geräte-Administratoren registriert haben oder vor Apps mit Nutzerdatenzugriff. Beide Rechte sind problematisch, weil sie Apps ermöglichen, sensible

## Sicherheitsfunktionen von Android

Android hat einige Maßnahmen in petto, um die Nutzer vor Schädlingen zu schützen. Eine davon greift schon, bevor Apps überhaupt installiert werden: Google scannt regelmäßig alle im Play Store angebotenen Anwendungen. Sofern sich hier Auffälligkeiten zeigen, werden die Verdächtigen näher untersucht und gegebenenfalls aus dem Store entfernt. Entsprechend gering ist die Gefahr, sich mit einer App aus dem offiziellen Store einen gefährlichen Schädling einzufangen.

Dieser Schutz greift natürlich nicht, wenn man in den Sicherheitseinstellungen des Mobilgeräts die Installation von Apps aus Fremdquellen aktiviert und sie per Sideload installiert. Apps sollten dann wirklich nur aus vertrauenswürdigen Quellen wie Amazon installiert werden. Wer Fremdquellen nutzt, sollte in den Google-Einstellungen unter Sicherheit die Option „Gerät nach Sicherheitsbedrohungen durchsuchen“ aktivieren. Dieser Miniscanner untersucht installierte Apps regelmäßig auf bekannte Signaturen. Er erreicht aber nicht die Erkennungsleistung der Virens scanner.

Selbst wenn Malware all diese Mechanismen umgangen hat, kann sie – anders als auf dem PC – bei Weitem nicht machen was sie will: Jede App läuft unter Android in einer Sandbox.

Der Zugriff auf kritische Systemfunktionen und -komponenten erfolgt nicht direkt, sondern nur über Androids Programmierschnittstellen. Um beispielsweise eine SMS verschicken zu können, muss die App bei der Installation das entsprechende Recht vom Nutzer erhalten. Seit Android 6 alias Marshmallow werden die Rechte einmalig bei der ersten Nutzung erfragt. Wer nicht blind jede Anfrage abnickt, läuft eigentlich kaum Gefahr, dass eine Malware heimlich Premium-SMS verschickt oder unbemerkt Abzocknummern anruft.

Darüber hinaus schottet die Sandbox die Speicherbereiche aller Apps voneinander ab. Eine Anwendung hat nur auf ihr eigenes Verzeichnis Zugriff. Das verhindert Manipulationen an Systemdateien und sorgt dafür, dass Schädlinge anderen Apps keine sensiblen Daten wie Passwörter oder Kreditkartennummer klauen können. Gleiches gilt für den Arbeitsspeicher: Jede App darf nur den für sie reservierten Bereich nutzen.

Richtig gefährlich wird es für den aufmerksamen Nutzer also nur dann, wenn der Schädling tatsächlich Lücken in Android ausnutzt. Hier helfen wie bei allen anderen Systemen nur regelmäßige Sicherheitspatches, die Google und hoffentlich die Hersteller regelmäßig ausliefern.

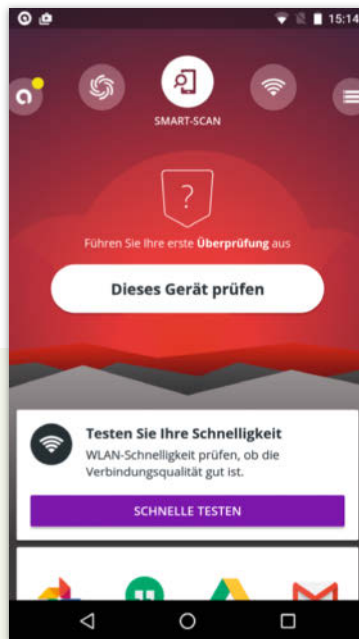


## Avast Mobile Security & Antivirus

Als einzige Security Suite im Vergleich gibt es die App von Avast ausschließlich kostenlos und ohne fremde Werbeanzeigen. Dafür trommelt Avast auf der Oberfläche recht penetrant für die anderen Apps des Unternehmens. Das Hauptfenster wartet mit vermeintlich vielen Funktionen auf, doch etliche Schaltflächen führen lediglich zum Play Store. Erst nach der Installation der entsprechenden Zusatz-App kann man Funktionen wie den Diebstahlschutz benutzen.

Das Erkennen von Malware und schädlichen Apps funktioniert ab Werk. Der Web- und der Echtzeitschutz überzeugten uns jedoch nicht. So schlug Avast weder beim hemmungslosen Bannerklicken auf Porno- und Warez-Seiten an, von denen man häufig auf den Play Store umgeleitet wird, um eine dubiose App zu installieren. Auch wurden wir nicht daran gehindert, den Eicar-Testvirus herunterzuladen.

Selbst als wir die Eicar-Datei mit einem Datei-Manager von Eicar.zip in Eicar.apk umbenannten und anschließend zu installieren versuchten, schlug der Wächter nicht an. Erst als wir einen Systemscan von Hand starteten, wurde der Testvirus gefunden. Gemessen am nicht hundertprozentigen Schutz des permanenten Wächters fanden wir den Speicherhunger der App zu hoch: Auf unserem Testgerät knappste Avast mit drei bis vier laufenden Diensten durchschnittlich 70 bis 290 MB vom Arbeitsspeicher ab.



Wie die anderen Tools im Test soll auch Avast beim Schutz der Privatsphäre helfen. Dafür findet sich unter dem Menüpunkt „Datenschutz“ ein Tool, das Apps nach ihren Berechtigungen scannt. Im Anschluss werden alle installierten Apps gestaffelt nach der Anzahl der von ihnen eingeforderten Rechte aufgelistet.

Leider gibt Avast nicht an, welche Rechte davon problematisch sind und welche nicht. Stattdessen lässt einen die App mit dem mulmigen Gefühl im Regen stehen, vermutlich viele kritische Apps zu nutzen. Der Datenschutz-Scanner prüft zusätzlich, zu welchem der unzähligen Werbenetzwerke einzelne Apps Daten übermitteln. Davon ist in der Ergebnisliste jedoch nichts zu sehen. Hat man eine App als Datenschleuder im Verdacht, muss man sie auswählen und bekommt erst in der Detailansicht die damit verknüpften Werbenetzwerke angezeigt. Besonders zuverlässig scheint die Analyse nicht zu sein: Die kostenlose Version von Shazam nutzt nachweislich mehrere Werbepartner, wurde von Avast aber als sauber klassifiziert.

- ↑ kostenlos
- ↓ unübersichtliche Oberfläche

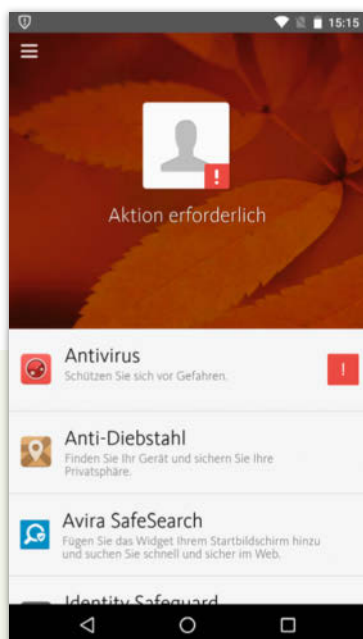
## Avira Antivirus Security

Die Security-Suite von Avira trommelt ähnlich wie Avast mit ihrem vermeintlich riesigen Funktionsumfang. Doch auch hier finden sich Menüeinträge, die keine Funktion bieten, sondern lediglich auf den Play Store umleiten und die Installation einer weiteren App erfordern. Zudem nervt das Tool schon beim ersten Aufruf nach der Installation mit nicht eindeutig als solcher gekennzeichneten Werbung, die sich zwischen die Avira-eigenen Tools mischt.

Wie bei Avast konnten wir auch hier die Eicar-Viren im Dateimanager umbenennen und die Installation starten, ohne dass Avira sich meldete. Unter unseren Stichproben fand der Scanner beim manuellen Aufruf aber diverse Adware-verseuchte Apps, die andere Scanner durchrutschen ließen, und warnte als einziger auch schon vor deren APK-Dateien.

Um Datenschutz kümmert sich Avira ebenfalls: Die entsprechende Funktion heißt „Privacy Advisor“ und soll vor Apps schützen, die Zugriff auf viele oder sensible Nutzerdaten haben. Dahinter verbirgt sich ein Scanner, der abklopft, welche Rechte einzelne Apps beim Betriebssystem angefordert haben.

Die Ergebnisse kategorisiert Avira nach geringem, mittlerem und hohem Risiko. Welche Zugriffsrechte als problematisch angesehen werden und welche weniger, bleibt jedoch im Verborgenen. Auch wird den Nutzern keine Hilfe gegeben, die potenziellen Risiken bestimmter Rechte einzuschätzen.



In der Praxis ist der Privacy Advisor deshalb eher nutzlos: Er stuft offenbar aufgrund von Zugriffen auf den externen Speicher und die Nutzerkontenverwaltung unter anderem den Firefox-Browser und die c't-App als Apps mit hohem Risiko ein. Unbedarfte Nutzer dürften solche falschen Warnungen eher verunsichern als beruhigen. Da Avira keine Rechteverwaltung oder eine Verknüpfung auf die entsprechende Funktion von Android bereithält, fühlt man sich mit den vermeintlichen Sicherheitsrisiken im Stich gelassen.

Auf Wunsch untersucht der „Identiy Safeguard“, ob die Kontakte auf dem Gerät kompromittiert wurden. Dabei vergleicht es die Mail-Adresse mit im Internet aufgetauchten Listen von gestohlenen Zugangsdaten anderer Anbieter.

Im Abo kostet die App von Avira knapp 8 Euro im Jahr, dafür gibt es den Web-Filter, häufigere Updates und einen erweiterten Support. Die Grundfunktionen lassen sich auch in der kostenlosen Version uneingeschränkt nutzen.

- 👆 findet viel Adware
- 👇 Privacy Advisor warnt auch bei sicheren Apps

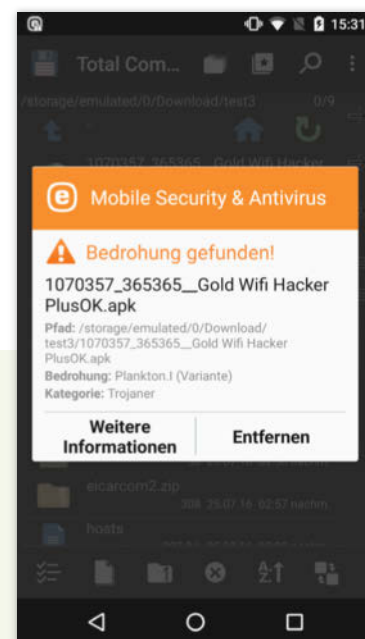
## Eset Mobile Security

Die Erkennungsleistung ist zwar bei allen Probanden prinzipiell nicht schlecht, doch Eset warnte als einziger rechtzeitig vor der Installation von Schädlingen, scannte den Speicher gründlich oder ordnete Gefahren sinnvoll ein.

Eset schiebt sich vor den eigentlichen Paket-Installer und überprüft die Apps auf Bedrohungen, ehe sie aufs Gerät gelangen. Anders als etwa bei Norton funktioniert das problemlos: Bei als sauber erkannten Apps gibt es eine kurze Bestätigung, bei Schädlingen eine deutliche Warnung. Dazu erhält man hilfreiche Infos über die Art der Bedrohung. Die Viren und Trojaner aus unserem Arsenal sowie den EICAR-Testvirus fing die Software zuverlässig ab. Auch über den Browser heruntergeladene und von Hand aufs Gerät geschobene APK-Dateien erkannte Eset zügig und warnte per Popup-Dialog.

Apps aus der Grauzone, die potenziell schädlich sein können, wurden erst nach der Installation bemängelt. Beim Start erscheint auch bei diesen ein eindeutiger Warndialog, über den sich die App entfernen lässt. Anders als die Konkurrenz warnt die Suite in der Bezahlversion deutlich davor, wenn die Installation aus unbekannten Quellen aktiviert wurde – immerhin ein Haupteinfallstor für Schädlinge bei Android.

Seine Kernaufgabe erfüllt Eset von den hier getesteten Sicherheitslösungen am besten. Hinweise auf Datenschutzprobleme sind vergleichsweise dezent und ersparen dem Nutzer unnötige Panik. Allerdings muss



er selber entscheiden, ob eine allzu neugierige App ein Problem sein könnte, denn ein Rating von grenzwertigen Apps gibt es nicht.

Der Phishing-Filter sprang beim Abgrasen von bekannten Malware-Domains und dubiosen Werbeseiten vergleichsweise selten an. Er arbeitet nur mit dem vorinstallierten Browser und mit Google Chrome. Ab Android 6 kommt die Suite gar nicht mehr mit dem Chrome-Browser zurecht, was bislang für keinen Konkurrenten eine Hürde darstellte.

Mit 125 MByte Speicherbedarf ist die Suite vergleichsweise genügsam, Auswirkungen auf Performance und Akku-Laufzeit konnten wir keine feststellen. Die Antivirus-Funktionen sind kostenlos, inklusive des Echtzeit-Scanners. Für Zusatzfunktionen wie automatische Updates und Scans, Diebstahlschutz, Phishing-Filter und Anruferblockierung werden 10 Euro im Jahr fällig.

- 👆 warnt früher als andere
- 👆 genügsam
- 👇 schwacher Browser-Schutz

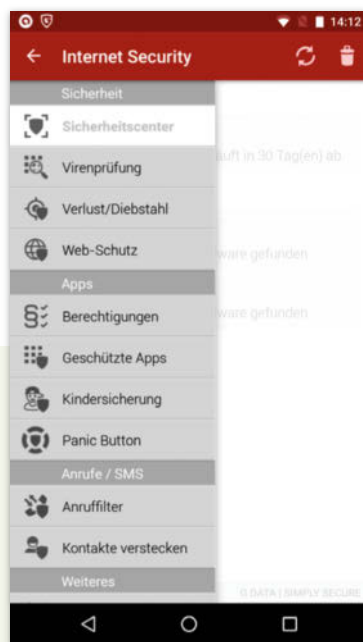
## G-Data Internet Security Light

Die Security-Suite von G-Data geht nicht so marktschreierisch zu Werke wie die anderen Testkandidaten, deren Oberfläche fast wie die Titelseite einer Boulevardzeitung aussehen, und versuchen, dem Nutzer möglichst markant ins Auge zu fallen. Stattdessen wirkt die Oberfläche hier angenehm ruhig, aufgeräumt und sieht mit ihrem Material Design übersichtlich aus.

Über das App-Menü am linken Bildrand erreicht man mit wenigen Fingertipps alle wichtigen Funktionen. Löblich: Bis auf den SMS-Schutz funktionieren alle Programmooptionen, ohne dass weitere Apps nachinstalliert werden müssen. Da Android seit Version 4.4 keine Standard-SMS-App mehr enthält, gestaltet sich der Zugriff auf die Nachrichten offenbar schwierig. G-Data bietet wie auch einige andere Hersteller aber einen eigenen Messenger an.

Beim Privatsphärenschutz hat das Tool ebenfalls die Nase vorn: Statt plump anhand der angeforderten Rechte zu entscheiden, ob eine App gut oder böse ist, listet G-Data die Berechtigungen selbst auf und zeigt an, wie viele Apps davon Gebrauch machen. So können Nutzer das tatsächliche Bedrohungspotenzial viel besser einschätzen.

Andere Funktionen der G-Data-Suite haben wir bei den Mitbewerben nicht gefunden. So gibt es einen Panic-Button, der ein Widget auf dem Homescreen erzeugt. Dieser ermöglicht dem Nutzer, in einer Notsituation mit einem Fingertipp per SMS



oder Mail den eigenen Standort an einen vorab festgelegten Kontakt zu verschicken. Apropos Kontakte: Die G-Data-Suite erlaubt es, Kontakte vor den Augen Neugieriger zu verstecken.

Der Speicherhunger ist mit rund 20 bis 80 MByte ebenfalls geringer als bei den anderen Sicherheits-Apps im Test. Doch der Schutz vor Malware klappte auch bei G-Data nicht perfekt. Obgleich die Signaturen sich nicht änderten, erkannte die App bei einem Scan einen Schädling, bei einem direkt darauffolgenden zweiten Durchlauf blieb er dagegen unentdeckt. Das permanente Überwachen funktionierte ebenfalls nicht zuverlässig: Auch hier konnten wir Testviren anstandslos herunterladen und mit dem Paket-Installer von Android öffnen, ohne dass die Security-Suite uns daran hinderte. Für das Jahresabo will G-Data 19 Euro per In-App-Kauf und bietet dafür als einziger sogar einen Kinderschutzmodus. Nach 30 Tagen Probezeit bleibt in der kostenlosen Version nur der Virenschutz bestehen.

- ↑ übersichtlich und geringerer Speicherhunger
- ↑ flexibel anpassbar

## Kaspersky Internet Security

Die Suite von Kaspersky enthält einen On-Demand-Scanner, einen Anruf- und SMS-Filter sowie einen Diebstahlschutz. Nervig fanden wir die häufig wiederholte Bitte um Bewertung im Play Store und um Weiterempfehlung. Die Oberfläche wirkt aufgeräumt, doch Einstellungen und Funktionen sind dahinter wild verteilt.

Der Virens scanner hielt uns auch im Echtzeitmodus und mit aktivem Webfilter nicht davon ab, die Eicar-Testdateien herunterzuladen. Erst beim Versuch, Pakete zu installieren oder auf eine Datei zuzugreifen, wurden problematische Elemente wahrgenommen. Das ist jedoch immer noch mehr, als fast alle anderen von uns getesteten Tools tun. Darüber hinaus laufen periodisch Scans im Hintergrund, deren Häufigkeit aber nicht konfiguriert werden kann. Zudem wird nur im Protokoll vermerkt, wenn dabei ein Schädling erkannt und verschoben wurde. Diese Berichte muss man umständlich in den erweiterten Einstellungen suchen.

Bekannte Schädlinge blockierte die Suite zuverlässig. Unsere Apps mit Adware ließ Kaspersky gewähren, obwohl explizit die Suche danach aktiviert war. Zusätzliche Filterkategorien gibt es nicht, ebenso keine Warnung vor problematischen Zugriffsrechten oder eine Einschätzung zu potenziell gefährlichen Apps.

Der Web-Filter unterstützt ausschließlich den Chrome-Browser. Die Filterleistung ist auch hier zwiespältig. Einerseits blockierte die App be-





kannte Seiten mit Schädlingen und leitete auf eine harmlose lokale Warnseite um. Andererseits schlug der Filter bei einschlägiger Pop-up-Werbung mit gefälschten Virenwarnungen und anzüglichen Versprechungen nach Übermittlung der Mail-Adresse niemals an.

Kaspersky Internet Security greift sich im Schnitt etwas über 100 MByte Arbeitsspeicher. Lief ein Scan im Hintergrund, reagierte das Smartphone behäbig. Ansonsten war vom Tool wenig zu bemerken, der Energiebedarf blieb im Rahmen von herkömmlichen Hintergrund-Apps. Als einzige Lösung bietet Kaspersky eine Smartwatch-App zur Fernsteuerung. Von der Uhr aus können damit Scans und Updates sowie ein Signalton auf dem Telefon ausgelöst werden. In der eingeschränkten Version ist Internet Security von Kaspersky kostenlos und werbefrei. Dann fehlen jedoch der Web-Filter, der Echtzeitscanner und die Möglichkeit, Kontakte vor anderen Nutzern zu verbergen. Mit 11 Euro pro Jahr gehört das Abo noch zu den günstigeren.

- ⬆ greift früher als andere ein
- ⬇ wenige Informationen zu Bedrohungen

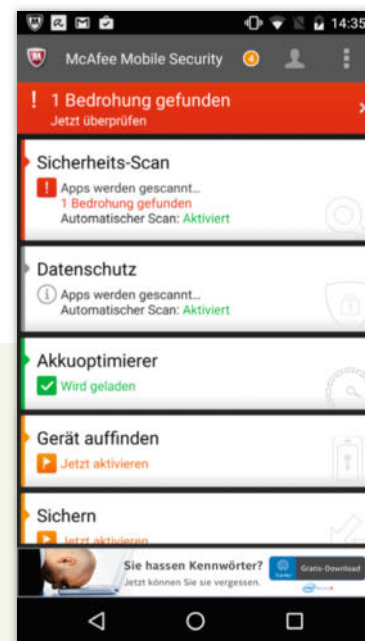
## McAfee Mobile Security

Auch McAfee Mobile Security verhinderte nicht den Download des Testvirus. Beim ersten Scan-Durchlauf nach der Installation ignorierte McAfee zudem alle im Download-Ordner vorhandenen Testdateien. Der Echtzeitscanner reagierte, wenn überhaupt, mit mehreren Minuten Verzögerung und verhinderte nicht das Ausführen der Schaddateien. Bei manuellen und automatischen Durchläufen wurden die problematischen Dateien immerhin erkannt.

McAfee gibt daher oft erst eine Warnung aus, nachdem die App installiert wurde. Das macht das Programm schnell und mit Details zur Art des Virus. Die verantwortliche APK-Datei wird jedoch nicht vom Gerät gelöscht. Auch McAfee ließ Apps mit Adware gewähren.

Das Programm warnt vor problematischen Zugriffsberechtigungen anderer Apps. Die grobe Einteilung lässt allerdings wenig Rückschlüsse auf die tatsächliche Gefährdung zu. Zusätzlich bewertet McAfee Anwendungen nach eigenen Kriterien und empfiehlt nur als vertrauenswürdig eingestufte Apps zu behalten. Doch schon die Telefon-App und der SMS-Messenger von Google werden als mittlere Gefährdung eingestuft und sind nicht als vertrauenswürdig gekennzeichnet. Bei vielen verbreiteten Apps wie Chrome oder Facebook fehlen die Einstufungen komplett.

Der Web-Filter funktioniert nur in Chrome. Bekannte Angreifer blockierte er zuverlässig und filterte auch Seiten in Inkognito-Tabs. Bei



pozenziell gefährlicher und nerviger Werbung schlug er deutlich häufiger an als etwa Kaspersky, verhinderte aber auch nicht jede nervige Umleitung mit gefälschten Virenwarnungen und teuren SMS-Abos.

Eher fragwürdig im Sinne des Datenschutzes ist die Option, Kontakte, SMS und Anruflisten zusätzlich bei McAfee zu sichern. So sollen bei Verlust oder Diebstahl die Daten nicht verloren gehen. Zahlende Kunden dürfen zusätzlich bis zu 2 GByte Bilder und Videos sichern.

Mit im Schnitt 135 und maximal 180 MByte knabberten die 5 Prozesse von McAfee merklich am Speicher. Zudem möchte die App dauerhaft im Hintergrund arbeiten dürfen und sich von Androids Stromsparmechanismus ausnehmen lassen. Auffällig hoch war der Energiebedarf dennoch nicht. Für Werbefreiheit, Medien-Backup und Telefon-Support verlangt McAfee happige 30 Euro im Jahr. Die umfangreichen restlichen Funktionen sind auch ohne Abo nutzbar, lediglich ein kleines Banner im Hauptmenü muss man dafür in Kauf nehmen.

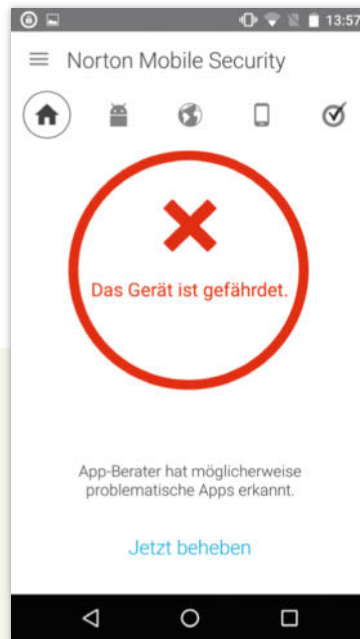
- ⬇ verwirrende App-Einstufungen
- ⬇ überladen mit Funktionen

## Norton Mobile Security

Der Systemscan von Norton Mobile Security arbeitet zwar schnell, findet aber nur bereits installierte Apps und bemängelt keine APK-Dateien von Schädlingen im internen Speicher. Wonach gesucht wird, lässt sich nicht konfigurieren, nur die Häufigkeit der automatischen Suche ist änderbar. Auch Norton greift erst ein, wenn die App bereits installiert wurde und das zudem recht zögerlich, sodass man die Meldung schon mal aus Versehen wegdrückt. Die APK-Datei löscht er nach der Erkennung nicht. Trotzdem genehmigt sich das Programm üppi-ge 100 bis 210 MByte RAM.

Eicar ließ sich problemlos herunterladen und schädliche Dateien sich öffnen, ohne dass der Scanner eingriff. Norton bietet sich zwar als Handler von APK-Dateien an, um Apps vor der Installation automatisch zu durchsuchen, doch das klappte auf unserem Testgerät mit aktuellem Android nicht mal ansatzweise. Weder kam dabei ein Scan-Ergebnis heraus, noch installierte er anschließend die App. Immerhin warnte Mobile Security als eines von wenigen Tools im Testfeld sofort vor Adware-verseuchten Apps.

Die Einschätzung der App-Zugriffsrechte ist mitunter irreführend. So warnt Norton zum Beispiel vor den harmlosen Apps Here Maps und Firefox – nicht etwa weil Werbung in den Programmen steckt, sondern weil die Datennutzung und der Energiebedarf höher seien als normal. Bei Shazam erkennt Norton zwar das Werbenetzwerk und bemängelt ein Daten-



schutzrisiko, stuft die App aber trotzdem als harmlos ein. Ohne Hintergrundwissen ist das keine große Entscheidungshilfe. Dennoch hilft Mobile Security durch die detailreichen Angaben bei der Analyse besser als die meisten anderen Tools. Die Einstufungen blendet das Tool auf Wunsch im Play Store ein.

Der Webfilter unterstützt außer Chrome auch andere populäre Browser wie Firefox und Opera. Bekannte Bedrohungen blockt Norton und informiert detailreich über die möglichen Probleme. Auffällig war allerdings, dass er diverse von Google Safe Browsing als Angreifer identifizierte Seiten in unseren Stichproben nicht bemängelte. Nervige und irreführende Werbung konnte ungehindert Pop-ups öffnen und zum Beispiel den Vibrationsmotor ansprechen. Mit fast 31 Euro beim In-App-Kauf ist das Jahresabo von Norton das teuerste im Vergleich. Die Premium-Variante darf dabei auf mehreren Geräten eingesetzt werden. Der kostenlosen Version fehlen App-Berater, Web- sowie Malware-Filter und viele Diebstahlschutz-Funktionen.

- ↑ umfangreiche App-Analyse
- ↓ kein Echtzeitscanner

## Security-Suiten für Android

Produkt	Mobile Security & Antivirus	Antivirus Security	Mobile Security	Internet Security Light	Internet Security	Mobile Security	Mobile Security
Hersteller	Avast Software	Avira	Eset	G Data Software AG	Kaspersky Lab	McAfee (Intel Security)	Norton
Version / Sprache	5.3.1 / deutsch	4.5 / deutsch	3.3.25.0 / deutsch	25.10.11.2 / deutsch	11.11.4.761 / deutsch	4.6.1.1156 / deutsch	3.15.0.3131 / deutsch
<b>Funktionsumfang</b>							
Virens Scanner	✓	✓	✓	✓	✓	✓	✓
Web-Filter / Firewall	✓ / ✓ <sup>3</sup>	✓ <sup>1</sup> / –	✓ <sup>1</sup> / –	✓ <sup>1</sup> / –	✓ <sup>1</sup> / –	✓ / –	✓ <sup>1</sup> / –
Gerät orten	– <sup>2</sup>	✓	✓ <sup>1</sup>	✓ <sup>1</sup>	✓	✓	✓ <sup>1</sup>
Gerät aus der Ferne sperren / löschen	– <sup>2</sup> / – <sup>2</sup>	✓ / ✓	✓ / ✓	✓ <sup>1</sup> / ✓ <sup>1</sup>	✓ / ✓	✓ / ✓	✓ / ✓ <sup>1</sup>
Apps sperren	✓	– <sup>2</sup>	–	✓	–	✓	–
App-Berechtigungen anzeigen / verwalten	✓ / ✓ (eingeschränkt)	✓ / –	✓ <sup>1</sup> / –	✓ / –	– / –	✓ / –	✓ / –
Anrufe/SMS blockieren	✓	✓	✓	– <sup>2</sup>	✓	✓	✓ <sup>1</sup>
Besonderheiten	RAM und Speicher bereinigen	Check für Android-Lücken und kompromittierte Daten	Überwachung von Android-Einstellungen	Kindersicherung, Kontakte ausblenden	Kontakte ausblenden	Backup von Kontaktdaten, „Akkuoptimierer“, RAM und Speicher bereinigen	Backup von Kontaktdaten, App-Risiko-einschätzung im Play Store
<b>Bewertung</b>							
Funktionsumfang / Schutzwirkung	○ / ○	○ / ⊕	⊕ / ⊕⊕	⊕ / ⊕	○ / ⊕	⊕ / ○	○ / ○
Bedienung / Anpassbarkeit	○ / ⊖	○ / ⊖	⊕ / ⊕	⊕ / ⊕	○ / ○	○ / ○	⊕ / ⊖
kostenlose Version / Werbung	✓ / –	✓ / ✓	✓ / –	✓ / –	✓ / –	✓ / ✓	✓ / –
Abo / Preis	kostenlos	✓ / 8 € pro Jahr	✓ / 11 € pro Jahr	✓ / 19 € pro Jahr	✓ / 11 € pro Jahr	✓ / 30 € pro Jahr	✓ / 31 € pro Jahr
<sup>1</sup> nur in der kostenpflichtigen Version <sup>2</sup> zusätzliche App <sup>3</sup> nur auf Geräten mit Root-Rechten							
⊕⊕ sehr gut    ⊕ gut    ○ zufriedenstellend    ⊖ schlecht    ⊖⊖ sehr schlecht    ✓ vorhanden    – nicht vorhanden    k. A. keine Angabe							

Daten mitzulesen. Außerdem lassen sich derlei Apps schwerer deinstallieren. Das gilt allerdings auch für die getesteten Sicherheitslösungen selbst. Die haben notwendigerweise Zugriff auf alle Aktivitäten des Nutzers.

Für unsere Tests haben wir die Sicherheits-Apps auf verschiedenen Smartphones der Nexus-Serie ausprobiert. Sie laufen mit einem aktuellen Vanilla-Android, was ausschließt, dass Betriebssystemanpassungen der Smartphone-Hersteller mit den Scannern ins Gehege kommen. Zudem bieten Nexus-Geräte einige für Entwickler praktische Funktionen, die aber auf Kosten der Systemsicherheit gehen, beispielsweise das Entsperren des Bootloaders oder USB-Debugging über die Android Debug Bridge (ADB). Beides erlaubt den Zugriff auf sensible Nutzerdaten und Speicherbereiche des Betriebssystems. Hier hätten wir uns von einer der Security-Suiten eine Warnung gewünscht. Auch als wir in den Einstellungen die Installation von Apps aus beliebigen Quellen erlaubten, blieben unsere Testkandidaten still.

## Fazit

Alle Security-Suiten versprechen ein Rundum-sorglos-Paket in Sachen Sicherheit. Was gut gemeint ist, dürfte viele Anwender überfordern: Die Oberfläche mancher der Testkandidaten sieht aus, als hätte man wahllos eine möglichst große Anzahl von

Schaltflächen mit einer Schrotflinte aufs Display geschossen. Diese Unübersichtlichkeit schafft kein Vertrauen – insbesondere, wenn viele der angepriesenen Zusatzfunktionen sich erst nutzen lassen, wenn man dafür weitere Apps des Herstellers installiert. Davon dürften die meisten Nutzer wohl aber keinen Gebrauch machen, denn viele Suiten reißen sich schon alleine bis zu 200 MByte des Arbeitsspeichers dauerhaft unter den Nagel.

Viele der angebotenen Funktionen lassen sich zudem mit schlankeren Apps genauso gut erledigen – beispielsweise eine App- oder Telefonsperre mittels PIN. Andere Dreingaben wie der Diebstahlschutz funktionieren zwar gut, sind aber dem Schutz der Privatsphäre nicht gerade förderlich: Statt den Anbietern der Security-Suiten Zugriff auf die eigenen Standortdaten zu gewähren, kann man ein verlorenes oder geklautes Smartphone von jedem beliebigen Computer aus mit dem Android-Gerätemanager genauso wirkungsvoll orten, sperren und zum Schutz sensibler Daten löschen.

Funktionen wie das Aufspüren datenhungriger Apps gelingen mit Bordmitteln sogar besser: Mit Ausnahme von G-Data und Norton zählen die Suiten oft nur die Anzahl der eingeforderten Rechte, brandmarken damit absolut harmlose Apps und sorgen so für unnötige Verunsicherung.

Bei ihrer eigentlichen Aufgabe – dem Aufspüren von Malware – schnitten unse-

re Probanden mittelmäßig ab. Ihre Signaturen mögen zwar bei einem manuell gestarteten Systemscan eine hohe Erkennungsrate haben, das reicht aber nicht aus, wenn die Wächter beim Umgang mit gefährlichen Apps zu spät oder überhaupt nicht Alarm schlagen. Die Mobile Security von Eset warnte als einzige bei heruntergeladenen Dateien sofort. Erst nach der Installation von schädlichen Apps griffen alle wirklich ein, nur Eset und Kaspersky fingen schon beim Aufspielen die Schädlinge ab. Avira warnte als einziger umfangreich vor APKs von werbeverseuchten Apps. Wer sich dagegen einen großen und anpassbaren Funktionsumfang in Kombination mit einer übersichtlichen Oberfläche wünscht, sollte einen Blick auf die Suite von G-Data werfen. Perfekten Rundumschutz bietet allerdings keine.

Unterm Strich gaukeln die Tools eine trügerische Sicherheit vor: Die Schutzmechanismen des Android-Systems und die Kontrollen im Play Store reichen in den meisten Fällen völlig aus. Denn wer keine Apps aus Drittquellen installiert und sich vor der Installation deren eingeforderte Rechte anschaut, geht ohne einen Virens Scanner kein nennenswertes Risiko ein. Größtes Einfallstor unter Android bleiben Bugs im Betriebssystem oder in installierten Apps. Hier sind aber die Hersteller gefragt, zeitnah Updates zu liefern und nicht die Verantwortung auf die Nutzer abzuwälzen. (asp) 





Michael Spreitzenbarth

## Schädlinge aufspüren und loswerden

Smartphones stellen traumhafte Angriffsziele dar: Die meisten tragen en masse kritische Daten und sind nonstop online. Dass das eigene Gerät ins Visier von Schädlingen gerät, ist also gar nicht unwahrscheinlich. Doch wie erkennt man eine Infektion und beseitigt sie?

Oft verwenden Nutzer ihre Smartphones sorgloser als ihre PCs. Dabei haben Kriminelle schon lange erkannt, welche Chancen diese Endgeräte für sie bieten: Egal, ob privat oder in der Firma genutzt – sie beherbergen sensible und aus Sicht Krimineller wertvolle Daten. Gleichzeitig fehlen meist Schutz- und Detektionsmaßnahmen wie Antiviren-Software oder die Einbindung von Proxies. Die Angreifer haben es somit ungleich leichter, sich unbemerkt Zugriff zu verschaffen.

Bedrohungen für Android können generell in zwei Klassen kategorisiert werden: webbasierte und applikationsbasierte. Die webbasierten Bedrohungen zielen auf Mobil-Browser und deren fehlerhafte Implementierungen ab sowie die tiefe Verzahnung mit dem darunterliegenden Betriebssystem. So unterstützen moderne Webbrowser Funktionen wie eingebettete Video-Player. Aufgrund deren Beschaffenheit, beispielsweise das Parsen großer Mengen externer Daten, schleichen sich regelmäßig ausnutzbare Schwachstellen ein – wie zuletzt die Stagefright-Lücke und dessen Exploit-Implementierung Metaphor gezeigt haben.

Angreifer können Nutzer dazu bringen einem Weblink zu folgen, den sie via Social-Media, Twitter- oder WhatsApp-Nachricht verschicken. Gerade Links in Nachrichten, die ein Nutzer per Social-Media-App von einer scheinbar bekannten Person erhalten hat, werden seltener auf Echtheit geprüft, als es bei einem Link per E-Mail der Fall gewesen wäre.

Der zweite Typ von mobilen Bedrohungen sind applikationsbasiert und stehen als App in den offiziellen App-Stores oder auf unseriösen Webseiten zum Download. Auf Marktplätzen wie Google Play besteht ein geringeres Risiko, dass man sich bei der App-Installation schadhafte Software einfängt. Google prüft die angebotenen Programme gründlich, ausgeschlossen ist eine Infektion aber nicht. Denn wie die Vergangenheit gezeigt hat, rutschen immer mal wieder Apps durch die Prüfung, die schadhaftes und ungewolltes Verhalten zeigen.

## Krankheitstypen

Schadhafte Android-Apps kann man in drei Bedrohungstypen gruppieren:

**Malware:** Angreifer wollen durch die Installation von Malware Zugang zum Gerät erhalten. Das Ziel: Daten stehlen, Telefonaktionen fernsteuern, den Nutzer erpressen oder das Gerät beschädigen. Malware wird

## Ist mein Smartphone infiziert?

Generell kann folgendes Verhalten ein Hinweis für Schadcode auf dem Gerät sein:

- unbekannte Positionen auf der Rechnung
- erhöhtes Datenvolumen
- erhöhter Akkuverbrauch
- ungewöhnliche Wärmeentwicklung
- viele Werbeeinblendungen
- lahme Reaktionen
- neue App-Icons
- ungewollte Reboots
- neue Geräteadministratoren

installiert, indem man den Nutzer dazu bringt, eine vertrauenswürdig aussehende App zu installieren oder es wird eine Schwachstelle im Gerät ausgenutzt.

**Spyware:** Das Ziel von Spyware, oft auch Remote-Access-Tools (RAT) genannt, ist es, Informationen über das Opfer zu sammeln und an die Person, die die Spyware installiert hat, zu senden. Spyware wird oft auf dem Gerät des Opfers installiert, indem sich der Angreifer kurzzeitig physischen Zugriff zum Smartphone verschafft, beispielsweise wenn das Endgerät unbeaufsichtigt im Büro oder in einem Café liegt oder während das Opfer abgelenkt wird. In einigen Fällen ist das aber gar nicht mehr nötig, da die Spyware-Tools auch mithilfe von Sicherheitslücken oder Social-Engineering-Techniken auf das Zielgerät kommen können.

**Grayware:** Oft auch als die „Kaffeefahrt“ unter den mobilen Apps bezeichnet. Diese Gruppe umfasst Apps, die der Nutzer selbst installiert hat, da er dachte, die Programme seien harmlos. Tatsächlich spionieren diese Apps jedoch oder leiten auf unseriöse Angebote um. Teilweise funktioniert die Software wie erwartet, da die Entwickler reale Funktionen integriert haben. Trotzdem werden Informationen über das System wie das Adressbuch des Nutzers oder seine Browser-Verläufe gesammelt. Das Hauptziel dieser Apps ist es, Daten für Marketingzwecke oder zum Verkauf in Untergrundmarktplätzen zu sammeln oder zusätzliche Werbung einzublenden. Man bezeichnet diese Applikationen auch oft als Potentially-Unwanted-Apps (PUA) oder Adware.

**APT:** „Advanced-Persistent-Threat“ oder eher unter „gezieltem Angriff“ bekannt, sind solche Programme oder Angriffe, die Eigenschaften von Malware und Spyware vereinen. Dabei sind sie aber auf eine klei-

ne Zielgruppe ausgelegt. Meist verändern die Angreifer bekannte Apps, um sie dann einem ausgesuchten Opfer unterzuschleichen. Die Manipulation der Apps ist enorm aufwendig und sie zu erkennen ist schwierig. Auch AV-Hersteller haben meist keine Chance, da diese Art von Software nur in geringen Stückzahlen auftaucht und exakt auf das Opfer zugeschnitten ist. Bekannt sind in diesem Bereich vor allem die Angriffe und manipulierten Apps der umstrittenen Firma Hacking-Team.

Das beliebteste Ziel für Angreifer und Malware-Autoren ist immer noch der Diebstahl von sensiblen Daten wie Telefonbucheinträge oder Zugangsdaten für Online-Plattformen. Es folgen Programme, die Bot-Netzen dienen. Sie bauen beispielsweise Verbindungen zu Command-and-Control-Servern auf, um Befehle in Empfang zu nehmen oder Daten dorthin abfließen zu lassen.

Dazugekommen sind in jüngerer Vergangenheit kommerzielle Malware-Applikationen beziehungsweise Spyware, die Privatpersonen oder Firmen ausspähen. Ebenso stark zugenommen hat in den vergangenen zwei Jahren schadhafte Software, die mTAN-Nachrichten abfängt und manipuliert.

Erinnern Sie sich noch an den BKA-Trojaner, der vor einigen Jahren im Umlauf war? Im Jahr 2015 kam mit den Crypto-Lockern eine identische Bedrohung für Android hinzu: Diese Malware verschlüsselt das Telefon oder die Nutzerdaten mit einem Passwort. Im Nachgang wird eine Meldung angezeigt, dass der Nutzer einen gewissen Betrag zahlen soll, um das Passwort für seine Daten zu erhalten. Diese Masche ist aus der PC-Welt seit einigen Jahren bekannt und nun auch im Android-Umfeld im Trend.

Type	App Name	md5	SDK	Package	Location	Date installed	Date last used
UserApp	TouchDown HD	e8a955a9c838017e994e7ff494a98afa	16	com.nitrodesk.honey.nitroid	/data/app/com.nitrodesk.honey.nitroid-1.apk	2016-01-17_17:00:02	2016-01-17_17:00:02
UserApp	Root Browser	bbf904f3c93c0cb27db8dfca0de8720d	17	com.jummy.root.browserfree	/data/app/com.jummy.root.browserfree-1.apk	2015-12-11_08:21:14	2015-12-11_08:21:14
UserApp	SulConFo	8c636232847c04d1330ab73900f5e65	8	com.magicsms.own	/data/app/com.magicsms.own-2.apk	2016-01-17_18:07:28	2016-01-18_10:21:30
UserApp	Apple Music	81090c307dc140a900e9df4718fe6f5c	23	com.apple.android.music	/data/app/com.apple.android.music-1.apk	2015-12-26_18:06:55	2016-02-16_22:27:37
UserApp	Sieve	b011baaa8aac34bdf68691e63a96a08	17	com.mwr.example.sieve	/data/app/com.mwr.example.sieve-1.apk	2015-12-10_12:50:12	2015-12-10_12:50:12
UserApp	Cydia Substrate	9c67c86fa51b47aef4de3303288cfaca	17	com.saurik.substrate	/data/app/com.saurik.substrate-1.apk	2015-12-10_11:01:09	2015-12-10_11:01:09
UserApp	drozer Agent	6e6ba57a704c5a0895ac9a152d4cc399	18	com.mwr.dz	/data/app/com.mwr.dz-1.apk	2015-12-09_17:35:43	2015-12-09_17:35:43
UserApp	AppExtract	35d1dca230f10ce80d6dc6f8e3e53c61	21	de.mspreitz.appextract	/data/app/de.mspreitz.appextract-1.apk	2016-02-29_16:31:22	2016-02-29_16:31:22
UserApp	Signal	82a47e5adc889d30c9a1b1a13509fd85	22	org.thoughtcrime.securesms	/data/app/org.thoughtcrime.securesms-2.apk	2015-12-11_08:23:57	2016-02-29_15:09:05

Mithilfe von AppExtract-Reports kann man beispielsweise Installationsdaten mit auffälligen Positionen auf der Mobilfunkrechnung abgleichen.

## Symptome

Glücklicherweise gibt es meist Hinweise auf einen Infekt: Tauchen unbekannte Positionen auf der Rechnung auf, sind oft Premiumdienste die Verursacher. Beispiele sind SMS-Nachrichten an Kurzwahlnummern oder Abo-Dienste, die Sie nicht wissentlich abgeschlossen haben. Erhöhtes Datenvolumen auf der Mobilfunkrechnung und in den entsprechenden Einstellungen des Smartphones (Einstellungen/Datenverbrauch) können ein Hinweis sein. Spyware, aber auch viele Malware-Apps versuchen Daten des infizierten Telefons an den Angreifer zu übersenden. Dies macht sich am Datenverbrauch bemerkbar.

Einige Schädlinge nehmen viel Rechenleistung in Anspruch, während sie im Hintergrund laufen. Die Folge: Der Akku leert sich schneller als gewohnt. Damit verbunden ist eine ungewöhnliche Wärmeentwicklung, obwohl das Smartphone nicht verwendet oder aufgeladen wird. Anderen Funktionen des Geräts stehen dann weniger Ressourcen zur Verfügung und so reagiert das Telefons eventuell besonders lahm auf Nutzereingaben. Viele Werbeeinblendungen können ebenfalls ein Zeichen für bösartige Software sein.

Ungewollte Apps legen meist neue Symbole an, die dann auf dem Home-Screen oder in der Liste der installierten Applikationen auftauchen. Malware, die noch nicht den nötigen Reifegrad erreicht hat oder sich im schlimmsten Fall Root-Zugang verschafft, verursacht sporadische Neustarts. Um mit ausreichend Rechten ausgestattet zu sein, registrieren sich einige Schädlinge in Androids Systemeinstellungen als Geräteadministratoren. Sie stellen damit sicher, dass man sich ihrer nicht so einfach entledigt. Die Liste findet man unter Einstellungen/Sicherheit/Geräteadministratoren.

Doch nicht alle diese Symptome deuten zwangsweise auf ein infiziertes Gerät: Auch System-Updates oder legitime Apps können solche Verhaltensweisen hervorrufen. Zeigt das Gerät auffälliges Verhalten, sollte man sein Telefon und die Mobilfunkrechnung über einen längeren Zeitraum im Auge behalten – und feststellen, ob es sich um einmalige Vorkommnisse beispielsweise

se durch ein Update im Hintergrund handelt oder ob die Vorkommnisse regelmäßig auftreten. Oft zeigen Geräte beispielsweise einen erhöhten Datenverbrauch, als Auslöser stellt sich dann aber nur eine E-Mail heraus, die im Ausgang des Smartphones hängenblieb. Erhärtet sich jedoch der Verdacht auf Schädlinge, sollte man die verdächtigen Apps eingrenzen und sein Telefon säubern.

## Suche nach verdächtigen Apps

Möchte man eine Infektion aufspüren, sollte man als Erstes die installierten Apps betrachten – mehr als 90 Prozent aller Infektionen werden über schadhafte Programme ausgelöst. Die Übersicht findet sich unter Einstellungen/Apps/Heruntergeladen. Klicken Sie eine dieser Apps an, sehen Sie im unteren Bereich oder über das Kontextmenü oben rechts alle Berechtigungen, die sie verlangt. Anhand derer kann ein erfahrener Nutzer oft schon erkennen, welches Programm eventuell das verdächtige Verhalten des Smartphones verursacht.

Auffällige Software genauer zu betrachten und zu bewerten gelingt am einfachsten mithilfe von Analyse-Apps wie AppExtract. Das kostenlose Programm erzeugt eine Liste mit allen installierten Apps mitsamt der Hash-Summen, Informationen über den Autor anhand des Zertifikats und Versionsnummern. Diese Daten können helfen, die App zu identifizieren und mit bekannten Apps abzugleichen. Auf Wunsch verschickt das Tools den Bericht direkt per E-Mail – beispielsweise an erfahrene Nutzer oder Analysten. Die im Report enthaltene MD5-Summe kann man nun mit Online-Datenbanken wie VirusTotal abgleichen und feststellen, ob die App als schädlich bekannt ist. Möchten Sie mehr erfahren, erhalten Sie mithilfe des AppExtract-Reports auch den Pfad, unter dem die APK-Datei der App zu finden ist. Diese kann man nun mithilfe



Die Android-Einstellung „Unbekannte Herkunft“ öffnet die Tür für Malware und sollte möglichst deaktiviert bleiben. „Apps verifizieren“ steigert hingegen die Sicherheit.



des folgenden Befehls auf einem Analyse-rechner mit installiertem Android-SDK zum manuellen Reversing übertragen:

```
adb pull /data/app/[Paketname].apk ~/malicious_apps/
```

## Manuelles Reversing

Das manuelle Reversing erfordert viel Wissen über Android und den Aufbau der Apps sowie Verständnis der gängigen Programmiersprachen Java und C.

Da jede App anders aufgebaut ist und es keine universelle Blaupause für das Reversing gibt, möchten wir nur kurz darauf eingehen, wie man generell vorgeht: Beginnen sollte man mit speziellen Tools wie Codeinspect, JADx-GUI, Androguard oder smali, die einem die ersten Schritte automatisch abnehmen. Sie erlauben es, die App zu dekompile, um wieder an einen Quellcode ähnlich dem ursprünglichen Code des Entwicklers zu gelangen.

Ist man hier angekommen, beginnt man üblicherweise beim Android-Manifest. Es beinhaltet die angeforderten Berechtigungen und gibt die Stelle im Quellcode an, die ausgeführt wird, wenn der Benutzer die App startet. Ebenso beschreibt es, ob die App auf bestimmte Events wie eingehende SMS-Nachrichten wartet und welches Quellcode-Fragment dann aufgerufen wird. Die an diesen Stellen verknüpften Quellcode-Fragmente sind ein guter Einstiegspunkt in die App und zugleich der Startpunkt für das aufwendige Reversing der App selbst. Ab hier hilft nur noch Erfahrung und Detektivarbeit.

**Required permissions**

- android.permission.ACCESS\_LOCATION (Unknown permission from android reference)
- android.permission.SEND\_SMS (send SMS messages)
- android.permission.ACCESS\_GPS (Unknown permission from android reference)
- android.permission.RECEIVE\_SMS (receive SMS)

**Activities**

- com.magicms.own.MagicSMSActivity

**Receivers**

- com.magicms.own.receiver.SMSReceiver

Antiviren-Dienste wie VirusTotal geben Hinweise darauf, ob eine App beispielsweise Premium-SMS-Nachrichten versendet.

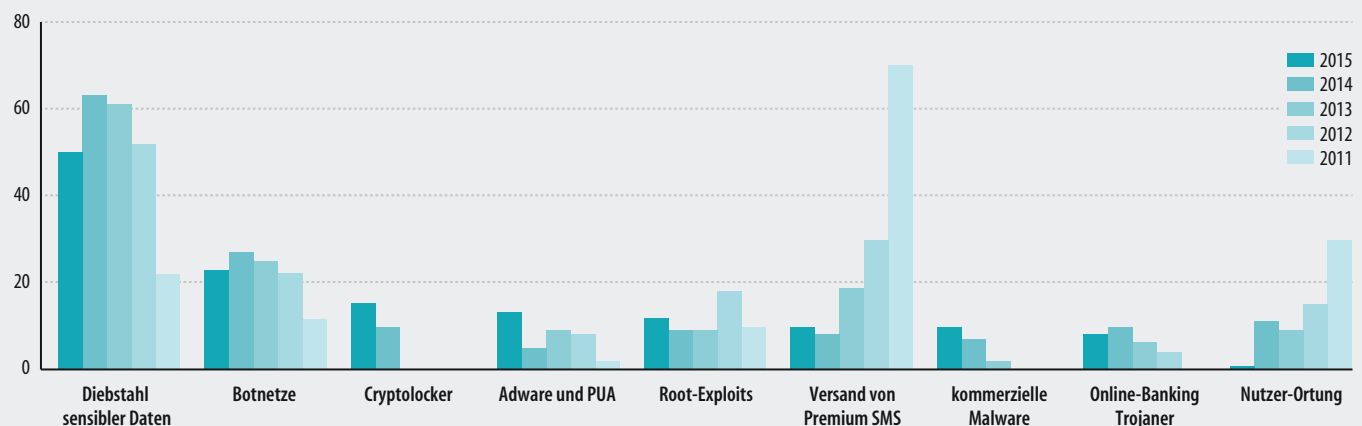
## Bekannte Spyware und deren Erkennung

Seit einigen Jahren hat sich ein eigener Markt für Überwachungssoftware beziehungsweise Spyware entwickelt. Oft werden diese Tools damit beworben, dass der

Käufer seine Kinder überwachen kann, um sie im Ernstfall aufzuspüren. Gerne wird auch die Überwachung des Ehepartners als Verkaufsargument angeführt, aber oft geht es eigentlich um Industriespionage. Dabei versprechen diese Tools alles, was man sich von derartiger Software wünscht:

## Das wollen Schädlinge erreichen

Die meisten Apps vereinen mehrere Bedrohungstypen und besitzen mehr als eine der abgebildeten Eigenschaften.





Spyware-Tools werden oft damit beworben, dass der Käufer seine Kinder oder Partner überwachen kann. Oft geht es aber um Industriespionage.

Telefon-Support, eine Garantie, dass die Software funktioniert und gelegentlich sogar, dass das Opfer nichts von der Software mitbekommt. Tipps, wie man einigen dieser Spyware-Lösungen auf dem eigenen Gerät auf die Schliche kommt, finden Sie in der Tabelle.

## Rooting erkennen

Sowohl Angreifer als auch ausgereifte Malware versuchen stets auf dem Smartphone Root-Rechte zu erlangen. So sind sie in der Lage, ihr Vorgehen vor dem Nutzer zu verbergen und auf dem Endgerät unentdeckt zu agieren, ohne dass lokale Sicherheitsrichtlinien sie bremsen. Erfolgreiches Rooting eines Smartphones ist deshalb schwierig zu erkennen. Folgende Hinweise können für ein Rooting des Endgerätes sprechen:

**Installierte Apps:** In der Liste der installierten Apps finden sich nach dem erfolgreichen Rooten oft Apps wie SuperSu und BusyBox.

**Kommandozeilen-Nutzer:** Verbinden Sie sich per Android Developer Bridge

(ADB) mit dem Smartphone, erhalten Sie Zugriff auf die Kommandozeile des Telefons – falls die Entwickleroptionen aktiviert sind. Gibt man hier den Befehl `id` ein, erscheint bei ungerooteten Geräten als Antwort „uid=2000(shell)“, bei gerooteten „uid=0(root)“.

**Kommandozeilen-Befehle:** Die Eingabe des Befehls `su` auf der Kommandozeile sollte die folgende Fehlermeldung verursachen: „/system/bin/sh: su: not found“. Erscheint jedoch ein Popup auf dem Smartphone-Display oder verändert sich die Kommandozeile, ist dies ein Zeichen für Rooting.

**Partitionen:** Durch Eingabe des Befehls `mount` erhalten Sie eine Übersicht über alle Partitionen des Smartphones. Hier sollte die Systempartition als ersten Wert ein „ro“ (read only) haben. Findet man hier „rw“ (read/write) ist das Gerät wahrscheinlich manipuliert.

**AndroidSE:** Hierbei handelt es sich um Regeln, die im Kernel dafür sorgen, dass gefährliche Systemaufrufe keinen Schaden verursachen. Diese Regeln sollten auf den meisten aktuellen Telefonen (android 5.0

und höher) auf „Enforcing“ stehen und können per Eingabe von `getenforce` abgefragt werden.

**Prozesse:** Durch Eingabe von `ps` erhält man eine Liste aller Prozesse, die gerade auf dem Smartphone laufen. Prozesse, die mit „daemonsu“ beginnen, sind ein Hinweis auf Rooting.

Fallen einer oder mehrere dieser Tests positiv aus, ist das Smartphone wahrscheinlich gerootet. Sie können dann davon ausgehen, dass der Angreifer oder die Malware volle Kontrolle über das Smartphone und alle darauf befindlichen Daten hat – inklusive der Tastatureingaben des Nutzers.

## Wie säubere ich mein Android-Endgerät?

In vielen Fällen – gerade wenn es um eher einfache Malware oder Adware geht – reicht es vollkommen aus, die verdächtige App zu deinstallieren. Haben Sie jedoch Spuren auf ein Rooting gefunden oder hat sich eine der Apps als Geräteadministrator eingetragen und konnte entsprechend walten, hilft nur das Zurücksetzen des Telefons auf Werkseinstellungen. In beiden Fällen sollten jedoch sämtliche Passwörter geändert werden, die auf dem Gerät gespeichert waren oder von dort aus verwendet wurden. Denn viele der schadhafte Apps spionieren genau diese Daten aus und können gegebenenfalls damit das Smartphone erneut infizieren.

Ebenso wichtig ist es, nach einem Werks-Reset genau zu prüfen, welche

## Spyware unter Android

Spyware	Hinweise auf eine Infektion
mSpy	wählen von #000* öffnet das User-Interface von mSpy
FlexiSpy	FSXGAD_<versionsnummer>.apk befindet sich auf der SD-Karte, unter /data/app/ befindet sich die Datei com.mobilefonex.mobilebackup-1.apk, die URL <a href="http://djp.cc">http://djp.cc</a> bleibt oft im Browserverlauf zurück, wählen von *#900900900 öffnet das User-Interface von FlexiSpy
PhoneSheriff	hinterlässt alle abgefangenen Daten und Einstellungen unter /data/com.studio.sp2/
MobileSpy	wählen von #123456789* öffnet das User-Interface von MobileSpy
OmniRAT	erzeugt einen zusätzlichen Geräte-Administrator mit dem Namen com.android.engine.Deamon

Daten und Apps aus einem eventuell vorhandenen Backup zurückgespielt werden. Mit dem Backup kann eine schadhafte App zurück auf das Smartphone wandern und die ganze Arbeit zunichtemachen.

War man das Opfer eines ausgereiften oder gar gezielten Angriffs, hilft oft nur der Kauf eines neuen Telefons oder das Überschreiben aller Partitionen: Inzwischen gibt es Malware, die auch ein Zurücksetzen überlebt. Sie infiziert die System- beziehungsweise Boot-Partition, wodurch sie sich bei jedem Neustart oder Werks-Reset wieder auf dem Smartphone installieren kann.

## Abwehr stärken

Auf dem Smartphone gelten ähnliche Verhaltensregeln wie im Umgang mit dem PC:

### 1. Apps vor der Installation prüfen:

Generell sollten Sie sich genau anschauen, welche App Sie installieren möchten. Welche Berechtigungen fordert die App an? Wer ist der Autor der App? Wie sind die Bewertungen? Wie lange gibt es diese App schon? Welche Apps hat der Autor noch in Google Play und wie sind die Bewertungen dort? All diese Fragen können helfen, eine legitime App zu erkennen.

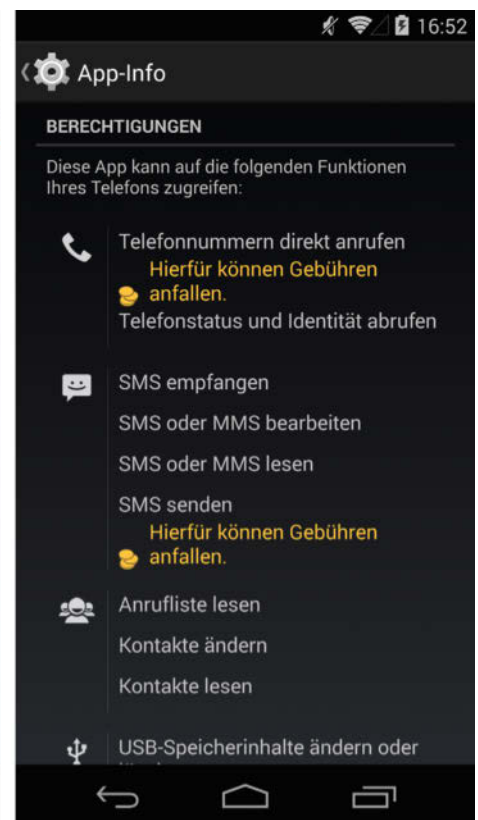
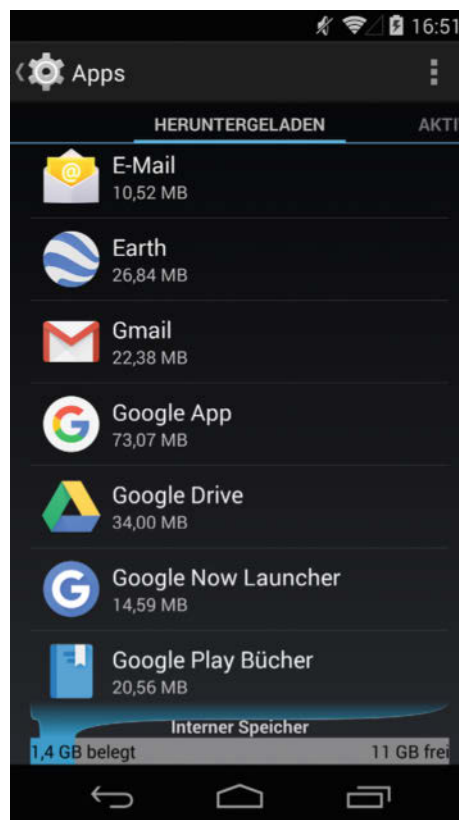
### 2. Apps nur aus dem Google Play

**Store installieren:** Kein anderer App-Store-Betreiber für Android hat so hohe Sicherheitsstandards wie Google.

**3. „Unbekannte Herkunft“ deaktiviert lassen:** Die Einstellung (Einstellungen/Sicherheit/Unbekannte Herkunft) auf dem Gerät verhindert, dass Apps aus unseriösen Quellen, E-Mails und von manipulierten Webseiten aus installiert werden. Hierdurch lassen sich viele der bekannten Infektionswege ausschließen.

**4. „Apps verifizieren“ aktivieren:** Dieses Setting (Einstellungen/Google/Sicherheit) bewirkt, dass Informationen über installierte Apps regelmäßig an Google gesendet werden, um dort mit schadhafte Apps verglichen zu werden. Im Fall eines Fundes wird der Nutzer darüber per Popup informiert.

**5. E-Mails und Social-Media-Nachrichten prüfen:** Auf dem PC kennt man das Verhalten und befolgt diese Regel auch konsequent: nur E-Mails und speziell deren Anhänge öffnen, wenn Sie den Absender kennen. Selbiges trifft auch zu beim Klicken auf Links innerhalb von E-Mails oder anderen Nachrichten auf dem Smartphone von WhatsApp, Facebook, SMS et cetera.



Anhand der von Apps geforderten Zugriffsrechte kann ein erfahrener Nutzer erkennen, welche Programm eventuell das verdächtige Verhalten des Smartphones verursachen.

**6. Das Gerät nicht selbst rooten:** Durch das Rooting erhoffen sich viele Nutzer einen Vorteil, da sie nun eine andere Bedienoberfläche auf ihr Telefon spielen können, neue Funktionen freischalten oder Custom-ROMs installieren können. Doch Rooting hat zur Folge, dass das Betriebssystem deutlich verwundbarer ist und die vorhandenen Sicherheitsmechanismen ganz abgeschaltet oder wirkungslos sind.

**7. Verschlüsselung aktivieren und Debugging nicht aktivieren:** Sie sollten als Nutzer prüfen, ob die Debug-Schnittstelle auch wirklich deaktiviert ist (Einstellungen/Entwicklertools/USB-Debugging). Denn über diesen Weg kann ein Angreifer – mit wenigen Minuten physischem Zugriff – das Telefon manipulieren und infizieren. Auch die Verschlüsselung des Smartphones ist hierbei ein wichtiger Schutz, da es der Angreifer dadurch deutlich schwerer hat, an Daten zu gelangen.

**8. Verwendung einer sicheren Display-Sperre:** Der Screenlock oder auch Displayschutz genannt schützt das Smartphone vor unberechtigtem Zugriff.

Dies ist enorm wichtig, da viele der schadhafte Apps oder Angriffe nur mit Interaktion des Nutzers installiert werden. Hat ein Angreifer kurzzeitig physischen Zugriff auf das Telefon, kann er es infizieren, ohne dass der Nutzer es bemerkt. Hier schützt ein Displayschutz mit einer längeren PIN oder einem echten Passwort.

All die hier erwähnten Maßnahmen bieten zwar keinen absoluten Schutz – den gibt es in der IT-Welt einfach nicht. Aber sie machen es einem Angreifer deutlich schwerer, das eigene Smartphone zu infizieren und sie schützen meist gegen die Malware, die für die breite Masse ausgelegt wurde.

Handelt es sich um ausgereifte oder gar gezielte Angriffe auf Android-Smartphones, fallen die Schutzmaßnahmen sehr aufwendig aus und die Chancen stehen meist schlecht, sich gegen diese Bedrohung erfolgreich zu schützen. (hcz) **ct**

Programme und Apps unter: [www.wct.de/wyha](http://www.wct.de/wyha)





Michael Spreitzenbarth

## Erpressungs-Trojaner werden mobil

**Erpressungs-Trojaner verschlüsseln Daten und geben sie nur gegen Lösegeld wieder frei. Auch auf Smartphones verbreitet sich die Schadsoftware. Der Autor hat im Rahmen seiner Tätigkeit als Forensikspezialist und Malware-Researcher einige dieser neuen Schädlinge analysiert.**

**E**rpressungs-Trojaner wie Locky haben Hochkonjunktur. Das liegt nicht zuletzt am funktionierenden Geschäftsmodell der Betrüger. Hat der Crypto-Locker die Daten des Anwenders verschlüsselt und somit jedem Zugriff entzogen, ist der Leidensdruck in vielen Fällen so groß, dass ein nennenswerter Teil der Betroffenen allein für die Chance auf

eine Wiederherstellung tief in den Geldbeutel greift.

Die Welle von Erpressungs-Trojanern trifft auch Smartphones. Der Antiviren-Hersteller Kaspersky berichtet etwa, dass sich die Zahl der mit Ransomware attackierten, deutschen Smartphone-Nutzer zwischen April 2015 und März 2016 im Vergleich zum Vorjahreszeitraum verfünffacht

hat. Die mobile Ransomware macht dabei interessanterweise eine ähnliche Entwicklung durch, wie deren Vorfahren aus der Windows-Welt.

Entscheidend für den aktuellen Erfolg der Erpresser ist die Tatsache, dass in den meisten Fällen ohne die Mithilfe der Kriminellen tatsächlich nur Backups eine realistische Perspektive bieten, wieder an die

Daten zu kommen. Das war bei den Vorgängern, die lediglich den Zugang zum PC verriegelten, noch anders.

Da fanden Experten fast immer einen Weg, die Sperre zu umgehen und zumindest die wichtigsten Daten zu retten. In vielen Fällen konnten sie den Rechner sogar mit wenigen Handgriffen wieder komplett freischalten – etwa indem sie ein Desinfec't von DVD booteten und von dort aus den Registry-Eintrag für die Windows-Shell wieder auf explorer.exe zurücksetzten. Bei Locky & Co hingegen zucken auch ausgewiesene Experten meist nur noch hilflos mit den Schultern und verweisen auf die hoffentlich existierenden Backups.

Genau diese Entwicklung zeichnet sich auch bei Smartphones ab. Die ersten Ransomware-Exemplare für Android sperren zwar den Zugang, lassen die Daten selbst aber intakt. Das lässt uns eine Reihe von Möglichkeiten, diese Sperre zu umgehen. Doch immer öfter finden wir auf analysierten Smartphones nur noch verschlüsselte Daten vor – echte Crypto-Locker machen sich auch hier breit.

## Das BKA-Trojaner-Revival

Ein typisches Ransomware-Exemplar der alten Schule, das immer noch verbreitet wird, ist SLocker – auch bekannt als Android BKA-Trojaner. Die Infektion erfolgt in aller Regel durch den Anwender selbst. Der muss dazu zunächst die Installation aus nicht vertrauenswürdigen Quellen zugelassen haben. Zeigt ihm beim Surfen eine Webseite ein Popup, das ihm eine App zur Installation anbietet und er akzeptiert das, schlägt SLockers Stunde. Alternativ kommt SLocker gelegentlich auch als angebliches Sicherheits-Update etwa für den Adobe Flash-Player via E-Mail.

Als erste Aktion macht SLocker ein Foto mit der Frontkamera. Danach setzt er im Hintergrund einen Timer, der – je nach Version – von 10 bis 180 Minuten herunterzählt. Ist diese Frist verstrichen, öffnet sich die App und zeigt nur noch einen vorgegebenen Bildschirm an. Ganz analog zu den BKA-Trojanern für den PC dichtet der dann seinem Opfer einen Gesetzesverstoß an. Dieser habe zur Sperre seines Geräts durch die Behörden geführt. In der deutschen Version sind das dann etwa Bundeskriminalamt und Bundesnachrichtendienst. Um die Betroffenheit zu verstärken, blendet er in diese Meldung das zuvor geschossene Foto ein.

Um diese Sperre zu entfernen und angeblich auch weitere Konsequenzen zu vermeiden, fordert SLocker die Zahlung

eines „Bußgeldes“ von 100 Euro, die mit einer PaySafe-Card zu entrichten sind. Das Feld zur Eingabe des Codes findet man direkt in der Erpressungsmeldung. Nach dessen Eingabe wird der Code der Karte an den Angreifer gesendet. Eine Routine zur Deinstallation der App haben wir beim Reverse Engineering unserer Beispiele nicht gefunden. Sprich: Auch nach der Zahlung bleibt das Gerät gesperrt.

Der Sperr-Bildschirm erscheint ebenso nach einem Neustart des Geräts direkt wieder. SLocker registriert sich dazu für den Intent „Boot\_Completed“, sodass ihn das System jedes Mal aktiviert. Der Anwender kann diese Sperre nicht ohne Weiteres umgehen. Da SLocker jedoch keine Daten verschlüsselt, gibt es mehrere Wege daran vorbei.

So gelang es uns mehrfach, das infizierte Smartphone über die gerätetypische Tastenkombination in den Recovery-Modus zu booten und es dort auf Werkseinstellungen zurückzusetzen. Die Daten des Nutzers, also unter anderem die installierten Apps und deren Daten, werden dabei gelöscht.

Den Verlust von Daten kann man in vielen Fällen vermeiden, indem man das Gerät im Safe-Mode bootet, in dem alle Third-Party-Apps deaktiviert sind. In den Safe-Mode kommt man, wenn man im Power-Off-Menü lange auf den Punkt Power-Off drückt. Dann öffnet sich eine Abfrage, über die Sie das Telefon in den Safe-Mode starten und dort dann die Trojaner-App löschen.

Wenn der Entwicklermodus bereits vor der Infektion aktiv war, kann man das auch vom PC aus über den Remote-Debugger via adb uninstall erledigen.

## Online-Banking-Betrüger sattelt um

Ganz so leicht macht es Xbot seinen Opfern nicht mehr. Dieser erstmals von den Netzwerk-Security-Spezialisten bei Palo Alto entdeckte und analysierte Schädling ist eigentlich ein klassischer Online-Banking-Trojaner. Die ersten Versionen tarnen sich auch primär als Banking-App für bekannte Banken in Australien und Russland. Sie sammeln vor allem im Hintergrund die SMS-Nachrichten mit mTANs ein und leiten sie an die Betrüger weiter.

Neuere Versionen dieser Malware tarnen sich inzwischen als WhatsApp oder andere beliebte Apps. Und sie können auch deutlich mehr als Online-Banking-Betrug. Zeichnet sich nämlich ab, dass da kein Geld zu holen ist, geben die Kriminel-

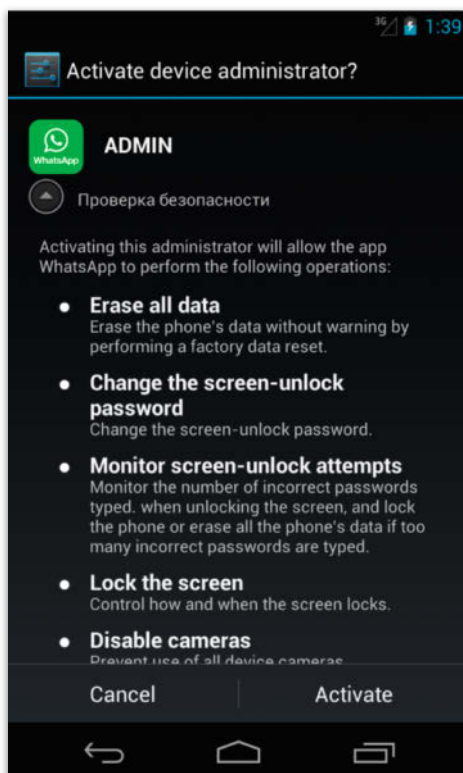
len aus der Ferne den Befehl, das Gerät zu sperren. Fieserweise verschlüsselt er dann auch die Inhalte der SD-Karte komplett.

Für derartige Aktivitäten muss sich Xbot jedoch als Geräteadministrator registrieren. In den Versionen, die wir bisher gesehen haben, macht er dies ganz primitiv und fragt einfach nach den entsprechenden Rechten. Lehnt der Nutzer dies ab, kann Xbot keine Daten verschlüsseln und sich auch nicht gegen eine Deinstallation wehren.

Solange die Malware noch keine Daten verschlüsselt hat, entfernt man sie ähnlich wie SLocker. Hat die Verschlüsselung bereits begonnen oder ist sie sogar erfolgreich durchgeführt worden, hilft nur ein Reversing der App, um zu verstehen, mit welchem Verfahren und welchem Schlüssel sie gearbeitet hat. Das erfordert dann tiefere Kenntnisse im Umgang mit dem Debugger und im Reverse Engineering.



**SLocker beschuldigt den Anwender diverser Straftaten und sperrt den Zugang zum Smartphone.**



Der als WhatsApp getarnte Erpressungs-Trojaner fordert ganz dreist Administrator-Rechte an. Gewährt man die, verschlüsselt er damit Daten auf der SD-Karte.

In den ersten Varianten setzte Xbot ein einfaches XOR mit dem Wert 50 ein. Das ließ sich recht einfach wieder rückgängig machen. Doch neuere Xbot-Versionen erhalten mit dem Verschlüsselungsbefehl einen individuellen Schlüssel. Das macht eine Datenrettung deutlich schwieriger. Uns ist bislang kein Fall bekannt, in dem diese erfolgreich durchgeführt wurde. Ebenfalls unbekannt ist, ob und wie die Erpresser nach einem Bezahlen des Lösegelds bei der Wiederherstellung der Daten helfen.

## Cyber Police im Einsatz

Mit Cyber Police hat der Alptraum jedes Android-Nutzers Gestalt angenommen. Es handelt sich dabei um einen richtigen Crypto-Locker vergleichbar zu Locky auf PCs.

Besonders bitter daran: Man kann sich den vorgeblichen Cyber-Polizisten auf fast jedem Android-Handy einfangen, auf dem nicht mindestens die 2014 erschienene Android-Version 5.0 aka Lollipop läuft.

Doch es kommt noch schlimmer: Erforderten SLocker und Xbot noch die Mithilfe

der Anwender, kann man sich Cyber Police einfangen, ganz ohne eine App zu installieren, etwas zu bestätigen oder auch nur die Installation aus nicht vertrauenswürdigen Quellen zu erlauben.

Alles was der Anwender tun muss, um sich zu infizieren, ist eine Webseite zu öffnen, auf der Cyber Police lauert. Diese nutzt dann eine Browser-Schwachstelle aus, die durch die Hacking-Team-Leaks bekannt wurde. Anschließend nutzt der Erpressungs-Trojaner die sogenannte Towelroot-Lücke, um sich Root-Rechte zu verschaffen.

Konkret nutzt die Exploit-Webseite mittels JavaScript eine Schwachstelle in der Bibliothek libxslt für Androids WebView aus, um ein ELF-Binary auf dem Endgerät mit den Rechten der WebView auszuführen. Dieses Binary enthält Bestandteile des TowelRoot-Exploits, um sich Root-Rechte zu verschaffen. Mit diesen Rechten wird dann die Ransomware auf dem Endgerät installiert, ohne die bekannten Meldungen und Abfragen bei einer Installation anzuzeigen. Im Nachgang beginnt sie sofort, alle Nutzer-Daten mittels der erlangten Root-Rechte zu verschlüsseln.

Auch Cyber Police registriert sich für den Boot\_Completed-Intent, um beim Neustart wieder aktiviert zu werden. Gegen eine Deinstallation setzt es sich mithilfe seiner Root-Rechte sehr nachdrücklich und zumeist erfolgreich zur Wehr. Hat man sich damit infiziert, hilft nur noch das Zurücksetzen auf Werkeinstellungen oder das manuelle Flashen mit einer neuen Firmware des Herstellers oder einer alternativen Variante wie Cyanogen.

## Risiko-Analyse

Im Lauf des vergangenen halben Jahres hat sich die Gefahrenlage insbesondere für Android-Nutzer drastisch verschärft. Anfangs hatte man Ransomware nur auf dubiosen oder FSK18-Webseiten gefunden. Sie wurden dort als eigenständige Apps angeboten, die dem Nutzer die Inhalte auch ohne Webbrowser zur Verfügung stellen – so zumindest das Versprechen. Hatte man sich eine dieser Apps installiert, meldete sich der Trojaner und verhinderte die Bedienung des Geräts.

Ließ sich dies noch durch „vorsichtiges Surfen“ – was immer das auch sein mag – und konservative Sicherheitseinstellungen vermeiden, präsentiert sich die Situation heute anders. Bereits Ende 2015 haben wir erste Anzeichen dafür gesehen, dass die Autoren dieser schadhafte

Apps versuchen, ihre Zielgruppe zu erweitern. Inzwischen findet man solche Apps als Drive-By-Downloads auf seriösen Webseiten oder in Werbenetzwerken integriert, die ein Angreifer erfolgreich infiziert hat. Über die Werbenetze kann sich der Schadcode auf Hunderten Webseiten verteilen.

Einige der aktuellen Cryptolocker sind dank öffentlich bekannter Exploits wie Towelroot und einfach ausnutzbarer Schwachstellen auf älteren Android-Versionen in der Lage, sich auf diesen Telefonen einzunisten, ohne dass der Nutzer selbst mit der Malware interagieren muss. Dies ist die wohl größte Änderung in der Gefahrenlage seit dem ersten Bekanntwerden von Ransomware für Smartphones.

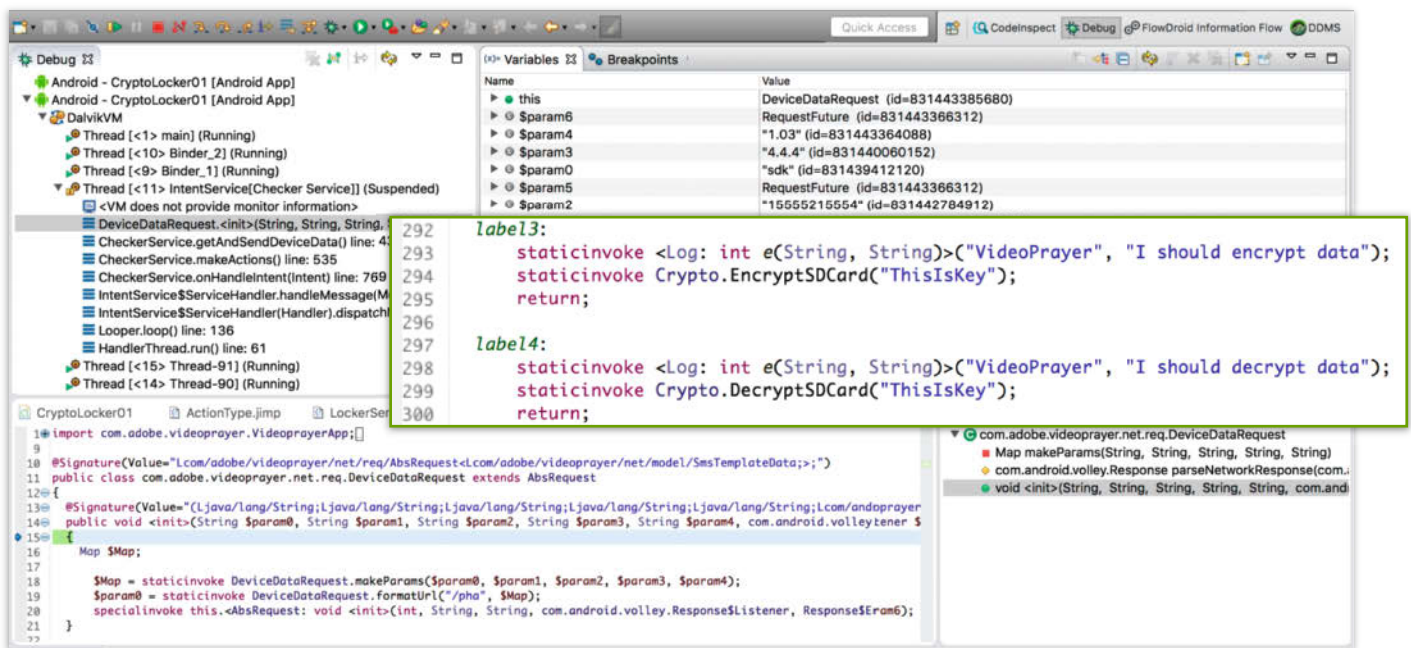
## Schutz

Sich vor diesen Gefahren konsequent zu schützen, ist nicht einfach. Natürlich gilt der Ratschlag aus der PC-Welt auch hier: Sichern Sie Ihre Einstellungen und Daten



Cyber Police präsentiert nicht nur einen Sperr-Bildschirm, sondern verschlüsselt tatsächlich die Daten des Nutzers.





Der Debugger enthüllt: Dieser Trojaner forscht das Smartphone systematisch aus und verschlüsselt die Daten auf der SD-Karte mit dem simplen Kennwort „ThisIsKey“.

regelmäßig. Dabei beweist die sonst im Security-Kontext oft geschmähte Cloud ihre Nützlichkeit. Wer seine Fotos automatisch in die Cloud synchronisiert, kann entspannt mit den Schultern zucken, wenn der Erpressungs-Trojaner die Originale auf dem Smartphone verschlüsselt: „So what?“ Es bleibt allerdings die Gefahr, dass sich Erpressungs-Trojaner an den in der Cloud gespeicherten Daten vergreifen. Dann kann man nur hoffen, dass der Cloud-Betreiber ein schlüssiges Backup-Konzept hat.

Darüber hinaus gelten die klassischen Sicherheits-Tipps für Android auch weiterhin. Installieren Sie Software nur aus vertrauenswürdigen Quellen. Achten Sie insbesondere auf plötzliche Popups beim Surfen und begegnen Sie diesen mit größtem Misstrauen. Immer öfter öffnen infizierte Webseiten Popup-Meldungen, die versuchen, sich durch Optik und Inhalt als Systemmeldungen zu tarnen. Spätestens wenn diese versuchen, etwas zu installieren, sollten Sie auf „Abbrechen“ klicken.

Man mag von Google halten, was man will, aber in Bezug auf ihren PlayStore geben sie sich viel Mühe, Unrat draußen zu halten. Die Installation einer App aus dem Third-Party-Store oder sogar von einer Webseite, über deren Betreiber Sie fast nichts wissen, ist allemal ein größeres

Risiko als das Pendant aus dem PlayStore. Am besten deaktivieren Sie die Installation aus nicht vertrauenswürdigen Quellen in den Sicherheitseinstellungen und beschränken damit die Installation auf den Google PlayStore. Das schützt auch vor fragwürdigen Mails und SMS-Nachrichten, die versuchen, Anwendern Malware-Apps unterzuschieben.

Das hält viel vom derzeit kursierenden Unrat fern – doch es genügt nicht mehr. Cyber Police & Co demonstrieren eindrucksvoll die Lücken in diesem Schutzkonzept. Sie kommen über bekannte Sicherheitslücken auf das Smartphone; der Anwender muss nichts mehr dazu tun. Versuchen Sie deshalb, Ihre Apps und insbesondere Android selbst auf dem aktuellen Stand zu halten.

## Weg damit

Die fatale WebView-Lücke betrifft Android-Versionen vor 5.0. Lässt sich das Smartphone nicht aktualisieren, hilft es ein wenig, zum Surfen statt des eingebauten Browsers etwa Firefox zu verwenden. Doch viele andere Apps nutzen ebenfalls WebView – das Gerät bleibt also verwundbar.

Solche Geräte sollte man deshalb ausmustern. Das klingt drastisch. Aber stellen Sie sich den Ärger vor, den der früher oder

später kaum noch zu vermeidende Malware-Befall bedeutet. Was wäre, wenn Ihr Smartphone weg wäre? Nicht irgendwann, sondern genau jetzt? Und nicht irgendwie weg, sondern ich hätte es – \*evil grin\*? Und Sie müssten mit einer Veröffentlichung all der vorgefundenen Informationen im Internet rechnen? Alles okay? Wenn Sie ein altes Smartphone haben und jetzt zögern, sollten Sie sich lieber nach einem neuen umschauen.

An dieser Stelle kommt oft der Verweis auf Antiviren-Software, die es ja mittlerweile auch für Android in großer Zahl gibt. Deren Installation mag ein bisschen schützen. Aber nach meiner Erfahrung eher ein kleines bisschen. Bei den letzten, von mir analysierten Malware-Samples war jedenfalls die von Virustotal diagnostizierte Erkennungsrate sehr niedrig.

In der PC-Welt bedeutet das noch nicht allzu viel, da die Echtzeit-Virenwächter außer dem reinen Dateicheck noch andere Möglichkeiten haben, bösartige Malware zu erkennen. So können sie einen Erpressungs-Trojaner direkt an seinem Verhalten erkennen. Unter Android gibt es keine Verhaltenswächter. Die nicht erkannten Schad-Apps hätten ein Android-Smartphone somit aller Wahrscheinlichkeit nach trotz Antiviren-Software infiziert. Ich würde mich lieber nicht auf deren Schutz verlassen. (ju)



Jörg Wirtgen

# Geräteverschlüsselung aktivieren

Die meisten älteren Android-Geräte verschlüsseln ihren internen Speicher nicht, sodass Diebe an die Daten gelangen können. Dabei lässt sich die Vollverschlüsselung einfach nachträglich aktivieren. Wir haben nachgemessen, wie die Geschwindigkeit unter der Verschlüsselung leidet: bei einigen Smartphones deutlich, bei anderen gar nicht.

**D**ie Vollverschlüsselung eines Smartphones und Tablets verhindert, dass sich Angreifer nach einem Diebstahl Zugriff auf die Daten des Geräts verschaffen. Gefährdet sind vor allem Geräte mit SD-Karte, aber Datenspionen kann auch Zugriff auf den unverschlüsselten internen Speicher gelingen, etwa bei aktivierter Debug-Schnittstelle oder über eine Sicherheitslücke. Vor dem Zugriff durch Ermittlungsbehörden

schützt die Vollverschlüsselung allerdings aufgrund eines Design-Problems wohl nur bei langen Passwörtern, wie jetzt bekannt wurde (siehe Seite 36).

Bei den meisten Geräten ab Android 3.0 aktiviert man die Vollverschlüsselung unter Einstellungen/Sicherheit. Achtung, das Verschlüsseln lässt sich nicht rückgängig machen. Sie können allenfalls das Gerät auf Werkseinstellungen zurücksetzen, müssen danach aber alles neu installieren.

Fehlt die Option zum Verschlüsseln, ist das ein Hinweis darauf, dass das Gerät schon verschlüsselt ist: Einige Hersteller verschlüsseln ab Werk, bei mit Android 6 und 7 ausgelieferten Geräten ist das sogar Pflicht. Abschalten lässt sich die Verschlüsselung dann selbst durch Zurücksetzen auf Werkseinstellungen nicht.

Auch wenn Google von Vollverschlüsselung (FDE, Full Disk Encryption) spricht: Verschlüsselt wird nur die Datenpartition

/data, in der sämtliche Daten sowie alle Apps liegen. Das Betriebssystem bleibt lesbar, aber da es sowieso schreibgeschützt ist, finden Angreifer hier keine persönlichen Daten. Android verwendet das auch bei der Linux-Vollverschlüsselung genutzte Modul dm-crypt, Details erklärt Android-Experte Nikolay Elenkov in seinem Blog [1].

Bis Android 4.4 forderte das System vor Einrichtung der FDE dazu auf, eine Zugangssperre per PIN, Geste oder Passwort einzurichten. Mit Android 5 entfiel das, erst mal unverständlich, denn eine Vollverschlüsselung ohne solche Zugangssperre erhöht die Sicherheit nicht. Der Vorteil: Liefert ein Hersteller sein Gerät vollverschlüsselt aus, ist es automatisch abgesichert, sobald der Anwender PIN oder Passwort einrichtet.

Android 7 ersetzt die FDE durch eine dateibasierte Verschlüsselung, die es Apps ermöglicht, nach einem Neustart schon zu arbeiten, bevor der Nutzer das Gerät entsperrt. Das funktioniert aber nur bei mit Android 7 ausgelieferten Geräten, ältere bleiben nach einem Update bei der FDE. Die Art der Verschlüsselung dürfte auf die Geschwindigkeit keine Auswirkung haben.

## Verwürfelung

Haben Sie sich fürs Verschlüsseln entschieden, hängen Sie das Gerät ans Netzteil, laden den Akku voll und tippen auf „Telefon verschlüsseln“. Der Verschlüsselungsvorgang startet das Gerät neu und dauert rund eine Viertelstunde, auf älteren Geräten auch länger.

Im Test klappte das bei allen Geräten problemlos, mit einer Ausnahme: Ein Samsung Note 1 brach die Verschlüsselung reproduzierbar ab und verlor dabei alle Daten – der GAU. Ursache ist möglicherweise die Partitionierung des internen Speichers in zwei Bereiche, wie unter Android 2.x üblich.

## Krypto-Messungen

Den Geschwindigkeitsverlust haben wir an mehreren Geräten unterschiedlicher Generationen untersucht: Asus ZenFone 2 deluxe, Motorola Moto G (3rd Gen.), Nvidia Shield, OnePlus One, Samsung Galaxy Note 4 und S6 sowie Wileyfox Swift. Gemessen haben wir mit den Benchmark-Apps PC Mark, A1 SD Bench, AndEBench Pro und Disk Speed Performance Test, die vergleichsweise wenig vom Caching abhängige Werte lieferten. Weil alle ähnliche Tendenzen zeigten, geben wir nur den Lese- und Schreib-Einzeltest von PC Mark an.

Unterscheiden muss man zwischen den absoluten Raten und dem relativen Geschwindigkeitsverlust. So verlor das sehr flotte Note 4 zwar mit am meisten (einige Einzelwerte erreichten nur noch 18 Prozent der unverschlüsselten Leistung), gehörte aber trotzdem zu den schnelleren verschlüsselten. Die Schreibrate des Shield wiederum blieb nahezu konstant – es war aber auch unverschlüsselt das langsamste Gerät im Testfeld.

Bei den absoluten Raten teilt sich das Testfeld in zwei Gruppen: die mit unter 100 MByte/s verschlüsselter Leserate und die darüber. Zu Letzterer zählen auch die mit Vollverschlüsselung ausgelieferten Geräte wie das Nexus 9, die wir zum Vergleich in der Tabelle aufführen. Da die Verschlüsselung nicht abschaltbar ist, bleiben wir die unverschlüsselten Vergleichswerte schuldig.

## Verschlüsselungshelfer

Der Trick der schnellen Geräte: Sie nutzen spezielle Krypto-Befehle ihrer Prozessoren. Da der ARMv8-Befehlssatz sie enthält, kommen sie auch beim Exynos im Samsung Galaxy S6 und S7 sowie beim Tegra

im Nexus 9 und Snapdragon 808 im Next-bit Robin zum Einsatz. Doch nicht jeder ARMv8-Prozessor unterstützt die Krypto-Befehle, wie das Wileyfox Swift zeigt. Vorsicht auch beim Nvidia Tegra: Unter dem Namen K1 gibt es zwei grundlegend verschiedene Prozessoren, den K1 T132 mit ARMv8 und schneller Krypto wie im Google Nexus 9 und den älteren K1 T124 nur mit ARMv7 wie im Nvidia Shield. Auch Intel-Prozessoren haben Krypto-Befehle und verschlüsseln daher schnell, so die Atom-Varianten im Asus ZenFone und Dell Venue 8.

Ob das eigene Android-Gerät die schnellen ARMv8-Kryptobefehle unterstützt, finden Sie mit Systeminfo-Tools heraus, bei AIDA64 beispielsweise im Reiter CPU ganz unten in der Zeile AES. Auch einen Intel-Prozessor erkennen die Tools.

## Neon scheint blass

Die älteren Prozessoren mit ARMv7 haben ebenfalls eine Krypto-Engine beziehungsweise die Befehlssatzerweiterung Neon, die eigentlich seit Android 5.1 die Verschlüsselung übernehmen soll.

## Verschlüsseln der SD-Karte: Besser ab Android 6

Android verschlüsselt nur den internen Gerätespeicher, nicht aber eine etwaige SD-Karte. Einige Hersteller erweitern Android in diesem Punkt, zu finden ist das dann auch im Sicherheits-Menü. Samsung bietet die SD-Verschlüsselung beispielsweise beim Note 4 an, verschlüsselt allerdings auf Dateiebene. Stecken Angreifer die Karte in einen PC, sehen sie also alle Datei- und Verzeichnisnamen sowie Erst- und Bearbeitungsdatum; nur die Inhalte der Dateien sind geschützt.

Ab Android 6 gibt es eine bessere Möglichkeit, nämlich die SD-Karte als internen Speicher zu formatieren. Sie finden das unter Einstellungen/Speicher, möglicherweise müssen Sie dort auf die SD-Karte tippen und hier oben rechts das Einstellungsmenü öffnen. Danach bietet Google an, die Daten vom internen Speicher auf die SD-Karte zu migrieren, was ratsam ist.

Nun können Sie Apps auf der SD-Karte installieren und installierte dorthin schieben. Auch haben Apps einen besseren Zugang zur SD-Karte. Als Nebenprodukt ist die Karte verschlüsselt.

Diese Verschlüsselung können Sie etwas einfacher rückgängig machen: Schieben Sie alle Apps in den internen Speicher; sichern Sie dann alle Daten von der SD-Karte, beispielsweise indem Sie das Gerät per USB an einen PC anschließen. Schließlich formatieren Sie die Karte wieder als mobil.

Geschwindigkeitseinbrüche waren sowohl bei der Samsung- als auch der Android-Lösung zu verzeichnen. Genaue Messwerte bleiben wir aufgrund von Problemen der Benchmarks mit externem Speicher schuldig. Die SD-Karten arbeiten allerdings sowieso langsamer als der interne Speicher und eignen sich daher nicht für geschwindigkeitskritische Zwecke.





Jörg Wirtgen

## Note-4-Alltag

Die langsame Verschlüsselung des Note 4 habe ich über mehrere Wochen ausprobiert. Alles funktionierte, auch ein Security-Update installierte sich problemlos. Installationen und Updates von Apps dauern nun einige Sekunden länger.

Störender: Einige Apps starten langsamer, beispielsweise braucht die Foto-App nun drei, vier Sekunden, vorher war sie nach zwei Sekunden bereit. Auch bei den Sofortnotizen kann ich nun erst nach vier Sekunden loskritzeln.

Insgesamt ist das Note noch immer schnell genug. Auch die Laufzeit leidet nicht; ich komme locker über den Tag. Mein Fazit: Etwas zäher ist alles, aber nicht so lahm, dass ich die Vollverschlüsselung rückgängig machen möchte.

Doch Android nutzt sie von sich aus nicht, angeblich weil Google beim Nexus 6 mit Snapdragon 805 auf Probleme gestoßen ist, vornehmlich beim Standby. Der Krypto-Experte Elenkov erwähnt in seinem Blog ein Smartphone mit Neon-Verschlüsselung, das OnePlus One [1]. Ausgeliefert wird es zwar mit dem Android-Derivat Oxygen OS nur mit Software-Verschlüsselung, aber alternativ gibt es Cyanogen OS mit funktionierender Neon-Unterstützung. Tatsächlich verschlüsselte Cyanogen OS mit 70 MByte/s doppelt so schnell wie Oxygen OS, doch auch das blieb weit hinter den unverschlüsselten 200 MByte/s zurück.

AIDA64 zeigt im CPU-Reiter in der Zeile Neon an, ob die ARMv7-Befehle vorhanden sind, doch das sagt nichts darüber aus, ob Android sie auch nutzt. Mehr Klarheit bringt ein Blick in die Datei `/proc/crypto`. Sie ist mit jedem Dateimanager lesbar, der das Wurzelverzeichnis anzeigt, auch auf Geräten ohne Root.

Die Datei enthält die installierten Kryptografie-Treiber, aus denen sich `dm-crypt` einen aussucht, vorzugsweise „`xts(aes)`“, falls vorhanden. Welche Hardware-Erweiterung der Treiber nutzt, lässt sich aus dem Namen allerdings nicht ablesen. Ein „`qcom`“ im Namen bedeutet zwar, dass spezielle Qualcomm-Treiber installiert sind und dass statt `dm-crypt` das optimierte `dm-req-crypt` verschlüsselt. Aber unklar bleibt, ob AES- oder Neon-Befehle zum Einsatz kommen.

Die Treiber mit Hardware-Unterstützung tragen sich allerdings auch unter weiteren Namen in diese Datei ein, und die sind aufschlussreicher: `__xts-aes-aesni` bei den Intel-Geräten, `__xts-aes-ce` beim Nexus 9 und Robin mit

ARMv8-Krypto sowie `__xts-aes-neonbs` beim OnePlus One mit Neon-Krypto. Beim OnePlus One mit Oxygen, Samsung Note 4 und Nvidia Shield mit Cyanogen fehlen diese Einträge.

Interessanterweise fanden wir bei drei weiteren Geräten eine Neon-Zeile: Motorola Moto G, Nvidia Shield mit dem Original-ROM und Wileyfox Swift. Offenbar nutzen auch sie die Neon-Befehle, das OnePlus One ist also nicht mehr das einzige. Das passt auch zu unseren Messergebnissen. Vor allem wird klar, dass die Neon-Verschlüsselung deutlich der ARMv8- und Intel-Verschlüsselung unterlegen ist – und sogar einer schnellen Software-Verschlüsselung, etwa des Note 4.

## Fazit

Vor dem Verschlüsseln sollten Sie mit Tools wie AIDA64 herausfinden, ob Ihr Gerät die ARMv8- oder Intel-Verschlüsselung beherrscht. Falls nicht, können Sie zwar mit einem Blick in `/proc/crypto` herausfinden, ob die Neon-Verschlüsselung unterstützt wird, aber das hilft nicht viel, denn besonders schnell ist sie nicht. Vom Verschlüsseln von Geräten mit Android-2.x-Partitionierung raten wir ab.

Selbst bei einem langsam verschlüsselnden Gerät bleibt der gefühlte Geschwindigkeitsverlust gering, da das Telefon im Alltag selten längere Dateizugriffe durchführt. Je moderner das Android-Gerät ist, desto weniger spricht also gegen die Vollverschlüsselung und den damit verbundenen Sicherheitsgewinn. (jow)

## Literatur

[1] Blog von Nikolay Elenkov: [nelenkov.blogspot.de](http://nelenkov.blogspot.de)

## Android-Geräte Verschlüsselung

Gerät	Prozessor	Krypto-Methode	unverschlüsselt lesen [MByte/s]	besser ► schreiben [MByte/s]	verschlüsselt lesen [MByte/s]	besser ► schreiben [MByte/s]	lesen [%]	schreiben [%]
Asus ZenFone 2 deluxe	Atom Z3580	Intel	137	80	111	67	81	83
Lenovo Moto G 3rd	Snapdragon 410	ARMv7	125	38	63	27	51	72
Nvidia Shield	Tegra K1 T124	ARMv7	93	31	57	31	62	100
Nvidia Shield (CyanogenMod)	Tegra K1 T124	—	74	33	40	27	54	83
OnePlus One (Oxygen OS)	Snapdragon 801	—	190	54	34	28	18	51
OnePlus One (Cyanogen OS)	Snapdragon 801	ARMv7	202	52	70	46	35	89
Samsung Galaxy Note 4	Snapdragon 805	—	183	77	72	59	39	77
Samsung Galaxy S6	Exynos 7 Octa	ARMv8	282	108	289	96	103	88
Wileyfox Swift	Snapdragon 410	ARMv7	121	50	66	33	54	66
Zum Vergleich: verschlüsselt ausgelieferte Geräte								
Dell Venue 8 7840	Atom Z3580	Intel	—	—	121	34	—	—
Google Nexus 9	Tegra K1 T132	ARMv8	—	—	140	49	—	—
Nextbit Robin	Snapdragon 808	ARMv8	—	—	175	68	—	—
Samsung Galaxy S7	Exynos 8 Octa	ARMv8	—	—	382	82	—	—

Durchschnitt aus drei Messungen mit PC Mark, Einzelwerte sequential read/write

# Schlaues Heim – Glück allein



Ihr eigenes  
Smart Home-Gateway  
jetzt **als Bundle** für  
nur 109,90 €



Jetzt für  
9,90 €  
bestellen!



[shop.heise.de/smarthome16](http://shop.heise.de/smarthome16) ✉ [service@shop.heise.de](mailto:service@shop.heise.de)  
Auch als eMagazin erhältlich unter: [shop.heise.de/smarthome16-pdf](http://shop.heise.de/smarthome16-pdf)

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten  
oder ab einem Einkaufswert von 15 €

 **heise shop**

[shop.heise.de/smarthome16](http://shop.heise.de/smarthome16) >

Jürgen Schmidt

# Probleme bei der Android-Vollverschlüsselung

**Die Vollverschlüsselung von Android weist ein ernsthaftes Design-Problem auf, das die geschützten Daten angreifbar macht, erklärt ein Sicherheitsforscher. Er belegt dies mit konkretem Code, der Brute-Force-Angriffe auf Geräten mit Qualcomm-Prozessor demonstriert.**

**A**ktuelle Smartphones und Tablets schützen die Daten ihrer Nutzer durch eine Vollverschlüsselung (Full Disk Encryption, FDE). Bei iPhones ist sie so gut, dass selbst das FBI Probleme hat, an die Daten zu kommen. Androids ähnliche Verschlüsselung leidet allerdings unter einem konzeptionellen Problem, das das Entschlüsseln der Daten deutlich leichter macht.

Sowohl bei Android als auch bei iOS schützt der Passcode des Benutzers auch dessen Daten. Wenn ein Angreifer Zugriff auf das Gerät bekommt, muss er den Code knacken, um die Daten zu entschlüsseln. Nun sind Passcodes typischerweise noch deutlich schwächer als etwa E-Mail-Kennwörter, viele Nutzer geben sich mit vier oder sechs Ziffern zufrieden. Mit einem vollwertigen PC und erst recht auf spezialisierten Cracking-Clustern ist es keine nennenswerte Hürde, alle möglichen Codes durchzuprobieren.

Deshalb kombiniert iOS den Passcode mit einem Hardware-Key, sodass Knackversuche nur auf dem jeweiligen Gerät erfolgen können. Eine nicht zu umgehende Zeitverzögerung zwischen zwei Versuchen erschwert zusätzlich den Brute-Force-Angriff. Dieser sogenannte UID-Key ist auf jedem Gerät anders und lässt sich nicht über eine Programmierschnittstelle auslesen.

## Qualcomm geknackt

Android macht es zwar im Prinzip genauso, aber der Schlüssel ist per Software zugänglich. Er wird innerhalb der sogenannten TrustZone gespeichert und kann sowohl durch signierten Code des TrustZone-Herstellers als auch durch Sicherheitslücken in dessen Software ausgelesen werden. Und hat der Angreifer erst einmal den Schlüssel, kann er den Passcode per Cracking-Cluster herausfinden und dann das Gerät entsperren.

Wie das geht, erläutert der Sicherheitsforscher Gal Beniamini detailliert in seinem Blog [1]. Insbesondere erklärt er am Beispiel der TrustZone von Qualcomm, wie man den Schlüssel über Sicherheitslücken extrahiert – und damit wäre direkt ein Großteil gerade der teureren Android-Geräte betroffen.

Zwar haben Qualcomm und Google bereits Updates veröffentlicht, die diese TrustZone-Lücken beseitigen (CVE-2015-6639 im Januar-Patch und CVE-2016-2431 im Mai-Patch 2016). Doch die kommen nicht auf jedem Gerät an; BlackBerry und Google patchen sehr schnell, Samsung etwas langsamer und nicht alle Geräte, andere eher zögerlich bis gar nicht. Außerdem weist Beniamini darauf hin, dass ein Angreifer aller Wahrscheinlichkeit nach auch danach noch durch Aufspielen einer alten Firmware mit TrustZone-Bug Zugang zu den Schlüsseln erlangen könnte.

## Gegenmaßnahmen

Der Kauf eines Smartphones mit SoC von Samsung, Mediatek, HiSilicon & Co. statt Qualcomm schützt vor der konkreten Lücke. Die Schwäche der Verschlüsselung bleibt aber bestehen und man ist angreifbar, sobald eine ähnliche Lücke in den anderen SoCs gefunden wird. Außerdem könnte der TrustZone-Hersteller dem Hilfersuchen von Behörden Folge leisten und den Schlüssel auslesen.

Auf allen Geräten erschwert ein langes Passwort den Angriff, denn auch mit dem TrustZone-Schlüssel muss der Angreifer ja das Passwort per Brute-Force knacken. Gegen lange Passwörter spricht, dass man sie bei jedem Entsperren des Geräts eintippen muss – außer man besitzt eines der Geräte, die sich per Fingerabdruck entsperren lassen.

Eleganter ist es, die eh unglückliche Kopplung von Entsperr- und Verschlüsse-

lungspasswort aufzuheben. Das geht beispielsweise mit der App „Cryptfs Password“ des Sicherheitsexperten Nikolay Elenkov, die allerdings Root-Zugriff benötigt. Dann muss man das lange Passwort nur beim Kaltstart des Geräts eintippen und zum Entsperren reicht ein kürzeres.

## Fazit

Um das Problem einzuordnen: Es handelt sich hier nicht um Sicherheitsprobleme der Größenordnung von Stagefright, über die Kriminelle Android-Geräte von außen etwa mit einer MMS kapern könnten. Hier geht es darum, dass jemand, der ein fremdes Gerät in die Hände bekommt, Zugang zu den darauf gespeicherten Daten erlangen kann.

Leicht ist das auch bei Geräten mit Qualcomm-Bug nicht. In der Regel wird der Angreifer zunächst ein Low-Level-Image des Flash-Speichers anlegen müssen. Das erfolgt entweder über den JTAG-Port im Gerät oder mit einem Lesegerät nach dem Auslöten des Chips. Anschließend besorgt er sich über die Sicherheitslücke oder mit Tools des Herstellers den Key aus der TrustZone, um dann eine Wörterbuch- und Brute-Force-Attacke auf den Passcode zu starten. Das sind eher Methoden von Strafverfolgern, Terrorfahndern oder Geheimdiensten als vom Handydieb an der Ecke. Doch Androids Vollverschlüsselung löst nicht alle Versprechen ein, Google sollte also sein Verschlüsselungskonzept dringend überdenken. (jow) 

## Literatur

- [1] Blog von Gal Beniamini: <https://bits-please.blogspot.de/>
- [2] <https://play.google.com/store/apps/details?id=org.nick.cryptfs.passwdmanager>



Jörg Wirtgen

# WebView-Irrtum verhindert Updates

Haben Sie Ihr Android-Smartphone bei der Einrichtung erst mal gründlich entrümpelt, weil es der Hersteller mit einem Haufen unnützer Apps vollgestopft hat? Dann sollten Sie überprüfen, ob Sie dabei nicht übers Ziel hinausgeschossen sind und Schadsoftware ein Einfallstor geöffnet haben.

**A**ndroid System WebView ist eine App mit einem offiziell klingenden Namen, bei deren Aufruf nichts passiert – scheinbar also wichtigerische Bloatware, die man deinstallieren oder deaktivieren will. Doch das ist nicht empfehlenswert: Ganz im Gegenteil erhöht die App die Systemsicherheit durch ihre pure Anwesenheit. Sie stellt nämlich anderen Apps eine aktuelle Browser-Engine ohne bekannte Sicherheitslücken bereit.

Ein grundsätzliches Problem von Android besteht darin, dass sich einzelne Teile des Betriebssystems nicht aktualisieren lassen. Anders als Microsoft bei Windows kann Google nicht direkt einen Patch verteilen, sondern muss die Gerätehersteller und teils sogar Mobilfunk-Provider mit ins Boot holen.

Als erste Gegenmaßnahme lagert Google zunehmend Komponenten in die sogenannten Play-Dienste aus. Diese Systemkomponente wird automatisch über den Play Store aktualisiert. Alle Erweiterungen und Sicherheits-Patches hierfür landen innerhalb weniger Tage auf der Mehrzahl aller Android-Geräte.

## Updates für WebView

Auch WebView, die Browser-Komponente von Android, will Google direkt mit Updates versorgen, um Schwachstellen wie etwa den UXSS-Bug vom Frühjahr 2015 schnell zu beheben. WebView kommt in den meisten der Apps zum Einsatz, die Internetseiten abrufen, darunter einige Browser, aber auch Mail-Apps und RSS-Reader – und auch die Werbe-Banner vieler Apps nutzen WebView. Seit Android 4.4 steckt in WebView als erste Verbesserung nicht mehr die Webkit-Engine von Apple, sondern die hauseigene

und daher sowieso mit Sicherheits-Patches versorgte Chromium-Engine.

Update-fähig ist WebView dadurch nicht, das bringt erst Android 5.0. Google hat WebView allerdings nicht in die Play-Dienste integriert, sondern liefert es in Form der App „Android System WebView“ aus. Begründet hat Google das nicht; vielleicht war es technisch nicht anders möglich oder spart Transfervolumen.

Die Auslagerung bringt aber einen gefährlichen Nachteil mit sich: Anders als die Play-Dienste-App lässt sich die WebView-App nämlich deaktivieren, woraufhin Android alle heruntergeladenen Updates deinstalliert und zukünftige ignoriert.

Von da ab wird nicht etwa jeglicher Aufruf von WebView unterbunden – was ein schöner Trick wäre, um Apps den Internetzugang zu sperren. Stattdessen graben die Apps die Version von WebView aus, mit der das Smartphone ausgeliefert wurde.


Damit läuft im besten Fall Chromium 44 (bei Android 6), schlimmstenfalls Version 36 (bei der Betaversion von Android 5). Die Apps verlieren somit alle neuen Fähigkeiten und Sicherheits-Patches – aktuell ist Chromium 55. Immerhin bleibt man vom UXSS-Bug verschont, denn den hat Google schon mit Chromium 30 im WebView von Android 4.4 beseitigt. Doch die nachfolgenden WebView-Changelogs erwähnen weitere Sicherheitslücken. Zudem bringen neue Chromium-Versionen auch neue Funktionen.

Betroffen sind alle Apps, die auf WebView zugreifen, darunter Schwergewichte wie die Facebook-App und Alternativ-Browser wie Mercury. Einige Browser sind nicht beeinträchtigt, weil sie ihre eigene Engine mitbringen, darunter Dolphin, Firefox, Opera und Googles eigene Chrome-App.

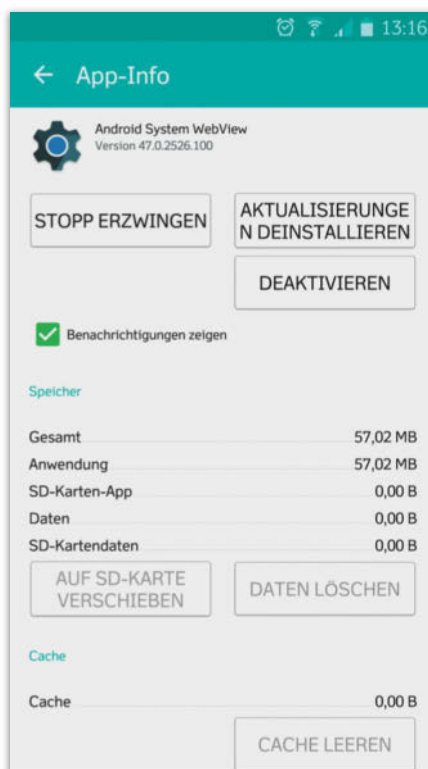
Android 6 und 7 mindern diese Gefahr etwas: Sie führen die WebView-App nicht mehr in der App-Liste, sodass man sie nicht irrtümlich deaktiviert. Sie und andere System-Apps tauchen erst auf, wenn man in der App-Liste oben rechts „Systemprozesse anzeigen“ klickt.

## Updates reaktivieren

Immerhin können Sie diese Sicherheitslücke leicht selbst stopfen. Am einfachsten öffnen Sie die Play-Store-App, suchen nach webview und tippen auf „Android System WebView“. Steht dort der Knopf „Deinstallieren“, ist alles im Lot – tippen Sie also nicht darauf. Heißt der Knopf „Aktivieren“, tippen Sie ihn an und kurz darauf das folgende „Aktualisieren“. Fertig. Sie können diese Schritte auch über den App-Manager erledigen, finden dort die WebView-App allerdings nicht so leicht.

Wenn Sie die App im Play Store nicht finden, nutzen Sie vermutlich Android 4.4 oder älter. Dann haben Sie einen unveränderlichen WebView und müssen nichts machen. Falls dort allerdings „Installieren“ steht, tun Sie das – bei manchen Custom-ROMs fehlt die WebView-App auch nach Installation eines Gapps-Pakets. (jow) 

**Die ab Android 5 vorhandene App „Android System WebView“ sollte aktiv bleiben. Die Knöpfe „Deaktivieren“ und „Aktualisierungen deinstallieren“ im Anwendungs-Manager verschlechtern Ihr System.**





Alexander Spier

# Android für Kinder absichern

**Immer früher kommen Kinder mit dem innigen Wunsch zu ihren Eltern, ein Android-Smartphone oder Tablet zu besitzen. Kann man die einem 10-Jährigen guten Gewissens überlassen? Ja, man kann, wenn sie gut geschützt sind.**

**E**s ist Elternabend. Irgendwann beginnt garantiert die Diskussion darüber, ob die Schüler ihre Smartphones mit in die Schule bringen dürfen oder nicht. Da stehen sich dann unvereinbare Positionen gegenüber: Die pädagogischen Fundamentalisten würden am liebsten jeden Touchscreen von ihren Kindern fernhalten, bis sie 18 sind. Die

Technik-Affinen heben kurz den Kopf und werfen gelangweilt ein, das Handy gehöre nun mal zum Alltag – bevor sie weiter ihre Facebook-Timeline checken.

Dabei gibt es einen gangbaren Weg zwischen diesen Extremen: Die auf dem Schulhof vorzufindenden Android- und Apple-Smartphones lassen sich durchaus kindgerecht konfigurieren. Sie ermögli-

chen es den Eltern, entwicklungsgefährdende Inhalte, ungeeignete Apps oder nicht altersgerechte Funktionen unzugänglich zu machen. Während Apples iOS dafür ausreichende Bordmittel mitbringt, sollten Android-Eltern eher auf Kinderschutz-Apps vertrauen. Im Folgenden erfahren Sie, wie Sie am besten vorgehen und wo die Tücken versteckt sind.

Android gibt Eltern von sich aus kaum Werkzeuge an die Hand, um Smartphones oder Tablets kindertauglich zu machen. Zwar existieren in den Einstellungen und im Play Store durchaus Ansätze, doch eine konsequente und alltagstaugliche Umsetzung fehlt dem mit Abstand am weitesten verbreiteten Smartphone-Betriebssystem und dem angeschlossenen Ökosystem. Wer seinem Kind ohne Bauchschmerzen ein Android-Handy in die Hand drücken will, kommt daher ohne schützende Apps von anderen Anbietern kaum aus; dazu später mehr.

## Jugendschutzlos

Die Jugendschutzeinstellungen des Play Stores dürften auf Dauer nicht einmal der Neugier eines Fünfjährigen standhalten. Grundsätzlich ermöglicht Google das Filtern der Inhalte nach der deutschen Altersfreigabe und den Schutz der Einstellung mithilfe einer PIN. Doch koppelt Google das nicht an den Account, es bleibt eine lokale Einstellung auf dem jeweiligen Gerät. Drückt der Sprössling in der App-Verwaltung beim Play Store auf „Daten löschen“, ist der Zugang wieder frei. Lediglich die Passwort-Abfrage vor kostenpflichtigen Apps und In-App-Käufen lässt sich so nicht umgehen.

Es fehlen Möglichkeiten, mit denen Kids eigenverantwortlich, aber geschützt Apps und andere Inhalte aus dem Google-Angebot nutzen können. Accounts für Kinder unter 13 kennt Google nicht, genauso wenig kann man sie einem Erwachsenen zuordnen und über dessen Konto verwalten. Die Familienbibliothek im Play Store ist für ältere Kinder zumindest ein sinnvoller Ansatz. Darüber kann man ein Familienkonto anlegen und andere Nutzer (über 13 Jahren) hinzufügen. Kinder unter 18 Jahren brauchen die Genehmigung des Familien-Admins, bevor sie eine App kaufen dürfen. In-App-Käufe sind immer zustimmungspflichtig. Welche Apps in der Bibliothek landen, kann der Admin entscheiden.

## Eingeschränkte Nutzer

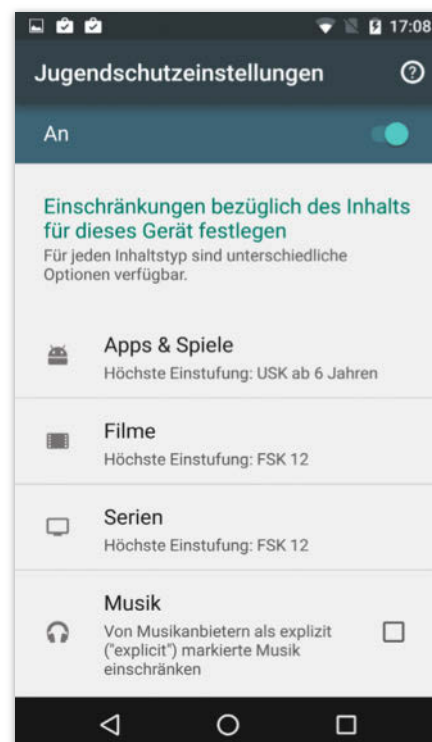
Ab Version 4.3 verwaltet Android auf Tablets mehrere Benutzerkonten. Mit Version 5 haben es die Nutzerprofile auch auf die Smartphones geschafft. Allerdings gibt es die Profilverwaltung nicht auf allen Geräten: Bei neueren Nexus-Geräten wird man fündig, doch einige Hersteller wie Samsung und Sony lassen sie bei ihren Smartphones immer noch heraus.

Die Nutzerkonten selbst taugen nicht zum kindergeschützten Zugang, denn die Zweitnutzer haben nahezu die gleichen Rechte wie der Gerätebesitzer. Interessanter ist das eingeschränkte Nutzerprofil, doch leider gibt es das sogar in der Android-Version nur auf Tablets. Hier geben Sie vor, welche der installierten Apps gestartet werden dürfen und ob Chrome-Browser, Kamera, Telefon und SMS erlaubt sind. Einige Apps bieten auf Basis des eingeschränkten Nutzers weitere Optionen wie eine Altersgrenze für Inhalte an. Andere Anwendungen laufen dagegen überhaupt nicht mit eingeschränkten Profilen zusammen, etwa die Notizen-App von Google.

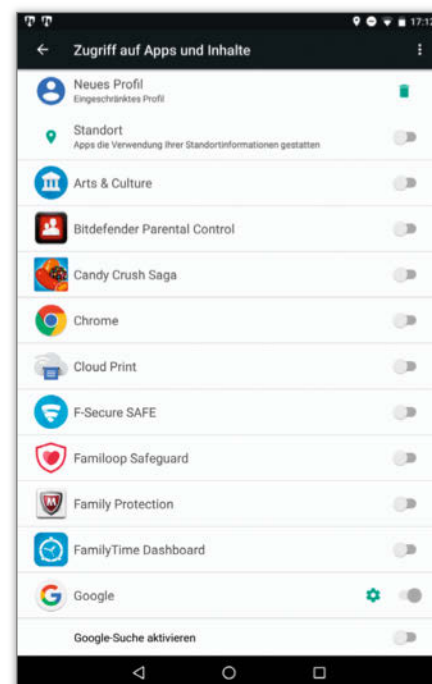
Das eingeschränkte Profil nutzt zwangsläufig die gleiche Google-ID wie der Hauptnutzer. Es greift damit auch auf seine Filme, Musik und Bücher zu. Lediglich der Play-Store-Zugriff und die Nachinstallation von APKs sind tabu. Der Nutzer darf in den Einstellungen vieles ändern und aktivieren, etwa den Flugmodus beenden und das WLAN konfigurieren. Er kann ebenso auf die App-Verwaltung zugreifen – freigegebene Apps können so deinstalliert, deren Einstellungen gelöscht und Updates entfernt werden. Verhindern lässt sich der Zugriff nicht.

Andere sinnvolle Einschränkungen wie eine maximale Verwendungsdauer oder Zeitsperren fehlen. Ein richtiger Kindermodus ist die Kontensteuerung daher schlichtweg nicht. Sie reicht aus, um dem Nachwuchs ein Gerät vorübergehend in die Hand zu geben. Vorher gilt es aber noch, das Gastprofil zu entfernen, welches auf vielen Geräten eingerichtet ist. Denn das nicht durch ein Passwort geschützte Konto hat mehr Rechte und erlaubt etwa das Einrichten eines Google-Kontos.

Will man dem Kind nur jeweils eine App vorübergehend zur Verfügung stellen, hilft die „Bildschirmfixierung“. Diesen simplen Kioskmodus aktivieren Sie in den Einstellungen unter Sicherheit. Dort legen Sie auch eine PIN oder ein Passwort zum Entsperren fest. Nun können Sie die im Vordergrund liegende App anpinen, indem Sie im Taskmanager ein Stück herunterscrollen und das Pin-Symbol antippen. Zugriffszeiten oder zulässige App-Bereiche wie im „geführten Modus“ von iOS gibt es allerdings nicht. Zudem kann das Gerät einfach ausgeschaltet werden, um aus dem Kioskmodus auszubrechen. Deshalb bleibt ein Zugangscode fürs eigene Profil unverzichtbar.



Die Altersfreigaben im Google Play Store sehen solide aus, sind aber dilettantisch geschützt: Sie lassen sich auch ohne Kenntnis der PIN einfach entfernen.



Android erlaubt es, Profile anzulegen und den Zugriff auf Apps zu steuern. Als Kinderschutz taugt das nur bedingt.





Bunt geht es bei Kids Place zu. Die App platziert sich als Launcher im Android-System und blockiert so den Wechsel zu nicht autorisierten Apps.

## App-Hilfe

Die gute Nachricht: Was Android vermissen lässt, können Sie größtenteils mithilfe von Apps aus dem Play Store nachrüsten. Das Angebot ist zahlreich und die grundlegende Funktionsweise meist ähnlich. Zugriffsteuerung, Zeitkontrolle und Standortverfolgung bieten viele Apps kostenlos. Erst für Webfilter, feinere Einstellungen und Nutzungsstatistiken sind In-App-Käufe oder Monatsgebühren fällig. Welcher Ansatz der Familie eher liegt und funktioniert, sollten Sie in aller Ruhe testen.

Nach der Installation erbitten die Programme meist, als „Bedienungshilfe“ für das System zugelassen zu werden. Einigen Apps muss auch der „Zugriff auf Nutzungsdaten“ oder Admin-Rechte eingeräumt werden, wenn sie danach fragen. Mit diesen Rechten ausgestattet, können die Dienste dann Aktivitäten des Nutzers mit-schneiden und Funktionen einschränken. So oder so ermöglichen die Rechte den Apps, Daten über die gesamte Verwendung des Geräts zu sammeln. Viele Dienste speichern diese Daten ebenso auf ihren

Servern wie den häufig integrierten Standortverlauf.

Der größere Teil der als „Kindersicherung“ oder „Elternkontrolle“ im Play Store erhältlichen Programme beschränkt einen herkömmlichen Geräte-Account und verhindert gemäß ihrer Regeln – auf Wunsch nur vorübergehend – den Zugriff auf bestimmte Apps und Funktionen. Sichtbar sind daher alle installierten Inhalte; die Schutz-Software grätscht erst beim App-Start dazwischen, etwa wenn die vorgegebene Nutzungsdauer abgelaufen ist.

Insgesamt tendieren viele Apps zur Vollüberwachung: Geofencing, Standortüberwachung und Aktivitätsberichte sind eingebaut. FamilyTime Parental Control etwa liest sogar SMS-Nachrichten mit und leitet sie an die Eltern weiter. Die grundlegenden Einschränkungen sind meist lokal auf dem Gerät einstellbar, teilweise aber nur über einen zweiten Geräte-Account und mit Registrierung beim Hersteller. Die ermöglicht bei vielen Apps die Konfiguration von außen, über ein anderes Gerät oder eine Webseite. Ideal sind Fernwartungsmöglichkeiten, wenn man den Kleinen viel Autonomie zugestehen will. Starten die zum Beispiel eine nicht erlaubte App, können sie die Freigabe bei den Eltern anfragen.

## Kinder-Oberflächen

Einen anderen Ansatz verfolgen Launcher und Container-Lösungen, sie ersetzen die Standardoberfläche des Smartphones. Ein empfehlenswerter Vertreter ist etwa Kids Place. Der kommt kindgerecht bunt daher und läuft auch ohne Fernzugriff. Bei ihm müssen die Eltern die gewünschten Apps explizit hinzufügen, zum Verlassen der Umgebung wird ein Passwort benötigt. Kids Place trägt sich als Launcher bei Android ein und blockiert so den Wechsel in andere Apps.

Kids Place startet auf Wunsch gleich beim Einschalten des Geräts und taugt somit auch dafür, den Kindern das Smartphone eigenverantwortlich zu überlassen. Umfangreiche, aber teils kostenpflichtige Funktionen sowie Plug-ins zur Zeitkontrolle ermöglichen eine fein abgestufte Kontrolle. Nach dem mit einem Code gesicherten Beenden stehen weiterhin alle Android-Funktionen ohne Passworteingaben und andere Eingriffe zur Verfügung. Falls das Gerät nicht dauerhaft in Kinderhände übergeben werden soll, eignen sich Launcher-Apps wie Kids Place deshalb am besten.

Auch einige Hersteller bieten eigene Kindermodi, zum Beispiel Samsung. Sie sind jedoch nicht darauf ausgelegt, dem Kind das Gerät komplett zu überlassen, sondern sie fungieren als Container-App, die der Hauptnutzer selber startet und lassen viele Optionen vermissen.

## Kleinarbeit nötig

Egal, welche Lösungen Sie nutzen: Diese beeinflussen nicht die Inhalte, die aus dem Play Store oder Diensten wie Spotify abgerufen werden können. Die App-Einstellungen muss man daher selbst am Gerät konfigurieren. Gewährt man dem Kind etwa Zugriff auf den Store, sollte man dort zumindest die Jugendschutzeinstellungen aktivieren und mit einem PIN-Code versehen. Einen Start einer neu installierten App kann dann wieder die Schutzsoftware verhindern.

Einmal korrekt eingerichtet, überstehen die Tools einen Neustart problemlos. Direkten Schutz vor Deinstallation und Rechteentzug sieht Android selbst aller-



Du kommst hier nicht rein! Kontrollwerkzeuge wie Eset Parental Control schieben klare Ansagen vor gesperrte Inhalte; die Kinder können aber um Erlaubnis bitten.

dings nicht vor – eine Passwortabfrage bei kritischen Änderungen fehlt, selbst bei eingeschränkten Android-Profilen. Daher müssen die Kindersicherungs-Apps den Zugriff auf die Einstellungen verhin- dern. Die meisten, wie Eset Parental Control, machen das von Haus aus. Sie gehen in kritischen Bereichen sofort dazwischen und verlangen das Zugangspasswort der Eltern. Intels Safe Family ignoriert das Problem in der Voreinstellung dagegen und ist deshalb problemlos auszuhebeln.

## Browser-Sorgen

Da der mobile Chrome-Browser keine eigenen Webfilter vorsieht, muss der Zugang ebenfalls anderweitig gebändigt werden. Eset Parental Control leitet beispielsweise sämtlichen Webtraffic per VPN über die eigenen Server und filtert die Zugriffe gemäß der Einstellungen der Eltern. Aufrufe gesperrter Webseiten werden zu einer an die Kinder gerichteten Erklärung umgeleitet. Andere Tools verwenden dafür Proxy-Server oder beobachten nur die auf-

gerufene Webseiten und gleichen sie mit den eigenen Filterlisten ab. Damit können sie aber etwa jugendgefährdende Werbe- banner nur eingeschränkt abfangen.

Eine weitere Option ist, einen speziellen Browser für Kinder wie den „Kids Safe Browser“ zu installieren und nur diesen freizugeben. Er integriert sich, wenn vorhanden, in den Kids Place Launcher, funktioniert aber auch autark. Die Schutz-Einstellungen des Browsers können Sie anders als bei Chrome mit einem Passwort schützen. Sie sind mit Blacklist, Whitelist und benutzerdefinierten Regeln umfangreicher als bei den anderen Apps. Für die vom Hersteller gepflegten Filterlisten müssen Sie ein kostenpflichtiges Abo abschließen. Die Filterqualität schwankte bei allen überprüften Tools deutlich. Welche Seiten gesperrt wurden und welche nicht, blieb oft undurchsichtig. Den Kindern über die Schulter zu schauen und eigene Filter und Freigaben anzulegen bleibt daher unerlässlich. Einmal konfiguriert taugen die Apps aber durchaus, dem Nachwuchs ruhigen Gewissens ein eigenes Smartphone zu überlassen.

## Google braucht Nachhilfe

Von den Apps, die wir uns für den Artikel angeschaut haben, hinterließen vor allem Eset Parental Control und Kids Place einen guten Eindruck. Auch weil sie sich sinnvoll lokal konfigurieren lassen, nicht einfach auszuhebeln sind und in der kostenlosen Grundversion ausreichend Möglichkeiten bieten. Wem diese Lösungen nicht liegen, findet im Play Store allerhand Alternativen.

Google muss sich vorhalten lassen, das Thema Kinderschutz in Android nach wie vor nicht anzupacken. Der Konzern verlässt sich auf die App-Entwickler, die aber augenscheinlich Schwierigkeiten haben, vernünftige Maßnahmen im Wildwuchs der Android-Versionen und Herstelleranpassungen umzusetzen. So müssen Eltern immer ein wachsames Auge darauf haben, was die Apps machen.

Für kleinere Kinder gibt es wenigstens spezielle Kinder-Tablets, um sie in die bunte Touch-Welt einzuführen. Was diese Geräteklasse taugt, erfahren Sie auf den folgenden Seiten.

(asp) **ct**



c't Digitale Fotografie

## Objektiv betrachtet:

Das beste Angebot für unsere Leser.

- 6x im Jahr Foto-Know-how in c't-Qualität
- Bequeme Zustellung direkt nach Hause – ohne Versandkosten.
- Mit Dankeschön-Geschenk, garantiert für Sie!



Die Welt der Fotografie ist komplex, faszinierend und herausfordernd zugleich. Die c't Digitale Fotografie taucht mit Ihnen tief in diese Welt ein – aus Leidenschaft.

Tiefenschärfe mit Leidenschaft.



Ihr Geschenk:  
Transcend SDHC-Karte 16 GB

Jetzt bestellen:  
[www.ct.de/foto-abo](http://www.ct.de/foto-abo)



Alexander Spier

## Tablets für Kinder im Vergleich

Schon herkömmliche Tablets bieten für Kinder jede Menge altersgerechte Inhalte. Amazon Fire Kids Edition und Kurio Tab 2 versprechen darüber hinaus eine sichere Kinder-Oberfläche sowie einfache Kontrolle durch die Eltern und sollen auch stürmischen Umgang überstehen. Wir haben sie mit dem klassischen Samsung Galaxy Tab A und dessen Kindermodus verglichen.

**E**gal ob zum Zeitvertreib oder zum Lernen, ob Bücher, Filme oder Spiele, kein anderes Gerät bietet so viele Möglichkeiten für Kinder und ist dabei so flexibel wie ein Tablet. Als Unterhaltungs- und Mitmachmaschine taugt es dank größeren Displays besser als das

Smartphone, trotzdem ist es noch klein und leicht genug zum Mitnehmen.

Doch herkömmliche Tablets bieten auch reichlich Möglichkeiten, an unpassende Dinge zu gelangen. Will man seinem Kind nicht ständig über die Schultern schauen, sondern ihm begrenzte

Autonomie einräumen, braucht es eine sichere Umgebung und ein einfach abzurufendes Angebot für Kinder auf dem Gerät. Damit es beim Herumtoben nicht gleich den Geist aufgibt, muss ein Kinder-Tablet zudem auch mal härtere Stöße aushalten.



Genau das versprechen Amazon Fire Kids Edition und Kurio Tab 2. Auf den ersten Blick unterscheiden sie sich mit ihren schreiend blauen Hüllen deutlich von normalen Geräten. Hinter den praktischen Gummirahmen stecken aber klassische Tablets mit Android beziehungsweise dem Amazon-Abkömmling FireOS. Vorinstallierte Kindersoftware erlaubt den Eltern, schnell eine kontrollierte Umgebung für den Nachwuchs zu schaffen. Amazon bietet sein Fire für 120 Euro an, Kurio will 130 Euro für das Tab 2 haben.

Das Samsung Galaxy Tab A 10.1 2016 ist dagegen ein herkömmliches Android-Tablet ohne spezielle Hülle oder vorinstallierte Kinderangebote. Wie alle neueren Samsung-Geräte hat es jedoch einen nachladbaren Kindermodus, der angepasste Inhalte und Steuerungsmöglichkeiten wie eine Zeitkontrolle beinhaltet. Wir haben die 10-Zoll-Version mit Full-HD-Display und Achtkern-Prozessor für rund 220 Euro getestet. Die kleinere 7-Zoll-Version mit identischer Software liegt mit 120 Euro preislich auf dem Niveau der beiden anderen Kandidaten, bietet aber eine etwas höhere Auflösung.

## Das Hardware-Dilemma

Die schwache Hardware der Kinder-Tablets ist ihr größter Nachteil. Beide haben ein 7-Zoll-Display mit lediglich 1024 × 600 Pixeln und den gleichen langsamen Quad-Core-Prozessor. Die CPU von MediaTek mit vier Cortex-A7-Kernen belegt in allen Benchmarks nur hintere Ränge. Die Leistung reicht aus, dass Android und Apps nicht hakeln und Videos flüssig ablaufen. Doch Ladezeiten ziehen sich spürbar. Hin und wieder hängt das System kurz bei manchen Aktionen, beispielsweise im Browser. Wegen der geringen Auflösung laufen viele Spiele noch mit brauchbaren Frameraten, einige anspruchsvollere Titel wie Real Racing 3 allerdings nur mit minimalem Detailgrad.

Wirklich ärgerlich sind die Displays: Bei ihnen passt die Auflösung des Panels nicht zum Seitenverhältnis, was zu sichtbaren

Verzerrungen und Eierköpfen führt. Das Amazon Fire sieht dank IPS-Technik und ordentlichem Schwarzwert ansonsten sogar recht gut aus, beim Kurio Tab 2 verdirbt ein TN-Panel mit schlechter Blickwinkelstabilität den ohnehin schwachen Eindruck weiter.

Unbenutzbar sind beide Tablets deswegen nicht – mit etwas Eingewöhnung machen sie trotzdem Spaß. Die Hardware ist insgesamt mit den Billig-Tablets bis 80 Euro vergleichbar [1]. Im Unterschied zu denen haben die hier getesteten Modelle keine größeren Macken und bieten etwa ausreichend schnellen WLAN-Empfang, sodass der Familienfrieden auf Dauer gewahrt bleibt.

Gegen das teurere Galaxy Tab A 10.1 sehen beide kaum Land. Sein Prozessor arbeitet flotter und dank größerem Arbeitsspeicher klappt auch der App-Wechsel schneller. Das Display überzeugt mit höherer Pixeldichte, Helligkeit und besserem Kontrast.

## Viel Auswahl für Kids

Die Stärken der Kinder-Tablets liegen bei den Inhalten. Amazon spendiert ein Jahr freien Zugang zu Freetime Unlimited, seiner Flatrate für Kinderinhalte. Die umfasst Zugang zu zahlreichen Apps, Filmen, Serien und Büchern, eingeteilt in drei Altersklassen von 3 bis 5, 6 bis 8 und 9 bis 12 Jahren. Das Kinderprofil kann darauf in der geschützten Umgebung einfach zugreifen.

Allerdings muss man dazu schon bei der Einrichtung des Geräts einem Abo zustimmen und ein Zahlungsmittel für 1-Klick-Käufe hinterlegen. Das Abo verlängert sich nach Ablauf des kostenlosen Zeitraums automatisch und kostet dann 5 Euro im Monat. Die Kündigung des Abos ist über die Einstellungen auf dem Gerät schnell erledigt, nur erinnern muss man sich daran.

Ohne Flatrate ist von der Einfachheit viel dahin. Dann müssen die Eltern die Inhalte zunächst bei Amazon erstellen, um sie danach dem Kind freizugeben. Als altersgerecht erkannte Medien lassen sich in

einem Schwung über ein aufgeräumtes Menü freischalten. Inhalte aus anderen Amazon-Flatrates darf der Nachwuchs aber nicht direkt nutzen, hierfür müsste man die jeweilige App freischalten. Das hebt aber auch die Inhaltskontrolle weitgehend aus.

Einige beliebte Spiele wie Asphalt 8 sind nicht für das Gerät verfügbar. Zudem fehlen im Amazon App-Store generell viele Android-Titel. Der Google Play Store lässt sich zwar mit Aufwand auf das Gerät bringen, doch mit dem Kindermodus sind er und die Apps daraus nicht kompatibel. Medien vom internen Speicher können im Kinderprofil nicht freigegeben werden, hingegen schon einzelne Webseiten und sogar gezielt Web-Videos von YouTube und Co.

## Kurio und Samsung

Auf dem Kurio Tab 2 sind diverse Apps vorinstalliert. In Kooperation mit SuperRTL gibt es Inhalte und Videos passend zu deren Kinderschiene Toggo sowie die Videoplattform kividioo. Die bietet für 6 Euro pro Monat Zugang zu rund 200 Kinderfilmen und -serien. Apps gibt es über den in der Kinderumgebung integrierten App-Store von Kidoz, der auch für andere Plattformen verfügbar ist. Der Shop verlangt eine Registrierung ebenfalls für die kostenlosen Inhalte. Die meisten App-Beschreibungen sind nur auf Englisch. Statt in Euro werden Preise in Münzen angezeigt, die vorher gekauft werden müssen.

Darüber hinaus erlaubt der Kindermodus, andere Apps auf dem Gerät freizuschalten, sodass das gesamte Android-Angebot zur Verfügung steht. Bei neu installierten Apps fragt das System selbstständig, ob man sie freigeben will. Optional lässt sich auch ein eigenes Google-Konto für das Kinderprofil freigeben und damit ein Zugriff auf Google-Inhalte erlauben.

Samsungs Kindermodus fällt beim Umfang deutlich zurück, einige Mitmachprogramme zum Malen und Singen sind dabei. Zwar gibt es auch hier einen angeschlossenen Shop, doch der ist abgesehen von einer Kooperation mit Lego schwach be-

Die beiden Kinder-Tablets werden durch abnehmbare Hüllen geschützt. Geht das Amazon Fire (links) trotz dicker Hülle kaputt, tauscht es der Hersteller kostenlos aus. Das Kurio Tab 2 ist ebenfalls robust, ihm fehlt aber die Garantie.



stückt. Viele Apps sind kostenpflichtig und müssen von den Eltern gekauft werden. Auch für kostenlose Programme ist die PIN der Eltern notwendig. Da die auch zum Entsperren des Kindermodus dient, kann man sie nicht einfach in Kinderhände geben. Zudem ist ein Samsung-Konto nötig. Auf Geräten anderer Hersteller kann man die erstellten Apps nicht nutzen. Installierte Programme aus dem Play Store lassen sich aber einzeln freigeben. Videos und Bücher gibt es im Samsung-Shop nicht, immerhin können lokale Musik- und Videodateien eingebunden werden.

Die sehr bunte Aufmachung und die Inhalte richten sich eher an jüngere Kinder, die dürften aber am Aufbau hin und wieder verzweifeln. Ein Wisch in eine bestimmte Richtung ruft etwa unvermittelt eine Seite mit Lego-Apps auf. Klare Icons für den Wechsel hin und zurück gibt es nicht. Auch der Store nervt und behauptet, es gäbe keine Inhalte, solange man nicht in eine Kategorie wechselt.

## Kontrolle ist besser

Damit die Kleinen nicht ständig vor dem Gerät hängen, lässt sich bei allen Kandidaten die Nutzungsdauer beschränken,

getrennt nach Werktagen und Wochenenden. Samsung erlaubt lediglich jeweils eine pauschale Zeitbeschränkung von maximal drei Stunden. Kurio und Amazon ermöglichen, zusätzlich ein Zeitfenster festzulegen, wann das Gerät überhaupt verwendet werden darf. Abends heimlich im Bett noch Benjamin Blümchen schauen geht also nur, wenn es die Eltern zulassen. Das Tab 2 ermöglicht es sogar, für jeden Tag getrennt eine maximale Sitzungsdauer und Pausenlängen dazwischen einzustellen. Lernprogramme können von der Zeitbeschränkung ausgenommen werden.

Bei Amazon Freetime können Eltern dem Kind Aufgaben stellen, etwa 30 Minuten am Tag zu lesen oder Lernvideos zu schauen. Den Zugang zum Unterhaltungsteil blockiert der Dienst auf Wunsch so lange, bis die Aufgabe erfüllt ist. Für Videos, Bücher, Apps und Internet können eigene Zeitvorgaben gemacht werden.


Die Web-Browser des Amazon und Kurio filtern unangemessene Inhalte über eine vom Hersteller gepflegte Liste und die Vorgaben der Eltern aus. Monatliche Beiträge wie bei Lösungen zum Nachrüsten kosten die Filterlisten nicht. Der Kindermodus von Samsung hat keinen eigenen

Web-Browser und muss manuell mit einem kindersicheren Browser nachgerüstet werden.

Einfach aus dem geschützten Profil ausbrechen kann das Kind bei keinem Gerät. Beim Samsung Tab A kommt es nach einer Bildschirmsperre aber auch nicht mehr alleine rein, denn dabei wird der Zugangscode für das Gerät abgefragt. Den sollte man jedoch setzen, damit nach einem Neustart das Tablet unzugänglich bleibt. Amazon Fire und Kurio Tab schützen das Elternprofil auch mit einer PIN, der Wechsel ins Kinderkonto ist aber jederzeit möglich. Optional darf sich das Kind ebenfalls ein Passwort dafür setzen.

## Fazit

Wer ein speziell für Kinder gemachtes Tablet kaufen will, muss spürbare Kompromisse eingehen. Robust genug sind beide Tablets dank der Schutzhülle, und zur Unterhaltung des Nachwuchses taugt die Hardware allemal. Für größere Aufgaben langt das aber nicht. Den lahmen Prozessor, das pixelige Display und eine generell sparsame Ausstattung haben die Geräte von Amazon und Kurio gemein, lediglich der Grad der Zumutung unterscheidet sich ein wenig. Schnellere Kindergeräte gibt es aber auch für Geld und gute Worte nicht, und so hat am Ende das Fire Kids Edition durch das weniger schlechte Display und den größeren Speicherplatz die Nase vorn. Angesichts der sinnvollen und bei beiden Herstellern durchdachten Kindersoftware ist das schade. Wer bereit ist, monatlich Geld auszugeben, bekommt bei Amazon ein einfach nutzbares reichhaltiges Entertainment-Angebot. Das Angebot von Kurio kann da zwar nicht mithalten, doch dank der Android-Basis findet man viel mehr Apps über den Play Store.

Das Galaxy Tab A von Samsung ist zwar insgesamt das deutlich bessere Tablet, doch kann dessen Kindermodus nicht wirklich überzeugen. Zu klein ist das Angebot und zu umständlich die Benutzung. Will man seinen Kindern Autonomie geben, gibt es bei Android bessere Software zum Nachrüsten (siehe Seite 38). Als gemeinsames Gerät für die Familie bleibt das Tab A allerdings eine gute Wahl und im Vergleich zu ähnlichen 10-Zoll-Konkurrenten ist es zudem günstig. (asp) 

## Literatur

- [1] Alexander Spier, Billiger geht nicht, Tablets mit Android, Windows und Fire OS bis 100 Euro im Vergleich, c't 27/15, S. 82

### Tablet für Kinder

Modell	Fire Kids Edition	Tab 2	Galaxy Tab A
Hersteller	Amazon, <a href="http://www.amazon.de">www.amazon.de</a>	Kurio, <a href="http://www.kurioworld.com">www.kurioworld.com</a>	Samsung, <a href="http://www.samsung.de">www.samsung.de</a>
Betriebssystem / Bedienoberfläche	Fire OS 5.3.4 / FireUI	Android 5.0 / Standard	Android 6.0 / TouchWiz
<b>Ausstattung</b>			
Prozessor / Kerne × Takt	MediaTek MT8127 / 4 × 1,3 GHz	MediaTek MT8127 / 4 × 1,3 GHz	Samsung Exynos 7870 / 8 × 1,6 GHz
Grafik	ARM Mali-450	ARM Mali-450	ARM Mali-T830
RAM / Flash-Speicher (frei)	1 GByte / 8 GByte (4,2 GByte) <sup>1</sup>	1 GByte / 8 GByte (1,5 GByte)	2 GByte / 16 GByte (9 GByte)
Wechselspeicher / mitgeliefert / max.	✓ / – / 128 GByte	✓ / – / 128 GByte	✓ / – / 128 GByte
WLAN / Dual-Band / alle 5-GHz-Bänder	IEEE 802.11 b/g/n / – / –	IEEE 802.11 b/g/n / – / –	IEEE 802.11 a/b/g/n/ac / ✓ / ✓
Bluetooth / NFC / GPS	4.0 / – / –	4.0 / – / –	4.2 / – / ✓
Akku / austauschbar / drahtlos ladbar	2980 mAh (11,3 Wh) / – / –	2820 mAh (10,7 Wh) / – / –	7300 mAh (27,7 Wh) / – / –
Abmessungen (H × B × T)	22 cm × 14 cm × 2,6 cm	19,6 cm × 11,5 cm × 2,1 cm	25,4 cm × 15,4 cm × 0,8 cm
Gewicht Gerät / Hülle	312 g / 90 g	276 g / 77 g	519 g / –
Besonderheiten	Schutzhülle	Schutzhülle, integrierter Standfuß	–
Kamera-Auflösung Fotos / Video	1600 × 1200 (1,9 MPixel) / 1280 × 720	1600 × 1200 (1,9 MPixel) / 1920 × 1080	3264 × 2448 (8 MPixel) / 1920 × 1080
Laufzeit Video / Spiele / Surfen WLAN <sup>2</sup>	6,3 h / 3,8 h / 6,5 h	4 h / 3 h / 5,4 h	12,9 h / 9,4 h / 12,9 h
<b>Display</b>			
Technik / Größe (Diagonale)	LCD (IPS) / 8,7 cm × 15,4 cm (7 Zoll)	LCD (TN) / 8,7 cm × 15,4 cm (7 Zoll)	LCD (IPS) / 13,5 cm × 21,6 cm (10 Zoll)
Auflösung / Seitenverhältnis	600 × 1024 Pixel (175 dpi) / 16:9	600 × 1024 Pixel (175 dpi) / 16:9	1200 × 1920 Pixel (226 dpi) / 16:10
Helligkeitsregelbereich / Ausleuchtung	34 ... 256 cd/m <sup>2</sup> / 81 %	8 ... 198 cd/m <sup>2</sup> / 64 %	4 ... 397 cd/m <sup>2</sup> / 89 %
<b>Preise und Garantie</b>			
Garantie	2 Jahre	1 Jahr	2 Jahre
Straßenpreis	120 €	130 €	120 €
<sup>1</sup> im Handel mit 16 GByte erhältlich <sup>2</sup> bei einer Helligkeit von 200 cd/m <sup>2</sup> gemessen			
✓ vorhanden – nicht vorhanden k. A. keine Angabe			



## Amazon Fire Kids Edition

Für die Kids Edition seines billigsten Fire-Tablets möchte Amazon mit 120 Euro immerhin den doppelten Preis haben. Im Karton liegt dafür zusätzlich eine sehr dicke blaue Gummihülle, die das Gerät vor Stürzen schützt. Das Überstehen einer bestimmten Fallhöhe garantiert Amazon nicht, verspricht aber – egal aus welchem Grund – kaputte Tablets innerhalb von 2 Jahren nach dem Kauf bedingungslos auszutauschen. Beim Ausprobieren mit Hülle überlebte das Gerät Stürze aus Tischhöhe.

Die Hülle hat Aussparungen für alle Knöpfe und Anschlüsse, dennoch gestaltet sich die Bedienung etwas fummelig. Insgesamt wiegt die Kombination mit 400 Gramm für die Größe recht viel. Der USB-Anschluss nervt, in ihm wackelten alle ausprobierten Kabel. Abgesehen davon ist die Verarbeitung des Geräts jedoch solide.

Die 16 GByte Speicherplatz erlauben mehr Freiheit bei der Bestückung. Einige Inhalte können auch auf die optionale MicroSDXC-Karte (bis 128 GByte) ausgelagert werden. Die Laufzeiten sind mit maximal 6,5 Stunden nicht üppig, aber über dem Niveau der Billig-Tablets. Die Stabilität von System und WLAN hat Amazon seit dem Erscheinen des Fire in den regelmäßigen Updates deutlich verbessert. Von der Kamera gibt es weiter nur verrauschte und detailarme Bilder.

- ↑ umfangreiches Medienangebot
- ↑ mit Hülle robust
- ↓ lahme Hardware
- ↓ schwer



## Kurio Tab 2

Das Kurio Tab 2 kostet mit 130 Euro noch ein wenig mehr als das Fire-Tablet und bringt eine ähnliche Hardware-Ausstattung mit. Die Hülle ist deutlich dünner und schützt weniger vom Gerät. Dafür ist die gesamte Konstruktion über 50 Gramm leichter und weniger klobig. Den Falltest vom Tisch überlebte es ebenfalls unbeschädigt. Eine Austauschgarantie bei selbst verschuldeten Defekten gibt es nicht. Eine gedruckte Kurzanleitung hilft sinnvoll beim richtigen Einrichten des Geräts.

Einfach, aber durchaus clever ist der integrierte Standfuß: Von der Rückseite lässt sich ein Plastikteil lösen und so in die Hülle stecken, dass das Tablet in zwei Positionen auf dem Tisch steht. Kurio verkauft das Tablet mit dem Zusatz „Motion Edition“; dahinter verbergen sich aber nur beigefügte Spiele, die die grobkörnige und streifige Frontkamera als Eingabegerät benutzen. Präzisere Bewegungssensoren gibt es nicht.

Nachteil der umfangreichen Software-Ausstattung: Von den mageren 8 GByte internem Speicher bleiben weniger als 2 GByte übrig. Eine MicroSD-Karte lässt sich nachrüsten, doch keine Apps darauf auslagern. Immerhin können die vorinstallierten Spiele gelöscht werden. Ein Micro-HDMI-Anschluss erlaubt die Ausgabe des Bildschirm Inhalts an den Fernseher. Der Akku reicht für höchstens 6 Stunden.

- ↑ viel Software dabei
- ↑ umfangreicher Kindermodus
- ↓ schlechtes Display
- ↓ langsam



## Samsung Galaxy Tab A 10.1

In fast allen Belangen hängt das Samsung Galaxy Tab A 10.1 die beiden Konkurrenten ab, kostet aber doppelt so viel. Der 10-Zoll-Bildschirm überzeugt dank hoher Auflösung mit scharfer Darstellung und eignet sich auch gut zum Lesen. Die Hintergrundbeleuchtung ist hell genug, um das Tablet auch draußen einzusetzen.

Die Verarbeitung fühlt sich sehr solide an, einen Sturz auf harte Oberflächen wie Stein dürfte das Gerät aber nicht überleben. Der Kauf einer Hülle ist also ratsam. Mit über 500 Gramm und 8 Millimetern Dicke ist das Tab A nicht das schlankeste 10-Zoll-Tablet. Das Mehr an Platz kommt aber dem Akku zugute: Die Laufzeiten sind hervorragend, mit fast 13 Stunden beim Surfen über WLAN gehört es in dieser Disziplin zu den besten 10-Zoll-Tablets.

Die CPU ist ausreichend flott, die Grafikeinheit dagegen schwachbrüstig. Sie bringt wegen der höheren Auflösung nicht mehr Frames pro Sekunde auf den Schirm als die beiden Kinder-Tablets. Der interne Speicher fasst 16 GByte, ist aber schon teils durch die Office-Programme von Microsoft belegt; ein MicroSDXC-Kartenslot ist vorhanden. In Innenräumen rauscht die 8-Megapixel-Kamera deutlich, draußen macht sie aber schöne Schnappschüsse. Das Tablet wird mit angepasstem Android 6.0 ausgeliefert.

- ↑ hohe Auflösung
- ↑ lange Laufzeiten
- ↑ zeitgemäße Ausstattung
- ↓ schwacher Kindermodus





Holger Bleich, Jörg Wirtgen

## Datenschutz trotz Handy

Weil Smartphones das wichtigste Kommunikationswerkzeug sind, landen darauf jede Menge sensible Daten, die das Gerät eigentlich nie verlassen dürften. Zwischen dem Datenschutzrecht und der gelebten Praxis klafft eine große Kluft, die sich aber schließen lässt.

Für Datenschützer war es der reinste Hohn: „Der Respekt für deine Privatsphäre ist in unseren Genen programmiert“, erklärte WhatsApp im Update zu seinen Nutzungsbedingungen Ende August 2016 – und ließ sich dann im selben Text weiter unten vom Nutzer abnicken, dass der Messenger-Service entgegen früherer Versprechen persönliche Kundendaten wie Telefonnummern künftig an seinen Mutterkonzern Facebook weiterreichen darf.

Der Bundesverband Verbraucherzentralen (vzbv) sieht die „rote Linie endgültig überschritten“. Facebook habe einen schleichenden Trend bestätigt, kritisierte vzbv-Chef Klaus Müller: „Verbraucher verlieren nach und nach die Hoheit über ihre Daten.“ Im November 2016 reagierte Facebook und stoppte die Datenweitergabe – vorerst.

Das Beispiel WhatsApp zeigt, wie schwer es insbesondere auf Smartphones geworden ist, private, vor allem personenbezogene Daten zugriffssicher zu verwahren.

Der zum De-facto-Standard avancierte Messenger lässt sich nur nutzen, wenn man ihm vollen Zugriff auf die Kontaktliste des Handys gewährt. Eine Möglichkeit, bestimmte Daten – etwa Geschäftskontakte – vom Upload in die WhatsApp-Cloud auszuschließen, bietet die App nicht.

Leider helfen die Smartphone-Betriebssysteme derlei datenhungrigen Apps sogar. Weder Android noch iOS sehen vor, dass die Nutzer gezielt bestimmte Daten vom Zugriff der Apps ausschließen dür-

fen. Egal, ob es um Kontaktdaten, Mails oder Kalender-Einträge geht: Die Handys stellen lediglich einen einzigen Pool bereit, in dem dann die Telefonnummer der Bahnauskunft genauso landet wie die des höchst sensiblen Geschäftskontakts.

Dass die Hersteller der Betriebssysteme kein Interesse daran haben, dem unkontrollierten Datenabfluss Einhalt zu gebieten, ist kein Wunder – sie wollen die Daten ja auch selbst. Ein Android-Smartphone ohne Anschluss an die Google-Cloud zu betreiben macht wenig Spaß. Auch Apple ermöglicht viele nützliche iOS-Funktionen nur iPhones, die permanent an die iCloud angedockt sind. Welche Daten tatsächlich auf den US-amerikanischen Servern der Konzerne landen, ist für den Nutzer selbst dann nicht zu durchschauen, wenn er – wie die wenigsten es tun – die ellenlangen Nutzungsbedingungen und Datenschutzerklärung studiert hat.

## Schutzwürdig

Dieses Gebaren stellt deutsche Handy-Nutzer sogar vor rechtliche Probleme, derer sich viele gar nicht bewusst sein dürfen. Denn anders als in den USA hat der Schutz personenbezogener Daten in Europa und besonders in Deutschland einen hohen Stellenwert.

Es geht dabei weniger darum, dass man seine eigenen Daten in die Cloud pumpt. Da gilt auch im deutschen Datenschutzrecht: Jeder ist seines eigenen Glücks oder Unglücks Schmied. Vielmehr wird es dann kritisch, wenn die Daten anderer Personen ins Spiel kommen – was auf einem Kommunikationsgerät wie dem Smartphone praktisch immer der Fall ist.

Welche Daten als personenbezogen oder „personenbeziehbar“ gelten und deshalb unter Schutz stehen, regelt hierzulande das Bundesdatenschutzgesetz (BDSG). Nach Paragraph 3 fallen außer Namen, Anschriften und Telefonnummern auch E-Mail- oder IP-Adressen darunter.

Noch stärker geschützt sind dem Gesetz zufolge die „besonderen Arten von personenbezogenen Daten“, also etwa Informationen über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und das Sexualleben. Zu deren Schutz gelten schärfere Genehmigungspflichten vor der Verarbeitung.

## Datenschutz-infiziert

Das Datenschutzrecht unterscheidet zwischen privater und nicht privater Nutzung

fremder Daten. Konkret: Falls auf Ihrem Smartphone nur die Daten von Freunden und Verwandten liegen und in die Cloud geschickt werden, greift das BDSG nicht – Sie sind datenschutzrechtlich aus dem Schneider.

Allerdings können andere Rechte trotzdem zu Problemen führen, wenn Sie nicht sorgsam mit den Daten umgehen. Einige Experten sehen beispielsweise bereits einen Verstoß gegen das Persönlichkeitsrecht darin, dass Telefonnummern von Nicht-WhatsApp-Nutzer durch WhatsApp-Nutzer bei Facebook landen. Bislang ist aber kein Fall bekannt, bei dem etwa jemand eine Privatbekanntschaft deshalb verklagt hätte.

Die Regeln des BDSG gelten allerdings dann für die gesamte Nutzung, sobald Sie auf Ihrem Smartphone mit geschäftlichen Daten in Kontakt kommen. Juristen sprechen davon, dass die berufliche Tätigkeit die übrigen Daten „infiziert“. Dazu genügt bereits, dass Sie einen geschäftlichen Kontakt im Handy speichern oder sich bisweilen über Ihr privates Mail-Konto mit einem Firmenkunden austauschen.

Nutzen Sie das Smartphone nicht ausnahmslos privat, gelten für Sie dieselben

Datenschutzbestimmungen wie für ein großes Unternehmen. Und dieses muss als sogenannte „verantwortliche Stelle“ gründlich abwägen, wem es Daten Dritter anvertraut, weil bei BDSG-Verstößen Ärger mit Aufsichtsbehörden, Bußgelder und dank Verbandsklagerecht neuerdings auch Klagen von Verbraucherschutz-Verbänden wie dem vzbv drohen.

Große Unternehmen allerdings verfügen in aller Regel über eine IT-Abteilung und einen Datenschutzbeauftragten, die private Mitarbeiter-Smartphones datenschutzkonform konfigurieren und rechtssichere Verträge beispielsweise mit Cloud-Anbietern aushandeln. Beim „Bring your own Device“ (BYOD) achten sie auf die strikte Trennung von privaten und geschäftlichen Daten.

## Privacy Shield

Kleinen Firmen, Freiberuflern oder gar Privatleuten stehen solche Möglichkeiten in aller Regel nicht zur Verfügung. Sie greifen beim Speichern der Daten auf konfigurierte und auf dem Smartphone vorkonfigurierte Cloud-Dienste zurück, also beispielsweise die von Google, Microsoft oder Apple.

### Participation

#### EU-U.S. PRIVACY SHIELD FRAMEWORK FRAMEWORK: ACTIVE

Original Certification Date: 8/12/2016

Next Certification Due Date: 8/12/2017

#### HR DATA AND NON-HR DATA COLLECTED

Personal data. Purposes vary according to the product, but often include: product registration and support; providing various business and consumer services; enabling sales and other transactions; conducting data analysis to improve products and services; and/or maintaining marketing relationships. Human resources data. For the purpose of administering and carrying out the employment or personnel relationship.

### Privacy Policy

#### HR DATA

Microsoft Data Protection Notice

Description:

This Microsoft Data Protection Notice describes the collection and use of personal employment data. The Notice is available to employees on Microsoft internal sites, services and apps.

Effective Date: 8/1/2016

#### VERIFICATION METHOD

Self-Assessment

#### NON-HR DATA

Document: [Microsoft Privacy Statement](#)

Description:

The Microsoft Privacy Statement explains what personal data we collect from you and how we use it.

Effective Date: 1/1/2016

Beim US-Handelsministerium ist das anerkannte Privacy-Shield-Zertifikat für Microsoft in der öffentlichen Datenbank einsehbar.

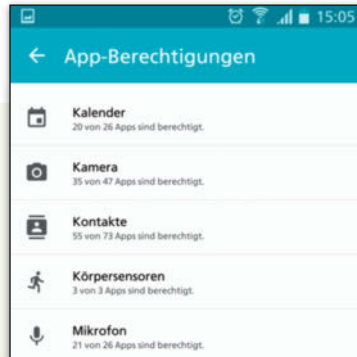
# Maßnahmen zur Datentrennung (1)



## Nur Web-Dienste

Die kritischen Daten landen erst gar nicht auf dem Smartphone, sondern man greift ausschließlich per Browser auf eine Web-Oberfläche zu. Das geht mit jedem Mobilgerät und PC, erfordert aber gehostete Dienste oder eine eigene Server-Infrastruktur.

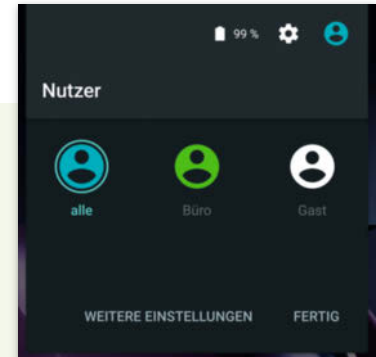
- ⬆️ Firma behält komplette Datenhoheit
- ⬆️ auch für Apps, beziehungsweise dann Server-Anwendungen möglich
- ⬆️ Infrastruktur meist vorhanden oder leicht nachrüstbar
- ⬇️ langsam und unkomfortabel
- ⬇️ kein Offline-Zugriff
- ⬇️ auch kein selektiver Zugriff auf Kontakte durch Apps



## App-Rechte einschränken

Die auf den ersten Blick naheliegendste Lösung: Allen kritischen Apps einfach den Zugriff auf Adressbuch und Termine verweigern. Geht unter iOS ganz gut, unter Android inzwischen auch einigermaßen. Löst allerdings keines der Probleme grundlegend, sodass zusätzlich weitere Maßnahmen erforderlich sind.

- ⬆️ auch ohne schützenswerte Firmendaten sinnvoll
- ⬆️ kostenlos
- ⬇️ kein zuverlässiger Schutz
- ⬇️ pauschale Sperre unpraktisch
- ⬇️ nicht jedem Mitarbeiter zumutbar
- ⬇️ ersetzt keine MDM-Lösung



## Mehrere Nutzer

Schützenswerte Daten zusammen mit sicheren Apps in einen separaten Nutzer-Account installieren; alle fragwürdigen oder privaten Apps im normalen Nutzer-Account belassen. Geht nur auf Android-Tablets und einigen Android-Smartphones; iOS hat immer noch keine Nutzerverwaltung.

- ⬆️ kostenlos
- ⬆️ einfach einzurichten
- ⬆️ Firmen-Account für App-Kauf möglich
- ⬆️ Apps im gesicherten Bereich nutzbar
- ⬇️ keine Benachrichtigungen aus anderem Bereich
- ⬇️ App-Installation ohne Google-Account umständlich
- ⬇️ ersetzt keine MDM-Lösung

Daraus ergibt sich aus datenschutzrechtlicher Sicht für sie ein Problem: Diese Dienste sind auf Bedürfnisse von Konsumenten zugeschnitten. Die abgeschlossenen „Verträge“ heißen Nutzungsbedingungen oder Allgemeine Geschäftsbedingungen und beschränken sich meist auf das niedrigste nötige Datenschutz-Niveau. Jedwede Haftung des Services ist üblicherweise gänzlich ausgeschlossen.

Oft hört man, es sei für EU-Bürger oder Firmen generell unzulässig, personenbezogene Daten bei den großen US-Cloud-Services abzugeben. Das ist nicht

ganz richtig, es gilt aber, einige Dinge zu beachten. Zumindest nicht sensible Daten im Sinne des BDSG dürfen in US-Clouds wandern, sofern die Anbieter ein „angemessenes Schutzniveau“ nach EU-Standards einhalten.

## Selbstzertifizierung

Bis 2015 wurde dieses Niveau über das Safe-Harbor-Abkommen zwischen der EU und den USA definiert. Nachdem der Europäische Gerichtshof (EuGH) dieses Abkommen wegen des zu geringen Schutzniveaus gekippt hat, gibt es seit Juli 2016 das

Nachfolge-Abkommen „EU-US Privacy Shield“. US-Anbieter können sich nach den vorgegebenen Datenschutz-Regeln beim US-Handelsministerium zertifizieren und sich so das „angemessene Schutzniveau“ attestieren.

Die Entscheidung, dieser Zertifizierung zu vertrauen, liegt nun bei demjenigen, der den Dienst nutzt, also bei Ihnen. Auf jeden Fall dürfen Sie nicht drauf vertrauen, was Ihnen der Anbieter erklärt, sondern müssen prüfen, ob die Zertifizierung auch wirklich existiert [1] und noch gültig ist (sie muss jährlich erneuert werden). Außerdem muss die Art der übermittelten



# CONNECTED LIVING ConnFerence

// 15.-16.2.2017, BERLIN //

**Buchen  
Sie  
JETZT!**

## CONNECTED LIVING ConnFerence 2017

Der Mensch im Fokus der Digitalen Transformation

Smart Banking  
im vernetzten  
Leben der  
modernen  
Kunden

Smart Living-  
und Smart  
Working Spaces

Auf dem  
Weg zu  
Wohnungs-  
wirtschaft 4.0 –  
Herausforderungen  
und Chancen

Sicherheit  
im  
Vernetzten  
Leben

Geschäfts-  
modelle und  
Marktstrategien im  
Connected Life

IoT Innovationen  
als Beschleuniger  
der Digitalen  
Transformation

Mit Keynotes von



Dr. Dirk Stenkamp,  
Vorstand der TÜV NORD AG,  
Board of Management -  
Industrial Service,  
IT / International Business



Dr. Heinrich Arnold,  
Chief Executive Detecon Digital,  
Executive Chairman,  
Telekom Innovation Laboratories



Dr. Sven Degelow,  
Mitglied des Vorstands,  
CMO comdirect Bank



Dr. Bernd Heinrichs,  
Managing Director Internet of  
Everything Sales und Innovation  
Centers in EMEAR, Cisco



Ingeborg Esser  
Präsidentin und  
Hauptgeschäftsführerin  
des GdW

Executive Sponsoren:



Goldsponsoren:



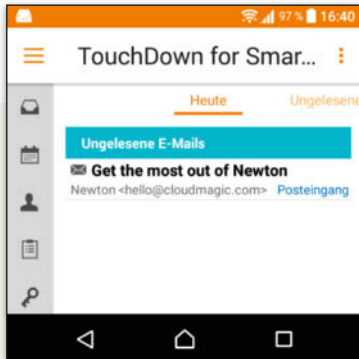
Eine Veranstaltung von:



Teilnahmegebühr (inkl. MwSt.): 940,00 Euro

[www.heise-events.de/connected-living](http://www.heise-events.de/connected-living)

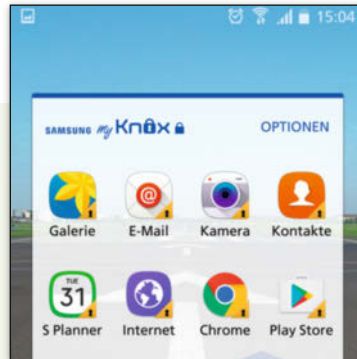
## Maßnahmen zur Datentrennung (2)



### Exchange-Container-App

Apps wie TouchDown synchronisieren sich mit Exchange, geben aber Kalender, Kontakte etc. nicht ans System weiter, sondern erlauben den Zugriff nur innerhalb der App. Die guten Apps kosten um 10 Euro, manche über 20.

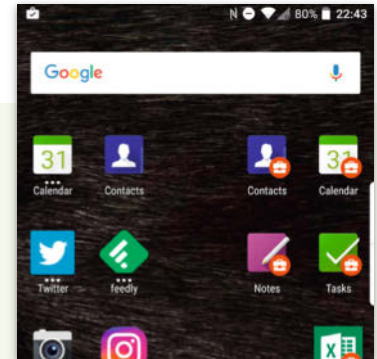
- ⬆️ wenig Aufwand
- ⬆️ bei jedem Gerät möglich
- ⬆️ Infrastruktur in vielen Firmen schon vorhanden
- ⬆️ Firma kann fernlöschen
- ⬇️ nur Mails, Kontakte, Kalender, Notizen, Aufgaben; keine Apps
- ⬇️ Mail-Anhänge nur im ungeschützten Bereich bearbeitbar
- ⬇️ Mail-Server für Privatleute kostenpflichtig (ab 1 Euro pro Monat)



### Lokal getrennter Bereich

Samsung MyKnox richtet einen sicheren Bereich mit separaten Konten und getrennten Daten für Apps ein. Läuft nur auf Samsung-Smartphones. Alle Apps dort nutzbar, wobei man natürlich nur unkritische für MyKnox freigeben sollte. Firmen haben keine Kontrolle über MyKnox-Container und ihre Daten.

- ⬆️ alle Apps mit separaten Einstellungen nutzbar, z. B. Fotos
- ⬆️ geschützter und privater Bereich gleichzeitig aktiv
- ⬆️ kostenlos
- ⬇️ nur auf Samsung-Smartphones
- ⬇️ ersetzt keine MDM-Lösung



### Fernadministration

Die Profi-Lösung: Auf jedem Smartphone einrichtbare, fernwartbare Workspaces mit getrennten Daten und Apps. Früher war ein eigener MDM-Server nötig, inzwischen gibt es auch gehostete Lösungen ab 3 Euro pro Gerät pro Monat. Erfordert trotzdem viel IT-Know-how.

- ⬆️ Apps und Daten komplett vom Privatbereich getrennt
- ⬆️ Firma behält komplette Datenhoheit
- ⬇️ für Privatpersonen nicht praktikabel
- ⬇️ hoher Einarbeitungsaufwand

personenbezogenen Daten von der Zertifizierung abgedeckt sein. Details zur Anwendung des Privacy Shields hat der Landesbeauftragte für Datenschutz Nordrhein-Westfalen in einer FAQ zusammengestellt [2]. Die vielleicht wichtigste Erkenntnis: Das Privacy Shield stellt nicht sicher, dass US-Behörden keinen Zugriff auf die Daten haben.

Microsoft hat sich bereits zum Start des Abkommens selbst zertifiziert und agiert seit dem 12. August 2016 unter dem Privacy Shield. Google ist ebenfalls beigetreten. Facebook folgte im Oktober 2016 – aber nicht für alle Konzernbereiche.

### Berufsgeheimnisse

In der Praxis werden nur wenige, problembewusste Nutzer diese Anforderungen des deutschen Datenschutzrechts tatsächlich befolgen. Die meisten anderen bewegen sich folglich mindestens im dunkelgrauen juristischen Bereich, wenn sie personenbezogene Daten anderer mit den US-Clouds synchronisieren und ihr Handy auch geschäftlich nutzen.

Wer die Clouds nutzt, sollte die Faustregel beachten: Je sensibler die Daten auf dem Handy sind, desto genauer sollte man abwägen, wem man sie unter welchen Bedingungen anvertraut. Geht es um mehr

als nur Kontaktdaten, also etwa Bilder oder Personalakten, sollten die Daten zumindest nur Ende-zu-Ende-verschlüsselt auf dem fremden Server landen [3].

Ohnehin gilt das für sogenannte Berufsgeheimnisträger, also etwa Ärzte, Beratungsstellen-Angestellte, Rechtsanwälte oder Versicherungsmakler: Sie unterliegen besonderen Schweigepflichten und machen sich sogar strafbar, wenn ihnen anvertraute personenbezogene Daten durch mangelnde Sorgfalt an Dritte gelangen. Dieser Sorgfalt werden sie eher gerecht, wenn sie statt US-amerikanische Dienste solche Cloud-Services nutzen, die ihren



Sitz in Deutschland haben. Sie unterliegen damit den strengen deutschen Datenschutzregeln und bleiben außerhalb des direkten Zugriffs ausländischer Ermittlungsbehörden.

Ein wenig nervig an dieser Stelle ist, dass das deutsche Datenschutzrecht allen, die geschäftlich personenbezogene Daten Dritter bei einem deutschen Dienst speichern wollen, eine zusätzliche Pflicht auferlegt, die für US-Unternehmen unter dem Privacy Shield nicht gilt: Sie müssen mit dem Anbieter einen Vertrag zur sogenannten Auftragsdatenverarbeitung nach Paragraph 11 BDSG abschließen. In aller Regel bereiten die Anbieter diesen Vertrag unterschriftsreif vor – der Aufwand hält sich also in Grenzen.

Kaum bekannt dürfte sein, dass auch besonders strenge Regeln für Finanzdaten gelten: Paragraph 146 der deutschen Abgabenverordnung regelt die „Ordnungsvorschriften für die Buchführung und für Aufzeichnungen“. Danach müssen alle steuerlich relevanten Daten auf inländischen Servern gespeichert sein. Will man die

Daten in eine ausländische Cloud verlagern, muss man zuvor eine schriftliche Genehmigung bei der zuständigen Finanzbehörde einholen.

## Am besten trennen

Auch Arbeitgeber stehen in der Datenschutz-Verantwortung. Gestatten sie ihren Mitarbeitern, auf dem privaten Smartphone Unternehmensdaten zu speichern, müssen sie Regeln dazu aufstellen. Der IT-Branchenverband Bitkom etwa stellt einen ausführlichen Leitfaden bereit, der in das Thema einführt [4]. In größeren Unternehmen ist eine Betriebsvereinbarung nötig.

Aus all dem wird deutlich, dass schnell mit dem deutschen Recht in Konflikt gerät, wer allzu unbedarft das private Smartphone auch beruflich nutzt. Es ist wohl übertrieben, gleich jeden Kontakt zu US-amerikanischen Clouds abzubrechen, wenn man etwa als Freiberufler einige Business-Kontakte auf dem Handy pflegt. Wickelt man aber beispielsweise

seine geschäftliche Mail mit dem privaten Smartphone ab, sollte man auf EU-Anbieter umsteigen.

Vor allem gilt jedoch: Die privaten und beruflichen Daten sind auf dem Gerät voneinander abzuschotten. Dass das funktioniert und gar nicht so aufwendig ist, zeigen wir in den folgenden Artikeln ausführlich. (hob) **ct**

## Literatur


- [1] Offizielle Datenbank Privacy-Shield-zertifizierter US-Unternehmen:  
[www.privacyshield.gov/list](http://www.privacyshield.gov/list)
- [2] FAQ zum EU-US Privacy Shield:  
<https://www.idi.nrw.de>
- [3] Dr. Hans-Peter Schöler, Bequem und sicher in die Cloud, End-to-End-verschlüsselnde Speicherdienste im Test, c't 19/15, S. 106
- [4] Bitkom-Leitfaden zu BYOD:  
<https://www.bitkom.org/Publikationen/2013/Leitfaden/BYOD/130304-LF-BYOD.pdf>

# Bleiben Sie auf der sicheren Seite

Jetzt für nur 9,90 € inklusive Desinfec't 2016/17 bestellen.



 [shop.heise.de/ct-security16](http://shop.heise.de/ct-security16)

 [service@shop.heise.de](mailto:service@shop.heise.de)

Auch als eMagazin erhältlich unter: [shop.heise.de/ct-security16pdf](http://shop.heise.de/ct-security16pdf)



 **heise shop**

[shop.heise.de/ct-security16](http://shop.heise.de/ct-security16) >







Stefan Porteck, Jörg Wirtgen

## Berufliche und private Daten voneinander abschotten

Den datenklaubenden Apps die Rechte zu entziehen, das klappt erstens nicht gut und reicht zweitens nicht aus, um Büro- und Privatleben digital auseinanderzuhalten. Unter Android stehen wirksamere Methoden zur sauberen Datentrennung bereit, Mehrbenutzerverwaltung und Samsung MyKnox etwa. Will man nur Kontakte, Termine und Mails schützen, sperrt man sie einfach in eine Exchange-fähige App ein.

**E**in Android-Gerät für alles soll es sein, für Berufliches und Privates. Doch wehe, die Klientendaten landen auf außereuropäischen Facebook- oder Google-Servern oder die privaten E-Mails von Kumpels auf dem Server des Arbeitgebers. Um solche Missgeschicke zu verhindern, gibt es für Android zahlreiche, größtenteils kostenlose Lösungen.

Der offensichtliche Ansatz: Identifizieren Sie die Apps, die Zugriff auf sensible

Daten haben, sperren Sie entweder den Zugriff, oder tauschen Sie sie gegen diskretere Alternativen. Das klingt zwar erstmal einfach, erfordert aber Ihre laufende Aufmerksamkeit und löst nicht alle Probleme der Datentrennung.

Dennoch bleibt es immer sinnvoll, sich über die Rechtesituation auf seinem Smartphone im Klaren zu sein. Besonders leicht klappt die Suche nach datenabziehenden Apps ab Android 6: Rufen Sie die

Systemeinstellungen und dort den Menüpunkt „Apps“ auf. Über das Icon mit dem Zahnrad gelangen Sie schließlich zu den App-Berechtigungen.

Hier listet Android nach Berechtigungskategorien sortiert alle Apps auf, die bestimmte Rechte eingefordert haben. In Bezug auf Firmendaten sind hiervon vor allem der Zugriff auf Kalender, Kontakte, Telefon und SMS-Nachrichten interessant; bei Interesse am Schutz

der Privatsphäre auch Apps mit Standortzugriff.

Auf den ersten Blick wird dort klar, dass die Anzahl der Apps mit Zugriff auf sensible Daten größer ist, als man vermuten würde. Selbst Anwendungen, die augenscheinlich nichts mit den eigenen Kontakten oder dem Kalender zu tun haben, räumen sich die Zugriffsrechte ein. Viele tun das mit gut gemeinten Absichten, wie der DB Navigator der Bahn, der den Kalenderzugriff nur dafür nutzt, um die Abfahrtszeiten einer gebuchten Reise in den Kalender einzutragen. Kritisch sind hingegen alle Apps einzustufen, die eine soziale Komponente bereitstellen – beispielsweise, um in Netzwerken möglichst bequem neue Bekanntschaften zu finden. Dazu gehören natürlich WhatsApp und Facebook, aber auch viele Spiele oder Tools wie die Musikerkennungs-App Shazam und Google Earth.

Sobald eine App anbietet, sich mit anderen Nutzern zu vernetzen, ist das fast schon ein sicheres Indiz, dass sie das Adressbuch abgreifen und an ihre Server schicken wird. Glücklicherweise können Sie seit Android 6 in genau diesem Einstellungs-Menü einzelnen Apps unerwünschte Zugriffsrechte entziehen. Da Apps schon seit rund einem Jahr darauf vorbereitet sein müssen, klappt das in den meisten Fällen problemlos. Ältere oder schlampig programmierte Apps quittieren den Zugriff auf ein entzogenes Recht schlimmstenfalls mit einem Absturz. Einige neuere verweigern ohne die Rechte die Zusammenarbeit. In solchen Fällen wird es Zeit für eine Alternative.

## Unter älterem Android

Für ältere Geräte ohne Update auf Android 6 kann man eine Rechtevergabe entweder per Root und speziellen Tools oder vielleicht per Update auf ein aktuelles CustomROM nachrüsten – beides ist weder trivial noch im Umgang mit Firmendaten uneingeschränkt empfehlenswert, da ein Root bei unsachgemäßem Umgang ein Sicherheitsrisiko darstellt.

Eine Alternative für ältere Android-Versionen ist die an der Uni Saarbrücken entwickelte, 4 Euro teure App „SRT AppGuard“. Sie listet nicht nur alle installierten Apps auf und klassifiziert sie nach den eingeforderten Rechten. Zusätzlich wendet sie einen Trick an, um Apps auch auf Smartphones ohne Root Rechte zu entziehen: Zunächst deinstalliert sie die ursprüngliche App und erweitert sie um eine Middleware, die API-Zugriffe abfängt und an AppGuard weiterleitet. Anschließend

wird die derart gepatchte App wieder installiert. Fortan können Sie in AppGuard einstellen, welche Rechte Sie der App gewähren wollen.

Durch diese Modifikation verlieren die Apps die Verbindung zum PlayStore und dessen automatische Updates. Damit sie nicht veralten, prüft AppGuard sie regelmäßig auf Updates und installiert diese samt Patch automatisch. Aufgrund dieser nicht Google-konformen Arbeitsweise ist die App nicht im Play Store erhältlich, sondern nur beim Hersteller. Beahlt wird per Vorkasse oder PayPal.

## Datenzugriff erwünscht

Egal, welche Android-Version: der Rechteentzug bleibt eine mühsame und fehlerträchtige Arbeit. Schon in kleinen Gruppen ist sie nicht jedem zuzumuten, und Betriebe dürfen sich gar nicht darauf verlassen, dass kein Mitarbeiter jemals eine missbräuchliche App übersieht.

Zudem sollen einige Apps ja durchaus auf bestimmte Kontakte oder Kalender zugreifen, nur halt nicht auf alle. Möchte man beispielsweise WhatsApp nutzen, müssen härtere Geschütze aufgefahren werden: Der Messenger greift sich alle Adressbücher, die er auf dem Smartphone findet, auch die lokalen Telefonbücher und den Speicher der SIM-Karte.

Der wichtigste Schritt bei der Datentrennung ist also, die beruflichen Kontakte, Termine, Mails und Dateien woanders zu speichern als die privaten. Ob Sie dann die privaten Daten bei Google, Microsoft oder Apple speichern, ist eine persönliche Geschmacksfrage – die dienstlichen Daten sollten jedenfalls auf einem Server des Betriebs oder wenigstens in der EU liegen.

## Exchange oder OwnCloud

Viele Betriebe nutzen für Mails, Kontakte und Termine Microsoft Exchange oder eine kompatible Lösung wie Zimbra oder Open XChange, die ebenfalls per ActiveSync oder dem neueren EWS-Protokoll erreichbar ist. Wenn die IT-Abteilung es erlaubt, kann man dort auch sein Privatgerät einhängen. Man gibt sich allerdings ein wenig der Firmen-IT preis: Die Admins können das Gerät fernlöschen, eine Verschlüsselung verlangen und Regeln für den Sperrbildschirm festlegen.

Privatkunden bekommen ActiveSync/EWS-Zugänge bei vielen deutschen Mail-Anbietern und Server-Hostern für rund fünf Euro Aufpreis, einige Angebote gehen schon ab einem Euro los. Kommerziell

nutzbare Zugänge lassen sich die meisten Provider etwas teurer bezahlen.

Die meisten Exchange-Server haben gute Web-Oberflächen, manche inklusive Online-Office. Sie reichen zumindest für die gelegentliche Nutzung nicht nur am Privat-PC, sondern auch per Smartphone völlig aus, sodass man gar nichts installieren oder lokal speichern müsste. Zudem können sich Mitarbeiter etwa Kalender gegenseitig freigeben. Dazu ist allerdings das neuere Protokoll EWS nötig, das nicht alle Server und Apps unterstützen.

Wenn es kostenlos sein soll und der potenzielle Zugriff der US-Geheimdienste nicht stört: Bei Microsoft bekommt man unter Outlook.com einen immerhin nach Privacy Shield zertifizierten, etwas eingeschränkten Exchange-Zugang.

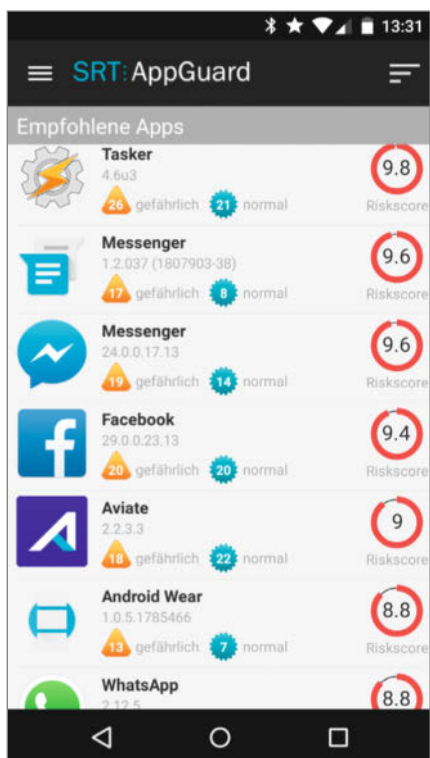
Für Selbstbastler siehts allerdings schlecht aus, denn die ActiveSync-Server wie Zimbra, Open Xchange und Co. sind kostenpflichtig. Lediglich von Zarafa gibt es die kostenlose Community Edition, die allerdings nicht trivial zu warten ist und dann noch ein lizenzierungspflichtiges ActiveSync-Modul benötigt.

Bequemer und günstiger lassen sich Kontakte und Termine auf eigenen Servern mit Hilfe der Open-Source-Cloud OwnCloud und dessen Fork NextCloud unterbringen. Beide Cloud-Anwendungen laufen auch auf langsamen Webservern und begnügen sich mit PHP und bei alleiniger Nutzung mit einer sqlite-Datenbank. Sie lassen sich recht einfach auf vielen NAS-Systemen und sogar einem Raspberry Pi installieren.

## Datentrennung Light

Damit WhatsApp & Co. keinen Zugriff auf die so separierten Daten bekommen, dürfen Sie den Firmen-Account nicht unter Android einbinden. Stattdessen installieren Sie eine App, die sich um diese Daten komplett selbst kümmert, ohne sie mit den systemweiten Android-Datenbanken zu synchronisieren. Die vielleicht bekannteste dieser Container-Apps ist TouchDown, für Android sowie iOS erhältlich. Zum Datenabgleich nutzt sie ActiveSync oder EWS.

Theoretisch wäre auch ein CardDAV/CalDAV-Container denkbar, womit man auch OwnCloud/NextCloud-Server und Nutzer von Mail-Providern wie posteo.de ohne ActiveSync an Bord hätte. Doch wir kennen keine App, die das gewährleistet – der Zweck aller uns bekannten CalDAV/CardDAV-Apps ist im Gegenteil, alle abgeglichenen Daten ins Android-System zu



**AppGuard entzieht auch unter älteren Android-Versionen ohne Root-Zugriff den Apps einzelne Rechte.**

synchronisieren, damit andere Apps darauf zugreifen können.

Für die Datentrennung per Container-App kommt also nur ActiveSync/EWS in Frage. Im Play Store findet man rund ein Dutzend Apps, die Mails per Exchange abgleichen, doch einige unterstützen nur das neuere EWS-Protokoll – viele Server benötigen aber noch das ältere ActiveSync. Damit die Apps auch zur Datentrennung taugen, müssen sie zusätzlich eine Kalender- und Kontakte-Verwaltung mitbringen, was etwa der BlackBerry Hub+, MailWise, Newton und RemoSync tun. Doch diese vier patzen bei der für die Container-Lösung entscheidenden Eigenschaft, nämlich den Abgleich der synchronisierten Daten mit den Android-Datenbanken auf Wunsch abzuschalten.

## Nur TouchDown und Nine

Microsofts Outlook-App kommt aus einem anderen Grund nicht in Frage: Sie ist gar keine echte Mail-App, sondern schickt die Zugangsdaten des Nutzers an Microsoft und überlässt den Datenabgleich deren Servern. Das ist genau das Gegenteil von Datentrennung: Mit der Outlook-App landen auch Mails, Kontakte und Kalender in

einer US-Cloud, die eigentlich sicher auf EU-Servern gespeichert sind. Die Outlook-App sollte man also nur für Microsoft-Konten nutzen.

So haben wir neben TouchDown nur eine App gefunden, die alle Kriterien erfüllt: Nine von 9 Folders. Beide sind umfangreiche Apps mit individuellen Stärken und Schwächen. Sie kosten je nach aktuellem Sonderangebot 10 bis 20 Euro, kostenlose Testversionen sind erhältlich.

Während TouchDown bei der Installation sicher konfiguriert ist, müssen Sie Nine beim Einrichten eines Exchange-Accounts anweisen, nicht auf die Kontakte und Adressen des Telefons zuzugreifen. Vergewissern Sie sich danach, dass in den Kontakte-Einstellungen der Haken bei „Kontakte synchronisieren, Nine-Kontakte sind mit den Gerätekontakten synchronisiert“ nicht gesetzt ist, genauso bei den Kalender-Einstellungen. Zudem sollten Sie unter Einstellungen/Sicherheit die Verschlüsselung der lokalen Daten aktivieren.

## Adress-Separation

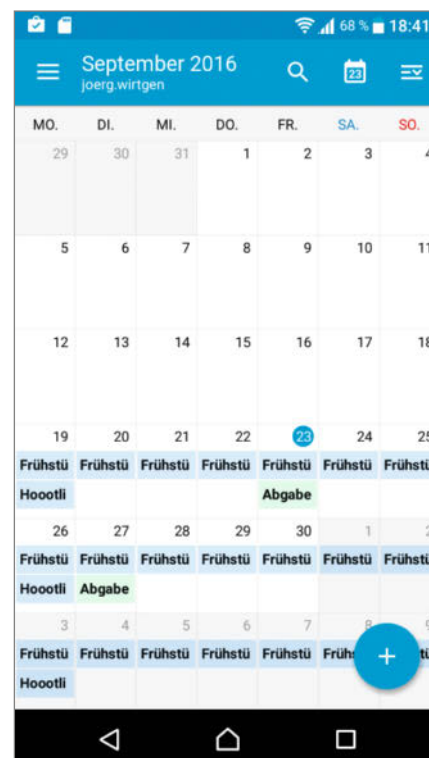
Unpraktisch an diesen Exchange-Containern: Anrufe oder SMS von Firmenkontakten erscheinen nur mit ihrer Nummer, ohne Name. Telefonate und SMS muss man aus der App initiieren. Auch gelingt der Kontakt über Dienste nur umständlich, deren Nutzer sich per Telefonnummer oder Mailadresse identifizieren.

TouchDown bietet dafür den selektiven Export einzelner Kontakte ins Android-System an. Diese stehen dann mit allen Feldern sämtlichen anderen Apps (mit Adressbuchzugriff) zur Verfügung.

Bei Terminen entsteht durch die Trennung kein so großer Komfortverlust. Allerdings zeigen weder die Android-Apps die beruflichen, noch die Container-Apps die privaten Termine, sodass man gegebenenfalls zwei Kalender überprüfen muss – unpraktisch, wenn sich berufliche und private Termine zeitlich überschneiden. Eine Exchange-App, die zusätzlich die Android-Kalender einbindet, haben wir nicht gefunden.

Manche Web-Oberflächen der Exchange-Server bieten ihrerseits die Möglichkeit, einen privaten Kalender einzubinden, sodass man immerhin dort alle Termine im Blick behält. Doch es lassen sich meist nur wenige Kalender-Anbieter auswählen, zudem gelingt die Anbindung nicht immer – wir haben keine praxistaugliche Verbindung hinbekommen.

Zwei Auswege sind denkbar: Man beschränkt die Terminfindung auf den



**Nine ist die modernere, flexiblere App; TouchDown wirkt kantiger und kommt mit mehr als einem Kalender nicht so gut zurecht.**

(Büro-)PC mit einem Tool, das alle benötigten Kalender abfragt; beispielsweise hat der Windows-Mailer eM Client eine gute ActiveSync- und CalDAV-Anbindung. Alternativ spricht man mit der IT-Abteilung ab, die Termine nicht ganz so rigide zu schützen und synchronisiert sie dann doch in Android – Nine beherrscht es, den Kalender ins System zu pumpen, die Adressen aber für sich zu behalten.

## Mehrere Nutzerkonten

Bei Mails mit Anhängen stößt die Idee der Exchange-Apps an eine Grenze, denn diese Apps bieten schon zum Anschauen der Anhänge und erst recht zum Bearbeiten bestenfalls rudimentäre Möglichkeiten. Sobald der Nutzer die Zahlen in der Excel-Tabelle korrigieren, das PDF mit Anmerkungen versehen oder die Präsentation abspielen will, geht das nicht in der App. Stattdessen wird die bearbeitende App gestartet und eine lokale Kopie der Datei landet auf dem Telefon – außerhalb der Reichweite der Firma. Einige Smartphones öffnen die Anhänge direkt in den Apps von Microsoft, Google oder Dropbox, die sie mit einem unbedachten Fingertipp in ihre Clouds hochladen.



Und schließlich helfen die Exchange-Lösungen gar nicht dabei, berufliche Apps zu nutzen. Hat man sich im Betrieb etwa auf die Nutzung eines sicheren Messengers verständigt, darf der trotzdem nicht parallel zu WhatsApp installiert werden.

Ab Android 6 gibt es einen sicheren und bequemen Weg zur zuverlässigen Datentrennung, der auch Apps umfasst. Das Kunststück gelingt mit Hilfe der eigentlich für Familien gedachten Verwaltung mehrerer Nutzerkonten. Leider implementieren das nur wenige Android-Hersteller wie Google selbst, Motorola und Sony, doch bei Geräten von Samsung etwa fehlt diese Möglichkeit.

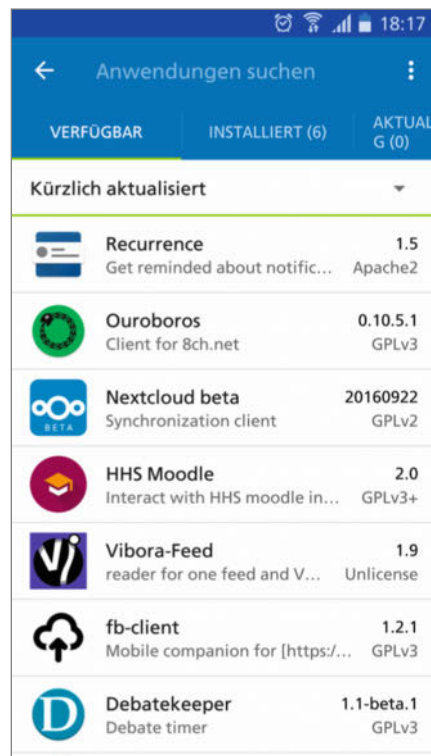
Die Einrichtung eines neuen Nutzers geht flott: Zunächst rufen Sie in den Systemeinstellungen den Menüpunkt „Nutzer“ auf und fügen dort über das Pluszeichen einen neuen Nutzer hinzu. Sie landen dann auf dem Anmeldebildschirm von Android, ähnlich der Ersteinrichtung Ihres Smartphones.

Zunächst bietet Android an, ein Google-Konto einzurichten – diesen Punkt überspringen Sie. Im nächsten Dialog vergeben Sie einen Nutzernamen wie „Dienstlich“. Bei der folgenden Einrichtung der Google-Dienste verbieten Sie alle Optionen wie den Standortdienst oder die Übertragung von Diagnosedaten. Die abschließende Frage nach dem Anlegen eines Mail-Accounts überspringen Sie auch.

Anschließend findet man eine frisch eingerichtete und vom anderen Nutzerkonto vollständig getrennte Android-Oberfläche vor. Das sollten Sie als Erstes mit einem individuellen Sperrmuster, besser PIN oder Passwort schützen. Fortan wechseln Sie über das Nutzerkonten-Symbol in der Quickstart-Leiste flink zwischen dienstlichen und privaten Nutzerkonten.

Apps in anderen Konten liegen in einem getrennten Speicherbereich und haben keinerlei Zugriff auf die hier gespeicherten Daten. Selbst mit einem Dateimanager ist es nicht möglich, auf die privaten Daten wie den Download-Ordner, Fotos oder Notizen des anderen Nutzerkontos zuzugreifen. Auf gerooteten Geräten gelingt der Zugriff auf fremde Nutzerkonten hingegen einfach; das behebt erst Android 7 mit der zusätzlichen Dateiverschlüsselung. Eine etwaige MicroSD-Karte bleibt für alle Nutzer lesbar.

Damit die Telefon-App von Google keine Telefonnummern von eingehenden Anrufen an Google-Server schickt, deaktivieren Sie dann in deren Einstellungen die Funktion „Anrufer-ID und Spam“. Wenn Sie nun dienstliche Kontakte in Googles Kontakte-



**Mit Hilfe des einigermaßen gefüllten F-Droid-Stores kann man die nötigsten Apps auch ohne Google-Account auf dem dienstlichen Nutzerkonto installieren.**

App eintippen wollen, bekommen Sie die Aufforderung, einen Google-Account einzurichten. Schlagen Sie das aus, bietet die App eine lokale Speicherung auf dem Gerät an.

Wegen der strikten Datentrennung sind Sie von Benachrichtigungen des jeweils inaktiven Accounts abgeschnitten: Keine WhatsApp-Nachrichten, während Sie Büro-Mails erledigen, keine Erinnerung an berufliche Termine, während Sie auf Facebook lesen. Lediglich Anrufe und SMS kommen in beiden Bereichen an und werden auch nach dem Nutzerwechsel in beiden Protokollen angezeigt, wenn Sie den Nutzer zuvor in den Nutzereinstellungen für Anrufe freigeschaltet haben. Ruft ein im jeweils inaktiven Nutzer gespeicherter Kontakt an, sehen Sie nur dessen Rufnummer, den Namen findet Android mangels Zugriff aufs Adressbuch nicht.

## Apps ohne Google

Sie können natürlich zur Installation von Apps auch ein Google-Konto einrichten, idealerweise ein speziell für den Business-Bereich neu angelegtes, das Sie so leer wie möglich halten. Oder eines vom Betrieb, damit der etwaige App-Käufe bezahlt. Wir

raten davon allerdings ab, da Sie dann höllisch aufpassen müssen, nicht doch eine Einstellung falsch zu setzen, worauf kritische Daten bei Google landen. Eine Idee wäre, den Google-Account nach der Installation aller benötigten Apps wieder zu löschen, noch bevor Sie die Firmenkontakte abgleichen. Die Apps bekommen dann allerdings keine Updates.

Ohne Google-Konto lassen sich Apps nur über Umwege installieren. Ein Weg ist, die APK-Datei der gewünschten App von vertrauenswürdigen Webseiten – beispielsweise [www.apkmirror.com](http://www.apkmirror.com) – herunterzuladen und manuell zu installieren; Android fragt daraufhin an, ob Sie die Installation aus fremden Quellen erlauben. Auf einigen Smartphones können Sie das dann nur für diese einzelne Installation erlauben, auf allen anderen müssen Sie die Option nach der Installation dringend wieder ausschalten – schließlich ist dieses Side-loading von dann doch nicht so vertrauenswürdigen Apps das Haupteinfallstor von Schädlingen unter Android.

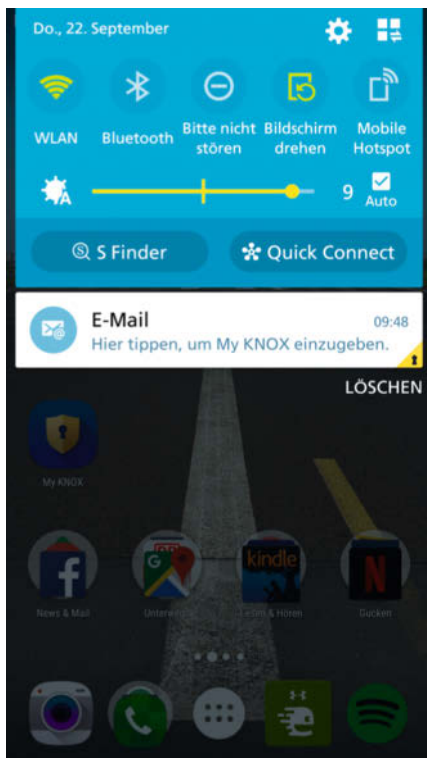
Die so installierten Apps bekommen keine automatischen Updates – man muss also regelmäßig nach neuen Versionen schauen und sie von Hand herunterladen und installieren. Wenn Ihnen das zu kompliziert ist, laden Sie sich die App des Amazon-Stores oder besser des Open-Source-Markets F-Droid herunter und installieren Apps aus deren Angebot. So gut gefüllt wie der Store von Google sind sie allerdings nicht.

Grundsätzlich sollte Ihre Devise sowieso sein, dass weniger mehr ist: Eine einzige zu neugierige App im Dienst-Account reicht aus, um den ganzen Aufwand auf einen Schlag zu vernichten. Im Idealfall nutzen Sie nur quelloffene Tools, verzichten auf Apps, die eine Registrierung verlangen und entziehen die nicht zwingend benötigten Rechte. Alle nicht vertrauenswürdigen Apps gehören ins normale Benutzerkonto, nicht ins berufliche.

## Kleine App-Auswahl

Die vielleicht wichtigste App auf dem Dienst-Account ist ein Mail-Client. Hierfür bietet sich das kostenlose und quelloffene K9-Mail an, das Sie auf der Projekt-Seite bei GitHub herunterladen können. Einziger Wermutstropfen: K9 unterstützt nur IMAP und das veraltete POP3, aber nicht ActiveSync oder EWS zur Kommunikation mit Exchange-Servern.

Einige ActiveSync-fähige Apps wie Nine oder RemoSync finden Sie im Amazon-Store, aber auch die vom Hersteller mitgelieferten Mailer sind einen Blick wert.



Bei MyKnox bleiben beide Konten aktiv und zeigen Benachrichtigungen an. Die von MyKnox sind aber erst dann vollständig lesbar, wenn der Container aufgeschlossen ist.

Oftmals mag sogar die Exchange-Unterstützung von Android selbst schon ausreichen, zumal sie auch Adressen und Termine synchronisiert – im abgeschotteten Nutzerkonto ja kein Problem.

Liegen die Termine und Kontakte auf einem CalDAV/CardDAV-Server, benötigt man weitere Apps, denn Android kennt diese Protokolle. Bei CardDAV hilft CardDAV-Sync von Marten Gajda. In der kostenlosen, auch auf der Homepage des Autors erhältlichen Variante beschränkt sie sich auf die wesentlichen Daten wie Telefonnummern und E-Mail-Adressen. Will man alle Kontaktfelder synchronisieren, werden für die Vollversion 1,90 Euro fällig. Spätestens ab hier führt kein Weg am Amazon- oder Google-Appstore vorbei, um die App aufs dienstliche Nutzerkonto zu bekommen. Gleiches gilt für die App CalDAV-Sync, die sich entsprechend um die Kalendereinträge kümmert; sie gibt es nur in einer rund 2,50 Euro teuren Version. Die Einrichtung beider Apps geht flott von der Hand: Nach dem Start müssen Sie lediglich Benutzernamen und Passwort sowie die URL des Adressbuch- und Kalender-Servers eintragen. Die genauen Adressen verraten die Server in ihren Web-Oberflächen.

Die Termine tauchen dann in der eingebauten Kalender-App von Google auf. Die besteht übrigens auf die Synchronisation mit einer Cloud – wollen Sie Termine nur lokal speichern, lässt sich diese Beschränkung mit dem Open-Source-Tool „Offline Calendar“ umgehen, das es im F-Droid-Store gibt.

## Nutzer deluxe: MyKnox

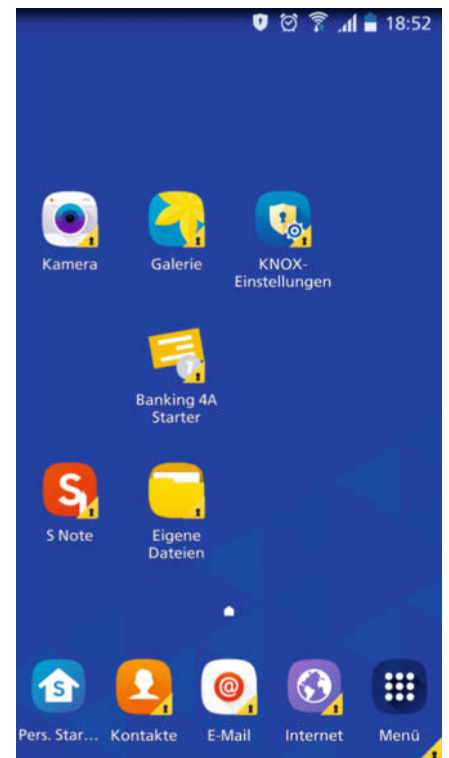
Mit so einem zweiten Nutzer lässt sich komfortabel arbeiten. Die größten Nachteile sind das mühsame Auftreiben von Apps und die fehlenden Benachrichtigungen des jeweils inaktiven Nutzers. Zudem fehlt wie auch bei den Exchange-Containern eine Möglichkeit, private und berufliche Termine parallel anzuzeigen.

Alle drei Probleme löst Samsung MyKnox, das allerdings nur auf neueren Smartphones des Herstellers funktioniert. Technisch ist MyKnox eine Art zweiter Android-Benutzer, der gleichzeitig zum ersten aktiv ist. So kommen beispielsweise WhatsApp-Nachrichten an den Hauptnutzer auch dann an, wenn man gerade eine App in MyKnox ausführt. Auch die Apps in MyKnox melden sich beispielsweise bei neuen Büro-Mails, natürlich mit einer abgespeckten Benachrichtigung ohne kritische Inhalte.

Die zweite Besonderheit: Sie können jede Ihrer Apps für den Container freigeben. Dort bekommen sie einen separaten Konfigurationssatz: Wenn Sie beispielsweise in MyKnox Fotos aufnehmen, zeigt die normale Galerie-App sie nicht an, nur die Galerie in MyKnox. Möglich ist auch, eine App zwar über den privaten Google-Account zu installieren, aber nur im Container zu nutzen – etwa einen Exchange-Client. Wenn eine über MyKnox gestartete App läuft, blendet Samsung unten rechts ein gelbes Schloss-Symbol ein.

In den Knox-Einstellungen finden Sie schließlich die dritte Besonderheit: Unter „Kontakte und Kalender freigeben“ können Sie sowohl die öffentlichen Termine und Kontakte in MyKnox einblenden wie auch die geschützten aus MyKnox exportieren. So halten Sie beispielsweise die Kontakte komplett getrennt, importieren aber die privaten Termine in MyKnox, um sie mit den beruflichen zu bearbeiten.

Weiterhin legen Sie in den Knox-Einstellungen fest, ob der Container per PIN, Muster, Passwort oder Fingerabdruck gesichert ist und unter welchen Bedingungen er sich wieder zusperrt. Hier wählen Sie auch, ob MyKnox wie eine eigene App oder wie ein Folder auf dem Startbild-



Sie können alle installierten Apps für MyKnox freigeben; sie bekommen dann separate Einstellungen. Während sie laufen, zeigen sie unten ein gelbes Schloss an.

schirm aussieht. Zudem richten Sie hier beliebige Konten ein, IMAP, Exchange, CalDAV/CardDAV, und mit den genannten Einschränkungen auch einen Google-Account. Zugang zu den Konten haben dann nur die Apps, die Sie explizit für den Container freigeben. So bekommt ein sicherer Messenger Zugriff auf alle Firmkontakte, aber WhatsApp sieht sie weiterhin nicht.

Denkbar ist auch – etwa auf Firmen-Smartphones – den Hauptnutzer sauber zu halten, vielleicht sogar ohne Google-Konto, und seinen privaten Google-Account samt WhatsApp & Co in MyKnox zu packen. Dort installierte Apps sind für den Hauptnutzer unsichtbar.

Für private Zwecke stellt MyKnox eine gute Lösung dar; schade, dass es offenbar keine ähnliche Funktion für Smartphones anderer Hersteller gibt. Aus Sicht der Firma reicht der Container aber nicht, weil die gesamte Verantwortung für eine sichere Konfiguration dem Mitarbeiter obliegt und weil die Firma ihre Daten etwa beim Diebstahl des Smartphones nicht zuverlässig aus der Ferne löschen kann. Da helfen dann nur die administrierbaren Container wie Android for Work. (jow) **ct**





# Top gepflegt!

ix. MEHR WISSEN.



Jetzt für  
**12,90 €**  
bestellen.



 [shop.heise.de/ix-dev17](https://shop.heise.de/ix-dev17)  [service@shop.heise.de](mailto:service@shop.heise.de)  
Auch als digitale Ausgabe erhältlich unter: [shop.heise.de/ix-dev17-pdf](https://shop.heise.de/ix-dev17-pdf)

Generell **portofreie Lieferung** für Abonnenten der Zeitschriften von Heise Medien und Maker Media oder ab einem Einkaufswert von 15 €.

 **heise shop**

[shop.heise.de/ix-dev17](https://shop.heise.de/ix-dev17)





Christian Wölbert

# Android ohne Google auf dem Fairphone 2

Die Datenkrake Google war mir schon immer unheimlich. Zum Glück bietet Fairphone eine Android-Variante ohne Google-Apps an: Das „Open OS“ wirkt wunderbar aufgeräumt und mein Akku hält jetzt deutlich länger.



**M**eine privaten Mails, Kontakte, Aufgaben und Termine habe ich vor ein paar Jahren von Google zum deutschen Anbieter Posteo umgezogen. Ich dachte immer, dass ich damit datenschutztechnisch schon im grünen Bereich liege.

Doch als ich neulich über myactivity.google.com stolperte, bekam ich heiße Ohren: jeder Suchbegriff, jedes angeklickte Suchergebnis, jeder auf Google News angeklickte Artikel, jedes angeschaut YouTube-Video – alles gespeichert. Dazu der Standortverlauf mit allen Orten, die ich besucht hatte. Alle WLAN-Passwörter. Hätte ich die Spracheingabe verwendet, hätte Google auch jedes Mal meine Worte mitgeschnitten und gespeichert.

Ich danke dem Unternehmen dafür, dass es seine Sammelwut wenigstens offenlegt, anders als viele andere Konzerne. Trotzdem will ich mich nicht mehr auf das Versprechen verlassen, dass nur ich diese Daten sehen kann.

Ich gehe meine Optionen durch. Ein neues, unter Pseudonym angelegtes Google-Konto?

Mit ein bisschen Fleißarbeit könnte trotzdem jeder meine Identität aus den Daten ableiten. Alle Google-Optionen auf dem Handy ausschalten, die Konto-Synchronisation, das Backup, den Standortverlauf, Google Now, den Geräte-Manager und den Kontoverlauf? Damit käme ich meinem Ziel schon nah, müsste aber im Alltag aufpassen, nicht aus Versehen wieder einen Schalter umzulegen, denn die Einstellungen verteilen sich auf viele Ecken von Android.

Das Google-Konto vom Handy schmeißen? Das wäre die einfachste Lösung. Ohne Google-Konto bringen mir aber auch viele Google-Apps nichts mehr, sie fressen nur noch unnötig Speicherplatz. Also klicke ich die doch am besten gleich mit.

## Custom-ROM ohne Garantieverlust

Die Google-Apps kann man leider nicht deinstallieren. Aber Fairphone, der Hersteller meines Smartphones, bietet ein zweites Betriebssystem an, als Alternative

zum vorinstallierten Android: eine Google-freie Android-Variante. Das „Fairphone 2 Open OS“ ähnelt Custom-ROMs wie CyanogenMod, die normalerweise ebenfalls Google-frei sind.

Da es vom Hersteller des Telefons selbst kommt, gibt es zwei Besonderheiten im Vergleich zu Custom-ROMs: Ich muss nicht fürchten, durch die Installation meinen Garantie-Anspruch zu verlieren. Und der Bootloader des Fairphone 2 ist ab Werk offen, was die Installation vereinfacht.

Also los gehts. Zuerst das Backup: Da ich Googles Cloud nicht mehr nutzen will, sichere ich meine WhatsApp-Datenbank und meine Fotos von Hand auf dem PC. Dahin schiebe ich auch das Threema-Backup. Mehr muss ich nicht sichern.

Dann versuche ich, Open OS mit Fairphones System-Updater-App zu installieren. Der Download direkt aufs Smartphone klappt, die Installation scheitert aber mit einer Fehlermeldung. Also gehe ich den umständlicheren Weg: Open OS auf den PC ziehen, Android Studio installieren, im Unterverzeichnis „platform-tools“ mit Shift und

rechter Maustaste die Eingabeaufforderung öffnen und Open OS mit

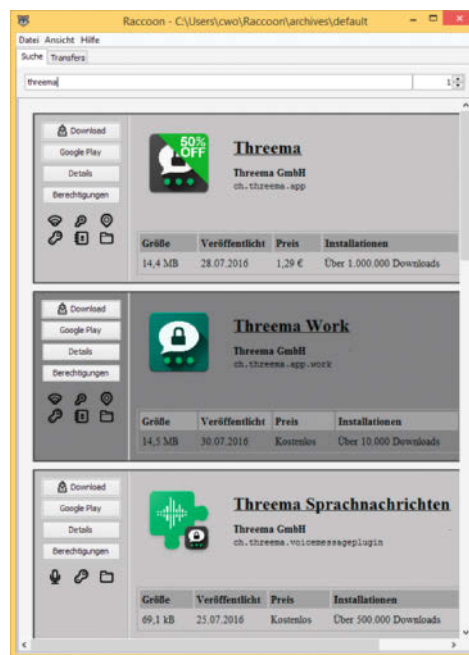
`fastboot -w update pfad/zu/image.zip`

installieren. Dazu muss das Handy via USB angeschlossen sein und sich im Fastboot-Modus befinden, den man erreicht, wenn man beim Einschalten die Leiser-Taste gedrückt hält. Die Installation dauert nur ein paar Minuten und klappt beim ersten Versuch.

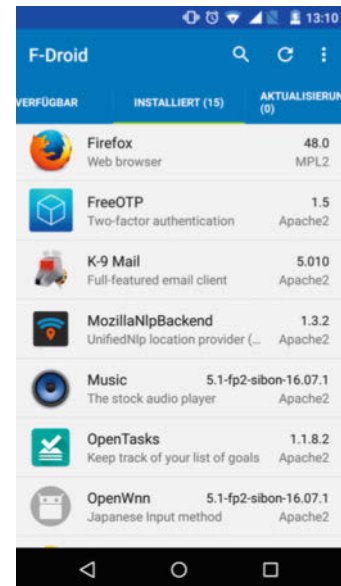
Nach dem Booten begrüßt mich ein wunderbar aufgeräumtes Android ohne Play Store, Gmail, Google+, Hangouts, Play Music und die ganzen anderen Google-Apps. Dann überlege ich, woher ich die Apps bekomme, die ich wirklich nutzen will. Theoretisch könnte ich alle mit dem APK-Downloader Raccoon aus dem Play Store auf meinen PC laden und dann via USB aufs Handy schieben.

Ich schaue aber erst einmal, wie weit ich mit anderen Quellen komme. Aus der Open-Source-Sammlung von F-Droid lade ich DAVdroid für die CalDAV-/CardDAV-Synchronisation, Firefox, den Mailer K-9 und die Navi-App OsmAnd. WhatsApp und Opera Mini bekomme ich auf den Webseiten der Entwickler. Threema könnte ich mit Raccoon aus dem Play Store ziehen, ich kaufe die App aber probenhalber erneut, direkt beim Entwickler auf [three-ma.ch](http://three-ma.ch).

Die Sonos-App lade ich von [apk.mirror.com](http://apk.mirror.com) herunter, einer Seite mit gutem Ruf, die nach eigenen Angaben bei jeder App anhand der Signatur prüft, ob sie wirklich vom angegebenen Entwickler stammt. Trotzdem checke ich das APK vorher auf [virustotal.com](http://virustotal.com), weil der Anteil von Schädlingen auf APK-Download-Seiten höher ist als in Google Play. Insbesondere bei neuen Apps und solchen, die bei Goo-



**App-Quellen:** Mit Raccoon lädt man Apps bei Google, ohne den Play Store auf dem Handy zu haben; bei F-Droid gibts Open-Source-Apps.



gle Geld kosten, sollte man sehr vorsichtig sein.

Um die beiden App-Läden von Amazon („Underground“ und „Appstore“) mache ich einen Bogen, weil ich mich dort wieder mit einem Nutzerkonto einloggen müsste und Amazon fleißig App-Nutzungsdaten sammelt.

## Bequemer Root-Zugang

Am Ende muss ich nur eine Handvoll Apps mit Raccoon aus dem Play Store laden: die App des Hannoveraner Verkehrsverbunds, den DB Navigator, die Spiegel-App, den Acrobat Reader und die Navi-App Here.

Dann noch die Backups wiederherstellen, Posteo konfigurieren und fertig ist die Einrichtung. Wenn ich wollte, könnte ich jetzt auch Root-Apps nutzen, denn in Open OS kann man den Root-Zugang mit einem Fingertipp freischalten.

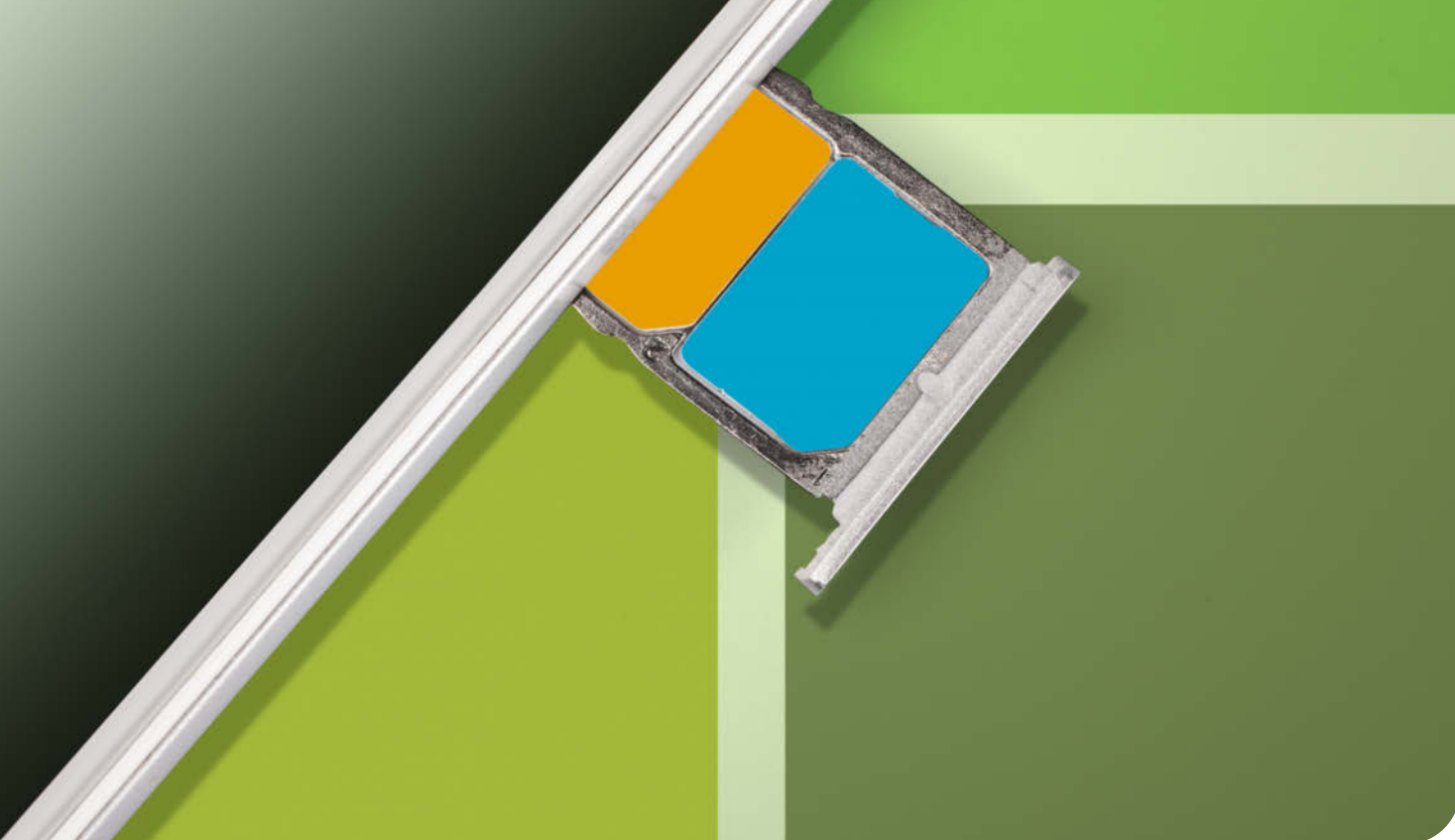
Im Alltag vermisse ich die Google-Apps bislang kein bisschen. Ab und zu werde ich wohl Google Maps im Browser nutzen, denn OsmAnd und Here kennen kaum Geschäfte und Restaurants. Open OS läuft absolut stabil, ohne Abstürze oder Fehlermeldungen. Fairphone liefert dieselben Sicherheits- und System-Updates wie für die Google-gespickte Variante. Da ich nur wenige Apps über Raccoon installiert habe, macht es mir wenig aus, diese ab und zu von Hand zu aktualisieren.

Der DB Navigator und Threema zeigen zwar keine Push-Nachrichten, weil sie dafür Googles Cloud-Messaging-Dienst bräuchten. Doch vom Navigator brauche ich keine Benachrichtigungen, und Threema habe ich auf halbstündigen Nachrichten-Abruf umgestellt. Laut Threema verbraucht das viel mehr Strom. Ich erlebe in der Praxis allerdings das Gegenteil: Seit dem Umstieg auf Open OS hält mein Akku im Alltag gefühlt doppelt so lang wie vorher. Ich weiß nicht, ob das an den gekappten Google-Synchronisationen liegt oder an etwas anderem, aber es versüßt mir den Abschied von den Google-Apps zusätzlich. (cwo) **ct**

## Allgemeine Tipps für Android ohne Google

Die großen Hersteller wie Samsung, HTC, LG oder Sony bieten anders als Fairphone zwar kein Google-freies Android an, aber auch aus ihren Smartphones kann man Google ausperren, indem man die Synchronisation persönlicher Daten abstellt, die vorinstallierten Apps deaktiviert und Play-Store-Alternativen nutzt. Die De-

tails haben wir in c't 2/16 beschrieben (ab S. 70). In c't 13/14 ab Seite 114 zeigen wir, zu welchen Google-URLs Android-Smartphones Kontakt aufnehmen und welche konkreten Maßnahmen welche dieser Verbindungen kappen. Tipps für den Umstieg auf ein Custom-ROM lesen Sie in c't 15/15 ab Seite 114.



Urs Mansmann

## Zwei SIM-Karten optimal kombinieren

Die richtige Kombination aus zwei SIM-Karten spart Kosten und optimiert die Leistung.  
Wir haben einige Vorschläge für Sie.

Mit einer zweiten SIM-Karte im Smartphone lässt sich eine Menge anfangen. Sie verbessert beispielsweise die Chance, immer erreichbar zu sein, auch in schlecht versorgten Gegenden. Hat SIM-Karte 1 keinen Empfang, leitet man die Anrufe per bedingter Rufumleitung bei Nichterreichbarkeit auf SIM-Karte 2 in einem anderen Netz um. Mit einer Allnet-Flat auf SIM-Karte 1 ist eine solche Rufumleitung in vielen Fällen sogar kostenfrei.

Die zweite Karte kann aber auch beim Sparen helfen. Speziell für Smartphones haben viele Anbieter Kombi-Tarife im Programm. Die bieten von allem etwas: Freivolumen für den Internetzugang, freie Telefonminuten und freie SMS. Allerdings haben solche Kombinationen auch Nachteile: Nur wer alle Bestandteile des Tarifs intensiv nutzt, fährt damit wirklich günstiger als mit einer Einzelabrechnung. Wenig-Telefonierer oder Wenig-

Surfer zahlen bei solchen Kombis oft drauf.

Nutzt man ein Dual-SIM-Gerät, kann man Telefonie und Datennutzung mit getrennten Verträgen abwickeln und spezielle Internet-Zugangsangebote für die Laptop-Nutzung ohne Telefonie einsetzen. Mit solchen Nur-Daten-Tarifen lässt sich kräftig sparen, besonders wenn man viel Datenvolumen benötigt. Bei der Telekom beispielsweise kosten 5 Gigabyte pro Monat in einem reinen Datentarif 29,95 Euro.

Nimmt man stattdessen den für Smartphones vorgesehenen Kombi-Tarif inklusive Telefonie, wird es erheblich teurer. Der Kunde kann dann beispielsweise zwischen 3 Gigabyte für 44,95 und 6 Gigabyte für 54,95 Euro im Monat wählen. Das lohnt sich nur, wenn man die im Bundle ebenfalls enthaltene Allnet-Flat wirklich braucht. Fast-nur-Surfer und Gelegenheitstelefonierer können so im

Monat rund 15 Euro sparen, ohne Kompromisse beim Datenvolumen oder bei der telefonischen Erreichbarkeit eingehen zu müssen. Auch bei einem geringeren Datenvolumen können Nur-Surfer noch kräftig sparen: Das günstigste Telekom-Vertragspaket mit 1 Gigabyte Volumen kostet nur 14,95 Euro im Monat.

Ähnlich sieht das Preismodell bei Vodafone aus. Die reinen Datentarife sind recht günstig, die Daten-Telefonie-Kombis erheblich teurer, weil auch hier eine Allnet-Flat mitbezahlt werden muss, egal, ob man sie braucht oder nicht. Auch hier spart man mit einer Trennung zwischen Daten- und Telefontarif.

Die Telekom legt ihren Datentarif-Nutzern nahe, VoIP zu verwenden. Das hat aber erhebliche Nachteile. Eine VoIP-Verbindung ist weniger stabil als ein klassisches Mobiltelefonat. Muss das Smartphone ständig in Empfangsbereitschaft für VoIP-Anrufe bleiben, kann sich



der Strombedarf im Ruhezustand deutlich erhöhen. Die Zwei-SIM-Lösung ist da erheblich eleganter, weil sie alle gängigen Stromsparmodi im Mobilfunknetz ermöglicht und dem Gerät in Nutzungspausen erlaubt, sich schlafen zu legen.

Trennt man Daten- und Telefon-SIM, ist man frei bei der Netzwahl. Während Telekom und Vodafone beim UMTS- und LTE-Ausbau gegenüber O2 deutlich spürbar die Nase vorn haben, gibt es bei GSM viel geringere Unterschiede zwischen den drei Netzen. Der Unterschied in der Qualität schlägt auf die Preise durch; Angebote fürs O2-Netz sind im Vergleich zu Angeboten für die „D-Netze“, also Telekom und Vodafone, deutlich günstiger.

Den Preisvorteil des O2-Netzes kann man für die Telefonie nutzen, ohne allzu große Nachteile bei der Erreichbarkeit hinnehmen zu müssen. Über den Provider Winsim beispielsweise bekommt man eine Allnet-Telefonie-Flat im O2-Netz derzeit schon für 8,99 Euro im Monat. Verzichtet man auf den enthaltenen Internet-Tarif und nutzt für den Online-Zugang stattdessen ein Angebot im erheblich besseren Telekom- oder Vodafone-Netz, bekommt man je nach Volumen schon für weniger als 20 Euro im Monat ein ordentliches Gesamtpaket mit guter Abdeckung und Bandbreite fürs Internet und guten Konditionen fürs Telefonieren.

## Günstig telefonieren

Ein interessantes Angebot für Telefonie bietet auch der VoIP-Anbieter Sipgate mit seiner Mobilfunkmarke Simquadrat. Sipgate ist ein virtueller Netzbetreiber, der das Netz von E-Plus nutzt. Für 4,95 Euro im Monat erhält der Kunde eine SIM-Karte mit mehreren Rufnummern, darunter auf Wunsch eine kostenlose Ortsnetzrufnummer und viele zusätzliche Funktionen, beispielsweise eine Spracherkennung für den Anrufbeantworter, die ein Transkript von aufgesprochenen Nachrichten per Mail zuschickt. Einrichten lässt sich unter anderem das Abweisen anonymer Anrufer, ein Parallelruf auf einer weiteren Rufnummer, die Anzeige einer beliebigen Rufnummer beim Angerufenen oder eine Preisansage bei abgehenden Anrufen. Für den Internet-Zugang ist das Angebot weniger interessant, zum einen, weil es das E-Plus-Netz verwendet, aber vor allem, weil es noch kein LTE bietet.

Gerade in puncto Telefonie gibt es noch weitere Spezialangebote. Anrufe ins

Ausland sind gerade in den Mobilfunknetzen oft ein teurer Spaß. Congstar beispielsweise verlangt für Anrufe in Länder außerhalb der EU 1,49 Euro pro Minute, andere Anbieter toppen das gar noch. Mit speziellen Discounter-Angeboten wie Lycamobile, Ortel oder Lebara kann man viele Ziele in Übersee für kleines Geld erreichen. Telefonate in einige Länder kosten gar nur 1 Cent pro Minute und sind damit deutlich billiger als die meisten in-nerdeutschen Telefonate. Allerdings verlangen die Anbieter einen Zuschlag von 15 Cent pro Verbindung und kappen Telefonate nach einer Stunde. Aber selbst mit diesen Haken und Ösen spart der Kunde unterm Strich noch eine Menge im Vergleich zu den Standard-Angeboten der Netzbetreiber und Provider. Für den täglichen Gebrauch sind solche Karten nicht so gut geeignet: Telefonate in deutsche Netze und Internet-Verbindungen laufen über die andere SIM-Karte im Gerät meistens günstiger.

Telefoniert man viel innerhalb der Familie, lohnt sich möglicherweise eine Community-Flatrate. 1&1 beispielsweise bietet seinen DSL-Kunden eine kostenlose SIM-Karte, jede weitere kostet 2,99 Euro im Monat. Dafür gibt es nur 100 Megabyte Datenvolumen – aber enthalten ist eben auch eine Flatrate ins Festnetz und zu 1&1-Mobilfunkanschlüssen, die für viele Nutzer interessant ist. Als alleinige SIM ist das Angebot für die meisten Anwender wegen des geringen Datenvolumens kaum zu gebrauchen.

Als Zweit-SIM erlaubt es, kostenlos innerhalb der Familie und zu Festnetzanschlüssen zu telefonieren.

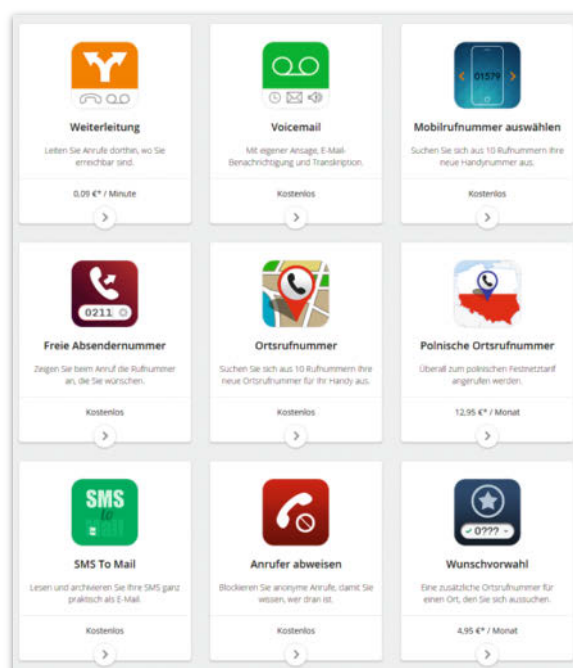
## Online im Ausland

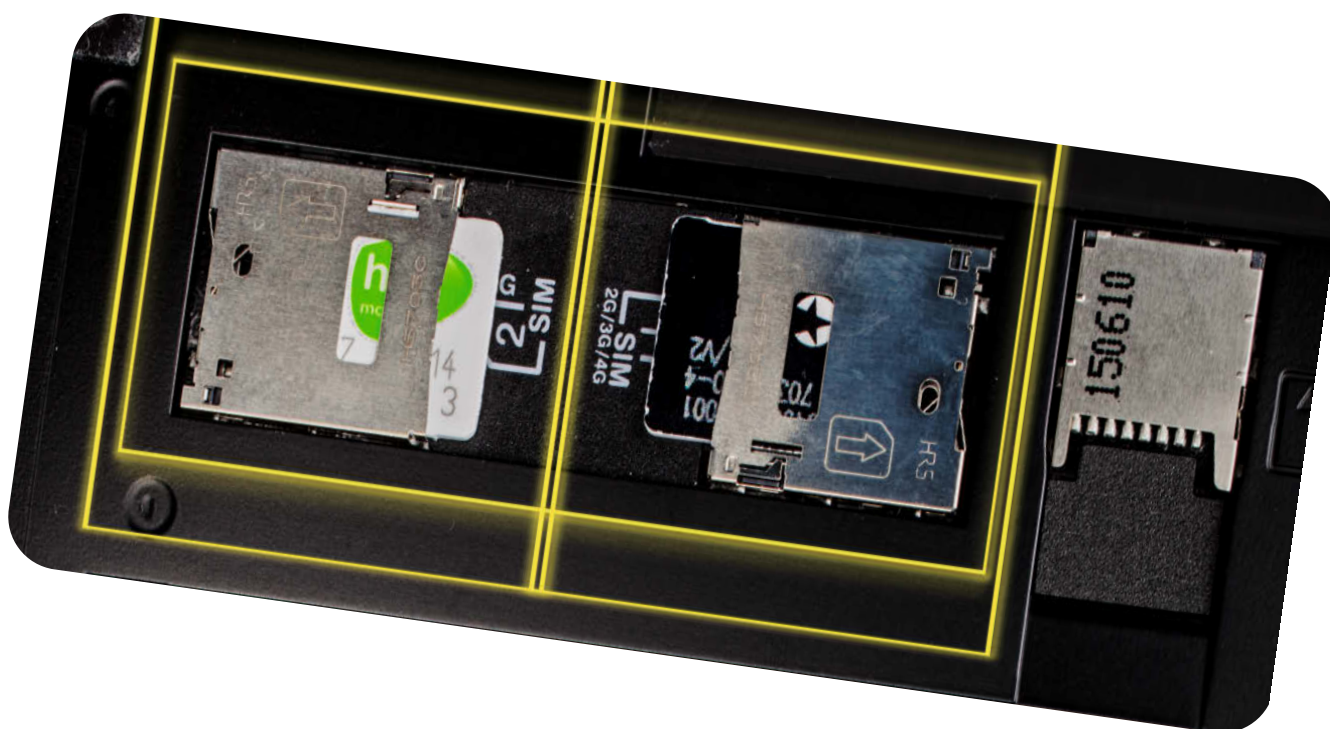
Den größten Trumpf des Dual-SIM-Geräts kann man im Ausland ausspielen, wenn man sich eine SIM-Karte vor Ort für den Internetzugang besorgt. Eine SIM des Nachbarlandes lohnt sich auch, wenn man in Grenznähe wohnt und öfter einmal auf der anderen Seite der Grenze unterwegs ist. Interessant ist sie aber auch für Urlauber.

Typischerweise zahlt man für ein Gigabyte Volumen zwischen 1 und 10 Euro. Die Nutzung einer örtlichen SIM bietet aber noch weitere Vorteile: Über die Rufnummer des Gastlandes ist man ohne Roamingkosten erreichbar, beispielsweise auch für Tourenanbieter oder Zimmervermittlungen vor Ort, und kann günstig lokale Nummern anrufen, beispielsweise um einen Tisch im Restaurant zu reservieren. Auch Anrufe nach Deutschland sind auf diese Weise oft erheblich günstiger als im Roaming-Tarif des heimatischen Netzbetreibers.

Mit einem Dual-SIM-Gerät ist man auf Wunsch aber dennoch weiterhin gleichzeitig unter der gewohnten Heimat-Rufnummer erreichbar. Den Daheimgebliebenen kann man eine vorübergehende Urlaubs-Rufnummer per WhatsApp mitteilen oder in der Mailbox-Ansage für die heimatische Mobilfunknummer aufsprechen. (uma) **ct**

**Der VoIP-Spezialist Simquadrat bietet rund 30 Zusatzleistungen für sein Mobilfunkangebot, viele davon sind kostenlos.**





Hannes A. Czerulla

## Smartphones mit zwei SIM-Karten-Slots

Gründe für ein Dual-SIM-Smartphone gibt es viele: clevere Vertragskombis, regelmäßiger Auslandsaufenthalt oder eine private und eine geschäftliche SIM-Karte. Einer der wenigen Gründe dagegen ist die eingeschränkte Auswahl an Smartphones. Dennoch findet man in jeder Preiskategorie attraktive Modelle mit speziellen Dual-SIM-Funktionen.

**D**as Smartphone-Feature Dual-Sim führt hierzulande nur ein Schattendasein, während in anderen Teilen der Welt kaum noch ein neues Handy ohne die Funktion auf den Markt kommt. Dual-SIM-Geräte kann man mit zwei SIM-Karten, also zwei verschiedenen Mobilfunkverträgen gleichzeitig betreiben. Sie haben dazu zwei SIM-Karten-Slots.

Für fast jeden Handy-Nutzer gibt es einen Grund, auf ein Dual-SIM-Telefon

umzusteigen. Meist geht es darum, Tarife jeglicher Art so zu kombinieren, dass man weniger zahlt und dennoch mehr bekommt als mit nur einem Mobilfunkvertrag. So lässt sich beispielsweise ein reiner Datentarif mit einem auf Telefonieren ausgelegten Prepaid-Tarif kombinieren. Datentarife, die eigentlich für Tablets und Notebooks gedacht sind, bieten oft für geringe Gebühren großes Datenvolumen über 5 GByte via schnellem LTE. Mit dem Prepaid-Tarif wäre man dennoch per Tele-

fon und SMS erreichbar und könnte sporadisch preiswerte Telefonate führen, ohne dafür regelmäßig Grundgebühren zu zahlen.

Eine Erleichterung sind Dual-SIM-Smartphones auch für Nutzer, die sowieso schon auf zwei SIM-Karten angewiesen sind und momentan zwei Geräte mit sich herumtragen. Moderne Dual-SIM-Handys betreiben nämlich beide SIM-Karten gleichzeitig. Hat man beispielsweise einen privaten und einen geschäftlichen Mobil-

funkvertrag, kann man auf Wunsch auf beiden Nummern gleichzeitig erreichbar sein. Wer regelmäßig ins Ausland reist, kann Roaming-Gebühren sparen. Dazu muss er bei der Grenzüberquerung nicht mehr die Karte wechseln, sondern lässt die ausländische SIM-Karte einfach im Gerät.

## Dual-SIM im Alltag

Grundsätzlich unterscheiden sich Dual-SIM-Smartphones kaum von anderen Mobiltelefonen. Von außen sieht man ihnen die Spezialfunktion nicht an und bis auf den SIM-Karten-Slot im Inneren ist auch die Hardware-Ausstattung die gleiche wie bei anderen Geräten. Einige Smartphone-Modelle gibt es sowohl in einer Single- als auch in einer Dual-SIM-Variante. Dennoch ist das Angebot in Deutschland begrenzt, da die hiesigen Mobilfunk-Provider durch

solche Geräte ihre Geschäftsmodelle bedroht sehen (siehe Kasten).

Markt-dominierende Hersteller wie Samsung, LG und HTC bieten fast nur Einstiegermodelle für unter 200 Euro mit Dual-SIM offiziell in Deutschland an. Eher wird man bei kleineren Marken fündig, die ein Nischendasein führen, etwa Gigaset, Microsoft und ZTE. Sie versuchen mithilfe des Alleinstellungsmerkmals Dual-SIM den großen Konkurrenten Kunden abzuluchsen.

Wie auch bei Single-SIM-Geräten sollte man aber mindestens 100 Euro für ein neues Smartphone veranschlagen. Preiswertere Modelle sind wegen mieser Displays und lahmer Hardware kaum als Smartphone zu gebrauchen. Möchte man nur telefonieren und SMS schreiben, sind klassische Dual-SIM-Handys wie das Nokia 225 für unter 50 Euro die bessere Wahl.

## Gehobene Ausstattung bei ZTE

Muss das neue Handy nicht nur als Zweit- oder Drittgerät herhalten, sondern als zuverlässiger Begleiter in jeder Alltagssituation dienen, sollte man zu mindestens in die Regionen zwischen 160 und 300 Euro vordringen. Hier sind vor allem chinesische Marken wie ZTE mit vielen Dual-SIM-Geräten vertreten. Sie bringen bereits Full-HD-Displays, brauchbare Sony-Kameras und 16 GByte Flash-Speicher mit. Auch das BQ Aquaris X5 ist hierfür ein gutes Beispiel. Jenseits der 400 Euro und mit gehobener Ausstattung wird die Auswahl dünn. Der Newcomer Gigaset bietet seine beiden Spitzenmodelle ME und ME pro an. Fast alle Geräte funken per LTE.

Beim Betriebssystem hat man die Wahl zwischen Android oder Windows 10 Mo-

## Import-Geräte mit Dual-SIM

Nur ein Bruchteil der Smartphones, die Dual-SIM beherrschen, schaffen es auch nach Deutschland. Der Grund ist, dass in Deutschland Smartphones größtenteils immer noch über die Mobilfunk-Provider verkauft werden und die Hersteller versuchen, ihre Modelle in den Provider-eigenen Läden und Online-Shops zu platzieren. Die Mobilfunkanbieter wollen, dass ausschließlich ihre SIM-Karte im Smartphone steckt, und nicht den Umsatz mit einem Konkurrenten teilen. Auch ist die clevere Kombination von hauseigenen Tarifen nicht im Interesse der Provider. So bieten ihre Shops fast ausnahmslos Single-SIM-Geräte an; die Hersteller passen sich diesen Anforderungen an.

Die Dual-SIM-Versionen von High-End-Smartphones wie dem Samsung Galaxy S7, LG G5 oder Sony Xperia Z5 sucht man vergebens in deutschen Läden. Eine Möglichkeit, in den Genuss dieser Modelle zu kommen, ist der Import auf eigene Faust. Allerdings muss man sich dann mit außereuropäischen Shops und dem Zoll herumschlagen und aufs Rückgaberecht verzichten. Stattdessen findet man via Preissuchmaschinen wie geizhals.de einschlägige deutschsprachige Händler, die inklusive Garantie und Rückgaberecht verkaufen. Fündig wurden wir beim etablierten Online-Shop notebooksbilliger.de und dem fast nur Dual-SIM-Geräte führenden ultimate-mobi.net.

Android enthält normalerweise ein deutsches Sprachpaket, auch wenn das Smartphone eigentlich nicht für den deutschsprachigen Markt gedacht ist. Es kann allerdings vorkommen, dass einzelne Apps oder Menüeinträge nicht übersetzt wurden. Erfahrungsgemäß findet man Mandarin-Schriftzeichen & Co. nur bei Herstellern, die gar nicht offiziell nach Deutschland verkaufen. Gelegentlich unterscheidet sich die Hardware minimal

von den hierzulande angebotenen Single-SIM-Varianten. Meist sind diese Bauteile gleichwertig.

## Frequenzchaos

Wichtiger ist es, auf die unterstützten Mobilfunkfrequenzen zu achten, die sich je nach Region unterscheiden: In Deutschland generell ungeeignet sind Geräte, die ursprünglich für den nord- und südamerikanischen Markt vorgesehen waren.

MHz-Angaben sind wenig aussagekräftig, wichtig ist die Unterstützung für das richtige E-UTRA-Band. Dieses nennt nicht nur die verwendete Frequenz, sondern auch weitere Parameter wie Sendeleistung, Kanalbreite und genauen Bereich oder Frequenzablage im Duplexbetrieb. Deshalb überschneiden sich viele E-UTRA-Bänder in weiten Teilen.

Die gängigen Frequenzbänder in Europa, Afrika und Asien für GSM sind 900 und 1800 MHz (E-UTRA-Bänder 8 und 3); die beherrscht jedes Gerät. UMTS in Deutschland findet bei 2100 MHz statt (Band 1). Auch dieses Band beherrschen alle handelsüblichen Smartphones, egal für welchen Markt sie produziert wurden.

Bei LTE empfiehlt es sich aber, genau hinzuschauen. In Deutschland werden die Bänder 20 (800 MHz), 3 (1800 MHz) und 7 (2600 MHz) eingesetzt. In absehbarer Zeit wird noch Band 28 (700 MHz) hinzukommen – die sogenannte Digitale Dividende II. Noch zukunftssicherer wird es, wenn das Gerät obendrein die Bänder 1 (UMTS 2100), und 8 (GSM 900) beherrscht, denn möglicherweise werden die Mobilfunkanbieter irgendwann die ihnen ursprünglich für UMTS und GSM zugewiesenen Bänder für LTE hernehmen wollen (Refarming).





### ZTE Blade L6

Außergewöhnlich schick und schlank für ein Einsteiger-Handy kommt das ZTE Blade L6 daher. Dafür ist der Akku klein, die Laufzeiten kurz und kein LTE an Bord. Das HD-Display sticht positiv hervor.

---

Test in c't 8/16  
100 €



### Microsoft Lumia 650

Das Lumia 650 Dual-SIM ist das preiswerteste aktuelle Dual-SIM-Smartphone mit Windows 10 Mobile. OLED-Display und Alurahmen findet man sonst kaum in dieser Preisklasse.

---

Test in c't 9/16  
120 €



### BQ Aquaris X5 Cyanogen Edition

Von Werk aus ist das Aquaris X5 CE mit der Android-Version Cyanogen OS ausgestattet. Die CPU könnte schneller sein, die restliche Hardware ist dem Preis angemessen.

---

Test in c't 9/16  
240 €

bile. Aus der aktuellen Windows-Phone-Generation können bislang aber nur das Microsoft Lumia 650 Dual-SIM und 950 Dual-SIM und das 100-Euro-Gerät Archos 50 Cesium mit zwei SIM-Karten umgehen. Gibt man sich auch mit älteren Modellen

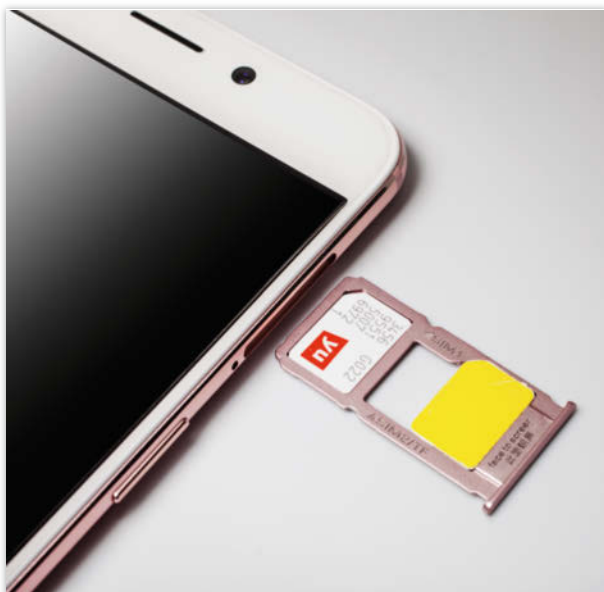
zufrieden, findet man Alternativen wie das Lumia 435 und 640. Windows 10 Mobile ist von Haus aus auf Dual-SIM vorbereitet. Android müssen die Hersteller anpassen und die notwendigen Menü-Einträge und Apps selbst integrieren. Daher

findet man die Dual-SIM-Einstellungen bei jedem Hersteller an anderer Stelle, mit anderer Bezeichnung und anderem Funktionsumfang.

In der Benachrichtigungsleiste von Android und Windows erscheint für jede SIM-Karte ein einzelnes kleines Mobilfunksymbol, das die Empfangsqualität der Verbindungen separat anzeigt. Die restlichen Dual-SIM-Einstellungen sind üblicherweise in die Systemeinstellungen integriert. In Android taucht je nach Hersteller beispielsweise ein Menü-Punkt „SIM-Kartenverwaltung“ oder „Dual-SIM-Karteneinstellungen“ auf. Dort lassen sich die Karten auch einzeln deaktivieren. SIM-bezogene Menüs, wie die APN-Einstellungen, tauchen einfach doppelt auf.

### Karten jonglieren

Auch Hardware-seitig sind die zwei SIM-Karten je nach Hersteller und Modell unterschiedlich integriert: In Handys, bei denen die SIM-Karten klassisch hinterm Rückendeckel liegen, sind meist zwei einzelne Halterungen vorhanden. Kann man das Gerät mit Speicherkarten bestücken,



Bei Smartphones mit Schublade und erweiterbarem Speicher muss man sich zwischen Speicherkarte und zweiter SIM-Karte entscheiden.



## Microsoft Lumia 950 Dual-SIM

Kein Windows-Phone ist besser ausgestattet als das Lumia 950. Mit hochauflösendem OLED-Display und Spitzenkamera lässt es wenige Wünsche offen – bis auf schickes Design.

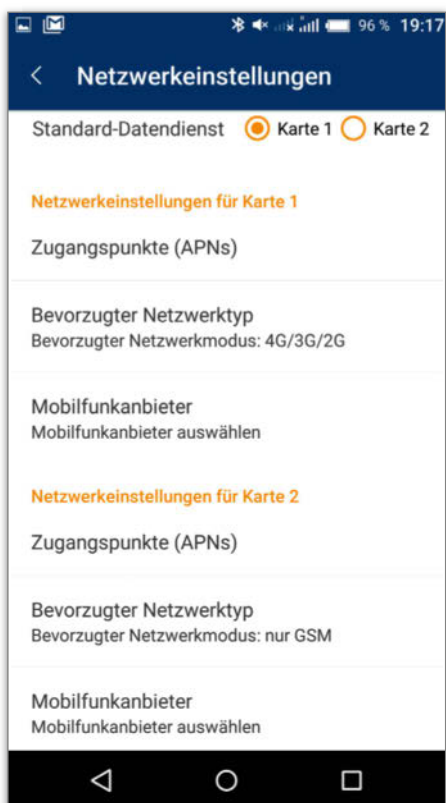
Test in c't 2/16  
330 €



## Gigaset ME

Das ME ist ein typischer High-End-Androide: Scharfes Full-HD-LCD, schneller Prozessor und Glas-Gehäuse. Die Kamera kann mit denen anderer Spitzenmodelle aber nicht ganz mithalten.

Test in c't 27/15  
240 €



ist dafür eine dritte Halterung eingebaut. Der Trend geht allerdings zum fest verschlossenen Gehäuse à la iPhone, Galaxy S7 & Co.: SIM- und Speicherkarten kommen in eine Art Schublade, die man in die Gehäuseseite schiebt.

Kann das Smartphone mit Speicherkarten umgehen, legt man SIM und Speicherkarte meist in dieselbe Schublade nebeneinander und schiebt sie ins Gerät. Handelt es sich um ein Dual-SIM-Handy, gibt es meist ebenfalls nur eine Schublade für zwei Karten. Der Platz für die zweite Karte ist so geformt, dass dort sowohl SIM-Karten als auch MicroSD-Karten Platz finden. Beides gleichzeitig geht allerdings nicht und so muss man sich bei solchen Geräten entscheiden, ob man lieber den Speicher ergänzt oder eine zweite SIM-Karte nutzt. In seltenen Fällen haben die zwei SIM-Slots unterschiedliche Formate – einer in Nano-Größe, der andere Micro.

**In Dual-SIM-Handys lassen sich zwei SIM-Karten unabhängig voneinander konfigurieren.**

Welche Karte man in welchen Slot legt, will bei einigen Geräten gut überlegt sein. Denn grundsätzlich kann immer nur eine Karte im UMTS- (3G) beziehungsweise LTE-Netz (4G) funken. Die zweite hat nur Zugriff aufs GSM-Netz (2G) mit extrem langsamer Datenübertragung – sollte also nur für Telefonie und SMS genutzt werden. Bei einigen Geräten ist die Art der Mobilfunkbindung vom genutzten Karten-Slot abhängig und man muss sich schon beim Einsetzen überlegen, welche SIM die mobile Datenübertragung übernehmen soll und mit welcher man ausschließlich telefoniert. Vor allem bei neueren, teureren Smartphones lässt sich aber auch im Betrieb die Datenkarte umschalten und je nach Situation der einen oder der anderen Karte der Weg ins 3G- oder 4G-Netz freigeben. Welche Karte man dazu verwenden möchte, fragt das System in der Regel nach dem ersten Start.

Per Telefon oder SMS ist man hingegen auf beiden Nummern gleichzeitig erreichbar. Android und Windows zeigen bei eingehenden Gesprächen und SMS an, über welche Karte sie ankommen. Bei einigen Geräten lässt sich sogar die Bezeichnung der Karten ändern. Nur wenn man gerade telefoniert, ist die andere Karte für die Länge des Gesprächs nicht erreichbar – was sich aber mithilfe einer Umleitung lösen lässt. Sollten auf den SIM-Karten Kontakte gespeichert sein, werden diese mit entsprechenden Symbolen in der Telefonbuch-App markiert. Startet man selbst einen Anruf oder schreibt eine SMS, fragen die Systeme nach, welche Karte man dazu nutzen möchte.

Auf Wunsch kann das Telefon ohne weitere Nachfragen auch immer dieselbe Karte verwenden. In diesem Fall bekommt der Nutzer im Alltag kaum noch mit, dass es sich um ein Dual-SIM-Gerät handelt. Einen Sonderfall bilden die Messenger WhatsApp und Telegram. Sie können immer nur mit einer Telefonnummer beziehungsweise einem Account gleichzeitig verknüpft sein.

Hat man noch keine zweite SIM-Karte und auch noch keinen Plan, wie man Dual-SIM sinnvoll nutzen soll, lohnt sich dennoch oftmals der Griff zu einem Dual-SIM-Modell. Denn im Zweifelsfall lassen sich alle Geräte auch nur mit einer SIM-Karte betreiben, ohne dass dadurch Nachteile entstünden.

Auf den Seiten 86 und 87 lesen Sie einen ausführlichen Test zu den Dual-SIM-Geräten Motorola Moto G4 und Moto G4 Plus. (hcz) **ct**



Urs Mansmann

## LTE ausreizen

LTE bietet viele Vorteile gegenüber UMTS: Bessere Netzabdeckung, weniger Stromverbrauch und ein mobiles Internet, das sich so anfühlt, als sei man zu Hause im WLAN. Wir erklären, wie Sie das Beste aus LTE herausholen.



**L**TE macht den entscheidenden Unterschied: Kollege Jan-Keno Jansen unternahm im vergangenen Sommer zusammen mit seiner Freundin eine Radtour entlang der Donau. Beide haben ein vergleichbares Smartphone, beide sind beim gleichen Netzbetreiber, der Telekom. Sie hat allerdings einen Vertrag mit LTE-Nutzung, er ohne. „Sie hatte immer Internet, ich fast nie“, schildert er seine Erfahrungen. Obwohl sein Handy LTE kann, buchte es sich nur gelegentlich ins UMTS-Netz ein. Meist war es im GSM-Netz unterwegs. Der Internet-Zugang darüber war für ernsthafte Nutzung zu langsam.

Viele Mobilfunknutzer machen sich keine Gedanken darüber, mit welcher Technik sie ins Netz gehen. Ob UMTS oder LTE, ist ihnen egal. Wer aus Bequemlichkeit oder vermeintlicher Sparsamkeit auf LTE verzichtet, handelt sich viele Nachteile ein.

Von LTE profitiert jeder, der mobiles Internet nutzt. Mit einem LTE-Smartphone ist das eine Kleinigkeit – bei einem Anbieterwechsel kann man die Rufnummer mitnehmen. Hat man noch kein LTE-fähiges Smartphone, halten sich die Kosten ebenfalls im Rahmen. Erhältlich sind einfache Modelle mit LTE schon ab rund 100 Euro.

Wer hauptsächlich in Ballungsgebieten unterwegs ist, kann die günstigen Angebote im O2-Netz nutzen. Ist man in einer ländlichen Gegend zu Hause oder viel unterwegs, sollte man eher auf Telekom und Vodafone setzen, weil diese ihr LTE-Netz erheblich besser ausgebaut haben.

Schon für unter 10 Euro im Monat bekommt man LTE-Tarife mit ordentlichem Transfervolumen und einer Bandbreite von mindestens 50 MBit/s. Das ist nicht teurer als vergleichbare Alttarife mit UMTS – der Umstieg lohnt auf jeden Fall.

In Deutschland laufen derzeit Mobilfunknetze aus drei Generationen parallel. Am besten in der Fläche ausgebaut ist die älteste Technik: Das 2G- oder GSM-Netz löste Mitte der 90er-Jahre das analoge C-Netz ab. Fast überall kann man damit telefonieren, es funktioniert bis fast in den letzten Winkel der Republik – bei Datenverbindungen jedoch liefert es kaum mehr als 200 kBit/s. Für moderne Smartphones reicht das vorne und hinten nicht.

UMTS liefert heute an vielen gut ausgebauten Stellen bis zu 42 MBit/s im Downstream. Das Netz weist aber in ländlichen Gebieten und besonders in den Mittelgebirgen große Lücken auf. Das gilt sogar für Telekom und Vodafone, die bei Netzab-

deckungstests mit dem ersten und zweiten Platz dicht beieinander abschneiden.

LTE wurde zu Beginn des Netzausbaus gerade zum Tilgen weißer Flecken in der DSL- und Mobilfunkabdeckung eingesetzt. LTE kann unter anderem Frequenzen im 800-MHz-Bereich verwenden. Die Reichweite dieser LTE-Frequenzen ähnelt der von 900-MHz-GSM auf dem Land. Die Versorgungsflächen sehen daher fast deckungsgleich aus – die Netzbetreiber mussten nur vorhandene GSM-Basisstationen ertüchtigen.

Unter anderem deshalb sind die LTE-Netze bei der Telekom und Vodafone erheblich dichter gewebt als die UMTS-Netze. Lediglich bei O2 läuft das 3G-Netz dem 4G-Netz von der Abdeckung her noch den Rang ab, wie Netzabdeckungskarten verraten. Wer außerhalb der Ballungszentren ein schnelles Netz sucht, hat bei Telekom und Vodafone mit LTE viel bessere Chancen, ins Netz zu kommen, als mit UMTS. LTE lässt sich allerdings nur nutzen, wenn sowohl das Mobilfunkgerät als auch der Tarif den Standard unterstützen.

LTE war zu Beginn des Ausbaus nur Premium-Kunden mit teuren Laufzeitverträgen vorbehalten. Erst ab rund 80 Euro Monatsgebühr gab es LTE bei Telekom und Vodafone; Nutzer anderer Tarife mussten sich mit UMTS begnügen. Inzwischen können selbst Prepaid-Kunden LTE bekommen; einige Provider stellen sogar die maximale Datenrate zur Verfügung. LTE ist im Massengeschäft angekommen.

LTE gibt es nur bei den Netzbetreibern selbst und ausgewählten Service-Providern wie Drillisch mit seinen zahlreichen Marken wie Maxxim, WinSIM, Simply oder Discotel. Die Billigtöchter der Netzbetreiber, Congstar (Telekom), Fyve (Vodafone) und Fonix (O2) sowie viele Mobilfunkmarken der Lebensmittel-Discounter bieten nur UMTS-Tarife an.

## Schnelle Technik

Das LTE-Netz zeichnet sich vor allem durch geringe Latenz aus. Das ist die Zeit, die vergeht, bis ein Datenpaket vom Smartphone oder Mobilfunk-Router zum Server übertragen wird und die Antwort von dort eintrifft. Im UMTS-Netz beträgt die Latenz oft 200 bis 300 Millisekunden – bei LTE sind es typischerweise 40, ähnlich wie an einem DSL- oder Kabelanschluss mit WLAN. Moderne Webseiten setzen sich aus vielen Elementen zusammen, die von etlichen Servern angeliefert werden. Eine Latenz von einigen hundert Millisekunden mag nach wenig aussehen, summiert sich aber

durch die Zahl der benötigten Ladevorgänge. Deshalb erscheinen Seiten mit LTE erheblich schneller als mit UMTS, selbst bei eingeschränkter Datenrate.

Das LTE-Netz birgt so viel Potenzial, dass die Telekom es sogar als Nachbrenner für DSL-Anschlüsse einsetzt. MagentaZuhause Hybrid kombiniert einen DSL-IP-Anschluss mit LTE. Anders als reine Mobilfunkangebote ist ein solcher LTE-Zugang nicht auf ein Transfervolumen beschränkt. Davon profitieren besonders Kunden, die per ADSL nur wenige MBit/s erhalten. Sie vervielfachen mit LTE ihre Bandbreite.

Die Technik setzen auch Bus und Bahn gerne ein: Wer das Glück hat, in einem ICE mit neuer Transponder-Technik zu sitzen, hat über weite Strecken perfekten LTE-Empfang. Auch der Bus-Marktführer FlixBus nutzt LTE, um die WLAN-Hotspots an Bord mit der Außenwelt zu verbinden.

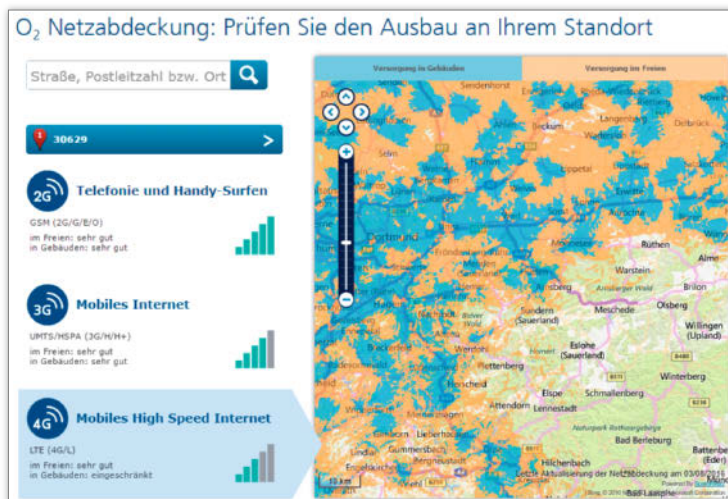
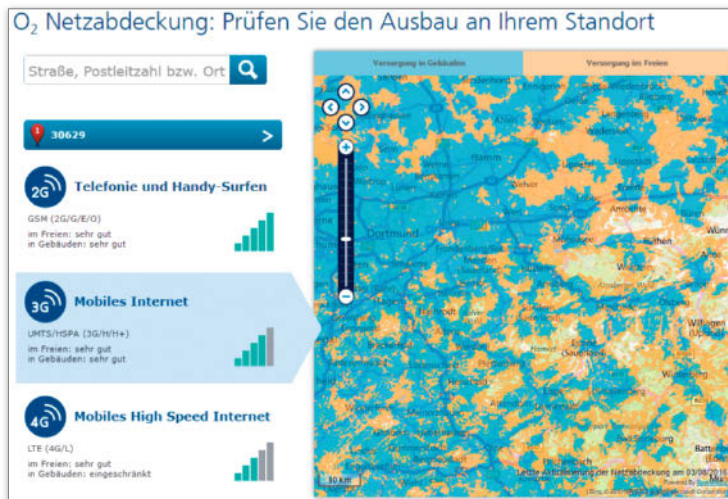
Als reines IP-Netz konzipiert, hat LTE erst nachträglich gelernt, auch Telefongespräche zu vermitteln (Voice over LTE, VoLTE). In deutschen LTE-Netzen begann die VoLTE-Aufrüstung vor rund zwei Jahren. Deshalb müssen nach wie vor viele Smartphones zum Telefonieren vom LTE auf das UMTS- oder GSM-Netz herunterschalten (Circuit Switched Fallback, CSFB). Im LTE-Netz begonnene IP-Verbindungen brechen dabei ab; der Rufaufbau dauert spürbar länger, die Akkulaufzeiten sind verkürzt. Mit VoLTE bleiben laufende IP-Verbindungen erhalten und die Sprachqualität erreicht beim Einsatz von Wideband-Codern ein deutlich höheres Niveau. Inzwischen gibt es auch hierzulande Smartphones, die VoLTE beherrschen.

Ob ein Smartphone VoLTE-Verbindungen aufbaut, zeigt es indirekt im Display an. Springt die Anzeige beim Telefonat von LTE oder 4G auf UMTS (3G) oder GSM (2G) um und danach zurück auf LTE, nutzt das Gerät für den Anruf höchstwahrscheinlich die konventionelle Telefoniefunktion der 2G- und 3G-Mobilfunknetze.

## Frequenzfragen

Die Anbieter in Deutschland nutzen für LTE derzeit drei Frequenzbänder: 800 MHz (E-UTRA Band 20), 1800 MHz (Band 3) und 2600 MHz (Band 7). Bald kommt der 700 MHz-Bereich (Band 28) hinzu, die Digitale Dividende II.

Das 800-MHz-Band eignet sich vorzugsweise zur Abdeckung großer Gebiete, weil sich damit hohe Reichweiten und bei guter Durchdringung von Gebäuden ein ordent-



**O2 ist der einzige Netzbetreiber in Deutschland, bei dem das LTE-Netz schlechter ausgebaut ist als das UMTS-Netz.**

Städten zur besseren Flächenversorgung nachgerüstet.

Anders verlief der Ausbau bei Vodafone: Beim Start des LTE-Netzes hatte das Unternehmen im 1800-MHz-Band nur 5 MHz zur Verfügung. Das ist für LTE zu wenig. Deshalb setzte Vodafone auch in den Städten 800 MHz ein. Bei kürzlich erfolgten Durchsatzprüfungen in Hannover lieferten moderne Smartphones nur an wenigen Stellen, beispielsweise um das Kongresszentrum HCC, Geschwindigkeiten von über 75 MBit/s. Doch inzwischen rüstet Vodafone zusätzliche Kapazitäten mit 1800 MHz nach. Dort hat das Unternehmen bei einer Frequenzauktion im Juni 2015 Nutzungsrechte für 20 MHz erworben. Schon zuvor hatte sich Vodafone 20 MHz im 2600-MHz-Band gesichert und an diversen Hotspots bereits eingesetzt. Koppelt Vodafone diese drei LTE-Bänder (Trägerbündelung, Carrier Aggregation), kommen insgesamt 50 MHz an Bandbreite zusammen. So liefert eine Zelle Bruttodatenraten bis 375 MBit/s. Bei besonders hohem Bedarf könnte der Netzbetreiber noch mit 2600 MHz nachlegen. Ein Testgebiet hat Vodafone beispielsweise in Langenhagen nördlich von Hannover ausgewiesen.

O2 setzt wie Vodafone auch in den Städten auf die Grundversorgung mit 800 MHz. Damit lassen sich große Flächen mit verhältnismäßig wenigen Basisstationen abdecken. Zugleich kann man so eine gute Indoor-Versorgung gewährleisten. Bei Bedarf, also für Hotspots, kann das Unternehmen auch 1800 und 2600 MHz hinzuschalten.

Entscheidend für die künftige Entwicklung wird die Zuweisung weiterer Frequenzbänder sein: Die Telekom sieht bereits Bedarf für weiteres Spektrum. Das Hauen und Stechen um Frequenzbereiche, insbesondere zwischen 300 MHz und 3 GHz, dürfte in den kommenden Jahren noch deutlich an Schärfe gewinnen.

## Vorteil durch moderne Technik

Mit einem Handy mit Trägerbündelung kann man die Vorteile des neuen Netzes erst richtig ausspielen. Eine Funkzelle hat man fast nie für sich alleine. Kann man mehrere Frequenzbänder gleichzeitig nutzen, steht mehr freie Kapazität bereit. Ist nur eines der Bänder stark belastet, beispielsweise durch einen Download, kann man die Kapazität des anderen Trägers nutzen. Datenraten jenseits von 150 MBit/s lassen sich nur mit LTE-Advanced errei-

licher Indoor-Empfang erzielen lässt. Jedoch stehen allen drei Netzbetreibern dort nur jeweils 10 MHz breite Spektrumanteile zur Verfügung. Gemäß aktuellen LTE-Spezifikationen lassen sich damit pro Sektor einer Funkzelle maximal 75 MBit/s zum Teilnehmer senden.

Bei 1800 und 2600 MHz stehen den Netzbetreibern hingegen 20 bis 30 MHz zur Verfügung. Mit 20 MHz breiten Kanälen lassen sich dort schon 150 MBit/s pro Sektor übertragen. Noch nicht in Benutzung sind die Bereiche bei 700 und 3500 MHz. Bei 700 MHz haben alle Netzbetreiber je 10 MHz ersteigert. Damit können sie ihre Kapazität im reichweitenstarken Frequenzbereich verbessern. Bei 3500 MHz hat O2 sogar 40 MHz zur Verfügung, die Telekom 20 – darin steckt also Potenzial für weitere 30 beziehungsweise 150 MBit/s Kapazität.

Mit höherwertigen Modulationsarten und zusätzlichen Antennen für parallele,

räumlich getrennte Übertragungen (Multiple Input Multiple Output, MIMO) lässt sich die Datenrate bei gleichbleibender Breite des Funkkanals steigern. Setzt man beispielsweise 256 QAM (Quadraturamplitudenmodulation) statt 64 QAM ein, kann man auf einem 20-MHz-Kanal 200 statt 150 MBit/s übertragen. Es gilt aber auch: Je höher die Modulationsstufe, desto besser müssen die Übertragungsbedingungen sein.

Die Telekom hat inzwischen Teile ihres Netzes für LTE-Advanced, also für die gleichzeitige Nutzung mehrerer Carrier, ausgebaut und bietet in Ballungsgebieten bis zu 300 MBit/s an. Ländliche Gebiete hat das Unternehmen mit 800 und die Städte zunächst mit 1800 MHz ausgebaut. Nach und nach werden zusätzlich 2,6 GHz in den Städten genutzt, 1800 MHz in ländlicheren Gegenden bei besonders hohem Bedarf und 800 MHz in den



chen, also durch die Nutzung mehrerer Träger. Selbst wenn ein Download einmal weit unter der Zielmarke von 300 MBit/s bleibt, erhält man durch die Trägerbündelung immer noch eine deutlich höhere Datenrate als die Nutzer, die nur ein Band nutzen können.

Wer auf einen möglichst zuverlässigen Internet-Zugang angewiesen ist, sollte sich zwei SIM-Karten zulegen. Sitzt man mit Karte 1 gerade im Funkloch, greift man auf Karte 2 zurück. Dazu kann man entweder ein Dual-SIM-Handy verwenden, bei dem sich die verwendete Daten-SIM per Software umstellen lässt (beispielsweise das Oneplus 3) oder man ergänzt das Single-SIM-Handy um einen mobilen Hotspot, der das zweite Netz bei Bedarf per WLAN bereitstellt. Für eine nur gelegentlich genutzte Zweit-SIM empfiehlt sich ein günstiger Prepaid-Tarif, der sich durch Aufladung aktivieren lässt, sobald er benötigt wird.

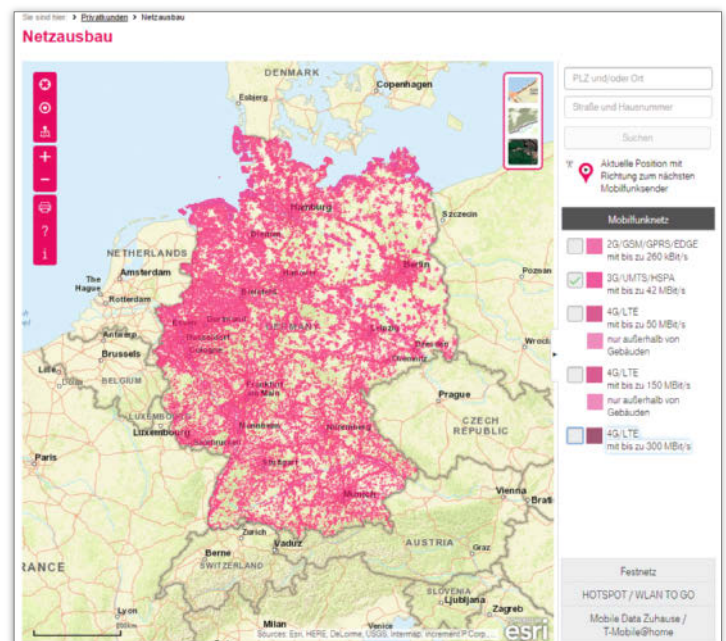
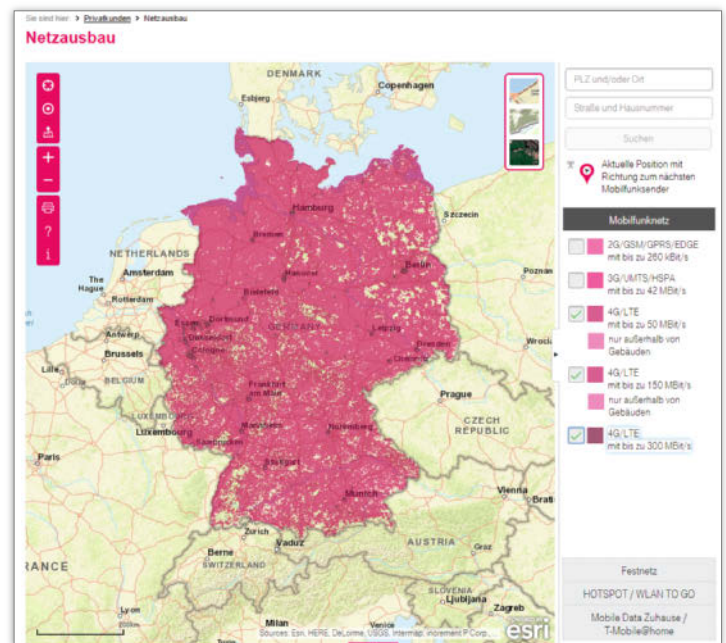
Die MIMO-Technik bringt in der Regel nur für die Basisstation etwas. Nur dort ist genug Platz, Antennen in größerer räumlicher Entfernung voneinander unterzubringen. Im Smartphone oder in mobilen Hotspots findet man LTE bestenfalls mit zwei Sendeempfangszügen ( $2 \times 2$  MIMO), weil kein Platz für mehr Antennen vorhanden ist und der Akku sonst über Gebühr belastet würde. Stationäre Mobilfunk-Router dürfen mehr Strom verbrauchen, bieten mehr Platz für bessere Antennen und lassen sich grundsätzlich auch mit externen Antennen einsetzen, was je nach Standort sehr hilfreich sein kann.

Für den Versand kleiner Datenmengen in der Machine-to-Machine-Kommunikation taugt das GSM-Netz ganz passabel. Für LTE-Handys ohne VoLTE-Technik stellt dieses Netz auch bundesweit sicher, dass die Telefonie reibungslos klappt. Alle Netzbetreiber versicherten uns auf Nachfrage, dass sie nicht planen, das GSM-Netz abzuschalten. Möglicherweise wird es aber ausgedünnt: Wo es nicht mehr ausgelastet ist, könnten beispielsweise Basisstationen auf 1800 MHz wegfallen und dort Platz machen für zusätzliche LTE-Kapazitäten (Spectrum Refarming).

## Ausbau nur für LTE

Auch das UMTS-Netz wird kaum weiter ausgebaut. Wo es bereits läuft, wird es wohl eine Zeitlang weiter angeboten. Noch ist es zu früh, allein auf LTE zu setzen. Langfristig könnten die 2G- und 3G-Netze aber abgeschaltet und deren Frequenzen für LTE eingesetzt werden. Wann es soweit

**Die Telekom hat das LTE-Netz in der Fläche sehr gut ausgebaut; UMTS hingegen ist in vielen Regionen gar nicht verfügbar.**



ist, wollten die Anbieter nicht beantworten. O2 ließ uns wissen, man halte sich „alle Optionen offen“. Vodafone sagt, man werde die Netze „bedarfsorientiert“ ausbauen. Derzeit gäbe es keine Planungen für eine Abschaltung, antwortete uns die Telekom.

Bei O2 ging es gezwungenermaßen erst einmal in die andere Richtung: Der Anbieter hat kürzlich das komplette vormalige LTE-Netz von E-Plus abgeschaltet. Bei der Übernahme des Konkurrenten musste Te-

lefonía einen Teil der Frequenzen abtreten – diesen freigewordenen Frequenzblock ersteigerte Vodafone. Dafür können ehemalige E-Plus-Kunden nun das insgesamt besser ausgebaute LTE-Netz von O2 nutzen. Örtlich kann sich die LTE-Versorgung dadurch zwar verschlechtern, insgesamt ist die Umstellung für bisherige E-Plus-Kunden aber ein Gewinn, weil das LTE-Netz von E-Plus das mit Abstand am schlechtesten ausgebaute aller Netzbetreiber war. (uma) **ct**





Daniel Berger

# LTE-Tarife fürs Smartphone

LTE verspricht schnelles Internet auch unterwegs. Das Tarif-Angebot ist vielfältig, aber auch unübersichtlich. Wer den passenden Tarif abschließen will, muss genau hingucken, was die Provider bieten.

**D**ie Konkurrenz im Mobilfunkmarkt ist groß und viele Anbieter kämpfen mit nicht immer feinen Methoden um Kunden. Das Strickmuster ist das gleiche: Die vielen Tarife, Rabatte und Fußnoten sollen die Übersicht und die Vergleiche erschweren, damit man mehr ausgibt. Umso ärgerlicher, wenn man den Fehler erst nach dem Vertragsabschluss bemerkt und dann lange Vertragslaufzeiten einen schnellen Ausstieg verhindern.

Es gibt aber einige Faustregeln, die die Auswahl erheblich erleichtern. Schätzen Sie zunächst ein, wie viel Ihnen mobiles Internet tatsächlich bedeutet und wie oft Sie täglich oder wöchentlich darauf zugreifen. Zu einem Vielsurfer kann man leicht verführt werden – beispielsweise wenn man öfter auf Busse, Bahnen und Freunde wartet. Dann sind Sie vielleicht auch ein Kandidat für süße Welpen-Videos oder Snapchat-Streams. Die Tarife mit reichlich Highspeed-Inklusiv-Volumen bleiben dennoch eher geschäftlichen Anwendern wie Außendienstlern oder Grafikern vorbehalten, die Entwürfe und Bilder unterwegs an Kunden senden. Die Preisspanne geht leicht bis zu 100 Euro und mehr im Monat. Dafür bekommt man um die 20 GByte Transfervolumen pro Abrechnungszeitraum.

## Weniger reicht auch

Wer LTE vor allem auf dem Weg zwischen zu Hause und Büro braucht und sonst mit WLAN gut versorgt ist, spart bei der Auswahl eines kleineren Angebots viel Geld. Fürs Lesen von Eilmeldungen und Artikeln reichen 1 bis 2 GByte im Monat aus. Und Pokémon Go ist auch noch drin: Bis Level 20 verbraucht das Spiel nur gut 150 MByte vom Datenvolumen.

LTE mit weniger als 1 GByte Übertragungsvolumen macht jedoch keinen Spaß: Das Internet fühlt sich zwar auch dann superschnell an, ist aber auch superschnell gedrosselt. Zwar ist auch der Nachkauf von Datenkontingenten möglich, doch im Vergleich zum Inklusiv-Volumen ist das teuer – pro GByte sind je nach Anbieter bis zu 20 Euro fällig. Manche auf kurzem Dienstweg beschafften Prepaid-Verträge mit kurzen Kündigungsfristen können da als Nachbrenner günstiger sein, wenn das Highspeed-Volumen des Postpaid-Vertrags aufgebraucht ist.

Große Vorsicht ist hingegen bei der „Datenautomatik“ angebracht: Einige Anbieter buchen bis zu dreimal 100 oder 250 MByte automatisch nach. WinSIM und

Yourfone bewerben diesen Service sogar als „fair“, obwohl die Kunden kaum eine andere Wahl haben: Die Datenautomatik ist „fester Tarifbestandteil“ und nicht kündbar. Dagegen hilft nur noch ein Volumenbegrenzer im Smartphone oder Mobilfunk-Router. Bei einigen Anbietern genügt immerhin ein Anruf, um diese unfeine Abkassier-Automatik abzustellen (Opt-out). Unsummen verschlingen die automatischen Nachbuchungen zwar nicht, aber 2 Euro für 100 MByte erinnern ans Internet-Café.

Sind Datenvolumen (und Datenautomatik) ausgereizt, drosseln die Anbieter die Geschwindigkeit drastisch: Die Drillisch-Marken WinSIM, Simply, Yourfone und DeutschlandSIM entschleunigen auf schneckenlangsame 16 KBit/s; branchenüblich sind 32 oder 64 KBit/s. Aber auch diese Drossel-Stufen fühlen sich an, als würde man von der Autobahn plötzlich in eine Spielstraße geraten. Selbst der Abruf einer WhatsApp-Nachricht dauert ewig. Ein verschicktes Selfie quält sich minutenlang durch die Leitung und blockiert den gesamten Datentransfer. Mit aktiver Drosselung ist der Internet-Anschluss praktisch unbrauchbar.

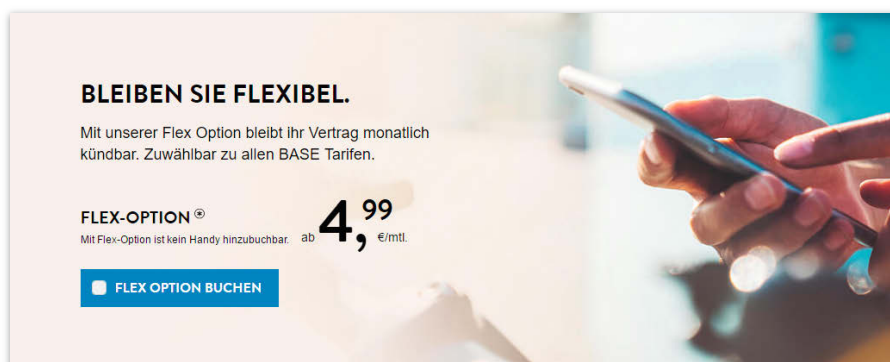
Doch welches monatliche Datenkontingent genügt? Sehr brauchbare Richtwerte liefern Smartphones, die über den Datentransfer Buch führen; bei Android findet man diese Angaben in den Einstellungen unter „Datenverbrauch“, bei iOS unter „Mobiles Netz“. Die Volumenzähler warnen auf Wunsch, wenn das Volumen knapp wird, arbeiten allerdings nicht genau. Wenn Provider blockweise Einheiten abrechnen, etwa auf Basis von 1, 10 oder 100 KByte, und bei der Berechnung aufrunden, kommt es regelmäßig zu Abweichungen. Wer es ganz genau wissen will, muss in die Verbindungsnachweise schauen. Zudem bieten viele Anbieter

Apps, die über den tatsächlich berechneten Datenverkehr informieren. Allerdings können diese Angaben zeitlich hinterherhinken.

## Langzeitbeziehung

LTE-Tarife und Aktionsangebote können sich unversehens ändern: Die Preise fallen zwar langsam, aber in vielen kleinen Schüben, und die Leistung steigt. Vodafone etwa hat jüngst die Preise seiner Red-Tarife gesenkt. Bei der vorigen Tarifrunde hat das Unternehmen das Inklusiv-Volumen erhöht. Deshalb sind Verträge mit langen Laufzeiten eher unattraktiv, auch wenn sie auf 24 Monate gerechnet deutlich billiger erscheinen als Angebote mit monatlichen Kündigungsfristen. Doch die Erfahrung zeigt, dass sich der Markt innerhalb von zwei Jahren zu sehr ändert. Attraktive Neuerungen gewähren die Anbieter meist nur Neukunden – Bestandskunden können nur in Ausnahmen vorzeitig in einen neuen, günstigeren Tarif wechseln. Und dann beginnt die Laufzeit von vorn; normalerweise dauert sie wieder zwei Jahre. Der Wechsel in einen teureren Vertrag samt Laufzeitverlängerung klappt hingegen problemlos – Unentschlossene können also erst mal klein anfangen und später aufstocken. Wer nach Vertragsablauf ein neues Abenteuer sucht, muss rechtzeitig Schluss machen, sonst verlängert sich der Vertrag um ein weiteres Jahr. Bei Zweijahresverträgen beträgt die Kündigungsfrist üblicherweise drei Monate.

Um auszuprobieren, ob LTE überhaupt nützlich ist, eignen sich Verträge mit Laufzeiten von einem Monat. Die meisten solcher flexiblen Angebote nutzen das LTE-Netz von O2. Darunter fällt die Firma Drillisch mit diversen Markennamen auf, etwa als Yourfone, Simply oder WinSIM. Das LTE-Netz von O2 liefert geringere Datenraten als die Netze von Telekom und Vodafone



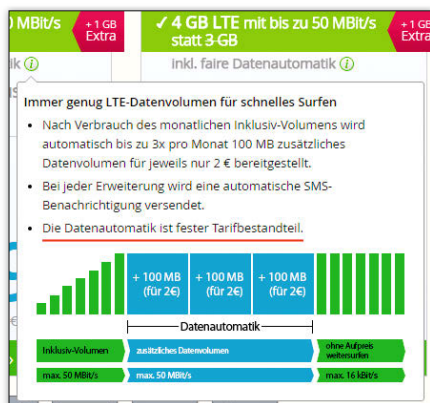
**BLEIBEN SIE FLEXIBEL.**

Mit unserer Flex Option bleibt Ihr Vertrag monatlich kündbar. Zuwählbar zu allen BASE Tarifen.

**FLEX-OPTION®**  
Mit Flex-Option ist kein Handy hinzubuchen. ab **4,99** €/mtl.

☐ FLEX OPTION BUCHEN

**Flexibilität hat ihren Preis: Wer sich vertraglich nicht lange binden möchte, zahlt monatlich mehr als bei einem Zweijahresvertrag – kann dafür aber monatlich kündigen.**



Ist das Datenvolumen aufgebraucht, buchen manche Anbieter ganz automatisch neues hinzu. Nicht immer lässt sich die „Datenautomatik“ abstellen: Bei WinSIM ist sie „fester Tarifbestandteil“.

und die Abdeckung ist schlechter. Immerhin will O2 die Abdeckung bis Ende des Jahres von derzeit 75 auf 90 Prozent der Bevölkerung verbessern.

Die schlechtere LTE-Abdeckung von O2 schlägt sich positiv im Preis nieder: Wenig-surfer bekommen für 10 bis 15 Euro im Monat 1 bis 2 GByte Volumen per LTE. Telekom und Vodafone verlangen mehr für

ihre besser ausgebauten Netze und bieten höhere Geschwindigkeiten. Bei Vodafone bekommt man in gut ausgebauten Regionen bis zu 225 MBit/s im Downstream. Die Telekom liefert in diversen Ballungsgebieten bis zu 300 MBit/s. In der Praxis erreicht man diese Spitzenwerte jedoch selten: Dafür braucht man eine Funkzelle für sich alleine und gute Funkqualität. Bestwerte der Durchsatzmessungen sind daher nachts oder in den frühen Morgenstunden erzielt worden.

Um mehr als 150 MBit/s per LTE zu laden, braucht man allerdings ein Gerät, das zwei oder mehr Träger bündelt. In ländlichen Gebieten sind die maximalen Datenraten grundsätzlich geringer, weil die Netzbetreiber breite Funkbänder, Trägerbündelung und andere Mobilfunk-Booster vorzugsweise dort einsetzen, wo es sich für sie rentiert – in dicht besiedelten Gebieten. Aber auch dort leistet LTE gute Dienste, etwa als Ersatz für den Fall, dass der Kabelanschluss ausfällt, oder als Hauptzugang zum Internet. Freilich hat der von der Bundesregierung forcierte LTE-Ausbau auf dem Land doch noch einige kleine Lücken gelassen. Welche das sind und wo man eine brauchbare Versorgung erwarten kann, zeigen die Netzbetreiber auf interaktiven Karten. Die Auflö-

sung reicht bis auf einige zehn Meter hinunter, sodass man zwar Straßenzüge erkennen kann, aber keine weiteren Details, etwa den Versorgungsgrad in den Wohnungen. Vielleicht kann auch einfach ein Freund mit seinem Smartphone und Tarif aushelfen und die LTE-Versorgung schnell vor Ort testen.

## Premium kostet

Bei den Flächendeckungskarten sollten Sie beachten, dass nicht alle Anbieter LTE meinen, wenn sie von schnellem Internet reden. 1&1 bietet beispielsweise Tarife mit „D-Netz-Qualität“ und meint damit allerdings das Vodafone-Netz. Doch LTE gibt es in diesen Tarifen nicht, sondern maximal HSPA+ mit bis zu 42,2 MBit/s. LTE bekommt man nur direkt bei Vodafone, dort aber immerhin auch als Prepaid-Angebot: Mit der „CallYa Freikarte“ samt „Allnet Flat“ kann man für 22,50 Euro im Monat 1,1 GByte mit voller LTE-Geschwindigkeit (225 MBit/s) versurfen; die Mindestlaufzeit beträgt einen Monat. Für weitere 10 Euro lassen sich 750 MByte hinzubuchen. Für „Mega-Surfer“ mit Bindungsängsten bietet auch die Telekom einen Tarif samt LTE mit einer Spitzengeschwindigkeit von 50 MBit/s. „Magenta Mobil Start“ kostet 2,95 Euro im Monat, der

## LTE-Smartphone-Tarife (Auswahl)

Anbieter	1&1	Base	DeutschlandSIM	Mobilcom	O2	O2	Simply
Netz	O2	O2	O2	O2	O2	O2	O2
Tarif	Basic/Plus/Pro	Light/Pur/Plus/Pro Flex	LTE M/1500/3000/5000/10000	Allnet 1/2/5 GB LTE	Loop Smart L/XL	Free S/M/L/XL Flex	LTE 1500/3000/5000/10000
Abrechnung	Postpaid	Postpaid	Postpaid	Postpaid	Prepaid	Postpaid	Postpaid
URL	www.1und1.de	www.base.de	www.deutschlandsim.de	www.mobilcom-debitel.de	www.o2online.de	www.o2online.de	www.simplytel.de
Internet-Flatrate							
Datenvolumen pro Monat	3/4/5 GByte	2/3/4/5 GByte	2/1,5/3/5/10 GByte	1/2/5 GByte	1/1,5 GByte	1/2/4/8 GByte	1,5/3/5/10 GByte
max. Datenrate Downstream	50 MBit/s	21,6 MBit/s	50 MBit/s	50 MBit/s	21,6 MBit/s	225 MBit/s	50 MBit/s
nach Verbrauch Freivolumen (Voreinstellung)	Drosselung auf 64 kBit/s	Drosselung auf 64 kBit/s	dreimal automatisch 100 MByte für je 2 €, dann Drosselung auf 16 kBit/s	Drosselung auf 32 kBit/s	L: dreimal 100 MByte für je 2 €; XL: dreimal 250 MByte für je 3 €, dann Drosselung auf 32 kBit/s	Drosselung auf 1000 kBit/s	dreimal automatisch 100 MByte für je 2 €, dann Drosselung auf 16 kBit/s
Telefonie und SMS							
Telefonie Festnetz	inklusive	inklusive	inklusive	inklusive	0,09 €/Min.	inklusive	inklusive
Telefonie netzintern	inklusive	inklusive	inklusive	inklusive	inklusive	inklusive	inklusive
Telefonie andere Mobilnetze	inklusive	inklusive	inklusive	inklusive	0,09 €/Min.	inklusive	inklusive
SMS Inland	inklusive <sup>1</sup>	inklusive <sup>2</sup>	inklusive	0,09 €/SMS	0,09 €/SMS	inklusive	inklusive
Freiminuten/-SMS							
freie Telefonate pro Monat	Flatrate	Flatrate	Flatrate	Flatrate	200 Einheiten <sup>3</sup>	Flatrate	Flatrate
freie SMS pro Monat	Flatrate <sup>1</sup>	Flatrate <sup>2</sup>	Flatrate	–	200 Einheiten <sup>3</sup>	Flatrate	Flatrate
Vertragliches							
Laufzeit/Verlängerung	1/1 Monat	1/1 Monat	1/1 Monat	1/1 Monat	1/1 Monat	1/1 Monat	1/1 Monat
Kündigungsfrist	14 Tage	30 Tage	30 Tage	14 Tage	30 Tage	30 Tage	30 Tage
Kosten							
Anschlusspreis	29,90 €	29,99 €	29,99 €	39,99 €	–	29,99 €	19,99 €
monatliche Kosten	19,99/24,99/29,99 €	14,98/19,98/24,98/29,98 €	14,99/19,99/24,99/39,99/69,99 €	12,98/17,98/22,98 €	14,99/19,99 €	29,98/39,98/49,98/59,98 €	9,99/12,49/19,99/34,99 €

<sup>1</sup> Basic: 0,10 €/SMS oder SMS-Flat für 4,99 €/Monat

<sup>2</sup> Light und Pur: 0,09 €/SMS

<sup>3</sup> insgesamt 200 Einheiten für Telefonate/SMS

– nicht vorhanden



zusätzlich buchbare Datentarif „Data Start L“ (1 GByte) kostet weitere 14 Euro im Monat. Für insgesamt 16,95 Euro im Monat kann man also ohne lange Vertragslaufzeit ins LTE-Netz der Telekom schnuppern. Attraktiv für Kunden ist das Fehlen einer Kündigungsfrist.

Will man langfristig (viel) mehr als 1 GByte, eignen sich die großen MagentaMobil-Tarife der Telekom oder die Red-Verträge von Vodafone besser. Die Preise sind bei beiden Anbietern ähnlich hoch und beginnen ohne Rabatte bei 30 Euro (Vodafone) und 35 Euro (Telekom) im Monat. Verlockend können Pakete sein, die ein subventioniertes Smartphone enthalten, das der Kunde in Monatsraten abbezahlt. Oft ist es aber unterm Strich günstiger, das Gerät unabhängig vom Vertrag zu kaufen. Zudem können Rabatte und Gutschriften entfallen, wenn man sich für ein subventioniertes Gerät entscheidet. Es lohnt sich also, den Taschenrechner auf dem alten Smartphone zu starten und ein bisschen zu rechnen.

Die Tabelle enthält Tarife ohne subventionierte Hardware. Gibt es denselben Tarif mit verschiedenen Laufzeiten, haben wir den mit der kürzeren aufgenommen. Das gilt etwa für 1&1: Wer sich nur 30 Tage anstatt 24 Monate binden möchte, zahlt mo-

natlich 5 Euro drauf – fährt langfristig aber vermutlich günstiger, weil er umgehend neue Angebote wahrnehmen kann.

Viele Anbieter locken Neukunden mit Rabatten und Aktionen. Dann erlassen sie etwa bei Online-Buchungen 10 Prozent des Monatspreises sowie die Anschlusskosten. Diese schlagen in vielen Fällen einmalig mit gut 30 Euro zu Buche. Manche Tarife gelten nur für die Mindestvertragszeit und danach steigen die Kosten, weil dann die regulären Tarifpreise gelten.

## Online gebucht

Außer Sonderoptionen und Rabatten bietet die Online-Buchung einen weiteren Vorteil: Hat man die Geschäftsbedingungen erst einmal gefunden, lässt sich der Vertrag samt seiner Fußnoten in aller Ruhe studieren. Am Telefon oder im Laden geht das kaum, zudem gibt es im Geschäft keine Widerspruchsmöglichkeit. Achten sollte man auf die Laufzeiten und Kündigungsfristen. Im Kleingedruckten steht auch, was nach Ablauf der Vertragslaufzeit passiert und ob es etwa eine Datenautomatik gibt.

Die meisten der Angebote sind Kombi-Tarife. Sie enthalten außer einem Datenkontingent zumeist Allnet-Flats, mit denen man in nationalen Netzen so oft telefonie-

ren und SMS verschicken kann, wie man will. Möchte man Tablet, Laptop oder mobilen WLAN-Router mit dem LTE-Netz verbinden, sind Daten-Tarife günstiger. Auch für Dual-SIM-Smartphones sind sie eine sinnvolle Ergänzung, die Telefonate laufen dann über eine zweite SIM-Karte. Über umständliche Umwege sind Telefonate aber auch mit Daten-SIMs möglich, etwa über VoIP und WhatsApp. Und manche Anbieter konzipieren einige Angebote zwar nur für den Internet-Zugang, gewähren aber dennoch Telefonate.

Viele Provider bieten optional SIM-Karten an, die man ins Tablet oder Smartphone stecken kann. Zu den Free-Tarifen L und XL von O2 ist eine Multicard kostenlos erhältlich; ansonsten kostet die zweite SIM-Karte 4,99 Euro im Monat. Bei Vodafone sind die Daten-SIMs ähnlich teuer. Die Drillisch-Marken verlangen für solche Angebote etwas weniger: Bei Yourfone etwa kostet eine Zusatz-SIM 2,95 Euro im Monat plus einmalig 4,95 Euro. (dbe) **ct**

## Literatur

- [1] Urs Mansmann, Teures Volumen, Mobile Breitband-Tarife für Vielnutzer, c't 16/16, S. 78

Smartmobil	Telekom	Telekom	Vodafone	Vodafone	WinSIM	Yourfone
O2	Telekom	Telekom	Vodafone	Vodafone	O2	O2
LTE XS/S/M/L	MagentaMobil Start L	MagentaMobil S/M/L/L+	CalliYa Allnet Flat	Red S/M/L	LTE All 2/3/4 GB	LTE XS/S/M/L
Postpaid	Prepaid	Postpaid	Prepaid	Postpaid	Postpaid	Postpaid
www.smartmobil.de	www.telekom.de	www.telekom.de	www.vodafone.de	www.vodafone.de	www.winsim.de	www.yourfone.de
2/4/5/6 GByte	1 GByte <sup>4</sup>	1/3/6/10 GByte	1,1 GByte	1/3/6 GByte	2/3/4 GByte	2/4/5/6 GByte
50 MBit/s	50 MBit/s	300 MBit/s	225 MBit/s	225 MBit/s	50 MBit/s	50 MBit/s
dreimal automatisch 100 MByte für je 2 €, dann Drosselung auf 16 kBit/s	Drosselung auf 64 kBit/s	Drosselung auf 64 kBit/s	Drosselung auf 32 kBit/s	optional dreimal 250 MByte für je 3 €, dann Drosselung auf 32 kBit/s	dreimal automatisch 100 MByte für je 2 €, dann Drosselung auf 16 kBit/s	dreimal automatisch 100 MByte für je 2 €, dann Drosselung auf 16 kBit/s
inklusive	0,09 €/Min.	inklusive	inklusive	inklusive	inklusive	inklusive
inklusive	inklusive	inklusive	inklusive	inklusive	inklusive	inklusive
inklusive	0,09 €/Min.	inklusive	inklusive	inklusive	inklusive	inklusive
inklusive	0,09 €/Min.	inklusive	inklusive	inklusive	inklusive	inklusive
Flatrate	Flatrate (netzintern)	Flatrate	Flatrate	Flatrate	Flatrate	Flatrate
Flatrate	Flatrate (netzintern)	Flatrate	Flatrate	Flatrate	Flatrate	Flatrate
1/1 Monat	4/4 Wochen	24/12 Monate	4/4 Wochen	24/12 Monate	1/1 Monat	24/12 Monate
30 Tage	—	3 Monate	—	3 Monate	30 Tage	3 Monate
29,99 €	9,95 €	29,95 €	—	34,99 €	19,99 €	29,99 €
12,99/17,99/22,99/27,99 €	14,95 €	34,95/44,95/54,95/79,95 €	22,50 €	29,99/39,99/49,99 €	9,99/12,99/15,99 €	14,99/19,99/24,99/29,99 €

Jörg Wirtgen

# Kaufberatung: Smartphones mit LTE

**Fast alle aktuellen Smartphones eignen sich für den LTE-Mobilfunk, doch wer eine zukunftssichere Ausstattung möchte, muss auf Details wie Kanäle und Trägerbündelung achten. Unter den günstigen Restposten und eBay-Schnäppchen verstecken sich mitunter noch Telefone ohne LTE.**

**D**ass ein Smartphone LTE beherrscht, sagt noch lange nichts darüber aus, wie gut es das Funknetz ausnutzt. Die Unterschiede stecken in den Details: Funkt es in allen drei hierzulande gängigen Bändern, eignet es sich für die zukünftigen, bündelt es zwei oder mehr? Für Reisende ist zudem die Gesamtzahl der unterstützten Bänder interessant.

Neben den drei hierzulande aktuell für LTE vergebenen Bändern B3 (1800 MHz), B7 (2600 MHz) und B20 (800 MHz) wird künftig auch das Band 28 (700 MHz) wichtig. Es wird im Rahmen der Digitalen Dividende II von DVB-T zu LTE umgewidmet und ergänzt in ländlichen Gebieten B20. Was mit den ebenfalls versteigerten

1500 MHz passiert, ist noch unklar, doch vermutlich kommt kein aktuelles Gerät damit zurecht. In weiterer Zukunft könnten zusätzlich B38 (2600 MHz in geänderter Betriebsart) und B1 (Abschalten von UMTS zugunsten LTE) interessant werden.

Die ersten LTE-Smartphones funkten nur in ein oder zwei Bändern. Deshalb kamen sie nicht bei allen Providern und in allen Gegenden ins LTE-Netz. Aktuelle Geräte haben diese Einschränkung nicht mehr, schon die unter 100 Euro kennen genügend Bänder. Die Top-Geräte unterstützen rund 20 der weltweit über 50 definierten Bänder.

Beim Bestellen und Kauf im Ausland sollten Sie achtgeben, eine europäische Version der Geräte zu bekommen. Beispielsweise kennen nur wenige chinesische und US-Versionen die Bänder 3 und 20.

## Gebündelt gefunkt

In einem LTE-Band sind Richtung Endgerät (Downstream) derzeit maximal 150 MBit/s möglich. Mehr geht nur per Carrier Aggregation (CA, Trägerbündelung). Dazu muss die Basisstation auf mindestens zwei Bändern gleichzeitig funken und die Bündelung unterstützen. Mit zwei Trägern sind 300 MBit/s möglich, mit drei 450 MBit/s. Das Normierungsgremium 3GPP fasst diese Ausbaustufen unter LTE Advanced (LTE-A) zusammen. In der für Deutschland nächsten Ausbaustufe LTE Advanced Pro

(LTE-AP) sind durch eine höherwertige Modulation mit weiterhin drei Trägern 600 MBit/s und mehr möglich. Der Begriff 4.5G bezeichnet uneinheitlich mal LTE-A, mal LTE-AP.

Einige Provider geben davon abweichende Transferraten an, Vodafone beispielsweise 225 oder 375 MBit/s. Das liegt daran, dass einige Bänder mit 10 statt 20 MHz betrieben werden und nur 75 MBit/s übertragen. In Deutschland sind davon B20 und B28 betroffen.

Welche maximale Datenrate ein Smartphone erreicht, beschreibt dessen Kategorie (Cat): Ab Cat 6 bündelt es zwei Träger (300 MBit/s), ab Cat 9 drei (450 MBit/s); ab Cat 11 funktioniert LTE-AP (600 MBit/s). Geräte der Kategorien 7, 10 und 12 bündeln auch im Upstream, doch das ist weltweit noch unbedeutend.

Über die Zahl der insgesamt unterstützten Bänder sagt die Kategorie allerdings nichts aus. Fehlt in den technischen Daten eines Handys die Kategorie, lässt sich die CA-Fähigkeit aus der Maximalgeschwindigkeit ableiten. Findet man die Angabe LTE-A, dürfte Cat 6 gemeint sein. Ist nur LTE angegeben, funkt das Handy vermutlich mit Cat 4 (150 MBit/s) oder gar nur Cat 3 (100 MBit/s).

## Cat 9, Cat 11, LTE-AP

In Deutschland nutzt derzeit kein Provider LTE-AP, sodass man keine Smartphones mit Cat 11 benötigt. Bisher sind auch nur wenige lieferbar: Asus Zenfone 3 Deluxe, Google Pixel/Pixel XL und Huawei Mate 9. Eine Version des Samsung Galaxy Note 7 sollte als erstes Smartphone Cat 12 mit vier Antennen unterstützen, doch Samsung musste es aufgrund der Akkuprobleme zurückrufen und einstellen.



**Selbst billige LTE-Smartphones kennen alle wichtigen LTE-Bänder, Spitzenmodelle wie das Samsung Galaxy S7 sogar rund 20.**

Die Flaggschiffe der meisten Hersteller eignen sich für Cat 9: Apple iPhone 7, BlackBerry Priv, HTC 10, LG G5, Motorola Moto Z, Samsung Galaxy S7/S7 Edge, Sony Xperia X, Xiaomi Mi Note Pro. In Europa kommen von BlackBerry, LG, Motorola und Sony allerdings nur Varianten mit Cat 6 auf den Markt.

In Deutschland kommt die Dreifachbündelung langsam in Fahrt. Vodafone hat inzwischen den Regelbetrieb mit B3, B7 und B20 gestartet, alle drei Bänder gibt es aber nur an wenigen Orten. Band 28 werden die Provider anfangs auf dem Land (2CA mit B20) verwenden, erst später wird es wohl auch in städtischen Bereichen in 3CA-Konstellationen Einzug halten.

Derzeit bringt Cat 9 daher wenig, zudem reicht die mit zwei Trägern erreichbare Geschwindigkeit für Smartphones. Wer nicht gerade regelmäßig seine PCs übers Smartphone per Tethering mit Internet versorgt, kommt also mit Cat 6 aus.

## Cat 6, LTE Advanced

Die Auswahl an Geräten mit Cat 6 ist immens, darunter fast alle Neuvorstellungen von 2016 sowie die teils zu verlockenden Preisen erhältlichen Top-Geräte aus 2015: Apple iPhone 6S/6S+, Google Nexus 6P, HTC One M9, Huawei P9, LG G4, Microsoft Lumia 950, Motorola Moto X, Samsung Galaxy Note 4 und S6 sowie Sony Xperia Z5 beispielsweise.

Auch günstige Geräte wie das Gigaset ME oder OnePlus 3 und kleinere wie das Sony Xperia Z5 Compact sind dabei. Unter 300 Euro gehts etwa mit dem Google Nexus 5X, Huawei Honor 6, LG G Flex 2, Samsung Galaxy A5 und S5 Neo los.

Sie alle unterstützen B3, B7 und B20, nur wenige aber B28. Allerdings sollte man sich nicht darauf verlassen, dass sie dann die zukünftige Bündelung von B20 und B28 zum Beschleunigen des ländlichen LTE von 75 auf 150 MBit/s beherrschen: Wir haben nur beim Nexus 5X und 6P überhaupt eine Liste mit Bündelungspaaren gefunden, und da fehlt das Paar B20+B28.

**Solche Spitzenwerte erreicht man selten, in der Praxis dürften auch mit LTE Advanced meist unter 100 MBit/s realistisch sein.**

Beim Neukauf gibt es jedenfalls kaum Gründe, ein Smartphone ohne Trägerbündelung zu wählen. Über den aktuell noch nicht so wichtigen Geschwindigkeitszuwachs hinaus verbessert Cat 6 die Robustheit gegen Empfangsstörungen, liefert an überlasteten Zellen mehr Kapazitäten und hat Luft für steigende Anforderungen. Dagegen spricht lediglich die höhere Stromaufnahme, aber die Geräte bündeln nur bedarfsweise.

## Auch nicht gerade lahm

Wer schon ein LTE-Smartphone mit Cat 3, 4 oder 5 hat, muss es nicht ausmüsten: Selbst die 75 MBit/s des ländlichen LTE sind für die meisten Smartphone-Anwendungen schnell genug – sogar das auf 7 MBit/s ausgebremste LTE der alten Congstar-SIMs macht aufgrund der verkürzten Signallaufzeit mehr Spaß als HSPA.

Es gibt auch Neugeräte, die trotz Beschränkung auf Cat 4 interessant bleiben, beispielsweise das Fairphone 2, Outdoor-Smartphones wie das Cat S60 und Samsung Xcover 3, die iPhone-Modelle 6, 6+ und SE sowie einige Dual-SIM-Geräte. Auch bei den Smartphones um 100 Euro ist der Verzicht auf Cat 6 verschmerzbar. Auf den drei wichtigen Bändern funken sie alle, kaum eines aber auf B28.

Bei Geräten ab etwa 150 Euro lohnt dennoch die Suche nach ähnlich teuren Alternativen mit Cat 6. Dabei verliert manches Schnäppchen seinen Reiz, darunter HTC M8, Google Nexus 5, LG G4s, Motorola G3 3rd, G4 (Plus), OnePlus X oder Samsung Galaxy S5 und S5 Mini.



Vorsicht auch bei älteren Modellen: So kennen das Galaxy S4 und das iPhone 5 nur Cat 3 (100 MBit/s), letzteres zudem nur Band 3. Dem OnePlus One fehlt Band 20.

Angesichts dieser Vielfalt gibt es keinen Grund mehr, bei Neukäufen auf LTE zu verzichten. Ach ja, der Akkulaufzeit schadet LTE nicht: Ganz im Gegenteil sparen die kürzeren Transferzeiten gerade bei großen und regelmäßigen Datenmengen Strom gegenüber HSPA+ oder älter. (jow) **ct**

## Smartphone-Geschwindigkeiten

Technik	Bezeichnung	Display-Anzeige	max. Geschwindigkeit [MBit/s]
GPRS	2.5G	G, 0	0,0576
EDGE	2.75G	E	0,236
UMTS	3G	3G, U	0,384
HSPA	3.5G	3.5G, H	14,4
HSPA+	3.5G	H+	bis 42,2
LTE (bis Cat 4)	4G <sup>1</sup>	4G, LTE	bis 150
LTE-A (ab Cat 6)	4.5G <sup>1</sup>	4G+	bis 600
LTE-AP (ab Cat 11)	4.5G	?	ab 600

<sup>1</sup> Manchmal findet man auch für LTE die Bezeichnung „3.9G“ und erst für LTE Advanced „4G“.

## Derzeit erreichbare Downlink-Geschwindigkeiten in Deutschland

Geräteklasse	Downlink theoretisch [MBit/s]	Trägerbündelung	Telekom [MBit/s]			Vodafone [MBit/s]				02 [MBit/s]
			Land	Stadt	gebündelt (2CA)	Land	Stadt	gebündelt (2CA)	gebündelt (3CA)	
Cat 3	100	–	75	100	100	75	100	100	100	225
Cat 4	150	–	75	150	150	75	150	150	150	225
Cat 6 + 7	300	2	75	150	300	75	150	225/300	300	225
Cat 9 + 10	450	3	75	150	300	75	150	225/300	375	225
Cat 11 + 12	600	3	75	150	300	75	150	225/300	375	225

Hier sind nur Kategorien aufgeführt, die in Smartphones vertreten sind. Die Uplink-Geschwindigkeit beträgt in allen deutschen Netzen 50 MBit/s.

Telekom: Cat 6 mit 300 MBit/s (20 MHz auf 1800 und 2600 MHz)

02: Cat 3 mit 225 MBit/s (10 MHz auf 800 MHz oder 20 MHz auf 2600 MHz)

Vodafone: Cat 6 mit 225 MBit/s (10 MHz auf 800 MHz, 20 MHz auf 2600 MHz); an wenigen Stellen Cat 9 mit 375 MBit/s (zusätzlich 20 MHz auf 1800 MHz) und möglicherweise dort auch Cat 6 mit 300 MBit/s





Hannes A. Czerulla

## Die besten Android-Handys im Vergleich

**Manchmal muss man sich etwas gönnen – eins der besten Smartphones beispielsweise. High-End-Telefone wie das HTC 10, LG G5 und Motorola Moto X Force bieten die besten Kameras, die hübschesten Displays und die längsten Laufzeiten. Und müssen sich im Test der Android-Referenz Samsung Galaxy S7 stellen.**

**S**chluss mit den Kompromissen! Wer beim Smartphone-Kauf nur auf den Preis guckt, denkt meist nach kürzester Zeit über den nächsten Kauf nach. Das System ruckelt, der Akku ist ständig leer und die Fotos der Kamera kann man niemanden zeigen. Mit einem Spitzenmodell wäre das nicht passiert. Denn die Hersteller stecken alles an Technik in ihre Flaggschiffe, was gerade up to date ist: hochauflösende, helle Displays, Kameras, die jede Kompaktknipse alt aussehen lassen, und fette Akkus mit Strom für zwei Tage.

Gutes Beispiel für die Kategorie der High-End-Smartphones ist das Samsung Galaxy S7. Es schnitt in unserem Einzeltest so gut ab wie kein Gerät zuvor und hat neue Maßstäbe in Sachen Display, Kamera und Design gesetzt. Bringt ein Hersteller

ein neues Android-Smartphone auf den Markt, muss es sich mit dem S7 messen. In diesem Test tun dies das Gigaset ME pro, HTC 10, Huawei P9, LG G5 und das Motorola Moto X Force.

Das ME pro ist das größte und am besten ausgestattete Gerät aus der Modellpalette der mittlerweile chinesischen Marke Gigaset. Mit 5,5 Zoll Bildschirmdiagonale rangiert es in der Kategorie „Phablet“. Auch auf das Moto X Force passt diese Bezeichnung. Sein 5,4 Zoll großer OLED-Bildschirm ist mit einer bruchsicheren Scheibe geschützt und soll auch den Aufprall auf harten Steinboden ohne Schäden überstehen. HTC streicht mit der Einführung des „10“ die Bezeichnung „One“ aus dem Namen seiner Top-Modelle. Parallel dazu gehen technische Paradigmenwechsel einher; unter anderem übersteigt die Display-

Auflösung erstmals Full HD. Der chinesische Hersteller Huawei schickt das schlanke, schicke P9 mit Doppelkamera ins Rennen. Das LG G5 soll mit ansteckbaren Hardware-Erweiterungen und ebenfalls zwei Hauptkameras punkten. Die Erweiterungen waren zum Test noch nicht verfügbar.

Die aktuelle Android-Version findet man nun auf dem LG G5 und HTC 10. Auf allen anderen läuft noch Android 6. Gigaset liefert das ME pro mit dem hoffnungslos veralteten Android 5.1.1 aus, dem beispielsweise der stromsparende Doze-Mode fehlt.

Zusätzlich stülpen bis auf Motorola alle Hersteller ihre eigenen Bedienoberflächen übers System und verändern mit Sense, EMUI oder TouchWiz genannten Oberflächen vor allem das Aussehen der Menüs und App-Symbole. Sie fügen eigene Programme hinzu, die meist die gleichen Auf-

gaben erledigen wie die sowieso installierten Standard-Apps von Google. Gigaset, Huawei und LG entfernen sogar das App-Menü aus dem System.

Das Problem der kurzen Laufzeiten versuchen die Hersteller mit größeren Akkus und Schnellladetechniken in den Griff zu bekommen. Immerhin hielten die Testgeräte meist um die zwei Tage ohne Laden durch. Dank Techniken wie Qualcomm Quick Charge sind die Akkus nach rund einer halben Stunde zur Hälfte geladen und liefern dann für fast einen Tag Energie. Der moderne Ladestecker USB Typ-C findet sich am G5, P9, ME pro und 10. Er wurde zwar zusammen mit USB 3.1 eingeführt, überträgt aber nur im ME pro und HTC 10 Daten mit bis zu 500 MByte/s, die anderen kommunizieren höchstens mit der USB-2.0-Geschwindigkeit von 60 MByte/s mit einem PC. Weiterer Vorteil der Typ-C-Stecker ist, dass sie wie Apple Lightning auch gedreht passen. Micro-USB-Anschlüsse haben hingegen den Vorteil, dass man quasi überall ein passendes Kabel findet.

Bei den Funkstandards gibt es kaum praxisrelevante Unterschiede: Alle Geräte beherrschen LTE mit theoretisch bis zu 300 MBit/s im Download, was nur die wenigsten Mobilfunktarife ermöglichen. 10 und S7 könnten sogar bis zu 450 MBit/s saugen, doch das bietet hierzulande noch kein Provider an. ME pro und Moto X Force können mit zwei unterschiedlichen SIM-Karten bestückt werden. Da die zweite SIM den Platz der Speicherkarte einnimmt, muss man sich zwischen Dual-SIM oder zusätzlichem Speicher entscheiden. Alle Geräte funken uneingeschränkt in 2,4- und 5-GHz-WLANs und kommunizieren via stromsparendem Bluetooth 4.1 oder 4.2. Auch bauen alle Hersteller wieder Speicherkarten-Slots ein und dimensionieren den internen Speicher mit 32 GByte ausreichend für große App-Sammlungen.

## Nicht alles High-End

Im Test treffen zwei CPU-Generationen aufeinander. Zur aktuellen Fraktion gehö-

ren der Exynos 8 Octa 8890 im Samsung Galaxy S7 und der Qualcomm Snapdragon 820 im HTC 10 und LG G5. Sie arbeiten wie alle Prozessoren im Test nach dem Big-Little-Prinzip, vereinen also langsame, stromsparende CPU-Kerne mit schnellen, stromhungrigen. Je nach Situation (Standby, Volllast etc.) arbeitet eine Kombination aus beiden Kernarten. Zur gleichen Generation zählt der HiSilicon Kirin 955 im Huawei P9.

Auch der über ein Jahr alte Snapdragon 810 im Gigaset ME pro und Motorola X Force gehört weiterhin zu den schnellen Smartphone-CPU. Doch von „High-End“ kann man hier nicht mehr sprechen, da seine Cortex-A57-Kerne nicht die Effizienz der moderneren Prozessor-Modelle erreichen. Außerdem ist seine Grafikeinheit Adreno 430 deutlich langsamer als der Adreno 530 des Snapdragon 820.

Für schnelle App-Wechsel und Programmstarts reichen 3 GByte Arbeitsspeicher. Apps starten aber auf den Telefonen mit mehr RAM etwas schneller und Programme laufen öfter im Hintergrund weiter, sodass sie nicht erst gestartet werden müssen, wenn man sie aufruft.

Ob das Display 1920 × 1080 oder 2560 × 1440 Pixel zeigt, spielt nur eine wichtige Rolle, wenn man das Smartphone in VR-Brillen wie der Google Cardboard einsetzen möchte. Ansonsten sind die Schärfenunterschiede höchstens im direkten Vergleich sichtbar. Dann wirkt das Galaxy S7 für geübte Augen einen Tick knackiger als beispielsweise das Huawei P9.

Im Alltag merkt der Nutzer eher wenig davon. Lieber sollte man sich die Frage stellen „LCD oder OLED?“. Bis vor Kurzem galt noch: Legt man mehr Wert auf Schärfe und Helligkeit, greift man lieber zum LCD. Stehen kräftige Farben und hoher Kontrast auf der Must-have-Liste, ist ein OLED das erste Mittel der Wahl.

Doch mittlerweile stellen auch LC-Displays einen Farbraum dar, der deutlich über sRGB hinausgeht und einige erreichen einen Kontrast von deutlich über 2000:1. Die OLED-Anzeigen haben eben-

falls kräftig nachgelegt. Hohe Helligkeit war früher eine Spezialität der LCDs, nun erreichen die beiden OLED-Geräte Galaxy S7 und Moto X Force mit über 500 cd/m<sup>2</sup> die höchsten Werte. Ausgefranzte, bunte Buchstaben sind ebenfalls Geschichte. Mit den hochwertigen LCDs im Test wird kein Nutzer unglücklich; wer aber die volle Farbenpracht und den höchsten Kontrast verlangt, sollte zu einem der OLED-Geräte greifen.

## Fazit

























Am Samsung Galaxy S7 gibt es so wenig zu bemängeln, dass es aus dem Test als Rundum-Sorglos-Paket hervorgeht. Es ist sowohl als Kameraersatz geeignet als auch als zuverlässiger Dauerläufer. Dennoch haben die Konkurrenten Kleinigkeiten zu bieten, die man am S7 nicht findet. Ein sauberes Android ohne Software-Ballast beispielsweise bekommt man nur mit dem Motorola Moto X Force. Sein bruchsaures Display-Glas ist ein weiteres Alleinstellungsmerkmal – leider auch sein unelegantes Äußeres. Bei den Laufzeiten liegt es als einziges Testgerät auf dem Niveau des S7.

Einen austauschbaren Akku hat nur das LG G5. Zusammen mit dem konservativ entworfenen HTC 10 bietet es sich in Bezug auf Fotoqualität und Performance am ehesten als Alternative zum S7 an. So lange wie der Titelverteidiger kommen sie aber nicht mit einer Akkuladung aus.

Fans von Schwarz-Weiß-Fotos finden eventuell Freude an der echten Monochrom-Kamera des Huawei P9, die eine bessere Tonwerttrennung bietet als nachträglich entfärbte Bilder. Für Spieler ist das P9 wegen der schwachen GPU als einziges ungeeignet und der Akku macht mit Abstand am schnellsten schlapp.

Hardware-Nachteile des Gigaset ME pro wie die ältere CPU stören im Alltag selten. Handfeste Nachteile bringt aber die veraltete Android-Version. Deswegen sollte man vom Kauf absehen. Ist einem die Dual-SIM-Funktion wichtig, bietet sich das Moto X Force als Alternative an. (hcz) **ct**

## Laufzeiten

Modell	Ladezeit auf 50% / 100%	Laufzeit Videowiedergabe (200 cd/m <sup>2</sup> ) [h] <small>besser ►</small>	Laufzeit Videowiedergabe (max. Helligkeit) [h] <small>besser ►</small>	Spiele (200 cd/m <sup>2</sup> ) <sup>1</sup> [h] <small>besser ►</small>	Laufzeit WLAN-Surfen (200 cd/m <sup>2</sup> ) [h] <small>besser ►</small>
Gigaset ME pro	41 min / 94 min	 9,5	 7,4	 4,4	 14,9
HTC 10	34 min / 89 min	 8,8	 6,9	 5	 12,8
Huawei P9	43 min / 123 min	 7,2	 4,6	 3,6	 12
LG G5	28 min / 85 min	 9,1	 8,6	 4,1	 10,8
Motorola Moto X Force	28 min / 106 min	 13,7	 9,4	 4,8	 16,2
Samsung Galaxy S7	33 min / 83 min	 14,8	 9	 7,8	 15,2

<sup>1</sup> Spiel: Asphalt 8



## Gigaset ME pro

Die Full-HD-Auflösung des Gigaset ME pro reicht für eine vollkommen scharfe Darstellung. Farbraum und Kontrast sind für ein LCD auf Spitzen-Niveau. Die Helligkeit könnte hingegen höher sein, denn 355 cd/m<sup>2</sup> reichen kaum aus, um das Display bei Sonne abzulesen. Die bei Tageslicht gute, aber nicht herausragende Kamera ist in der Dunkelheit wegen zu viel Rauschens kaum zu gebrauchen. Bildern fehlt es generell an Schärfe.

Den Fingerabdrucksensor auf der Rückseite erwischt man meist nur mit der Fingerflanke und braucht deswegen gelegentlich mehrere Versuche. Das Gehäuse besteht wie beim S7 aus Glas und Metall, ist aber nicht ganz so handlich.

Als Betriebssystem läuft die veraltete Android-Version 5.1.1, die auf einem Smartphone dieser Preisklasse nichts mehr zu suchen hat. Immerhin hat Gigaset die mit Android 6 eingeführte Verwaltung der App-Rechte selbst nachgerüstet. Ansonsten hat der Hersteller hauptsächlich am Design der Bedienoberfläche herumgebastelt und das praktische App-Menü entfernt. Alle App-Verknüpfungen landen auf den Startseiten.

Der verwendete SoC Snapdragon 810 gehört zur vorhergehenden Prozessorgeneration. Bei Dauerbelastung kämpft er mit Wärme-problemen und reduziert schon nach Sekunden seinen Takt. Im Alltag bekommt man die negativen Auswirkungen aber nicht zu spüren.

- ⬆ Dual-SIM
- ⬆ edles Glasgehäuse
- ⬇ veraltete Android-Version



## HTC 10

HTC-typisch präsentiert sich das „10“ im robust wirkenden Metallgehäuse, das nach Schutzart IP53 gegen Staub und immerhin gegen „Sprühwasser“ geschützt ist. Regen verträgt es, untertauchen sollte man es nicht. Wegen der bauchigen Form liegt das vergleichsweise schwere 10 sicher in der Hand, wirkt aber plumper als beispielsweise das schlanke Huawei P9. Unterhalb des Displays sitzt eine berührungsempfindliche Sensorfläche, die einerseits als Home-Button und andererseits als flotter, zuverlässiger Fingerabdrucksensor dient.

Das Display ist scharf und kontraststark, aber nicht besonders hell. Blickt man von schräg oben darauf, zeigt sich ein leichter Rotstich, der aber normalerweise nicht auffällt. Die Kamera produziert Fotos mit hohem Kontrast und realitätsnahen Farben. In nur 0,6 Sekunden ist sie einsatzbereit. Zu den Bildrändern nimmt die Schärfe deutlich ab und Software-Filter rechnen Strukturen zusätzlich kaputt. Zwar fängt der Bildsensor dank 1,55 Mikrometer großer Pixel viel Licht ein und lichtet auch bei unter 5 Lux Objekte klar erkennbar ab, verschluckt bei mäßiger Beleuchtung aber Details.

Bei der Gestaltung der Software hat sich HTC stärker an Googles Vorstellungen orientiert als in der Vergangenheit, aber dennoch überflüssige Apps integriert. Die Hersteller-eigenen Programme erfüllen die gleichen Aufgaben wie die ebenfalls installierten Google-Apps.

- ⬆ hochwertiges Gehäuse
- ⬆ gute Fotos
- ⬇ mäßig helles Display



## Huawei P9

Wie beim LG G5 sitzen auf der Rückseite des Huawei P9 zwei Hauptkameras, doch im P9 haben beide die gleiche Auflösung und Brennweite (12 Megapixel, 27 Millimeter) und arbeiten im Team. Der Unterschied ist, dass nur eine in Farbe aufnimmt; die andere schießt gleichzeitig Schwarz-Weiß-Fotos und soll so den Fokus beschleunigen und kann auf Wunsch nachträglich den Fokus versetzen. Schnell arbeitet der Fokus, doch nicht ganz so schnell wie beispielsweise beim Galaxy S7. Die Monochrom-Bilder bekommt der Nutzer nur zu Gesicht, wenn man die Kamera-App in den entsprechenden Modus schaltet. Auf Farbfotos überstrahlen helle Stellen und könnten farbkraftiger ausfallen, übertreffen aber dennoch die Bilder der meisten anderen Smartphones.

Für fast alle Anwendungen stellt der Huawei-eigene Octa-Core-Prozessor Kirin 955 mehr als genug Leistung zur Verfügung. Flaschenhals der Hardware ist der ARM-Grafikchip, der mit nur vier Shader-Einheiten in Grafik-Benchmarks hinterherhinkt.

Das Unibody-Gehäuse aus Metall steht auf einer Qualitätsstufe mit der Glashülle des Galaxy S7. Obwohl es nur 7 mm in der Tiefe misst, fasst der Akku 3000 mAh. Der Strom reicht meist nicht ganz für zwei Tage Nutzung. Da der Fingerabdrucksensor sehr weit oben im Rückendeckel sitzt, muss man häufig umgreifen, um ihn zu erreichen. Er ist nicht ganz so flink wie bei anderen Telefonen.

- ⬆ hochwertiges Gehäuse
- ⬆ helles, farbkraftiges Display
- ⬇ im Vergleich kurze Laufzeiten





## LG G5

Die Stärken des LG G5 sind der austauschbare Akku, das beste Smartphone-LCD und zwei Hauptkameras mit verschiedenen Brennweiten. Mit einem Kontrast von 2341:1 und vollem sRGB-Farbraum macht das Display sogar den bislang unerreichten OLED-Bildschirmen im Test Konkurrenz.

Das Gehäuse ist aus einem Stück Aluminium gefertigt. Da es aber von einem plastikartigen Material überzogen ist, kommt das Metall nur an den Kanten zum Vorschein. Die matte Oberfläche und die abgerundeten Kanten machen das Gehäuse griffig. Weniger ergonomisch ist der im Power Button integrierte Fingerabdrucksensor, den man meist nur mit der Fingerflanke trifft, weshalb er nicht immer reagiert.

Android 7 zeigt sich reaktionsschnell und flüssig – dem schnellen Qualcomm-Prozessor Snapdragon 820 und 4 GByte RAM sei Dank. Bei der Kamera umgeht LG das Problem der Festbrennweite mit gleich zwei Hauptkameras mit unterschiedlicher Brennweite und Auflösung: Eine nimmt 16-Megapixel mit Smartphone-üblichen 78 Grad auf, die Sekundär-Knipse fotografiert 8 Megapixel und 135 Grad. Erstere rangelt mit dem S7 um die Kamerakrone. Einzige Schwächen sind leichter Rotstich und Rauschen im Dunkeln (unter 5 Lux). Die Superweitwinkel-Fotos mit 8 Megapixel zeigen Verzerrungen und weniger Details an den Bildkanten. Auch diese Aufnahmen fallen mehr als brauchbar aus.

- ⬆ bestes LCD
- ⬆ wechselbarer Akku
- ⬇ Metallgehäuse mit Plastikhülle



## Motorola Moto X Force

Motorola übernimmt Android 6 für das Moto X Force von Google, ohne große Änderungen vorzunehmen oder eigene Software aufzuspielen. Ein aufgeräumtes System und schnelle Updates sind das Resultat.

Äußerlich kommt das Motorola Moto X Force weit weniger schick daher als die anderen Edel-Handys. Die geriffelte Kunststoffrückseite unseres Geräts war zwar griffig, konnte aber nicht mit dem Glas und Metall der Konkurrenten mithalten. Dafür ist das Display von einer bruchsfähigen Frontscheibe namens ShatterShield geschützt, die im Test alle Stürze überstand. Motorola gibt sogar eine vierjährige Garantie gegen Brüche. Gegen Kratzer ist der Bildschirm aber nicht besser geeignet als andere. Eine Nanobeschichtung schützt die elektronischen Bauteile im Inneren vor Spritzwasser und Staub – ohne Garantie.

Technisch überzeugt das 5,4 Zoll große Display: Dank OLED-Technik zeigt es zusammen mit dem Bildschirm des S7 die kräftigsten Farben und den höchsten Kontrast im Test, spiegelt aber stärker. CPU und GPU sind etwas angestaubt. Spürbaren Einfluss auf die Performance hat das nicht. Fotos rangieren mit einem leichten Rotstich im Testmittelfeld.

Wer das Moto X Force direkt auf Motorola-Webseite bestellt, kann Farben und Material der Rückseite selbst auswählen. Als einzigem Smartphone im Test fehlt dem Motorola Moto X Force der Fingerabdrucksensor.

- ⬆ bruchsfähiges Display
- ⬆ sauberes Android
- ⬇ plumpes Gehäuse



## Samsung Galaxy S7

Samsung hat beim Galaxy S7 fast alles richtig gemacht. Die Kontrast- und Farbwerte des AMOLED-Displays sind für die LCDs der Konkurrenten unerreicht. Gleichzeitig strahlt die Anzeige am hellsten und zeigt das beste Bild im Test. Der hauseigene Prozessor animiert Android so flink wie auf keinem anderen Gerät und hält seinen Maximaltakt in Benchmarks und Spielen länger als die Qualcomm-CPU. Der Fingerabdrucksensor im mechanischen Home-Button reagiert fast so schnell und fehlerfrei wie im iPhone 6s.

Im S7 steckt auch die beste Kamera: Mit realistischen Farben, hohem Kontrast und blitzschnellem Auslöser können einige Konkurrenten ebenfalls dienen. Wird es aber dunkel, lichtet das S7 mit Abstand am meisten ab – bei vergleichsweise wenig Rauschen. Dazu hat Samsung die Auflösung auf 12 Megapixel beschränkt und die Sensorpixel mit 1,4 Mikrometer besonders groß dimensioniert.

Die High-End-Technik ist in ein edles, handliches Gehäuse aus Metall und (widerstandsfähigem) Glas gekleidet. Gegen Staub und Wasser ist es nach IP68 geschützt, sodass man es auch unbeschadet untertauchen kann. Nur zwei kleine Mankos zeigen sich: Erstens ist der (lang durchhaltende) Akku fest eingebaut, zweitens hat das S7 Micro-USB statt die moderne Typ-C-Buchse. Alternativ lädt der Akku kabellos auf Qi- oder Powermat-Stationen.

- ⬆ bestes Display
- ⬆ beste Kamera
- ⬆ lange Laufzeiten


## High-End-Smartphones


Modell	Gigaset ME pro	HTC 10	Huawei P9	LG G5	
Ausstattung					
Betriebssystem	Android 5.1.1 / Gigaset UI	Android 7.0 / Sense 8	Android 6.0 / EMUI 4.1	Android 7.0 / UX 5.0	
Prozessor / Kerne	Qualcomm Snapdragon 810 / 4 × 1,8 GHz, + 4 × 1,5 GHz	Qualcomm Snapdragon 820 / 2 × 2,2 GHz + 2 × 1,6 GHz	HiSilicon Kirin 955 / 4 × 2,5 GHz + 4 × 1,8 GHz	Qualcomm Snapdragon 820 / 2 × 2,2 GHz + 2 × 1,6 GHz	
Grafik	Qualcomm Adreno 430	Qualcomm Adreno 530	ARM Mali-T880 MP4	Qualcomm Adreno 530	
Arbeitsspeicher / Flash-Speicher (frei)	3 GByte / 32 GByte (23,4 GByte)	4 GByte / 32 GByte (23,9 GByte)	3 GByte / 32 GByte (25 GByte)	4 GByte / 32 GByte (23,5 GByte)	
Wechselspeicher / maximal	MicroSDXC / 200 GByte	MicroSDXC / 200 GByte	MicroSDXC / 200 GByte	MicroSDXC / 200 GByte	
WLAN / Dual-Band / alle 5-GHz-Bänder	IEEE 802.11 a/b/g/n/ac / ✓ / ✓	IEEE 802.11 a/b/g/n/ac / ✓ / ✓	IEEE 802.11 a/b/g/n/ac / ✓ / ✓	IEEE 802.11 a/b/g/n/ac / ✓ / ✓	
Bluetooth / NFC / GPS	4.1 / ✓ / ✓	4.2 / ✓ / ✓	4.2 / ✓ / ✓	4.2 / ✓ / ✓	
Fingerabdrucksensor / für VR-Brillen geeigneter Gyrosensor	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	
Mobile Datenverbindung <sup>1</sup>	LTE (300 MBit/s Down, 50 MBit/s Up), HSPA (42,2 MBit/s Down, 5,76 MBit/s Up)	LTE (450 MBit/s Down, 50 MBit/s Up), HSPA (42,2 MBit/s Down, 5,76 MBit/s Up)	LTE (300 MBit/s Down, 50 MBit/s Up), HSPA (42,2 MBit/s Down, 5,76 MBit/s Up)	LTE (300 MBit/s Down, 50 MBit/s Up), HSPA (42,2 MBit/s Down, 5,76 MBit/s Up)	
Dual-SIM	✓	—	—	—	
Akku / austauschbar / drahtlos ladbar	4000 mAh / — / —	3000 mAh / — / —	3000 mAh / — / —	2800 mAh / ✓ / —	
USB-Anschluss	Typ-C	Typ-C	Typ-C	Typ-C	
Fingerabdrucksensor	✓	✓	✓	✓	
Abmessungen (H × B × T)	15,4 cm × 7,6 cm × 0,8 cm	14,6 cm × 7,2 cm × 1 cm	14,5 cm × 7,1 cm × 0,7 cm	14,9 cm × 7,4 cm × 0,9 cm	
Gewicht	200 g	162 g	144 g	157 g	
Schutzart	—	IP53	—	—	
Farbvarianten	schwarz	gold, grau, silber	grau, silber	gold, grau, silber	
Kamera-Tests					
Kamera-Auflösung Fotos / Video	21,4 MPixel (5344 × 4008) / 2K (2048 × 1080)	12 MPixel (4000 × 3000) / 4K (3840 × 2160)	11,8 MPixel (3968 × 2976) / Full-HD (1920 × 1080)	15,9 MPixel (5312 × 2998) / 4K (3840 × 2160)	
Auto- / Touchfokus / Fotoleuchte (Anzahl)	✓ / ✓ / ✓ (2)	✓ / ✓ / ✓ (2)	✓ / ✓ / ✓ (2)	✓ / ✓ / ✓ (1)	
Frontkamera-Auflösung Fotos / Video	6 MPixel (3264 × 1836) / Full-HD (1920 × 1080)	5 MPixel (2592 × 1944) / Full-HD (1920 × 1080)	8 MPixel (3264 × 2448) / Full-HD (1920 × 1080)	8MPixel (3264 × 2448) / Full-HD (1920 × 1080)	
Display-Messungen					
Technik / Diagonale (Größe)	LCD (IPS) / 5,5 Zoll (12,1 cm × 6,8 cm)	LCD (IPS) / 5,5 Zoll (12,1 cm × 6,8 cm)	LCD (IPS) / 5,2 Zoll (11,4 cm × 6,4 cm)	LCD (IPS Quantum) / 5,3 Zoll (11,7 cm × 6,6 cm)	
Auflösung / Seitenverhältnis	1920 × 1080 Pixel (402 dpi) / 16:9	2560 × 1440 Pixel (539 dpi) / 16:9	1920 × 1080 Pixel (426 dpi) / 16:9	2560 × 1440 Pixel (555 dpi) / 16:9	
Helligkeitsregelbereich / Ausleuchtung	5 ... 355 cd/m² / 90 %	7 ... 367 cd/m² / 89 %	8 ... 523 cd/m² / 88 %	3 ... 536 cd/m² / 82 %	
Kontrast / Farbraum	2095:1 / sRGB	1771:1 / sRGB	1400:1 / sRGB	2341:1 / sRGB	
Die runden Diagramme geben die Winkelabhängigkeit des Kontrasts wieder. Blaue Farbanteile stehen für niedrige, rötliche für hohe Kontraste. Kreise markieren die Blickwinkel in 20-Grad-Schritten. Im Idealfall ist das ganze Bild pink.					
winkelabhängiger Kontrast: Kreise im 20°-Abstand					
0	200	400	600		
Bewertung					
Bedienung / Performance	⊕ / ⊕	⊕ / ⊕⊕	⊕ / ⊕	⊕ / ⊕⊕	
Ausstattung Software / Hardware	⊕ / ⊕	⊕ / ⊕⊕	⊕ / ⊕	⊕ / ⊕⊕	
Display	⊕⊕	⊕⊕	⊕⊕	⊕⊕	
Laufzeit	⊕	⊕	○	⊕	
Kamera Fotos / Videos	⊕ / ○	⊕ / ⊕⊕	○ / ○	⊕⊕ / ⊕⊕	
Preis	250 €	550 €	450 €	520 €	
<sup>1</sup> Herstellerangabe					
⊕⊕ sehr gut   ⊕ gut   ○ zufriedenstellend   ⊖ schlecht   ⊖⊖ sehr schlecht   ✓ vorhanden   — nicht vorhanden   k. A. keine Angabe					

## Benchmarks

Modell	Coremark (Singlethread) besser ►	Coremark (Multithread) besser ►	GFXBench 3.0 Manhattan [fps] besser ►	GFXBench 3.0 Manhattan Offscreen [fps] besser ►
Gigaset ME pro	6566	31138	25	24
HTC 10	11176	31277	29	48
Huawei P9	10403	54378	19	18
LG G5	11204	31512	30	44
Motorola Moto X Force	7267	35173	17	26
Samsung Galaxy S7	10857	44713	26	42

# Smarte Gadgets

Motorola Moto X Force	Samsung Galaxy S7
Android 6.0.1	Android 6.0.1 / TouchWiz
Qualcomm Snapdragon 810 / 4 × 2 GHz + 4 × 1,5 GHz	Samsung Exynos 8 Octa / 4 × 1,6 GHz + 4 × 2,3 GHz
Qualcomm Adreno 430	ARM Mali-T880 MP12
3 GByte / 32 GByte (24 GByte)	4 GByte / 32 GByte (24,8 GByte)
MicroSDXC / 200 GByte	MicroSDXC / 200 GByte
IEEE 802.11 a/b/g/n/ac / ✓ / ✓	IEEE 802.11 a/b/g/n/ac / ✓ / ✓
4.1 / ✓ / ✓	4.2 / ✓ / ✓
— / ✓	✓ / ✓
LTE (300 MBit/s Down, 50 MBit/s Up), HSPA (42,2 MBit/s Down, 5,76 MBit/s Up)	LTE (450 MBit/s Down, 50 MBit/s Up), HSPA (42,2 MBit/s Down, 5,76 MBit/s Up)
✓	—
3760 mAh / — / ✓	3000 mAh / — / ✓
Micro-USB	Micro-USB
—	✓
15 cm × 7,8 cm × 1 cm	14,2 cm × 7 cm × 0,8 cm
167 g	150 g
interne Beschichtung	IP68
selbst gestaltbar	gold, schwarz, weiß
21,4 MPixel (5344 × 4008) / 4K (3840 × 2160)	12,2 MPixel (4032 × 3024) / 4K (3840 × 2160)
✓ / ✓ / ✓ (2)	✓ / ✓ / ✓ (1)
5 MPixel (2592 × 1944) / Full-HD (1920 × 1080)	5 MPixel (2592 × 1944) / 2560 × 1440
OLED (AMOLED) / 5,4 Zoll (12 cm × 6,8 cm)	OLED (AMOLED) / 5,1 Zoll (11,2 cm × 6,3 cm)
2560 × 1440 Pixel (541 dpi) / 16:9	2560 × 1440 Pixel (581 dpi) / 16:9
5 ... 504 cd/m² / 92 %	2 ... 566 cd/m² / 96 %
>20.000:1 / AdobeRGB	>20.000:1 / AdobeRGB
	
⊕ / ⊕	⊕ / ⊕⊕
⊕⊕ / ⊕	⊕ / ⊕⊕
⊕⊕	⊕⊕
⊕⊕	⊕⊕
⊕ / ⊕⊕	⊕⊕ / ⊕⊕
380 €	490 €

3DMark Ice Storm Unlimited
besser ►

24580
28078
20048
28913
26555
29401



HIER  
BESTELLEN!

 **heise shop**

[shop.heise.de/hardware](http://shop.heise.de/hardware) ►





Stefan Porteck

## Die Google-Smartphones Pixel und Pixel XL im Test

**An Selbstbewusstsein scheint es Google nicht zu mangeln: Beide Pixel-Smartphones tragen Premium-Preisschilder. Wir haben getestet, ob sie einen Mehrwert gegenüber den günstigeren Konkurrenten bieten.**

**M**it Preisen von 750 bis 870 Euro für das Pixel mit 5-Zoll-Diagonale und 900 bis 1010 Euro für das 5,5"-Modell Pixel XL gehören Googles neue Geräte zu den teuersten Android-Smartphones. Während Google in der Nexus-Ära überwiegend gute Hardware für schmale Geldbeutel anbot, liegen die Pixel in Apple-Preisregionen.

Auch an anderer Stelle eifert Google den iPhones nach: Beim Design der Pixel-Phones hat man sich offenbar großzügig von Apple „inspirieren“ lassen. So sieht insbesondere die Vorderseite der silbernen Modelle dem iPhone so ähnlich, dass viele Kollegen auf den ersten Blick nicht merken, dass sie ein Android-Gerät in den Händen hielten. Auch die Rückseite sieht nach iPhone aus. Einziger Unterschied: Das obere Viertel um den Fingerabdrucksensor verziert Google mit poliertem Glas.

Unabhängig davon wirkt das gebürstete Alu-Gehäuse mit seinen abgerundeten Kanten sehr edel. Die Smartphones geben in der Hosentasche nicht nach und klappern oder knarzen auch nicht. Die drei Alu-Buttons sitzen fest und haben einen klar definierten Druckpunkt. Die Kameralinse sitzt ohne hässlichen Buckel bündig in der Rückseite.

Beide Pixel zählen zu den ersten Smartphones, die vom neuen Qualcomm Snapdragon 821 (MSM8996pro) angetrieben werden. Dessen Vier-Kern-Prozessor läuft mit einem maximalen Takt von 2,15 GHz. In unseren Benchmarks lagen die Pixel auf vergleichbarem Niveau wie die direkten Konkurrenten Apple iPhone 7, Samsung Galaxy S7 und OnePlus 3. Bei Praxistests sorgte das für ruckelfreies Spielen und geschmeidige VR-Erlebnisse. Hierbei gefiel auch die ausgewogen klingende Audiowiedergabe.

Zusammen mit den 4 GByte Arbeitsspeicher liefern die Pixel-Phones ohne nerviges Stocken der Android-Oberfläche. Wer allerdings viele Fotos, Songs und Filme speichert, kommt schnell ans Limit des Gerätespeichers, der in der kleinen Ausstattungsvariante mit 32 GByte eher knapp bemessen ist. Für das Aufstocken auf 128 GByte verlangt Google einen Aufpreis von jeweils 110 Euro. Die Möglichkeit, den Speicher mit SD-Karten zu erweitern, fehlt. Immerhin darf man unbegrenzt viele Fotos und Videos in voller Qualität bei Google Fotos in die Cloud laden.

Der Akku im kleinen Pixel fasst 2770 mAh, der im Pixel XL 3450 mAh. Dank Schnellladetechnik über den USB-Typ-C-Stecker halten die Geräte nach 15 Minuten am Stromnetz bis zu 7 Stunden lang durch. Vom Drahtlos-Laden hat Google sich wieder verabschiedet. Die Akku-Kapazität sorgte bei der Videowiedergabe in unserem Testlabor für eine Laufzeit von elf (Pixel XL) und elfeinhalb Stunden (Pixel). Damit liegen sie im oberen Mittelfeld. Zum Vergleich: Das Nexus 6P schafft 10,3 Stunden, das Galaxy S7 14,8 Stunden und der Akku des Note 7 reichte für 15,1 Stunden.

### Farbkünstler

Die rückseitige Smartphone-Kamera soll laut Google die beste aller Zeiten sein. Die vordere Linse knipst mit 8 Megapixeln, die hinten mit Dual-Blitz und mit 12,3 Megapixeln. Der Sony-Sensor mit 1,55 µm großen Pixeln soll viel Licht durchlassen und eine besonders kurze Auslösezeit bieten.

Unsere Tests und Messungen bescheinigen der Pixel-Kamera tatsächlich sehr gute Ergebnisse: Die Schärfe ist minimal besser als beim bisherigen Primus, dem Samsung Galaxy S7. Kräftige Farben erscheinen bei beiden Modellen genauso satt wie beim S7 und beim iPhone 7. Im direkten Vergleich erkennt man, dass die Fotos aber insgesamt einen Hauch bläulicher und weniger knackig anmuten als bei Samsung. Bei schwachem Umgebungslicht schleicht sich ein leichtes Bildrauschen ein, wie es bei Apple und Samsung aber auch auftritt.

Die AMOLED-Displays der Pixel-Telefone spielen hingegen nicht in der ersten Liga. Das kleine Modell löst mit 1920 x 1080 Bildpunkten auf, was zwar im Alltag völlig ausreicht, doch bei VR-Anwendungen aufgrund der verwendeten PenTile-Matrix die Pixel-Struktur störend sichtbar macht. Das größere Pixel XL hat 2560 x 1440 Bildpunkte und macht somit auch in VR-Brillen eine gute Figur.

Die Rückseite des Pixel XL aus gebürstetem Alu kommt ohne Buckel für die Kameralinse aus.



allen Android-Geräten verfügbar sein soll. Falls nicht, ist das – zumindest bei aktuellem Stand – kein herber Verlust: Wir konnten dem Assistant keine sinnvolle Information oder Funktion entlocken, die Google Now unter Android 7 nicht auch beherrscht. Angedungte Features wie das Bestellen von Kinokarten oder Tischreservierungen funktionieren in Deutschland derzeit noch nicht.

## Fazit

Technisch zählen die Pixel-Phones unbestritten zur Oberklasse. Sie sehen ziemlich edel aus, ihre Hardware ist sehr gut, der neue Launcher wirkt frischer und hat mit dem Assistant einiges Potenzial. Obendrein gibt es bei den Pixel-Telefonen unlimitierte Foto- und Video-Backups in der Cloud und stets die neuste Android-Version mit regelmäßigen und zeitnah veröffentlichten Sicherheits-Updates.

Diese Kombination löst einen starken Haben-wollen-Reiz aus. Doch neu sind auch die gesalzene Preise. Schaut man zur Konkurrenz, bekommt man technisch ebenbürtige Alternativen für locker 200 Euro weniger und kann dort eventuell sogar den Speicher erweitern. Sollten aber wie bei den ehemaligen Nexus-Geräten die Preise doch noch irgendwann merklich fallen, könnten die Pixel-Phones den Mitbewerbern einige Kopfschmerzen bereiten. (spo) **ct**

OLED-typisch haben beide Displays ein supersattes Schwarz und somit einen enormen Kontrast. Die maximale Helligkeit beider Displays liegt bei 430 cd/m<sup>2</sup> und ermöglicht damit auch bei Sonnenschein eine gute Lesbarkeit. Zudem zeichnen sich die Displays durch einen sehr großen Farbraum aus. Wegen der Winkelabhängigkeit sehen bei gekipptem Gerät helle Flächen auf dem Pixel leicht grünlich und beim Pixel XL leicht lilastichig aus. Die Blickwinkelcharakteristik kann nicht mit der des iPhone 7 mithalten und liegt etwa auf dem Niveau anderer OLEDs wie beim Galaxy S7 oder OnePlus 3.

Geräte. Bei unseren Testkandidaten ließ sich der Bootloader entsperren, um etwa alternative ROMs zu installieren.

Interessantes Potenzial hat der neu eingebaute Google Assistant, der besser kontextbezogene Infos liefern soll und Google Now ergänzt. Wie bereits in der Chat-App Allo vorgeführt, versteht er natürliche Sprache und greift auf bereits gesammelte Informationen zurück. Bislang schweigt sich Google noch darüber aus, ob er künftig auf

## Zu Diensten

Google liefert seine Pixel-Phones bereits mit Android 7.1 aus. Die bedeutendste Neuerung ist der bislang nur hier verfügbare Pixel-Launcher. Zu seinen Features gehören ein unter dem Homescreen liegender App-Drawer, andere Ordner-Icons und eine weniger aufdringliche Suchleiste.

Funktionale Verbesserungen sind die sogenannten App-Shortcuts: Lässt man den Finger auf einem App-Icon liegen, öffnet sich nicht die App, sondern ein Menü mit einigen ihrer Funktionen. So zeigt beispielsweise die Telefonie-App die zuletzt gewählten Kontakte an. Viele Nutzer dürfte es freuen, dass der Nachtmodus mit wärmeren Display-Farben nun fest zum Repertoire gehört.

Zumindest die Smartphones, die nicht über Provider, sondern im Google Store angeboten werden, scheinen genauso offen zu sein wie die ehemaligen Nexus-

## Google-Smartphone

Modelle	Pixel (XL)
Betriebssystem	Android 7.1
Varianten	Anthrazit, Silber
<b>Display-Messungen</b>	
Technik / Größe (Diagonale)	OLED / 5 Zoll (12,7 cm) (OLED / 5,5 Zoll (14 cm))
Auflösung / Seitenverhältnis	1920 × 1080 Pixel (441 dpi) / 16:9 (2560 × 1440 Pixel (534 dpi) / 16:9)
Helligkeitsregelbereich	6 ... 430 cd/m <sup>2</sup> (7 ... 430 cd/m <sup>2</sup> )
<b>Ausstattung</b>	
Prozessor / Kerne, Takt	Qualcomm Snapdragon 821 / 2 × 2,15 GHz, 2 × 1,6 GHz
Grafik	Adreno 530
RAM / Flash-Speicher (frei) / Wechselspeicher	4 GByte / 32 GByte (128 GByte) / –
WLAN / Dual-Band / alle 5-GHz-Bänder	IEEE 802.11 802.11 a/b/g/n/ac / ✓ / ✓
Bluetooth / NFC / GPS	4.2 / ✓ / ✓
Lichtsensoren / für VR-Brillen geeigneter Gyrosensor	✓ / ✓
mobile Datenverbindung	LTE Cat 11 (600 MBit/s Down, 75 MBit/s Up)
Akku / austauschbar / drahtlos ladbar	2770 mAh (3450 mAh) – / –
Abmessungen (H × B × T)	14,4 cm × 7,0 cm × 7,5 mm – 8,5 mm (15,5 cm × 7,6 cm × 7,5 mm – 8,5 mm)
Gewicht	143 g (167 g)
<b>Test: Kamera</b>	
Kamera-Auflösung Fotos / Video	4048 × 3036 (12,3 MPixel) / 3840 × 2160 (4K)
Sensor-Pixel-Größe / Blende	1,55 µm / f/2.0
optischer Bildstabilisator / Fotoleuchte (Anzahl)	– / ✓ (1)
Frontkamera-Auflösung Fotos / Video	3264 × 2448 (8 MPixel) / 1920 × 1080
Sensor-Pixel-Größe / Blende	1,4 µm / f/2.4
Preis	760 € (32 GB), 870 € (128 GB) (900 € (32 GB), 1010 € (128 GB))
✓ vorhanden – nicht vorhanden	



Hannes A. Czerulla

# Sony Xperia X im Test

Beim Android-Smartphone Xperia X baut Sony eine hochwertige Hauptkamera und eine 13-Megapixel-Frontknipse ein. An anderen Stellen wird das Gerät seinem High-End-Anspruch aber nicht gerecht.

**S**ony-Kameras findet man nicht nur in den herstellereigenen Smartphones, aber die besten Modelle spart sich Sony für die hauseigenen Telefone auf. So auch beim Xperia X: Als Hauptkamera hat der Hersteller eine 23-Megapixel-Knipse eingebaut. Vorne sitzt eine der schärfsten Selfie-Kameras mit 13 Megapixel.

Im Labor lichtet die Rückkamera ungewöhnlich viele Details ab. Farben wirken realistisch – abgesehen von einer leichten Grün-Tendenz. Im Freien zeigen sich auf den ersten Blick die gleichen Stärken wie drinnen. Doch zu den Ecken und seitlichen Rändern hin nimmt die Schärfe massiv ab. Bereits bei Dämmerung tritt deutliches Bildrauschen auf. Wahrscheinlich ist die Kamera deshalb standardmäßig auf 8 Megapixel eingestellt und nicht auf das Maximum.

Das 5-Zoll-LCD zeigt fast so kräftige Farben wie OLED-Bildschirme und kann den AdobeRGB-Farbraum größtenteils darstellen. Zwar beträgt der Kontrast nur 1302:1 und Schwarz wird nicht vollkommen dunkel dargestellt, im Alltag fällt das aber nicht auf.

Die Gehäuserückseite besteht aus mattem Metall, was man aber weder sieht noch fühlt. Eher ähnelt die Haptik einer Mischung aus hochwertigem Plastik und Alu. Schick und elegant wirkt das Gerät dennoch. Das Gehäuse ist nicht gegen Wasser oder Staub geschützt; der Akku lässt sich nicht entnehmen.

Der Fingerabdrucksensor sitzt im Gehäuserahmen und ist in den Einschaltknopf integriert. Der Sensor reagiert so schnell, dass man meist nicht mitbekommt, dass man ihn benutzt hat. Die Knöpfe für Lautstärke und Kamera hat der Hersteller ungeschickt platziert, da sie auf

Höhe der Innenhandfläche liegen und man umgreifen muss, um sie zu erreichen.

Zum Laden hat das Xperia X einen Micro-USB-Anschluss und noch keine Typ-C-Buchse. Dennoch ist der 2620-mAh-Akku nach rund einer dreiviertel Stunde zur Hälfte geladen. Mit weniger als neun Stunden Videolaufzeit und zwölf Stunden Websurfen fallen die Laufzeiten durchschnittlich aus.

Beim Telefonieren in leiser Umgebung gefällt die Sprachqualität auf beiden Teilnehmerseiten. Kommen jedoch Hintergrundgeräusche hinzu, macht sich die

Geräuschunterdrückung mit einem dauerhaften Zischeln beim Gesprächspartner bemerkbar.

Der Mittelklasse-Prozessor Snapdragon 650 ist eines 400-Euro-Smartphones nicht würdig. Auch erwartet man in dieser Preisklasse mindestens 4 GByte Arbeitsspeicher.

Da das Xperia Z5 mit schnellerem Prozessor, wasserdichtem Gehäuse und sonst gleicher Ausstattung 430 Euro kostet, gibt es bis auf die hochauflösende Frontkamera keinen Grund, zum teureren Xperia X zu greifen. (hcz) **ct**

## Sony Xperia X

### Ausstattung

Betriebssystem	Android 7.0
Prozessor / Kerne	Qualcomm Snapdragon 650 / 2 × 1,8 GHz, 4 × 1,4 GHz
Grafik	Qualcomm Adreno 510
Arbeitsspeicher / Flash-Speicher (frei)	3 GByte / 32 GByte (20,2 GByte)
Wechselspeicher / maximal	MicroSDXC / 200 GByte
WLAN / Dual-Band / alle 5-GHz-Bänder	IEEE 802.11 a/b/g/n/ac / ✓ / ✓
Bluetooth / NFC / GPS	4.2 / ✓ / ✓
Mobile Datenverbindung <sup>1</sup>	LTE (300 MBit/s Down, 50 MBit/s Up), HSPA (42,2 MBit/s Down, 5,76 MBit/s Up)
Akku / austauschbar / drahtlos ladbar	2620 mAh (0 Wh) / — / —
USB-Anschluss	Micro-USB 2.0
Fingerabdrucksensor	✓
Abmessungen (H × B × T)	14,3 cm × 6,9 cm × 0,8 cm
Gewicht	153 g

### Kamera-Tests

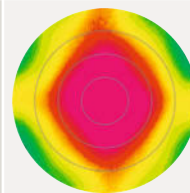
Kamera-Auflösung Fotos / Video	22,9 MPixel (5520 × 4140) / Full-HD (1920 × 1080)
Auto- / Touchfokus / Fotoleuchte (Anzahl)	✓ / ✓ / ✓ (1)
Frontkamera-Auflösung Fotos / Video	13 MPixel (4160 × 3120) / Full-HD (1920 × 1080)

### Display-Messungen

Technik / Diagonale (Größe)	LCD (IPS) / 11 cm × 6,2 cm (5 Zoll)
Auflösung / Seitenverhältnis	1920 × 1080 Pixel (443 dpi) / 16:9
Helligkeitsregelbereich / Ausleuchtung	5 ... 514 cd/m² / 95 %
Kontrast / Farbraum	1302:1 / fast AdobeRGB

Display Blickwinkelabhängigkeit: Die runden Diagramme geben die Winkelabhängigkeit des Kontrasts wieder. Blaue Farbanteile stehen für niedrige, rötliche für hohe Kontraste. Kreise markieren die Blickwinkel in 20-Grad-Schritten. Im Idealfall ist das ganze Bild pink.

Winkelabhängiger Kontrast:  
Kreise im 20°-Abstand  
0 200 400 600



Preis	360 €
-------	-------

<sup>1</sup> Herstellerangabe



# GNADENLOS DURCHLEUCHTET

RADIKAL DIGITAL: DAS PAPIERLOSE c't-ABO

**3x c't  
DIGITAL**

NUR 9,30 €\*

## ERLEBEN SIE c't IN DIGITALER QUALITÄT:

- **BEQUEM** alle 14 Tage freitags in der c't-App\*\*
- **LESEN** im On- und Offline-Modus
- **UMFASSEND** suchen in allen verfügbaren Ausgaben
- **ZUSÄTZLICH** als PDF auf dem Desktop lesen



## UNSER GESCHENK AN SIE:

Mit dem praktischen Wäschefalter bekommen Sie Ihr Wäschechaos im Handumdrehen in den Griff. Achtung! Das leidliche Thema könnte zur Lieblingsbeschäftigung werden!

Solange Vorrat reicht!

**JETZT BESTELLEN:**  
[ct.de/digital](http://ct.de/digital)

\*Preis in Dt. inkl. MwSt. Auslandspreise können abweichen.  
\*\*Verfügbar für Android (Tablet, Smartphone, Kindle Fire)  
und iOS (iPad, iPhone)



Hannes A. Czerulla

## Motorola Moto G4 und Moto G4 Plus mit zwei SIM-Slots

**Motorolas Moto-G-Serie steht für ein vorzügliches Preis/Leistungs-Verhältnis. Im Vergleich zu den Vorgängern sind die aktuellen Vertreter Moto G4 und Moto G4 Plus zwar etwas teurer geworden, bieten aber für viele Nutzer ideale Ausstattung und zeigen im Test nur punktuelle Schwächen.**

Das Motorola Moto G4 und Moto G4 Plus gleichen sich äußerlich wie ein Android-Smartphone dem anderen. Die Display-Diagonale beträgt bei beiden 5,5 Zoll und die Plastikgehäuse sind bis auf ein Detail identisch: Nur das G4 Plus besitzt unterhalb des Displays einen Fingerabdrucksensor. Der Sensor fällt vergleichsweise klein aus und wirkt wie ein üblicher mechanischer Home-Button. Er ist blind zu ertasten, da sein Rahmen leicht aus dem Gehäuse hervorsteht. Berührt man ihn, schaltet er das Display an und entsperrt es. Der Sensor funktioniert zuverlässig und sogar einen Hauch schneller als der flinke Sensor des iPhone 7. Als Home-Button lässt er sich absurderweise aber nicht nutzen – die drei Android-Tasten stellt das System als virtuelle Schaltflächen auf dem Bildschirm dar.

Bei beiden Geräten handelt es sich um Dual-SIM-Smartphones. Es lassen sich also zwei SIM-Karten gleichzeitig nutzen, etwa um Geschäfts- und Privat-Handy zusammenzufassen oder zwei Tarife clever zu kombinieren. Beide Slots haben das aus der Mode gekommene Micro-SIM-Format.

Wer Nano-SIM-Karten besitzt, findet in den Halterungen entsprechende Adapter. Für MicroSD-Speicherkarten gibt es einen dritten Slot, sodass man den Speicher ergänzen und gleichzeitig zwei SIM-Karten betreiben kann. Ungewöhnlicherweise können beide SIM-Karten das UMTS-Netz nutzen – normalerweise muss sich eine Karte nur mit GSM zufriedengeben. Daten sendet und empfängt dennoch immer nur eine Karte, die dann als einzige auch via LTE funken kann. Welche das sein soll, legt man im außergewöhnlich umfangreichen Dual-SIM-Menü fest.

Auf Wunsch hilft ein Schritt-für-Schritt-Assistent beim Einrichten der SIM-Karten. Dazu stehen vier Nutzungsprofile zur Auswahl: In der Basis-Einstellung wählt man dauerhaft, welche Karte für Anrufe, welche für SMS und welche für Daten zuständig ist. Im Automatikmodus lernt das Smartphone durch Nachfragen, welchen Kontakt man mit welcher SIM-Karte anruft. Außerdem kann man eine Haupt- und eine Nebenkarte bestimmen, die dann nur noch manuell für ausgehende Anrufe und SMS eingesetzt wird.

Die vierte Möglichkeit ist, SIM-Karten und Google-Konten als privat oder geschäftlich zu markieren. Kontakte aus einem geschäftlichen Google-Adressbuch rufen die Geräte dann nur noch über die entsprechende SIM-Karte an. Alternativ lassen sich Kontakte einzeln der jeweiligen Kategorie zuordnen.

Die Telefonakustik enttäuscht: Die Stimme des Gesprächspartners tönt unangenehm blechern, fast schrammelnd aus dem Hörer, und der Lautsprecher übersteuert regelmäßig. Die Geräuschunterdrückung lässt entweder Hintergrundgeräusche durch oder hackt die Stimme ab. Für Vieltelefonierer disqualifizieren sich die Geräte dadurch.

### Ungleiche Zwillinge

Wie bei Motorola-Smartphones üblich läuft auf den G4-Modellen Android so gut wie ohne zusätzliche Software des Herstellers. Man findet im System nur eine Hilfsdatei und eine App, um Schnellstart-Gesten festzulegen. Auch das Design und die Menüs bleiben unangetastet, sodass Android übersichtlich und modern aussieht.

Erfahrungsgemäß liefert Motorola schnell und lang Updates.

Die Bildschirme haben ähnliche Merkmale: LCD IPS, 5,5 Zoll, Full-HD-Auflösung. Letztere reicht absolut für eine Darstellung ohne sichtbare Bildpixel. Farben sind kräftig, der Farbraum ist nicht übermäßig groß. Während die Vorgänger-Modelle vergleichsweise kompakt sind, fallen die G4-Modelle relativ groß aus.

Im Display-Labor zeigen die beiden Modelle Unterschiede: Während der Kontrast des Moto G4 Plus bei überdurchschnittlichen 1912:1 liegt, erreicht das Moto G4 nur 1596:1 – das fällt nur auf, wenn man die Geräte nebeneinander hält. Auch die maximale Helligkeit unterscheidet sich um rund 100 cd/m<sup>2</sup>, wobei beide Bildschirme mit über 400 cd/m<sup>2</sup> hell genug sind für den Einsatz bei Sonnenschein. Unterm Strich zeigen beide Displays eine durchschnittliche Qualität.

## Durchschnitts-Hardware

Eher unterdurchschnittlich fällt die Fotoqualität aus: Außenaufnahmen fehlt es an Kontrast, schattige Bereiche sind komplett schwarz, helle Bereiche überstrahlen. Innen aufgenommene Bilder gefallen schon besser und bis auf leichtes Bildrauschen und einen Rotstich beim G4 gibt es wenig auszusetzen. Die höhere Auflösung der Hauptkamera im G4 Plus sorgt für sichtbar mehr Detailtiefe. Videos nehmen die Knipsen nur in Full-HD-Auflösung auf und stabilisieren sie einigermaßen zuverlässig digital.

Die Laufzeiten sind vergleichsweise lang, nämlich über 11 Stunden Videoschauen und fast 16 Stunden Websurfen. Zwar kann man den Gehäusedeckel werkzeuglos öffnen, doch der Akku dahinter ist fest eingebaut. NFC hat der Hersteller keinem der Smartphones spendiert und über LTE fließen die Daten mit maximal 150 MBit/s.

Beim Prozessor handelt es sich in beiden Modellen um den Mittelklasse-Chip Qualcomm Snapdragon 617 mit acht Kernen. Alle Cores basieren auf der sparsamen Cortex-A53-Architektur, sind aber unterschiedlich hoch getaktet. Dass die CPU nicht zu den schnellsten gehört, merkt man an den zögerlich startenden Apps und zähen Animationen. Wer noch kein aktuelles Smartphone der Spitzenklasse in der Hand hatte, wird sich aber an der Geschwindigkeit nicht stören.

Das G4 Plus gibt es auch in einer 64-GB-Version, dessen Arbeitsspeicher 4 GByte groß ist; alle anderen Varianten greifen auf 2 GByte RAM zurück. Die besser ausgestatteten Modelle erhält man bislang nur

über den Motorola-Webshop, wo man außerdem zwischen acht verschiedenen Gehäusefarben wählen kann. Andere Händler bieten nur Schwarz und Weiß an.

## Fazit

Das Motorola Moto G4 und das Moto G4 Plus mit sauberem Android bieten sich als günstige Alternativen zum Google Pixel an. Ein Schnäppchen wie einige Vorgänger sind sie aber nicht mehr. Dennoch gehören sie zu den empfehlenswertesten ak-

tuellen Geräten um 300 Euro. Die mäßigen Kameras und die miese Sprachqualität machen sich negativ bemerkbar – gerade bei Dual-SIM-Smartphones hätte Motorola mehr Wert auf gute Telefoneigenschaften legen müssen.

Interessenten sollten die Geräte vor dem Kauf in die Hand nehmen, da 5,5 Zoll nicht jeder Hands Sache sind. 50 Euro Aufpreis fürs Plus-Modell lohnen sich: Fingerabdrucksensor, bessere Kamera und mehr Speicher sind das Geld allemal wert.

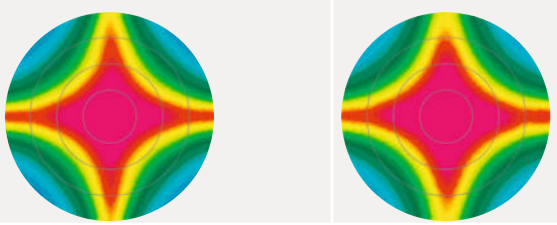
(hcz) **ct**

### Laufzeiten

Modell	Laufzeit Videowiedergabe (200 cd/m <sup>2</sup> ) [h] besser ►	Laufzeit Videowiedergabe (max. Helligkeit) [h] besser ►	Spiele (200 cd/m <sup>2</sup> ) <sup>1</sup> [h] besser ►	Laufzeit WLAN-Surfen (200 cd/m <sup>2</sup> ) [h] besser ►
Motorola Moto G4	11,6	7,5	3,9	16,1
Motorola Moto G4 Plus	11,1	8,6	3,9	15,8
<b>zum Vergleich</b>				
Google Nexus 5X	8,6	6,4	4	14
Motorola Moto X Play	13,4	9,5	4,1	19
Samsung Galaxy S7	14,8	9	7,8	15,2

<sup>1</sup> Spiel: Asphalt 8

### Android-Smartphones

Modell	Motorola Moto G4	Motorola Moto G4 Plus
<b>Ausstattung</b>		
Betriebssystem	Android 7.0	Android 7.0
Prozessor / Kerne	Qualcomm Snapdragon 617 / 4 × 1,5 GHz, 4 × 1,2 GHz	Qualcomm Snapdragon 617 / 4 × 1,5 GHz, 4 × 1,2 GHz
Grafik	Qualcomm Adreno 405	Qualcomm Adreno 405
Arbeitsspeicher / Flash-Speicher (frei)	2 GByte / 16 GByte (10,8 GByte)	2 GByte / 16 GByte (10,8 GByte)
Wechselspeicher / maximal	✓ / – / 200 GByte	✓ / – / 200 GByte
WLAN / Dual-Band / alle 5-GHz-Bänder	IEEE 802.11 a/b/g/n / ✓ / ✓	IEEE 802.11 a/b/g/n / ✓ / ✓
Bluetooth / NFC / GPS	4.2 / – / ✓	4.2 / – / ✓
Mobile Datenverbindung <sup>1</sup>	LTE (150 MBit/s Down, 50 MBit/s Up), HSPA (42,2 MBit/s Down, 5,76 MBit/s Up)	LTE (150 MBit/s Down, 50 MBit/s Up), HSPA (42,2 MBit/s Down, 5,76 MBit/s Up)
Akku / austauschbar / drahtlos ladbar	3000 mAh / – / –	3000 mAh / – / –
USB-Anschluss	Micro-USB 2.0	Micro-USB 2.0
Fingerabdrucksensor	–	✓
Abmessungen (H × B × T)	15,3 cm × 7,7 cm × 1 cm	15,3 cm × 7,7 cm × 1 cm
Gewicht	154 g	153 g
<b>Kamera-Tests</b>		
Kamera-Auflösung Fotos / Video	13 MPixel (4160 × 3120) / Full-HD (1920 × 1080)	15,9 MPixel (4608 × 3456) / Full-HD (1920 × 1080)
Auto- / Touchfokus / Fotoleuchte (Anzahl)	✓ / ✓ / ✓ (2)	✓ / ✓ / ✓ (2)
Frontkamera-Auflösung Fotos / Video	5 MPixel (2592 × 1944) / Full-HD (1920 × 1080)	5 MPixel (2592 × 1944) / Full-HD (1920 × 1080)
<b>Display-Messungen</b>		
Technik / Diagonale (Größe)	LCD (IPS) / 5,5 Zoll (12,1 cm × 6,8 cm)	LCD (IPS) / 5,5 Zoll (12,1 cm × 6,8 cm)
Auflösung / Seitenverhältnis	1920 × 1080 Pixel (402 dpi) / 16:9	1920 × 1080 Pixel (402 dpi) / 16:9
Helligkeitsregelbereich / Ausleuchtung	18 ... 502 cd/m <sup>2</sup> / 81 %	19 ... 426 cd/m <sup>2</sup> / 96 %
Kontrast / Farbraum	1596:1 / sRGB	1912:1 / sRGB
Display Blickwinkelabhängigkeit: Die runden Diagramme geben die Winkelabhängigkeit des Kontrasts wieder. Blaue Farbanteile stehen für niedrige, rötliche für hohe Kontraste. Kreise markieren die Blickwinkel in 20-Grad-Schritten. Im Idealfall ist das ganze Bild pink.		
winkelsabhängiger Kontrast: Kreise im 20°-Abstand		
		
Preis	200 € (16 GByte) / 234 € (32 GByte)	250 € (32 GByte) / 314 € (64 GByte)

<sup>1</sup> Herstellerangabe





Christian Wölbert

# Freie Smartphone-Werkstätten im Test

Klatsch – einmal nicht aufgepasst, schon fliegt das Handy auf die Straße und das Display ist hinüber. In solchen Fällen reparieren unabhängige Handy-Doktoren günstiger als die Hersteller. Allerdings arbeiten manche extrem langsam oder verlangen nachträglich mehr Geld. Auch die Qualität der Ersatzteile unterscheidet sich.

**D**ie Handy-Doktor-Branche ist für Kunden schwer durchschaubar: Jeder, der glaubt, einen Schraubendreher richtig herum zu halten, darf eine Werkstatt aufmachen und loslegen. Hinter einer schicken Webseite können sich ausgebildete System-Elektroniker mit ausgeklügelter Ersatzteil-Logistik und professioneller Buchhaltung verbergen – oder aber Hobby-Schrauber, die ihre Teile einzeln bei eBay bestellen.

Bei der Auswahl unserer Testkandidaten haben wir Amateure sowie lokale Anbieter, die sich auf Laufkundschaft konzentrieren, von vornherein aussortiert: Die Werkstätten sollten bundesweit arbeiten, eine möglichst breite Palette an Reparaturen anbieten und nicht erst seit gestern am Markt sein. Aufgrund dieser Kriterien haben wir uns für Handyreparatur 123, Letsfix, McRepair, und Tec-Repair entschieden. Die ersten drei sind Versand-Werkstätten, sie betreiben jeweils nur eine zentrale Werkstatt und nehmen Geräte per Post entgegen.

Tec-Repair hingegen repariert die gängigsten Smartphone-Modelle in rund 100 Filialen von Media Markt und Saturn direkt vor Ort. Die Firma gehört zur Media-Saturn-Holding, und ihre Reparatur-Tresen stehen mitten in den Filialen der Elektromärkte. Im Folgenden bezeichnen wir Tec-Repair deshalb als „Media Markt/Saturn“.

## Die Aufgabe

Alle Werkstätten bekamen von uns dieselbe Aufgabe gestellt: Sie sollten bei einem Samsung Galaxy S4 und einige Wochen später bei einem iPhone 5 jeweils das gesplitterte Display komplett austauschen, also nicht nur das Glas, sondern die gesamte Display-Einheit inklusive OLED beziehungsweise LCD. Beim iPhone sollten sie außerdem den Akku tauschen.

Die Testgeräte bearbeiteten wir vorher mit gezielten Schlägen auf eine Bordsteinkante so, dass nur die Gläser splitterten, nicht aber die darunter liegenden Displays. (Lerneffekt dabei: Smartphone-Hüllen tau-

gen nur etwas, wenn sie die Ecken des Handys schützen.) Anschließend funktionierten alle Testgeräte, abgesehen vom gesplitterten Glas, noch einwandfrei.

## Transparenz und Kostentreue

Die Reparatur-Aufträge ließen wir von zwei Personen erstellen, die nicht mit der c't-Redaktion in Verbindung gebracht werden können. Dadurch stellten wir sicher, dass die Werkstätten genauso agieren wie bei normalen Kunden. Anschließend werteten wir nicht nur das Reparatur-Ergebnis und die Dauer aus, sondern auch die Kommunikation der Anbieter sowie die Kosten- und Termintreue. Außerdem untersuchten wir die Qualität der Ersatzteile, vor allem die Helligkeit der Ersatz-Displays und die Laufzeit der Ersatz-Akkus.



Bei den iPhones sollten die Werkstätten außer dem Display auch den Akku tauschen.

Alle Anbieter gaben die Preise für unsere Test-Reparaturen auf der Webseite an – wir mussten also nicht erst um einen Kostenvoranschlag bitten. Fragwürdig erschien uns die Aussage von Letsfix, dass man „nur originale Ersatzteile“ verwende, denn Original-Teile von Apple gibt es auf dem freien Markt kaum.

Vorbildlich wirkten die Angaben bei Media Markt/Saturn: „Apple keine Original-Ersatzteile, Samsung Original-Ersatzteile; Reparatur kann Einfluss auf den Herstellergarantiestatus des Gerätes nehmen“.

## Geschwindigkeit und Kommunikation

Alle Versand-Werkstätten außer McRepair gaben auf ihren Webseiten ziemlich präzise an, wie viele Tage die Reparatur (ohne Versandzeiten) angeblich dauern

### Reparaturgeschwindigkeit

Anbieter	iPhone-5-Reparatur [Tage] ◀ besser	Galaxy-S4-Reparatur [Tage] ◀ besser
Handyreparatur 123	2	1
Letsfix	5	1
McRepair	8	13
Media Markt/Saturn (Tec-Repair)	1	1

Tage = nur Werktagen von Mo. bis Fr., ohne Versandzeiten; Letsfix: beide Reparaturversuche zusammengezählt

### Qualität der iPhone-5-Ersatzteile

Anbieter	Akkulaufzeit [h] besser ▶	Displayhelligkeit <sup>2</sup> [cd/m <sup>2</sup> ] besser ▶
Handyreparatur 123	7,2	284
Letsfix	6,9	300
McRepair	7,8	451
Media Markt/Saturn (Tec-Repair)	7,8	401

Akkulaufzeit: bei Videowiedergabe mit 200 cd/m<sup>2</sup>



handyreparatur123  
Klick Klick Hurra

## Handyreparatur 123

Die Werkstatt mit Sitz in Jena macht schon auf den ersten Blick einen professionellen Eindruck: informative Webseite, einfacher Bestellvorgang, viele Bezahlmethoden. Im Test bestätigte sich dieser Eindruck. Handyreparatur 123 reparierte schneller als die Konkurrenz, schickte aussagekräftige Status-Mails und verwendete beim Rückversand frustfreie und sichere Verpackungen. Das iPhone-Ersatz-Display leuchtete allerdings nicht so hell wie die der anderen Werkstätten.

- ⬆️ schnell
- ⬆️ gute Kommunikation
- ⬇️ relativ teuer



LETSFIX

## Letsfix

Letsfix bietet ein breites Portfolio an Reparaturen, die Abläufe wirken aber ein wenig amateurhaft. Für den Hin-Versand bekommt man, anders als bei der Konkurrenz, keinen Retouren-Aufkleber, man muss also noch einmal 5 bis 7 Euro extra ausgeben. Nach einer der beiden Test-Bestellungen erhielten wir keine Bestätigungsmail. Als einzige Werkstatt benötigte Letsfix für eine Reparatur zwei Versuche. Die Reklamation nach dem ersten Versuch lief aber problemlos ab.

- ⬆️ schnell
- ⬇️ Patzer bei der Qualitätskontrolle

## McRepair

## McRepair

Die Webseite von McRepair wirkt noch konfuser als die von Letsfix, deswegen kostete uns schon der Bestellvorgang einige Nerven. Aber das war erst der Anfang, denn beide Reparaturen dauerten ewig. McRepair war die einzige Versand-Werkstatt im Test, bei der wir erst nach der Reparatur zahlen konnten, was die Wartezeit nochmals verlängerte. Immerhin stimmte die Qualität der Ersatzteile.

- ⬆️ gute iPhone-Ersatzteile
- ⬇️ sehr langsam
- ⬇️ verwirrender Bestellvorgang

soll. Im Test wurden zwei, drei oder maximal vier Tage versprochen. Auf der Webseite von McRepair fanden wir nur die wenig hilfreiche AGB-Klausel, dass die Werkstatt das Gerät „spätestens nach acht Wochen“ zu reparieren habe. Media Markt/Saturn versprach die Reparatur „in der Regel vor Ort innerhalb von 1 bis 2 Stunden“.

Handyreparatur 123 brauchte dann im Test tatsächlich nur einen beziehungsweise zwei Werkstage plus Versandzeit. Un-

schlagbar schnell war – erwartungsgemäß – die Sofort-Reparatur bei Media Markt/Saturn: Unser Galaxy S4 konnten wir nach knapp zwei Stunden wieder abholen, das iPhone sogar schon nach einer Dreiviertelstunde.

McRepair brauchte bei beiden Geräten erheblich länger als die anderen Werkstätten. Geschlagene dreizehn Werkstage lag zum Beispiel unser Galaxy S4 in der Werkstatt von McRepair. Inklusive Wochenenden und Hin- und Rückversand warteten

wir insgesamt sogar drei Wochen auf das Gerät.

Auf E-Mail-Anfragen antwortete McRepair schnell. Allerdings nützte uns das wenig, denn als wir nach unseren Geräten fragten, bekamen wir nur belanglose Ausreden zu lesen. McRepair ließ uns wissen, dass man „aufgrund anhaltender Lieferschwierigkeiten unseres Zulieferers auf alternative Ersatzteilhersteller ausweichen“. Obwohl wir darum gebeten hatten, teilten die Werkstätten keine konkreten Termine mit.

## Smartphone-Werkstätten

Anbieter	Handyreparatur 123	Letsfix	McRepair	Media Markt/Saturn (Tec-Repair)
Typ	Versandreparatur	Versandreparatur	Versandreparatur	Vor-Ort-Reparatur
Sitz	Jena	Stralsund	Berlin	in circa 100 Filialen von Media Markt und Saturn
Zahlungsarten	PayPal, Kreditkarte, Sofortüberweisung, Lastschrift, Vorkasse	PayPal, Sofortüberweisung, Lastschrift, Vorkasse, Nachnahme	PayPal, Überweisung	an der Kasse des Marktes (z. B. bar, mit EC-Karte)
<b>Reparaturkosten im Test</b>				
iPhone 5: Displaytausch	94,95 €	89,99 €	75 €	89 €
iPhone 5: Akkutausch	48,95 €	49,99 €	49 €	39 €
Galaxy S4: Displaytausch	158,95 €	139,99 €	149 €	129 €
Versandkosten	inklusive (ab 90 € Bestellwert)	nur Rückversand inklusive	inklusive	–
Gesamtkosten	302,85 €	286,87 €	273,00 €	257,00 €
<b>Bewertung</b>				
Kommunikation	⊕⊕	○	○	⊕⊕
Reparaturgeschwindigkeit	⊕⊕	⊕	⊖	⊕⊕
Ersatzteilqualität	○	⊕	⊕	⊕
⊕⊕ sehr gut   ⊕ gut   ○ zufriedenstellend   ⊖ schlecht   ⊖⊖ sehr schlecht   ✓ vorhanden   – nicht vorhanden   k. A. keine Angabe				





## Media Markt/Saturn

Einzige Vor-Ort-Werkstatt im Test. Die kleinen Reparatur-Tresen stehen in insgesamt 100 Filialen der beiden Elektro-Ketten. Wir ließen unser Samsung Galaxy S4 im Saturn in Braunschweig reparieren und unser iPhone 5 im Media Markt in Nienburg/Weser. Beide Male kamen wir nach wenigen Minuten an die Reihe und konnten das Smartphone weniger als zwei Stunden später wieder abholen. Insgesamt die schnellste, einfachste und günstigste Reparatur.

- ⬆ extrem schnell
- ⬆ günstig
- ⬆ gute Ersatzteile

## Reparatur- und Ersatzteilqualität

Besonders ärgerlich ist es, wenn das Gerät nach der Reparatur immer noch nicht funktioniert. Genau das passierte Letsfix mit unserem iPhone. Die Werkstatt tauschte das gesplitterte Display zwar aus, testete das Handy danach aber offensichtlich nur oberflächlich. Jedenfalls funktionierte der Touchscreen nicht richtig, als das Gerät wieder in unserer Redaktion eintraf. Er reagierte nur, wenn man ungewöhnlich fest aufs Display drückte, und selbst dann nicht immer.

Wir beschwerten uns. Letsfix bat uns daraufhin, ein Video einzuschicken, in dem das Problem ersichtlich wird. Nachdem wir das getan hatten, durften wir das Gerät erneut einschicken. Letsfix baute innerhalb von einem Tag kostenlos ein neues Display ein. Danach funktionierte das iPhone wieder einwandfrei – Letsfix hat also immerhin die Reklamation gemeistert. Die anderen Werkstätten brauchten jeweils nur einen Versuch.

Unser Test bestätigte die alte Erfahrung, dass die freien Werkstätten in der Regel Original-Samsung-Displays verwenden, aber keine Original-Apple-Displays (siehe c't 24/14, S. 130). Denn alle vier Testkandidaten bauten Original-S4-Displays ein. Die meisten iPhone-Displays leuchteten

aber nicht so hell wie Apples Original: Die von Media Markt/Saturn erreichten rund 400 cd/m<sup>2</sup>, die von Handyreparatur 123 und Letsfix sogar nur rund 300 cd/m<sup>2</sup>. In die Nähe von Apples Original kam nur das Display von McRepair (450 cd/m<sup>2</sup>), es war aber nicht so gleichmäßig ausgeleuchtet.

Vermutlich stecken in den Ersatz-Displays Original-LCDs aus ehemals gesplitterten Displays, die mit neuen Gläsern wiederaufbereitet wurden. Die Ersatz-Akkus schafften Laufzeiten von sieben bis acht Stunden. Das sind Werte, die im Alltag für die meisten Nutzer noch akzeptabel sind.

Jedenfalls kann man sich nicht darauf verlassen, dass freie Werkstätten eine gleichbleibende Ersatzteil-Qualität bieten. Das heißt, wer im Test gute Ersatzteile hatte, kann morgen schon schlechtere haben – aber auch umgekehrt.

## Fazit

Unter den Versand-Werkstätten schnitt Handyreparatur 123 am besten ab: Der Anbieter reparierte extrem schnell und informierte auf der Webseite und in den Status-Mails vorbildlich. Einziger Wermutstropfen war die geringe Helligkeit des iPhone-Ersatz-Displays.

Letsfix leistete sich im Test einen Schnitzer, es kann aber durchaus sein, dass das übersehene Touchscreen-Problem ein seltener Ausrutscher einer grundsätzlich guten und schnellen Werkstatt war.

Es ist ein wenig unfair, die Reparatur im Media Markt oder Saturn mit den Versand-Werkstätten zu vergleichen. Im Test gefiel uns der Vor-Ort-Service dennoch am besten, weil er am schnellsten und günstigsten war. Wenn man in der Nähe eines Media Markt oder Saturn mit Tec-Repair-Tresen wohnt, ist er die beste Option. Allerdings sollte man vorher anrufen und fragen, ob die passenden Ersatzteile auf Lager sind.

Bei Android-Smartphones ist der Preisvorteil der freien Werkstätten im Vergleich zu den autorisierten meist größer, außerdem ist die Chance größer, dass sie ebenfalls Original-Ersatzteile einsetzen. Hat man den Schaden nicht selbst verursacht und noch Garantie oder Gewährleistung, sollte man natürlich immer den Händler oder Hersteller mit der Reparatur beauftragen.

Egal welche Werkstatt, auf jeden Fall sollte man vor dem Einsenden das Gerät und die gut gepolsterte Verpackung fotografieren, die SIM und eine etwaige Speicherkarte entnehmen sowie alle privaten Daten sichern und löschen. (cwo) **ct**

# DENKEN SIE WEITER.

3 Ausgaben Technology Review mit **34% Rabatt** testen und Geschenk erhalten.



**GRATIS**

**WÄHLEN SIE IHR GESCHENK!**

Zum Beispiel:  
4-teiliges Reisetaschenset



## IHRE VORTEILE ALS ABONNENT:

- **VORSPRUNG GENIEßEN.**  
Früher bei Ihnen als im Handel erhältlich.
- **PREISVORTEIL SICHERN.**  
Mehr als 34 % Ersparnis im Vergleich zum Einzelkauf während des Testzeitraums.

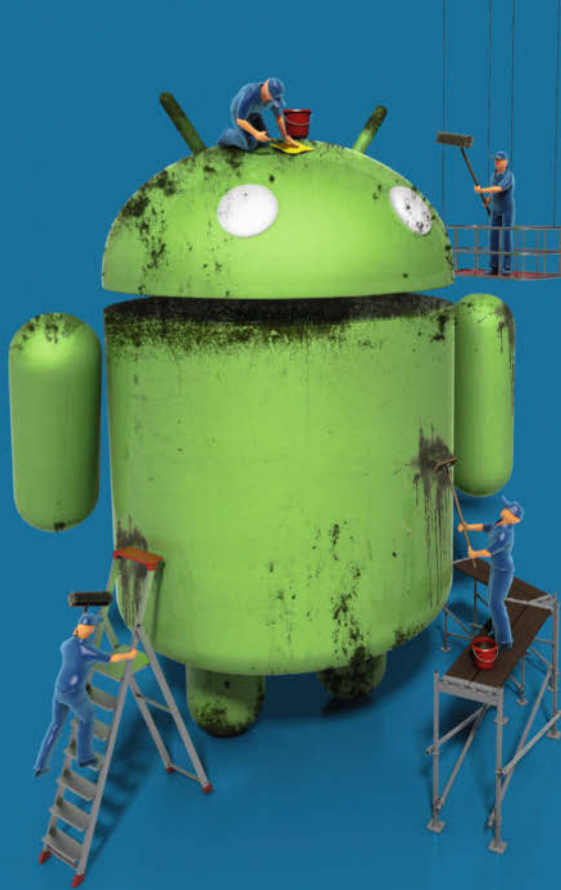


**JETZT AUCH KOMPLETT DIGITAL:**

- Bequem auf Ihrem Tablet oder Smartphone
- Für Android, iOS oder Kindle Fire

Jetzt bestellen und von allen Vorteilen profitieren:

**WWW.TRVORTEIL.DE**



Alexander Spier

## Systemoptimierer-Apps auf den Zahn gefühlt

Das System ruckelt schon wieder, ein Update scheitert aus Platzmangel oder der Akku ist überraschend schnell leer: Welcher Android-Nutzer kennt das nicht. Zahlreiche Tools im Play Store versprechen schnelle und einfache Abhilfe auf Knopfdruck. Wir testen, welche helfen und was Placebo ist.

Endlich, mein System läuft wieder optimal! Zumindest verspricht das die App in großen Buchstaben und freundlichem Grün. Mülldateien wurden beseitigt, der Arbeitsspeicher aufgeräumt und das System um exakt 41,8 Prozent beschleunigt. So eine Erfolgsmeldung auf Knopfdruck befriedigt ungemein. Zwar läuft die Oberfläche subjektiv tatsächlich schneller und an dem freigeschaufelten Speicher gibt es wenig Zweifel. Aber sind Android und die Apps wirklich so schlecht, dass sie Tuning-Tools brauchen?

Dass sich Tuning-Tools unter Android einer enormen Beliebtheit erfreuen, verwundert nicht: Die Verwendung ist simpel und der Erfolg gut darstellbar. Selbst die

großen Smartphone-Hersteller gehen dazu über, solche Werkzeuge prominent einzubinden und damit ein vergleichbares „Erlebnis“ zu bieten – Samsung etwa nennt seines „Smart Manager“. Dabei sollte ein High-End-Gerät wie das Galaxy S7 eigentlich kein Tuning nötig haben. Zudem bleibt die Frage, warum das System die Aufgabe nicht gleich selbst übernimmt, wenn die Daten überflüssig sind und nur die Performance verringern.

Wir haben uns einige der zahlreichen Vertreter aufs Gerät geholt, darunter den verbreiteten Clean Master sowie Avast Cleanup, Avira Optimizer, CCleaner und DU Speed Booster. Da Funktion und Wirkungsweise nahezu identisch sind, gehen wir nur auf die Unterschiede ein. Als Test-

objekte dienten ein Motorola Moto G3 mit 1 GByte RAM und 8 GByte internem Speicher, ein Google Nexus 5 mit 2 GByte RAM und ein Samsung Galaxy Tab 3 mit ebenfalls 1 GByte RAM, lahmem Prozessor und altem Android 4.4.

### Das Kreuz mit dem Arbeitsspeicher

Android gilt zu Recht als vergleichsweise hungrig nach Arbeitsspeicher. Es räumt Apps mehr Freiheiten ein, im Hintergrund aktiv zu bleiben oder im Speicher zu verweilen, als iOS oder Windows für Smartphones. Hinzu kommt, dass die Bandbreite an Geräten enorm groß ist: Ob High-End-Flaggschiff oder 50-Euro-Billig-

Smartphone, beide müssen prinzipiell die gleichen Aktivitäten mitmachen.

Bei schwach ausgestatteten Modellen kommt daher Frust auf, weil es sowohl an RAM und CPU-Leistung als auch an Flash-Speicher mangelt. Geht dem System der Arbeitsspeicher aus, spürt der Nutzer das mitunter, wenn Apps sekundenlang ruckeln, die Oberfläche langsam lädt und Animationen hängen. Sind viele Anwendungen installiert und im Hintergrund aktiv, straucheln sogar High-End-Geräte kurzzeitig.

Ein Grund dafür ist die Art der Speicher-verwaltung: Das System räumt den Speicher immer dann auf, wenn ein bestimmter Schwellenwert erreicht ist. Die „Garbage Collection“ benötigt CPU-Leistung – entsprechend sind schwache Smartphones nicht nur häufiger, sondern auch deutlicher von Denkpausen betroffen.

Zusätzlich kann Android laufenden Apps bei knapp werdendem Speicher signalisieren, diesen teilweise oder ganz freizugeben. Erst wenn der Stand trotzdem kritisch wird, werden Hintergrunddienste gestoppt und Apps geschlossen. Welche rausfliegen, versucht Android selber festzulegen. So verbleiben häufig benutzte Apps möglichst permanent im Speicher, während andere schnell ans Ende der Liste rutschen.

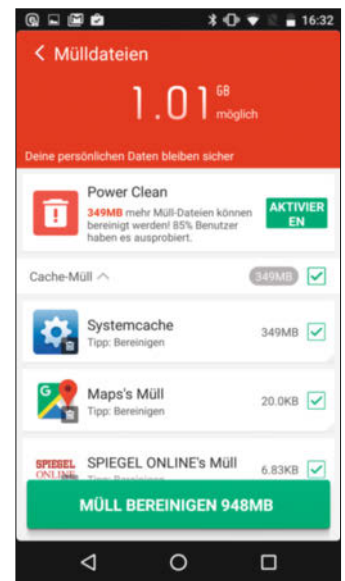
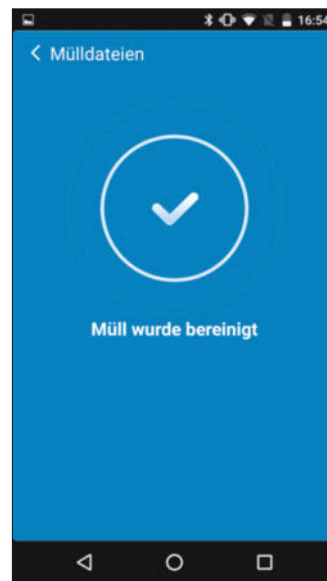
Diese Entwicklung versuchen die Tuning-Tools selbst vorzunehmen. Doch ihre manuellen Eingriffe sind selten von Dauer: Denn Hintergrunddienste dürfen auch von alleine wieder starten. So tauchen Apps wie Facebook nach wenigen Augenblicken wieder auf. Spätestens wenn ein entsprechendes Ereignis auftritt, starten ungefragt dazugehörige Apps wie etwa Google Fit. Ohne Root-Zugriff fehlt die Möglichkeit, den Autostart von Apps effektiv zu verhindern.

Das ist auch nicht unbedingt nötig, denn die meisten Hintergrunddienste brauchen zwar ein wenig Arbeitsspeicher, stehen aber so gut wie keine CPU-Zeit. Die Auswirkungen auf Laufzeit und Performance sind entsprechend marginal. Ab Android 6 verhindert zudem der Doze-Modus allzu häufiges Aufwachen aus dem Standby und lässt Apps nicht mehr autonom agieren.

Letztendlich nehmen Tuning-Tools vorweg, was das System ohnehin erledigen würde, handeln aber rücksichtsloser. Teilweise wirkt sich das sogar negativ auf Performance und Energiebedarf aus: Anwendungen beanspruchen beim Neustart länger und mehr Leistung, als wenn sie aus dem RAM aufwachen.

Trotzdem gibt es Gründe, den Speicher aufräumen zu wollen. Sei es, weil man sich

**Bunte Erfolgsmeldungen und optimistische Einschätzungen zum Speicher-gewinn gehören bei den Tuning-Tools zum Handwerk. Besonders der Clean Master verspricht viel.**



ein geschmeidigeres System erhofft oder damit etwa beim Zocken nicht im falschen Moment Hänger auftauchen.

## Bitte frei machen

Um die Auswirkungen der Speicherbereinigung zu messen, ließen wir einige anspruchsvollere Benchmarks mit viel Speicherbedarf durchlaufen – den PCMark 2.0 und den GFXBench. Zuvor starteten wir ein paar speicherintensive Spiele, Chrome, Facebook und andere Apps, bis das RAM vom System als zu 90 Prozent belegt angezeigt wurde. Anschließend starteten wir den jeweiligen Benchmark sofort oder bereinigten erst noch den RAM. Egal ob wir den Speicher freiräumten oder nicht, die Testergebnisse verändern sich nicht signifikant: Weder beim Nexus mit 2 GByte Arbeitsspeicher noch den beiden schwächeren Geräten gab es Unterschiede in der Performance.

Umgekehrt schauten wir, ob sich die Ladezeiten verbessern, wenn der Speicher frei ist. Dafür wählten wir das Spiel Asphalt 8, das sich je nach Gerät bis zu 400 MByte Speicher gönnt. Auch hier ergaben sich keine entscheidenden Unterschiede zwischen gesäuberten und normalem Zustand. Die Zeit zum Starten schwankte zwar stärker als die Benchmarks, doch ob der Speicher zuvor voll war, hatte keine Auswirkungen. Auf den langsameren Geräten hing Asphalt 8 zudem genauso oft im Spiel und an den gleichen Stellen. War das Spiel noch im Speicher, startete es jeweils innerhalb weniger Sekunden.

Auffällig war, wie verschwenderisch einige der Tools mit dem Speicher umgingen. So war der größte dauerhafte Speicherfresser auf dem Nexus 5 der Clean Master. Im Schnitt belegte er 150 MByte, in der Spitze sogar bis zu 500 MByte – also mehr als ein ressourcenfressendes Spiel. Die App selbst verschwieg ihren Speicherbedarf.

Clean Master und DU Speed Boost ließen sinnvollerweise Dienste in Ruhe, die entweder ohnehin neu starten oder vermeintlich vom Nutzer gebraucht wurden. So wurden die Play-Dienste im Speicher gelassen, aber auch Facebook nicht immer automatisch geschlossen. Warum es die Tools dann hin und wieder doch taten, bleibt ihr Geheimnis.

Ungeschickt ging der Avast Cleaner vor. Er schlug abgesehen von der Android-Oberfläche alle laufende Dienste zum Beenden vor. Dazu gehörten die Widgets auf der Startseite, der Samsung-Launcher und systemnahe Apps. Entsprechend rucklig verlief der Wechsel auf die Startseite. Am Ende blieb nur ein Speichergewinn von mageren 40 MByte übrig, statt der versprochenen 200 MByte. Der Avira Optimizer zeigte dagegen nur wenige Apps an, bei denen sich das Sparen eventuell lohnte und die gerade nicht aktiv waren. So konnte er zwar nicht mit Zahlen protzen, griff dafür aber nicht so brutal in Androids Speicher-verwaltung ein.

Geschmeidiger als zuvor lief insbesondere das Galaxy Tab 3 letztendlich nicht. Räumten das System oder die Tools auf, mussten Apps und Teile der Oberfläche



immer wieder neu in den Speicher geladen werden. Entsprechend ruckelte die Oberfläche beständig leicht. Andererseits reagierte das schnellere Nexus 5 trotz angeblich vollem Speicher durchgängig flott. Das Moto G räumte schon von alleine so gründlich auf, dass es selten ans Speicherlimit geriet. Nach speicherhungrigen Apps mussten allerdings gelegentlich die Oberfläche und das Hintergrundbild neu laden – was kein Optimierer verhindern kann.

Das zweite große Feature der Tuning-Tools ist das Freiräumen des internen Speichers. Bis zu 2 GByte mehr Platz versprechen die meisten nach dem Einsatz. Auch hier kneift es hauptsächlich die Besitzer von günstigen Smartphones.

## Der Speicherplatz wird knapp!

Die Anzeige in den Einstellungen ist nicht einmal die ganze Wahrheit: Wenn Android deutlich davor warnt, dass kaum mehr Speicherplatz vorhanden sei, werden in der Speicherübersicht mehrere Hundert freie Megabyte angezeigt – so viel, dass die größte App noch aktualisiert werden kann. App-Installationen, egal wie winzig, sind nicht mehr möglich. Schwindet der freie Platz weiter, führt Android einige Updates nicht mehr aus und schränkt Systemdienste ein.

Ohne Apps und eigene Dateien zu löschen lässt sich nur durch Leeren diverser Caches und temporärer Dateien Speicherplatz gewinnen. Den App-Cache nutzt nahezu jede Anwendung, um ihren Start zu beschleunigen und wiederholte Down-

loads zu vermeiden. Besonders bei Apps wie Facebook, die viele Elemente aus dem Netz laden, wächst der Cache mitunter beachtlich. Andere benötigen nur wenige KByte.

Das Löschen des App-Cache beeinflusst weder Nutzerdaten noch essenzielle Bestandteile der Anwendung. Allerdings verzögert es die folgenden Starts mitunter deutlich und verbraucht zusätzliches Datenvolumen, wenn die App wieder Daten nachladen muss.

Android selbst kann diesen Cache ebenfalls bereinigen, holt sich im Bedarfsfall aber nur so viel zurück, wie es für eine bestimmte Aktion braucht. Eine regelmäßige automatische Bereinigung findet nicht statt. So wächst der Zwischenspeicher zusammengerechnet teilweise auf mehrere Gigabyte an.

Seit Android 6 dürfen Apps den Cache anderer Anwendungen nicht mehr einfach so löschen. Daher fordern einige Tuning-Apps beim Nutzer an, als Bedienungshilfe agieren zu dürfen. Damit erhalten sie allerdings potenziell Zugriff auf persönliche Daten und können andere Aktivitäten auf dem Gerät steuern und mitlesen.

## Müll verzweifelt gesucht

Viele Tuning-Tools suchen außer dem App-Cache nach weiteren temporären Dateien, denn längst nicht jede App weist diese gegenüber dem System so aus. Asphalt 8 lädt zum Beispiel beim ersten Start 60 MByte herunter, die nicht über das System direkt gelöscht werden können. Zusätzlich wird nach heruntergeladenen

APK-Dateien, nach der Deinstallation übrig gebliebenen Resten und alten Backups gesucht, etwa von WhatsApp.

Beim erzielbaren Speicherzugewinn gibt es zwischen den Tools unter gleichen Bedingungen extreme Unterschiede: Avast verspricht nur 5 MByte, CCleaner 26 MByte, Avira genau wie DU 190 MByte und Clean Master mal eben 870 MByte. Letzterer rechnet einfach die RAM-Belegung hinzu, kam ohne aber nur auf 80 MByte.

Keine Anwendung verrät genau, wann das Löschen von bestimmten Daten sinnvoll ist und wann nicht. Automatisch werden zwar nur der Cache und temporäre Dateien gelöscht – doch um möglichst hohe Zahlen zu erreichen, werden auch mitunter fragwürdige Elemente optional aufgeführt. Der Avira Optimizer stellt kommentarlos alle große Dateien zur Disposition, würde so aber zum Beispiel Testvideos unseres Benchmarks entfernen. CCleaner führt die Zwischenablage und die Anrufliste auf.

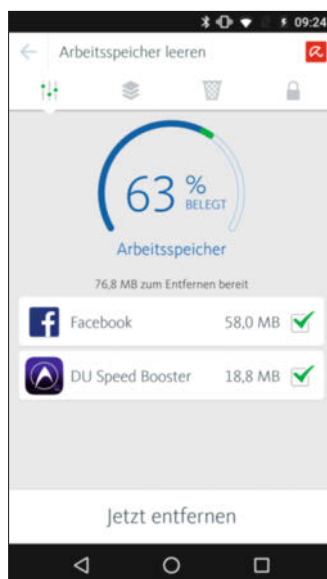
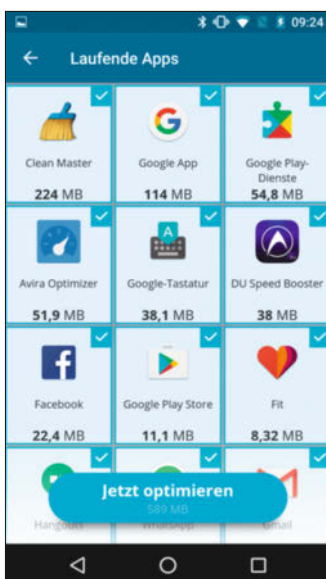
Entsprechend müßig war das Aufräumen: Wenige Stunden später waren die meisten Daten im gleichen Umfang wieder da, wenn wir das Gerät benutzten. Sinnvoller ist es, erst nach einigen Wochen oder Monaten bei akutem Bedarf aufzuräumen. Dann erwischt man zumindest einige tatsächlich nicht mehr gebrauchte und überflüssige Daten, die nicht sofort wieder generiert werden. Von 2 GByte gelöschten Daten auf einem privat genutzten Gerät waren nach wenigen Tagen trotzdem wieder über 700 MByte zurück. Das reicht, um einen kurzfristigen Engpass zu beseitigen; den Platzmangel lösen die Tools auf Dauer jedoch nicht.

Manche Apps bieten sinnvollere Ansätze für einen dauerhaften Speichergewinn. Avast Cleanup weist auf länger nicht mehr genutzte Apps hin. Das Tool kann zudem nach doppelten Dateien scannen und bietet an, Dokumente und Fotos in die Dropbox zu verschieben. Der Clean Master sucht identische sowie vermeintlich unscharfe Bilder.

Positiv bleibt zu erwähnen, dass kein Tool im Test ungefragt wichtige persönliche Daten löschte oder Probleme mit anderen Apps verursachte. An einigen Stellen muss der Nutzer mitdenken, was er selbst ankreuzt, doch die Automatismen sind zuverlässig genug, um keine unwiderprüflichen Schäden zu verursachen.

## Optimistische Versprechen und dubiose Werbung

Die meisten Programme versprechen, die Laufzeit zu verlängern und den Prozessor



Während Avast Cleanup (rechts) radikal alle Apps und Dienste zum Abschluss vorschlägt, zeigt der Avira Optimizer nur wenige, aber sinnvolle Einträge.

zu entlasten. Grundsätzlich ist die Behauptung durchaus naheliegend, denn ein im Hintergrund aktiver Dienst nutzt die CPU und hält das Gerät über Gebühr wach. Allerdings überwacht keines der getesteten Tools tatsächlich die CPU-Zeit oder Hintergrundaktivitäten, um echte Akkufresser zu identifizieren. Clean Master wirft stattdessen zufällige Warnungen zu Temperatur und CPU-Last aus, die auch mal während eines Spiel gemessen wurden. Zur Behebung werden wie üblich pauschal Apps beendet, die damit nichts zu tun hatten. Die anderen Tools sparen sich diese Verunsicherung immerhin. Einen Einfluss der „Optimierungen“ auf die Akku-Laufzeit konnten wir nicht feststellen.

Auch an anderen Stellen fiel der Clean Master von Cheetah Mobile unangenehm auf. Er sicherte sich zahlreiche Zugriffsrechte, darunter auch auf die Kontakte und den Standort. Er schlug überall Alarm oder versprach technisch fragwürdige Vorteile wie schnelleres Aufladen. Ziel ist jedoch nur, möglichst viel Werbung auf den Bildschirm zu bringen.

Nimmt man alle Angebote blind an, hat man am Ende einen zusätzlichen Lockscreen, eine Pin-Eingabe für bestimmte Apps, ein eigenes Benachrichtigungszentrum, einen Virens scanner, einen App Store und jede Menge Warnungen zu überhitzenden Prozessoren und vollem Speicher auf dem Smartphone – alle mit Werbung versehen. Zusätzlich lauern in der App überall als Funktion getarnte Anzeigen. Auch der DU Speed Booster drückte dem Nutzer Werbung und unnütze Funktionen auf.

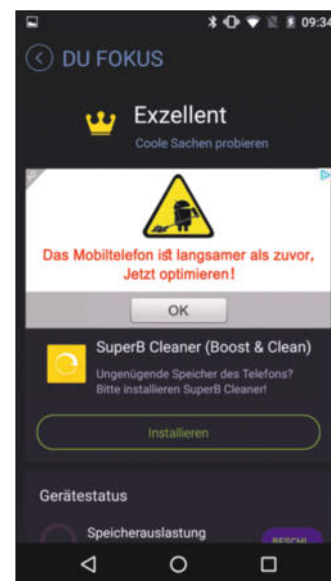
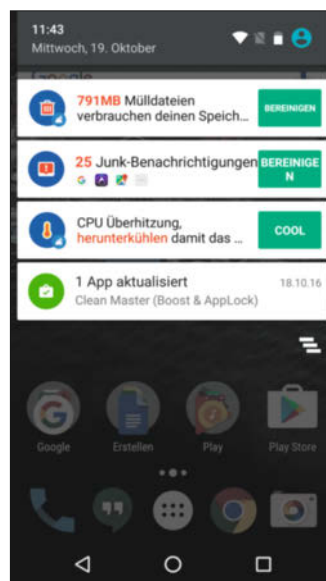
CCleaner und Avira Optimizer sind in Sachen Werbung deutlich zurückhaltender und belegen zudem wenig RAM. Avast Cleanup bietet für 8 Euro pro Jahr Werbefreiheit.

## Selbstanalyse

Messwerte hin oder her – die Erfahrung aus dem Alltag zeigt, dass Android selbst bei Überfluss an Speicher irgendwann ruckeln und lahm reagieren kann. Besonders mit reichlich Apps ausgestattete und lange nicht neu gestartete Systeme neigen zu solchen Aussetzern. Trotzdem muss man nicht zwangsläufig auf Tuning-Tools zurückgreifen.

Über den Task-Wechsler lassen sich Apps manuell beenden und aus dem Speicher werfen. Viele können auch direkt beendet werden, in dem man lange genug den Zurück-Button benutzt – gerade bei Spielen eine weniger aggressive Methode,

**Clean Master (rechts) nervte mit jeder Menge Werbung und ständigen Benachrichtigungen über angebliche Probleme. Auch der DU Speed Booster warf mit Werbung um sich.**



sie aus dem Speicher zu befördern. Ein gelegentlicher Neustart des Smartphones hilft Android ebenfalls auf die Sprünge.

Android bietet zudem selbst Möglichkeiten, problematischen Diensten und Apps auf die Schliche zu kommen. Über den Akku-Verlauf findet man besonders energiehungrige Apps, die möglicherweise im Hintergrund das System verlangsamen. In der Detailansicht der Anwendung führt Android zudem die Zeit auf, wie lange sie im Hintergrund aktiv waren. Speicherfressern kommt man in den Einstellungen unter (Arbeits-)Speicher auf die Schliche. Hier werden allerdings nur langfristige Statistiken geführt. In den Android-Entwicklereinstellungen gibt es eine Übersicht der momentanen Verbraucher, inklusive der von ihnen genutzten Dienste.

Wer es genau wissen will, nimmt Tools wie System Monitor oder OS Monitor. Sie zeigen aktuell laufende Apps und geben Infos zur Speicher- sowie Prozessorauslastung.

Ab Android 6 sorgt der Doze-Modus für einen sparsameren Standby. Das eigentlich für gerootete Geräte gedachte Greenify erlaubt es, Doze auch ohne Root den eigenen Wünschen anzupassen. Bei einigen Apps lassen sich Hintergrund-Updates sogar direkt in der Anwendung deaktivieren.

## Fazit

Android hat systembedingt Schwächen beim Umgang mit Ressourcen, worunter Geräte mit lahmmer Hardware durchaus spürbar leiden. Doch so verständlich der

Wunsch nach einer einfachen Leistungssteigerung per Software ist, so wenig eignen sich die zahlreichen Tools im Play Store dafür. Insbesondere der ständige Eingriff ins Speichermanagement erweist sich als unnötig und teilweise sogar kontraproduktiv. Ohne Root-Rechte fehlen den Apps schlicht die Möglichkeiten, effektiver zu agieren als das System selbst – sie arbeiten gegen Windmühlen. Auch wenn dadurch auf langsameren Geräten kurzzeitig Ruckler vermieden werden, ändern sie nichts an der App-Performance.

Besser eignen sich die Werkzeuge, um dringend benötigten Platz freizuräumen. Denn zumindest bei länger nicht mehr gestarteten Apps bleiben mitunter unnötige Daten liegen. Doch auch hier kämpft man mit Mitteln, die der App-Entwickler so nicht vorsieht. So räumt man oft Dinge aus dem Weg, die früher oder später wieder heruntergeladen werden. Eine dauerhafte Lösung der Speicherkrise ist das nicht.

Besser ist es, Apps zu deinstallieren, die man nicht dringend benötigt. Immerhin bieten einige Tools wie Avast Cleanup eine schnelle Übersicht, welche Apps lange nicht mehr benutzt wurden. Auch ständig aktive Programme mit hohem RAM-Bedarf sind Kandidaten für den Frühjahrsputz, wenn man diese selten aktiv verwendet.

Ärgerlich wird es, wenn ausrechnet das vermeintliche Tuning-Werkzeug selbst der Übeltäter ist. Besonders Clean Master tat sich nicht nur dabei besonders negativ hervor. Die Unverfrorenheit, mit der der Anbieter das Gerät mit Werbung verseucht, wiegt der begrenzten Nutzen jedenfalls nicht auf. (asp)



Bild: Fairphone

Christian Wölbert

## Fairphone verwendet als erster Hersteller Fairtrade-Gold

Das niederländische Start-up Fairphone hat Lieferketten für Fairtrade-Gold aus Peru und konfliktfreies Wolfram aus Ruanda aufgebaut. Projektmanagerin Bibi Bleekemolen erklärt im Interview, wie das geklappt hat.

**G**roße Elektronik-Hersteller wie Apple und HP nennen zwar die Namen von direkten Zulieferern und Metall-Schmelzhütten. Sie decken allerdings ihre Lieferketten nicht komplett auf und verraten nicht, aus welchen Bergwerken die von ihnen verwendeten Metalle stammen. Wir sprachen mit der Fairphone-Mitarbeiterin Bibi Bleekemolen über die Lieferketten.

**ct:** Frau Bleekemolen, wie viel Fairtrade-Gold haben Sie für die Fairphone-Produktion gekauft?

**Bibi Bleekemolen:** 100 Gramm. Diese Menge pures Gold brauchen wir zur Herstellung von Goldsalz für die elektrochemische Behandlung von 100 000 Fairphone-Leiterplatten.

**ct:** Was war die Herausforderung dabei?

**Bleekemolen:** In Südamerika gab es schon Fairtrade-Goldminen. Dieses Gold wurde

bislang in Europa zu Schmuck verarbeitet. Allerdings ist fast die gesamte Elektronik-Fertigung in China konzentriert. Und die chinesischen Produzenten dürfen ausschließlich an der Börse in Shanghai Gold kaufen. Das Gold wird dort zwischengelagert und mit anderen Lieferungen vermengt. Die ursprünglichen Quellen dokumentiert die Börse nicht.

Wir konnten deshalb den Weg des fairen Golds nicht bis zu unseren chinesischen Zulieferern verfolgen. Normalerweise akzeptieren wir keine Aussagen wie „das geht nicht“, aber das war tatsächlich eine große Herausforderung.

**ct:** Wie haben Sie dann doch den Durchbruch geschafft?

**Bleekemolen:** Nach einem Jahr intensiver Gespräche hatte der Goldsalz-Hersteller Zhaojin Kanfort die Idee, das Gold über seine Niederlassung in Hongkong zu importieren und von dort an seine Fabrik weiterzuleiten. Dieser Weg ist zwar auch

streng reguliert, aber das Gold muss nicht physisch in der Börse in Shanghai gelagert werden.

**ct:** Wie kommt das Gold dann genau ins Handy?

**Bleekemolen:** Zhaojin Kanfort vermischt es mit anderen Lieferungen und stellt daraus Goldsalz her. Ab diesem Punkt können wir das Fairtrade-Gold nicht mehr physisch nachverfolgen. Es handelt sich um einen Massenausgleich, der bei Fairtrade explizit möglich ist. Der Hersteller AT&S verwendet das Goldsalz von Zhaojin für die Fairphone-2-Platinen.

**ct:** Ist der Aufwand nicht ziemlich groß für 100 Gramm?

**Bleekemolen:** Es ging uns nicht um die Menge. Es ging uns darum, der Industrie und den Verbrauchern zu zeigen, dass man Fairtrade-Gold für Elektronik verwenden kann. Wir möchten, dass auch andere



Hersteller über ihre Lieferkette nachdenken. Es würde uns sehr freuen, wenn sie ebenfalls Fairtrade-Gold einsetzen. Die Elektronikindustrie ist der drittgrößte Goldverbraucher nach der Schmuckbranche und dem Finanzsektor.

**ct:** Warum kleben Sie kein Fairtrade-Logo auf das Fairphone, wie bei Bananen oder Kaffee?

**Bleekemolen:** Das wäre irreführend. Das würde den Eindruck erwecken, dass das Telefon schon zu 100 Prozent fair wäre. Uns geht es nicht um Greenwashing. Wir wollen darauf hinweisen, welche Chancen in Fairness stecken – aber auch darauf, wie komplex das Thema ist.

Wir sagen lediglich, dass man mit dem Kauf des Fairphone 2 den Abbau von Fairtrade-Gold in Peru unterstützt. Und wir sind bislang der einzige Elektronik-Hersteller, der das sagen kann.

**ct:** Außer mit Fairtrade-Gold wirbt Fairphone auch mit „konfliktfreiem“ Tantal, Zinn und Wolfram. Wie schwierig war es, diese Lieferketten aufzubauen?

**Bleekemolen:** Konfliktfreies Zinn und Tantal aus dem Kongo beziehen wir schon seit dem ersten Fairphone über bestehende Lieferketten, die von anderen Initiativen aufgebaut wurden. Darüber hinaus verwenden wir von August an konfliktfreies Wolfram aus Ruanda im Fairphone 2. Hier war unser

Beitrag, dass wir die österreichische Wolfram Bergbau und Hütten AG überzeugt haben, wieder Erz aus Ruanda zu beziehen.

**ct:** Warum waren die Lieferungen aus Ruanda unterbrochen worden?

**Bleekemolen:** Das lag hauptsächlich an einem US-Gesetz, das 2010 in Kraft trat, dem Dodd-Frank-Act. Das Gesetz erhöhte den administrativen Aufwand beim Einsatz von Rohstoffen aus dem Kongo und seinen Nachbarländern wie Ruanda. Die Hütte wollte damals weiterhin in Ruanda kaufen, doch ihre Kunden haben sie davon abgehalten.

Wir suchen aber explizit nach konfliktfreien Mineralien in Konfliktregionen, um die lokale Wirtschaft dort zu unterstützen. Im Kongo hat ein Arbeiter mal zu mir gesagt: „Das einzige, das schlimmer ist, als in einer Konfliktregion Erz abzubauen, ist, gar nichts abbauen zu können. Kein Bergbau, kein Geld. Kein Geld, kein Leben.“

**ct:** Wie haben Sie die Wolfram-Hütte überzeugt?

**Bleekemolen:** Den Vorstand haben wir schnell für uns gewonnen. Doch wir waren als Kunde viel zu klein für eine eigene Lieferkette. Deswegen musste die Hütte erst ihre anderen Kunden überzeugen, wieder Wolfram aus Ruanda zu akzeptieren. Als das geklappt hatte, mussten wir noch den Komponenten-Hersteller ins Boot holen.

Das Wolfram dient als Gegengewicht im Vibrationsmotor.

**ct:** Auch andere Elektronik-Hersteller sagen, dass sie konfliktfreie Rohstoffe verwenden. Was ist der Unterschied zu Fairphone?

**Bleekemolen:** Je mehr andere Unternehmen auf das Thema aufmerksam werden, desto besser. Das ist sehr unterstützenswert und Teil unserer Mission bei Fairphone.

Wie andere Hersteller versuchen wir, unsere Lieferkette von oben nach unten aufzudecken, also vom direkten Zulieferer über die Komponentenhersteller der zweiten und dritten Ebene bis zur Metallhütte. Das ist langwierig und am Ende kann man vielleicht sagen, dass die Lieferkette konfliktfrei ist.

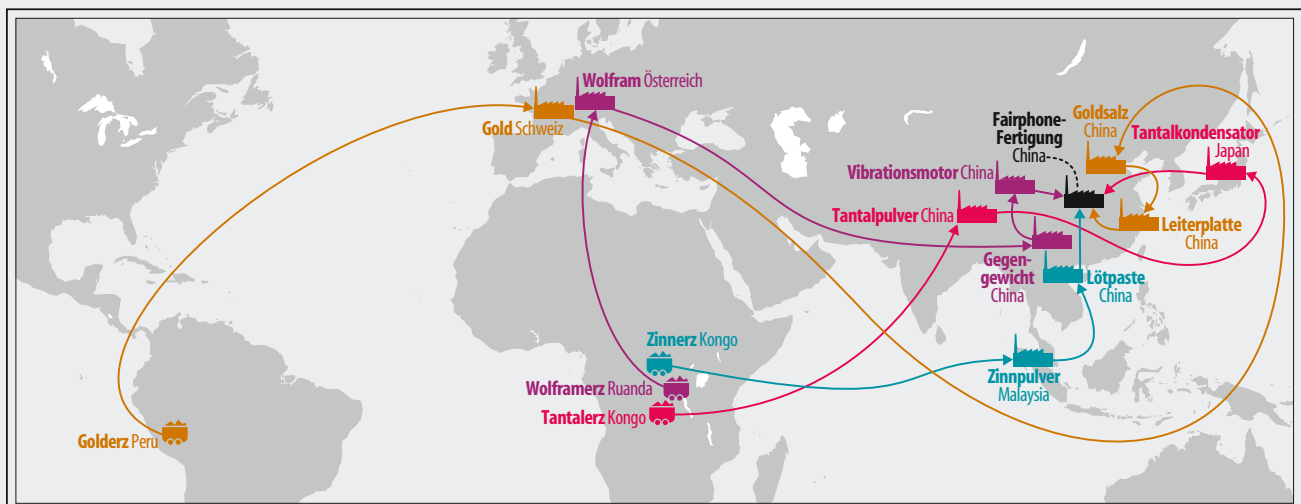
Wir wollen aber auch direkt Bergwerke unterstützen, die die Wirtschaft in Konfliktregionen fördern. Deswegen arbeiten wir auch von unten nach oben, setzen also bei den Bergwerken an.

**ct:** Welche Metalle knöpfen Sie sich als Nächstes vor?

**Bleekemolen:** Es ist noch zu früh für eine Entscheidung. Wir müssen immer zwei Seiten betrachten: die Bedeutung der Metalle für das Endprodukt und die Verbesserungen, die wir bei der Förderung erreichen können. Wir arbeiten an einer Liste von Mineralien, auf die wir uns als Nächstes konzentrieren werden. (cwo) **ct**

## Rohstoff-Transparenz

Als einziger Hersteller legt Fairphone den Weg von der Mine bis zum Smartphone offen – zumindest für vier Metalle.





André Kramer

# Apps zur Bildbearbeitung

**Instagram hat vorgemacht, wie man Schnappschüsse auf die Schnelle für Social Media aufpeppt. Das neue Lightroom Mobile zeigt, wie weit das Potenzial mobiler Bildbearbeitung reicht. Foto-Apps können sich hinsichtlich Foto-Entwicklung und -Effekten mit Desktop-Schergewichten messen.**

**A**m PC nimmt man sich einen Abend Zeit, um die Urlaubsbilder aufzuhübschen. Hier zählen großer Funktionsumfang der Software und die Qualität des Resultats. Fotobearbeitung auf Mobilgeräten soll in erster Linie effizient sein. Schnappschüsse vom Smartphone müssen schnell und nach wenigen Handgriffen auf Facebook landen. Wer unter Zeitdruck das benötigte Werkzeug nicht findet, wird die App nach kurzer

Zeit nicht mehr benutzen. Es reicht nicht, einen Haufen Werkzeuge auf dem kleinen Touchscreen unterzubringen und so anzuordnen, dass sie mit den Fingern bedienbar sind. Im Gegenteil: Das kann sogar kontraproduktiv sein. Gute Benutzerführung ist das A und O.

Gelungene Android-Apps, haben wir in der Tabelle und auf den folgenden Seiten zusammengefasst, darunter Aviary, Dramatic Black & White, Facetune, Instagram,

Lightroom Mobile, Perfectly Clear, Photo-Director, Photoshop Mix, Pixlr, Snapseed, TouchRetouch und VSCO. Die beiden Kästen stellen zwei weitere vor, die nur für je eines der Betriebssysteme verfügbar sind.

## Ein klares Profil

Wer gelten will, muss auffallen, denn bei etwa 2,4 Millionen Apps im Google Play Store gerät man schnell in Vergessenheit.

Gut aufgestellt sind Apps, die sich einer spezifischen Funktion besonders gelungen annehmen. Adobe hat aus diesem Grund seine bisherige Strategie verworfen, mit Photoshop Touch das Desktop-Konzept in die mobile Welt zu tragen. Stattdessen wächst nun eine App-Familie, deren Mitglieder klar definierte Aufgaben haben: Photoshop Sketch für Zeichnungen, Photoshop Mix für Montagen, Photoshop Fix für Bildverbesserung und so weiter. Die Kehrseite ist, dass den Kunden nun der Überblick in der ausufernden App-Familie verloren geht. Das im Oktober 2015 vorgestellte Retuschewerkzeug Photoshop Fix stand lange nur für iOS zur Verfügung, ist mittlerweile aber auch für Android verfügbar.

Auch erfolgreiche Apps anderer Hersteller besitzen ein geschärftes Profil: Perfectly Clear wendet einen effektiven Bildverbesserungsalgorithmus an, Facetune verbessert Porträts, TouchRetouch retuschiert störende Objekte im Bild, Dramatic Black & White versteht sich auf effektvolle Schwarz-weißumsetzung.

## Berührt, geführt

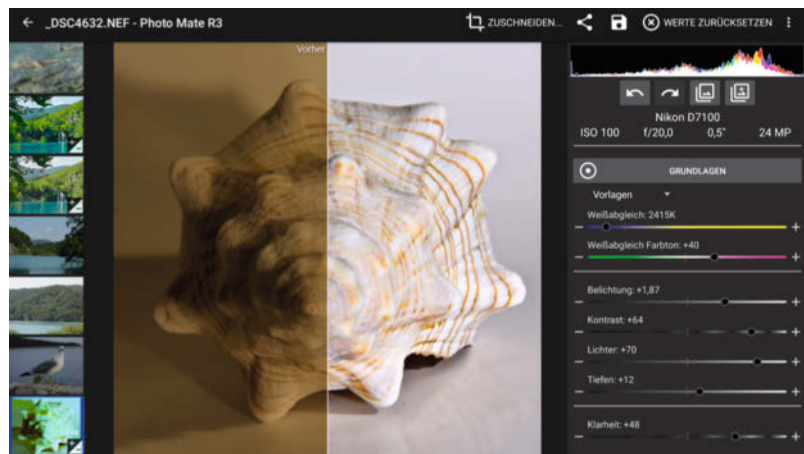
Fast ebenso wichtig ist einfache Bedienung. App-Nutzer befinden sich oft in turbulenter Umgebung. Um den Schnappschuss vom Junggesellenabschied mit Erfolg zu bearbeiten, während die Freunde lärmern, muss die App klar vorgeben, was zu tun ist.

Im Idealfall führt sie vom Öffnen übers Bearbeiten bis zum Export Schritt für Schritt durch den Prozess. Besonders gut gelingt das bei Instagram und Perfectly Clear. Bei Apps mit weniger klarer Reihenfolge der Arbeitsschritte muss die App zumindest deutlich machen, wie der Nutzer zum Ergebnis kommt. Photoshop Mix, Snapseed und VSCO informieren etwa knapp und effektiv über alle wichtigen Arbeitsschritte.

## Unterm Strich

Bei vielen Funktionen leidet die Übersicht einer Foto-App. Wenn sie außerdem vornehmlich schrille Effekte bietet, wie Befunky oder Pho.to Lab, sollte man seine Zeit besser nicht damit verschwenden. Apps vom Kaliber „Funny Camera“, die Bilder verzerren oder in ein Passepartout mit Vollmond und drei heulenden Wölfen setzen, bieten zwar das gewünschte klare Profil, aber kein realistisches Szenario mit geschmackvoller Anwendung.

## Photo Mate R3



**Torsten Simons Raw-Entwickler für Android Photo Mate R3 importiert Rohdaten direkt von einer angeschlossenen Kamera.**

Photo Mate R3 bearbeitet Licht und Farbe von JPEG- sowie Raw-Dateien mit ähnlichen Werkzeugen wie Lightroom, wenn auch mit weniger gutem Resultat. Das nichtdestruktiv bearbeitete Bild exportiert die App auf Wunsch inklusive Wasserzeichen als JPEG-, PNG- oder TIFF-Datei. Entwicklungseinstellungen merkt sie sich bis

zum Export. Die Installation ist kostenlos, nach 72 Stunden werden allerdings 9 Euro fällig. Die ausladende Oberfläche lässt sich nur auf einem Tablet anständig bedienen. Was die App interessant macht: Sie erkennt per USB angeschlossene Kameras und importiert darauf gespeicherte Fotos aufs Mobilgerät.

VSCO ist ein Allrounder, dem man Aufmerksamkeit schenken sollte. Auch Aviary und Pixlr bieten sinnvolle Werkzeuge für kreative Bildverbesserung. Ein Highlight bei Aviary ist der Meme-Modus, in dem sich ein Bild um Schrift ergänzen lässt. Pixlr lässt sich um Pixlr-o-matic mit vielen tauglichen Effekt-Presets ergänzen. Ansonsten gilt für Aviary, Pixlr und Cyberlink PhotoDirector, dass bei vielen Werkzeugen meistens nicht alle professionellen Ansprüche genügen. Snapseed bietet spektakuläre Ef-

fekte und ein einzigartiges Bedienkonzept. Schwarzweißbilder gelingen sehr gut mit Dramatic Black & White, gute Porträts mit Facetune und kristallklare Landschaftsaufnahmen mit Perfectly Clear.

Die vorgestellten Apps führen nach wenigen Handgriffen entscheidende Verbesserungen herbei. Sicher befinden sich unter den Millionen Apps noch viele unentdeckte Perlen. Wenn Sie Ihre Lieblings-App vermissen, informieren Sie uns!

(akr) **ct**

## Foto-Apps für Android und iOS

Programm	Hersteller	Web	Systemanf. Android	Preis
Aviary	Adobe	aviary.com	Android ab 4.1 (v4.8)	kostenlos
Dramatic Black & White	JixiPix	jixipix.com	Android ab 4.0 (v2.26)	2,09 €
Facetune	Lightricks	facetuneapp.com	Android ab 4.1 (v1.1)	1,99 €
Instagram	Facebook	instagram.com	Android var. (v10.0)	kostenlos
Lightroom Mobile	Adobe	adobe.com	Android ab 4.1 (v2.2)	kostenlos
Perfectly Clear	Athentech	athentech.com	Android ab 2.3 (v4.3)	0,79 €
PhotoDirector	Cyberlink	cyberLink.com	Android ab 4.1 (v4.5)	kostenlos
Photoshop Mix	Adobe	adobe.com	Android ab 4.3 (v2.3)	kostenlos
Pixlr	Autodesk	pixlr.com	Android ab 6.0 (v3.0)	kostenlos
Snapseed	Google	google.com	Android ab 4.1 (v2.12)	kostenlos
TouchRetouch	AVDA	adva-soft.com	Android ab 4.0 (v4.0)	1,99 €
VSCO	VSCO	vSCO.co	Android ab 4.0 (v14)	kostenlos





## Aviary

### Typ: Foto-Allrounder

Aviary war früher eigenständig, wurde dann von Adobe gekauft und ausgeschlachtet. Von der App darf man daher vermutlich keine großen Entwicklungssprünge mehr erwarten. Dennoch taugt sie für Foto-Entwicklung und Effekte.

Die beschrifteten Icons erleichtern die Orientierung. Aviary bietet 19 Kategorien. „Verbessern“ verspricht mit Einstellungen für Landschaft, Essen oder Nacht Ein-Klick-Resultate. Der Effektbereich hält zahlreiche sinnvolle und zeitgemäße Einstellungen parat, die sich per In-App-Kauf um viele weitere ergänzen lassen. In Kombination mit einem der schnörkellos schlichten Rahmen ist das Bild damit fast fertig.

Der Anpassen-Bereich bringt Regler für Belichtung, Kontrast, Farbtemperatur, Sättigung, Lichter und Schatten mit. Weichzeichner und Vignettierung lassen sich per Maske selektiv anwenden. Außerdem gibt es Werkzeuge zum Geraderichten und Beschneiden. Insgesamt bietet Aviary alles Wichtige. Das Textwerkzeug und die Porträtfunktionen sind wenig brauchbar. Der Meme-Generator hingegen versieht Fotos internetkonform mit plakativem Text. Für die Weitergabe bietet Aviary vier Platzhalter für Facebook, Instagram, WhatsApp, Google+ und Dropbox.

**Fazit:** Aviary bringt viele, klar beschriftete Werkzeuge mit. Nicht jedes einzelne überzeugt, in der Summe ist die App aber breit aufgestellt.

- ➡ großer Funktionsumfang
- ➡ enthält auch schlechte Werkzeuge



## Dramatic Black & White

### Typ: Schwarzweiß-Maler

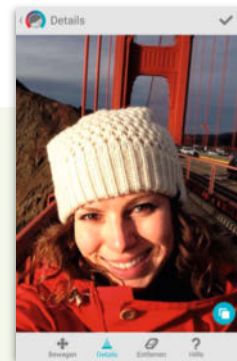
Der Hauptarbeitsbereich von Dramatic Black & White umfasst Funktionen wie Öffnen, Beschnitt, Export als JPEG und Weitergabe an WhatsApp-Kontakte oder beliebige auf dem Mobilgerät eingerichtete Apps. Die übrigen vier Arbeitsschritte beinhalten einen Bereich mit Effekt-Presets, zwei mit Reglern für Helligkeit und Kontrast beziehungsweise Farbanteile und einen letzten für dunkle Randabschattung wie aus der Dunkelkammer.

Die App hält in drei Kategorien insgesamt 36 Vorschläge bereit, die man mit mehreren Werkzeugen weiterbearbeiten kann. Per Regler wählt man zwischen den Polen Weich und Scharf, Dunkel und Hell sowie wenig und viel Kontrast. Außerdem kann man die Anteile der Kanäle Rot, Grün und Blau, die Stärke des Presets und die Menge künstlichen Filmkorns bestimmen. Letzteres erinnert leider unangenehm an digitales Bildrauschen.

Im letzten Arbeitsschritt kann man die Stärke der Vignettierung einstellen, deren Form man sehr intuitiv über den oben gezeigten Kreis mit seinen vier Anfassern bestimmt. Leider legt das Programm die Vignette nur dunkel an. Eine weiße Vignettierung ist nicht vorgesehen.

**Fazit:** Eine gute App für die Schwarzweißumsetzung ist gar nicht so leicht zu finden. Dramatic Black & White überzeugt mit guten Resultaten und einer klaren Benutzerführung.

- ➡ kontrastreiches Schwarzweiß
- ➡ Korn wirkt wie Bildrauschen



## Facetune

### Typ: Porträtretusche

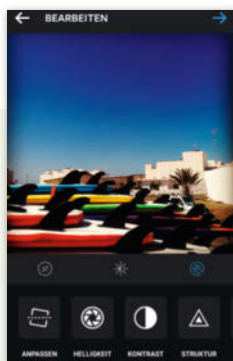
Facetune bringt alle wichtigen Werkzeuge für die Porträtbearbeitung mit. Zunächst wählt man eine Funktion aus, bekommt beim ersten Aufruf eine kleine Einführung und kann sich dann mit dem Werkzeug austoben, indem man einen Bereich bearbeitet, durch Ausblenden der Ebene das Ergebnis kontrolliert und mit dem Radierer den Effekt an ungewünschten Regionen zurücknimmt.

Facetune hellt Zähne und das Weiße im Auge auf, glättet Hautfalten, schärft Details, formt das Bild um, stempelt Pickel weg, trägt Hautfarbe auf, korrigiert rote Augen, malt Unschärfe ins Bild und ergänzt Filter sowie Bilderrahmen. Im Großen und Ganzen erledigt die App ihre Aufgabe gut. Der Aufheller und die Hautglättung arbeiten subtil, verbessern das Bild aber deutlich. Der Radierer hilft dabei sehr.

Die App korrigiert rote Augen absolut fehlerfrei, indem man den Pupillenbereich mit dem Werkzeug überlagert und dessen Größe anpasst. Auch der Klonstempel leistet gute Dienste, ist in der Bedienung aber etwas fitzelig. Die Gitterverzerrung reagiert eine Spur zu heftig auf Wischgesten. Effekte wendet das Programm deutlich zu stark an und die Rahmen wirken aufdringlich.

**Fazit:** Facetune versammelt die klassischen Werkzeuge für die Porträtbearbeitung und macht seine Sache im Großen und Ganzen gut. Die Effekte überlässt man aber lieber einer anderen App.

- ➡ umfangreiche Porträtbearbeitung
- ➡ unbrauchbare Effekte



## Instagram

### Typ: Soziales Netzwerk

Die Instagram-App füttert das gleichnamige soziale Netzwerk über die integrierte Kamera-App oder aus dem Speicher des Smartphones. Auf einem iPhone 4s oder höher speichert Instagram Fotos in einer Auflösung von 2048 × 2048 Pixeln. Unter Android variiert die Auflösung. In der Web-Ansicht hat Instagram die Auflösung 2015 von 640 auf 1080 Pixel Kantenlänge angehoben.

Instagram hat das quadratische Format wieder populär und zu seinem Markenzeichen gemacht – ein anderes Seitenverhältnis lässt die App nicht zu. Die dreigeteilte Bildbearbeitung schlägt zunächst 26 Fertigeffekte vor. Die Liste lässt sich erweitern, reduzieren oder umsortieren. Anschließend holt der Lux-Filter Schatten hervor, dunkelt Lichter ab und erhöht den Kontrast. Im dritten Schritt kümmert sich die App um Ausrichtung, Helligkeit, Kontrast, Sättigung, Schatten, Hervorhebung, Vignettierung, Tilt-Shift und Schärfe.

Die Bilder landen auf Instagram und wahlweise zusätzlich auf Facebook, Twitter, Tumblr oder Flickr. Zusatz-Apps ergänzen weitere Funktionen: Die App Layout fügt Fotos zu Collagen zusammen. Die neue App Boomerang erstellt Cinemagramme, eine Mischform aus Foto und Video mit einem bewegten Element.

**Fazit:** Instagram setzt den Standard für Bildeffekte im Netz und in Foto-Communities. Wer seinen Alltag im Bild mit Freunden teilen will, kommt daran kaum vorbei.

- ↑ exzellente Effekte
- ↑ große Community



## Lightroom Mobile

### Typ: Raw-Entwickler

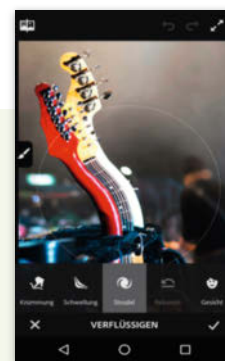
Lightroom Mobile ist vor allem für Nutzer interessant, die ihre Foto-Bibliothek des Desktop Lightrooms auch auf dem Mobilgerät bearbeiten möchten und umgekehrt. So landen Smartphone-Fotos im Lightroom-Katalog auf dem PC oder Mac. Dort freigegebene Sammlungen erscheinen wiederum in Lightroom Mobile in Form von DNG-Stellvertretern, die zwar in der Auflösung, nicht aber in der Farbtiefe reduziert sind. So kann man sie mit Lightroom-Werkzeugen auf dem Tablet oder Smartphone bearbeiten und anschließend am kalibrierten Monitor auf dem Desktop abstimmen.

Lightroom Mobile bearbeitet die Grundeinstellungen und synchronisiert auch sie mit der Desktop-Version. Die App hat außerdem die Paletten Teiltonung, Gradationskurven, Dunstentfernung und den HSL-Dialog bekommen. Damit bietet die App den Löwenanteil der Funktionen des Entwicklungsmoduls aus Lightroom CC.

Die App selbst nimmt DNG-Raw-Dateien auf, wenn das Smartphone das Camera2-API bereitstellt. Das sind etwa das Google Nexus 5 und 6, das Samsung Galaxy S6 und S7 sowie das LG G4 und G5. Mit der Zeit dürften mehr Geräte folgen, die Raw-Aufnahmen unterstützen.

**Fazit:** Lightroom Mobile bietet die beste Raw-Entwicklung, die es auf Mobilgeräten derzeit gibt. Wer die Desktop-Version nutzt, kann beides verbinden.

- ↑ sehr guter Raw-Entwickler
- ↑ kooperiert mit Lightroom



## Photoshop Fix

### Typ: Fotokorrektur

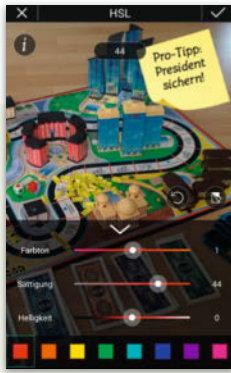
Adobes Fotokorrektur-App enthält Photoshop-Werkzeuge, die vor allem bei der Beauty-Retusche zum Einsatz kommen. Dazu zählen das Bereichsreparatur- und das Ausbessern-Werkzeug, der Verflüssigen-Filter sowie Abwedler und Nachbelichter. Außerdem beschneidet, dreht und spiegelt die App, sie korrigiert Belichtung, Kontrast, Sättigung, Tiefen und Lichter mit Lightroom-Werkzeugen und legt eine Vignettierung übers Bild. Um Photoshop Fix nutzen zu können, ist lediglich eine kostenlose Adobe-ID nötig. Creative-Cloud-Kunden profitieren vom direkten Export in den CC-Web-Speicher beziehungsweise nach Photoshop oder Lightroom.

Mit dem Verflüssigen-Filter lassen sich Bilder ausbeulen und verformen, etwa um Nasen zu korrigieren. Das funktioniert per Fingergeste erstaunlich gut, wenn auch längst nicht so präzise wie mit dem Grafiktablett am Desktop. Auch Bereichsreparatur und Ausbessern leisten gute Arbeit. Im Unterschied zu vielen anderen Apps lässt sich die Wirkung der Werkzeuge per Regler zurücknehmen, um sie subtiler zu gestalten.

Weitere Fingerpinsel tragen Farbe auf oder wenden Einstellungen für Sättigung, Schärfe, Unschärfe, Aufheller oder Abdunkler an. Auch diese leisten gute Arbeit.

**Fazit:** Mit Photoshop Fix ist Adobe ähnlich wie bei Lightroom die Portierung professioneller Funktionen aufs Mobilgerät gelungen.

- ↑ professionelle Funktionen
- ↑ Zusammenarbeit mit Photoshop



## PhotoDirector

### Typ: klassische Bearbeitung

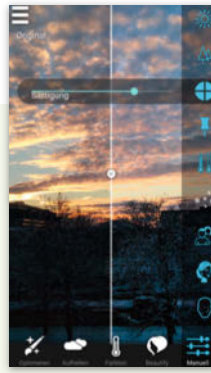
Cyberlink PhotoDirector bringt Funktionen klassischer Bildbearbeitung aufs Mobilgerät. Die Werkzeuge sind beschriftet und von links nach rechts angeordnet. Zunächst bearbeitet die App Ausrichtung und Beschnitt. Unter Anpassen finden sich Weißabgleich mit Grauwertpipette, Gradationskurven, Tonwertkorrektur und HSL-Dialog mit acht Farbbändern für Farbton, Sättigung und Helligkeit. Abgesehen vom destruktiven Tonwert-Regler leisten alle Werkzeuge, was sie versprechen.

Die Entfernen-Funktion retuschiert automatisch markierte Bereiche, was bei gleichmäßigem Hintergrund gut funktioniert. Die gut 50 Effekte taugen wenig. Besser wirken die vielen Texturen für Lichtlecks, Dreck, Kratzer und Blendenflecken, die sich in der Intensität reduzieren lassen. Ein Weichzeichner lässt sich als Vignette oder in Tilt-Shift-Art anwenden.

In den Niederungen der App finden sich etliche eher aufdringliche Effekte wie Sprechblasen, Spiegelung, Rahmen und Passepartouts sowie Szenen, die das Foto auf den Times Square verfrachten, und Überlagerungen mit Blitzen und Sonnenuntergängen.

**Fazit:** PhotoDirector bringt das Desktop-Konzept aufs Smartphone. Das wirkt nicht immer gelungen, empfiehlt sich aber für Nutzer, die auf Gradationskurven und Co. nicht verzichten mögen.

- ↑ klassische Funktionen zur Bildbearbeitung
- ↓ teils schlecht an Mobilgeräte angepasst



## Perfectly Clear

### Typ: Bildkorrektur

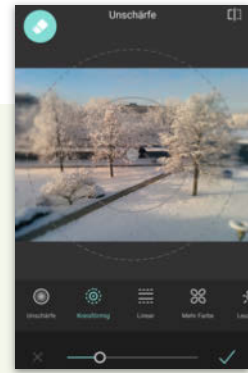
Perfectly Clear korrigiert die Lichtsituation automatisch und bringt eine Kamera mit, die auf Wunsch Porträts nur bei geöffneten Augen und Lächeln schießt sowie Panorama- und HDR-Bilder erstellt. Die Panorama-funktion setzt gute Lichtverhältnisse voraus, sonst macht sie wenig Freude.

Nach Öffnen eines Fotos optimiert die App Licht- und Farbverhältnisse. In der Regel führt das zu einem subtil verbesserten Foto. Wenn das Resultat nach dem ersten Durchgang noch nicht gefällt, kann man die Korrekturprofile Optimierte, Aufhellen, Farbton und Beautify durchprobieren.

Der manuelle Modus bietet gut beschriftete Korrekturregler für zwei Aufgaben: allgemeine Bildkorrektur mit Reglern für Belichtung, Kontrast, Sättigung, Schärfe, Farbton und Rauschen entfernen sowie Porträtretusche mit Reglern für Hautfarbe, Glätten, Schönheitsfehler entfernen, Blitz entfernen, Gesichtsverschönerung, Zähne aufhellen, Augen verschönern, Augen vergrößern und Augenringe entfernen. Original und bearbeitete Version trennt die App über einen Vorhang, den man einfach per Fingergeste verschieben kann. Das fertig bearbeitete Bild lässt sich auf Facebook, Twitter, Amazon Cloud Drive oder via E-Mail veröffentlichen und an installierte Apps weitergeben.

**Fazit:** Perfectly Clear beschränkt sich auf Fotokorrektur und führt mit einem klaren Bedienkonzept zu guten Ergebnissen.

- ↑ gute Korrektur
- ↓ häufig zu vorsichtig



## Pixlr

### Typ: Fotoallrounder

Die aussagekräftig beschrifteten Werkzeuge von Pixlr verteilen sich auf fünf Kategorien. Die sinnvolle Unterteilung in Bildkorrektur, selektive Anpassung, Effekte, Rahmen und Text erschließt sich schnell.

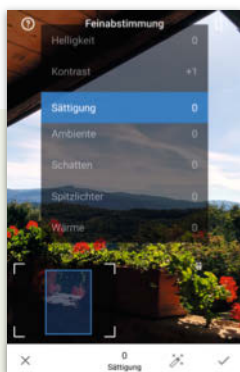
Die Korrektur umfasst neben Belichtung, Kontrast, Lichtern, Schatten und Sättigung auch sinnvolle Exoten wie Lebendigkeit und Klarheit. Leider berechnet die App das Resultat nicht live, sondern erst, wenn man den Regler losgelassen hat. Außerdem erzeugt die Korrektur harsche und destruktive Ergebnisse. Sehr flüssig funktioniert hingegen das Werkzeug zum Drehen und Spiegeln.

Die selektive Anpassung arbeitet Schatten und Lichter gut und dank weicher Kante subtil heraus. Witzig ist der Modus zum selektiven Verpixeln, etwa von Gesichtern. Die zahlreichen Effekte zum Kolorieren, Verblässen und Weichzeichnen wirken interessant und dezent – zumindest, wenn man sie etwas zurücknimmt. Hinzu kommen hochwertige Texturen mit Rahmen, Kratzern, Lichtlecks, Boken und Vignettierung. Das Textwerkzeug bietet detaillierte Optionen für Fonts und Farben. Das Bild wandert danach zu Facebook, Twitter, Instagram oder an eine andere Apps.

**Fazit:** Pixlr bietet viele Funktionen und gute Effekte, die man sich aber erarbeiten muss. Dabei hilft die Beschriftung der Werkzeuge.

- ↑ vielseitige Effekte
- ↓ destruktive Bildkorrektur





## Snapseed

### Typ: Effektmaschine

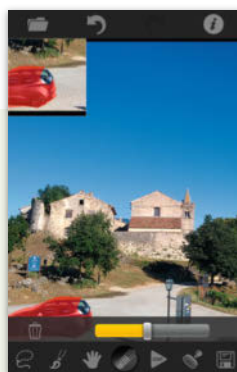
Snapseed stammt ursprünglich vom Spezialisten für Bildbearbeitung Nik. Nach dem Kauf hat Google einige Funktionen der Software in Android integriert. Nach Auswahl einer Funktion wählt ein Wisch von oben nach unten die Regler aus, ein Wisch von links nach rechts stellt den Wert ein.

Die Feinabstimmung von Belichtung, Kontrast, Schatten, Lichtern und Farbe, die Ausrichtung des Horizonts und die Bildschärfe passt Snapseed mit hochwertigen Algorithmen an. Die Lichtsituation korrigiert die App auf Wunsch automatisch. Einige Funktionen finden sich in anderen Apps nicht. Der Strukturregler etwa hebt lokale Kontraste an und erzeugt einen interessanten Effekt. Mit einem Korrekturpinsel lassen sich Bildbereiche gezielt aufhellen oder abdunkeln. Kontrollpunkte, eine spezielle Nik-Technik, bearbeiten Helligkeit, Kontrast oder Sättigung selektiv.

Die hochwertigen Effekte tragen aussagekräftige Titel wie Drama, Grunge, Fokuseffekt, Retrolux oder Vintage. Mit vielen Parametern lassen sie sich detailliert und mit variabler Stärke anwenden. Export nach Facebook und Co. sucht man vergeblich; die App speichert das Bild nur im Smartphone.

**Fazit:** Snapseed bietet hochwertige Effekte und Werkzeuge für die Bildkorrektur. Das eigenwillige Bedienkonzept macht Spaß und führt zu guten Bildern.

- 👍 gutes Bedienkonzept
- 👍 hochwertige Algorithmen



## TouchRetouch

### Typ: Objektretusche

AVDA, der Entwickler von TouchRetouch, hat der Versuchung widerstanden, unnötigen Klimbim zu integrieren. Die App retuschiert unerwünschte Objekte in Fotos – weiter nichts.

Zunächst markiert man im geöffneten Foto das störende Motiv. Dazu stehen entweder Pinsel und Radierer oder das Lasso-Werkzeug zur Verfügung. Das wirkt hemdsärmelig, allerdings muss ein Objekt für die Retusche nicht hundertprozentig exakt ausgewählt sein. Ein Druck auf Start rekonstruiert die markierte Stelle mit Material aus der Umgebung, was erstaunlich gut funktioniert. Sollte das Ergebnis den Ansprüchen nicht genügen, hilft ein Klonstempel aus. Das Bild lässt sich in den Telefonspeicher exportieren und an installierte Apps weitergeben. Veröffentlichung in sozialen Netzen ist nicht vorgesehen.

Unter Android 6 gelang es im Test nicht, aus der App heraus mit der Kamera-App ein Foto aufzunehmen. Beim Öffnen fragt die App, ob sie die Auflösung reduzieren soll. Soll sie nicht – besser wäre schnellere Bildverarbeitung, denn alles in allem reagiert sie etwas träge. So lässt sich unterm Strich einiges kritisieren; seinen eigentlichen Zweck erfüllt TouchRetouch allerdings.

**Fazit:** Die App TouchRetouch hat genau eine Funktion und die beherrscht sie: die Retusche von unerwünschten Objekten.

- 👍 gute Bildrekonstruktion
- 👎 langsame Verarbeitung



## VSCO

### Typ: Effekte und Community

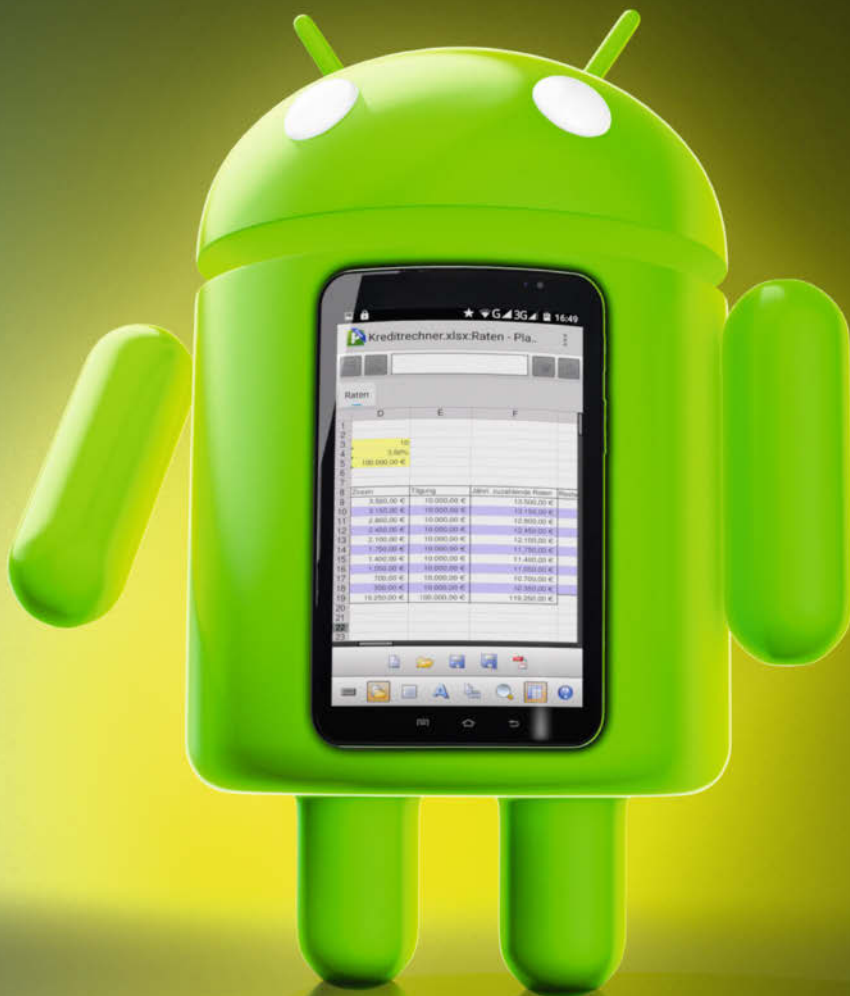
Auf den ersten Blick orientiert sich die Visual Supply Company an Instagram: VSCO besitzt eine einfache Kamera-App, wendet Effektfiter auf Fotos an und veröffentlicht sie auf einer Community-Seite. Die mit Namen wie B1, C2 oder G3 benannten Effekte lassen sich bei zu harter Umsetzung per Regler abschwächen. Schließlich kann man mit 16 Werkzeugen Belichtung, Kontrast, Schatten, Lichter, Ausrichtung, Schärfe, Sättigung und dergleichen bearbeiten. Dafür bieten diese je einen Regler. Die App exportiert Bilder, teilt sie auf Instagram, Facebook, Google+, versendet sie per E-Mail oder gibt sie an beliebige installierte Apps weiter.

Die eigene Community namens Grid verdient einen Blick. Anders als Facebook oder Instagram geht es hier nicht um Likes und Shares; man veröffentlicht lediglich sein Bild. Visual Supply will Interaktion schaffen, aber die Nutzer nicht zwingen, Spielchen um Aufmerksamkeit zu spielen.

Abgesehen von der Seitenleiste mit Einträgen für die Bibliothek oder den Shop kommt die App vollkommen ohne Text aus. Der Anwender muss also Icons interpretieren. Diese sind zwar formschön, offenbaren ihre Bedeutung aber erst nach etwas Beschäftigung mit der App.

**Fazit:** VSCO enthält alles Nötige für gute Farbeffekte. Die Community bietet Content ohne Spielchen.

- 👍 gute Farbeffekte
- 👍 Community ohne Likes



Dieter Brors

## Apps zum Schreiben, Rechnen und Präsentieren

Mit dem Smartphone hat man theoretisch unterwegs alle Infos griffbereit. In der Praxis braucht man gute Office-Apps, um E-Mail-Anhänge und Dokumente aus der Cloud lesen und bearbeiten zu können. Solche Apps müssen nicht einmal etwas kosten.

**D**ank ihrer großen Displays und der hohen Auflösung eignen sich aktuelle Smartphones besser als frühere Modelle, um Texte, Tabellen und Präsentationen jederzeit zu lesen und zu überarbeiten oder um Attachments aus der E-Mail-App heraus zu öffnen. Auf Dokumente, die bei einem Cloud-Dienst gespeichert sind, kann man von überall her zugreifen. Was man braucht, sind Office-Apps, die das ursprüngliche Erscheinungsbild getreu wiedergeben und die Dateien nach dem Bearbeiten verlustfrei wieder zurückspeichern. Wenn eine Smartphone-App eigenmächtig an der Formatierung herumfuscht oder Objekte, die sie nicht kennt, einfach eliminiert, kann sie das am PC mühevoll gestaltete Dokument unbrauchbar machen.

Damit der Anwender die Inhalte besser lesen kann, lassen sich die meisten Apps zwischen Lese- und Seitenlayout-Ansicht umschalten. Beim Betrachten blenden sie meist Fußnoten, Kopf- und Fußzeilen aus, manchmal auch Bilder. Den Text umbrechen sie automatisch am Displayrand. Im Seitenlayout kann man dagegen alle Inhalte so betrachten, wie sie auch auf Papier erscheinen.

## Kleines Display setzt Grenzen

Office-Apps eignen sich nicht nur zum Sichten von Dateien. Auf dem PC erzeugte Dokumente, Tabellen und Präsentationen lassen sich auch innerhalb der Apps formatieren. Zwar dürfte wohl niemand auf die Idee kommen, ein längeres Manuskript auf dem Smartphone einzutippen. In bestehenden Dokumenten kann man aber durchaus kleinere Korrekturen vornehmen, Bilder einfügen oder Formatierungen anpassen. Selbst große Smartphone-Displays setzen beim Gestalten Grenzen, da sich Elemente wie Bilder oder Textrahmen bei Weitem nicht so exakt wie am PC positionieren lassen – zumal Tastatur und Symbolleisten je nach App bis zur Hälfte des Bildschirms belegen, selbst wenn man das Smartphone hochkant hält. Der übliche Workflow sieht dann so aus, dass man auf dem Smartphone nur den Entwurf oder ein Groblayout erstellt und die weitere Gestaltung am PC vornimmt.

Wir haben die sechs gängigsten Office-Pakete für Android-Smartphones getestet. Docs To Go, Polaris Office und WPS Office vereinen Textprogramm, Tabellenkalkulation und Präsentationssoftware in einer einzigen App. FreeOffice Mobile, Google Docs und Microsoft Office setzen sich aus

einzelnen Apps zusammen, die man über Google Play einzeln installiert. Alle Apps lassen sich kostenlos installieren, manche laufen zunächst nur eingeschränkt und schalten den vollen Funktionsumfang erst nach Kauf einer Lizenz frei. Details zu den einzelnen Apps zeigt die Tabelle auf Seite 109.

## Starke Unterschiede

Als Testplattform diente ein unspektakuläres Elephone P8000 mit 5,5-Zoll-Display und Android 5.1. Schon im Funktionsumfang unterscheiden sich die Apps zum Teil wesentlich – unabhängig davon, ob sie etwas kosten oder sich gratis nutzen lassen. So beschränkt sich Docs To Go selbst nach Kauf der 12 Euro teuren Lizenz auf rudimentäre Bearbeitungsfunktionen.

Beim Bearbeiten bestehender Dokumente oder zum Anzeigen von E-Mail-Attachments kommt es darauf an, wie gut die Apps Dateien in den meist verbreiteten Dokumentformaten lesen und schreiben, also Word-, Excel- und PowerPoint-Dateien. Von einer Office-App sollte man heutzutage erwarten, dass sie auch Dateien im Open Document Format (ODF) öffnet und speichert, das unter anderem OpenOffice und LibreOffice verwenden und seit Jahren ein ISO-Standard ist. Von den getesteten Apps unterstützt jedoch nur FreeOffice ODF-Dateien. Wie gut der Dokumentaustausch funktioniert, haben wir anhand mehrerer Textdokumente, Tabellen und Präsentationen getestet – von denen einige recht komplex mit Fußnoten, Verzeichnissen und Animationen gestaltet waren.

## Fazit

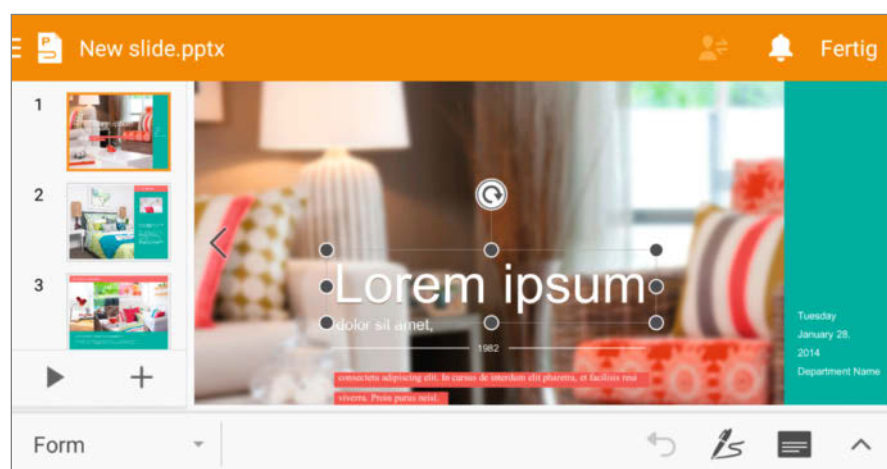
Für welches Paket man sich entscheidet, hängt letztendlich vom Einsatzzweck ab. Google Docs richtet sich vor allem an Nutzer von Googles Online-Office-Programmen, eignet sich aber nur zum Editieren einfacher Word-, Excel- oder PowerPoint-Dateien. Docs To Go wurde einst für kleine Displays entwickelt und zeigt Dokumente sehr kompakt an, unterdrückt aber viele Elemente. Bei dem geringen Funktionsumfang eignet sich die App zum Lesen und für kleinere Korrekturen.

Polaris Office bietet eine Vielzahl an Funktionen und sticht durch Besonderheiten wie das Vorlesen von Texten hervor. Derzeit mangelt es der App allerdings an Stabilität. Eine Alternative dazu bildet WPS Office. Wer Daten mit dem Smartphone erfasst, profitiert von der erweiterten Tastaturbelegung für Zahlen und Formeln, die in vergleichbarer Form keiner der Konkurrenten bereitstellt. Schwächen zeigen sich allerdings beim Bearbeiten von Microsoft-Office-Dateien.

Wer auf bestmögliche Kompatibilität zu Microsofts Office-Paket Wert legt, ist naturgemäß mit Microsofts Apps mit am besten bedient. Sie bieten alles Wichtige, was man auf dem Smartphone benötigt, und überzeugen durch eine sehr gute Bedienung. Die FreeOffice-Apps von SoftMaker stehen Microsofts Office-Apps in nichts nach. TextMaker, PlanMaker und Presentations arbeiten zuverlässig und gehen ebenfalls pfleglich mit Word-, Excel- und PowerPoint-Dateien um.

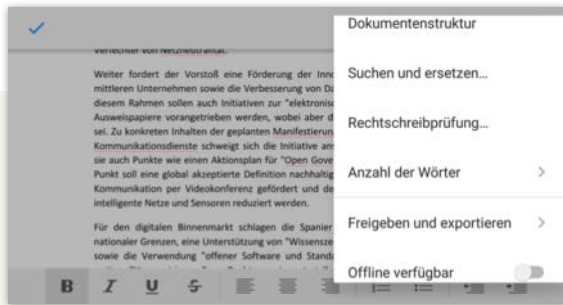
(db) **ct**

Download: [www.ct.de/w4su](http://www.ct.de/w4su)



Auf Smartphones lassen sich Bilder oder Textrahmen zumindest grob positionieren. Der Feinschliff muss aber am PC erfolgen.





## Google Docs

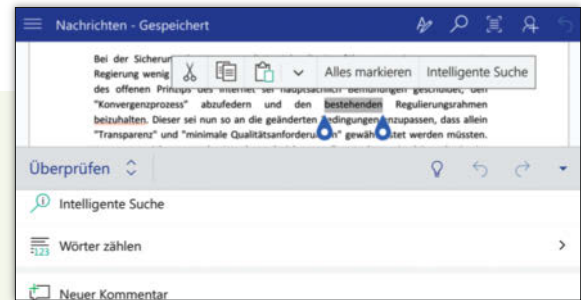
Google sieht seine Office-Apps als Ergänzung zum eigenen Online-Office. Um damit Word-, Excel- und PowerPoint-Dateien erzeugen und bearbeiten zu können, muss man dies in den Einstellungen aktivieren. Die Apps speichern automatisch in der Cloud, sichern Dokumente auf Wunsch aber zusätzlich auf dem Smartphone.

Die Oberflächen der Apps sind gut an Smartphones angepasst. Standardmäßig umbricht Google Docs den Text am Bildschirmrand. In Dokumenten, die vom PC aus im Word-Format auf Google Drive gespeichert wurden, fehlen dann allerdings Elemente wie Verzeichnisse, Kopf- und Fußzeilen oder Fußnoten. Sie werden erst in der Layout-Ansicht sichtbar und lassen sich nicht editieren.

Tippt man ins Dokument oder positioniert den Cursor, erscheint eine virtuelle Tastatur. Die Tabellenkalkulation blendet darauf eine zusätzliche Zeile mit wichtigen Zeichen zur Formeleingabe ein. Rechenfunktionen lassen sich per Dialog auswählen. Die App kennt nur englische Funktionsnamen. Google Präsentationen bietet elf Designs mit Feldern für Objekte wie Titel, Text und Aufzählungen. Über das Plus-Symbol in der Symbolleiste fügt man Textrahmen, Bilder, Tabellen oder Linien ein. Die App eignet sich zum Überarbeiten bestehender Folien oder um unterwegs eine neue Präsentation grob anzulegen.

Auf Kompatibilität zu Microsoft Office kommt es Google offenbar nicht an. In importierten Word-Dateien ändert Google Docs nicht nur das Layout, sondern mitunter auch die Schriftart. Nach dem Speichern bleibt vom Originallayout nicht viel übrig. Excel-Tabellen, die nicht zu komplex sind, lassen sich gefahrlos bearbeiten. Findet die Tabellen-App nicht unterstützte Elemente, warnt sie, dass diese entfernt werden, falls man die Tabelle bearbeitet.

- 🔴 schlechter MS-Office-Support
- 🔴 geringer Funktionsumfang



## Microsoft Office

Microsofts Office-Apps lassen sich auf Smartphones und kleinen Tablets mit einem kostenlosen Microsoft-Account nutzen; Tablets mit einer Display-Größe über 10 Zoll erfordern eine Office-365-Lizenz. Anders als die frühere Office-Mobile-App unterstützen die aktuellen Versionen auch Dropbox und den lokalen Speicher. Wenn man Office 2016 unter Windows benutzt und Smartphone und PC mit demselben Microsoft-Konto verknüpft, synchronisieren die Apps die Liste der zuletzt auf OneDrive verwendeten Dateien.

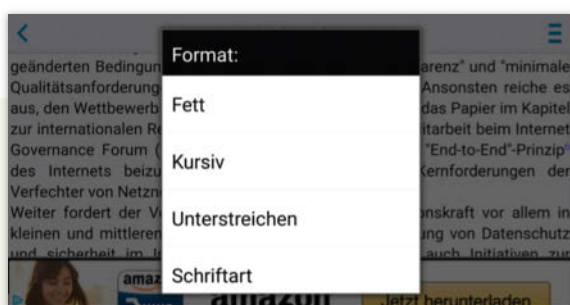
Die Struktur der App-Oberflächen lehnt sich an die der Desktop-Programme an, bietet allerdings deutlich weniger Einträge. Eine Symbolleiste präsentiert die wichtigsten Befehle zum Formatieren und Einfügen von Bildern, Tabellen und anderen Objekten. Antippen eines Pfeils klappt das eigentliche Menü auf.

Texte, Tabellen und Präsentationen lassen sich vielseitig bearbeiten. In Textdokumenten kann man sowohl Kommentare als auch Fußnoten anlegen oder Kopf- und Fußzeile bearbeiten. Die Rechtschreibprüfung läuft auf Wunsch im Hintergrund und lädt Wörterbücher nach Rückfrage aus dem Web.

Excel bietet einen riesigen Fundus an Rechenfunktionen. Der Auswahl-Dialog hilft mit kurzen Erklärungen bei der Formeleingabe. Diagramme lassen sich innerhalb der App erzeugen. Dazu stehen dieselben Typen wie in Excel 2016 zur Verfügung – inklusive Sunburst und Wasserfall. Andere elementare Funktionen fehlen in der Mobil-Version, etwa bedingte Formatierungen, die lediglich in bestehenden Tabellen angezeigt werden.

Präsentationen lassen sich jetzt auch auf dem Smartphone gestalten: Textrahmen und andere Objekte kann man beliebig auf der Folie platzieren, Seitenübergänge animieren – ein enormer Fortschritt gegenüber Microsofts früheren Office-Mobile-App.

- 🟢 durchdachte Bedienoberfläche
- 🟢 großer Funktionsumfang



## Docs To Go

Die Oberfläche von Docs To Go ist so gestaltet, dass Symbolleisten und Menü keinen Platz auf dem Display verschwenden. Nach Antippen des Befehl-Symbols in der Titelleiste öffnet sich ein Menü mit den Befehlen.

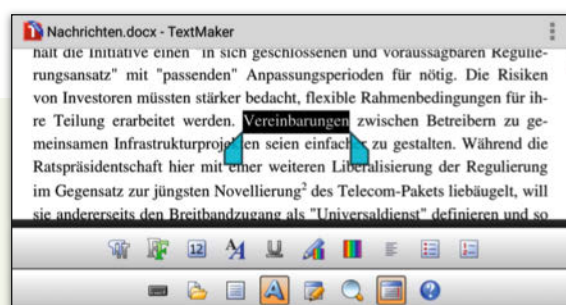
Der Funktionsumfang ist sehr eingeschränkt, reicht aber aus, um einfache Texte zu erfassen oder Tabellen zu berechnen. In bestehenden Word-Dokumenten lassen sich zwar Fußnoten editieren, aber keine neuen hinzufügen. Bilder erscheinen gar nicht auf dem Display, sondern werden nur als Platzhalter angezeigt. Solange man diese nicht löscht, bleiben die Objekte in der Datei erhalten. Eine Seitenlayout-Ansicht gibt es nicht.

Das Textmodul dient vor allem zum Betrachten vorhandener Dokumente sowie zur Eingabe von Notizen und kurzen Texten. Gestalten muss man die Dokumente später am PC.

In Tabellen hilft eine Liste aller Rechenfunktionen dabei, Formeln zusammenzustellen. Diese Liste ist allerdings nur alphabetisch sortiert und nicht in Kategorien aufgeteilt. Findet Docs To Go in importierten Tabellen nicht unterstützte Objekte, werden die Dateien nur zum Lesen geöffnet. Welche Elemente fehlen, verschweigt die App. Durch den Schreibschutz können sie aber wenigstens nicht kaputtgehen.

In Präsentationen lassen sich zwar Folien erstellen, man kann aber nur Text ohne jegliche Formatierung eingeben. Auf diese Weise lassen sich mit Docs To Go lediglich Rohfassungen von Präsentationen erzeugen, die man später am PC in einem Präsentationsprogramm gestalten muss. Bestehende PowerPoint-Präsentationen zeigt Docs To Go zwar an, spielt dabei aber keine Animationen ab. Ansonsten bietet die App nur rudimentäre Editierfunktionen in der Gliederungsansicht, die sich rein auf den Text beziehen.

- 👉 geht mit der Displayfläche sparsam um
- 👎 eingeschränkte Editierfunktionen



## FreeOffice Mobile

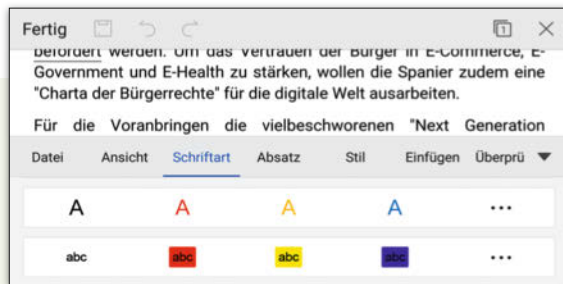
SoftMaker hatte die drei Apps TextMaker, PlanMaker und Presentations für Smartphones ursprünglich kostenpflichtig angeboten. Nach dem Erscheinen der Bezahlversionen mit dem Namenszusatz HD, die für Tablets optimiert sind, wurde das Grundpaket mit den ursprünglichen Apps unter dem Namen FreeOffice Mobile zur Gratisnutzung freigegeben. Diese werden weiterhin gepflegt und aktualisiert.

Die zweckmäßige Oberfläche der drei Apps ist gut auf Smartphone-Displays abgestimmt. Eine Symbolleiste stellt die wichtigsten Befehle bereit, ein Menü offenbart alle Funktionen. TextMaker öffnet auch Dokumente im Open Document Format (ODF); Nutzer von LibreOffice oder OpenOffice sollten aber nicht zu viel erwarten, denn der ODF-Support betrifft wirklich nur Texte.

Der Funktionsumfang reicht zwar nicht an den von Desktop-Programmen heran, dennoch lassen sich auch komplexe Textdokumente, Tabellen und Präsentationen bearbeiten. TextMaker kann Aufzählungen und Nummerierungen formatieren sowie Fußnoten und Verzeichnisse erzeugen. PlanMaker verwendet deutschsprachige Funktionsnamen, die mit denen von Excel weitgehend identisch sind. Vorhandene Diagramme zeigt es an, es kann aber keine erzeugen. Presentations stellt für Folien diverse Layouts bereit. Textfelder, Bilder und andere Objekte lassen sich beliebig verschieben, Animationen sind dagegen nicht möglich.

TextMaker, PlanMaker und Presentations zeigen auch komplexe Textdokumente, Tabellen und Präsentationen originalgetreu an: Bilder, Textfelder und Fußnoten stehen nach dem Bearbeiten an den ursprünglichen Stellen. Beim Import von Excel-Tabellen gehen allerdings Datenbalken und Sparklines, die über bedingte Formatierungen erzeugt wurden, verloren. PlanMaker zeigt dann eine Warnung an.

- 👉 hohe Geschwindigkeit
- 👉 guter MS-Office-Support



## WPS Office

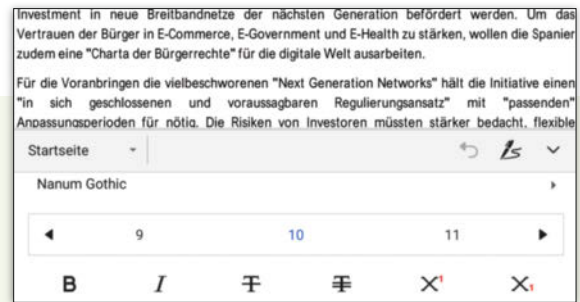
Auch WPS Office vereint alle Komponenten in einer App. Neu angelegte Dateien speichert es in den aktuellen Microsoft-Formaten, liest und schreibt aber auch die alten Binärformate. Außer den großen Cloud-Diensten lassen sich beliebige WebDAV-Server als Speicherort einbinden.

Hält man das Smartphone hochkant, belegen die Symbole zu den Menüeinträgen das halbe Display. Den Dokumentinhalt, der vergrößert und mit automatischem Textumbruch angezeigt wird, kann man nicht skalieren: Zoomen mit zwei Fingern ist nicht möglich und auch im Menü gibt es keinen Zoom-Befehl.

In Texten kann man Kommentare, Tabellen oder Textrahmen einbetten sowie Kopf- und Fußzeilen bearbeiten. Bilder lassen sich zuschneiden, drehen und skalieren. Verzeichnisse und Fußnoten werden zwar angezeigt, aber nicht bearbeitet. In Präsentationen sind Objekte wie Textrahmen oder Bilder frei platzierbar und skalierbar. Zur Zahlen- und Formeleingabe in Tabellen – etwas knifflig aufgrund der englischsprachigen Funktionsnamen – stellt die App eine spezielle Tastatur bereit, wodurch das lästige Umschalten zwischen Text- und Zahlenbelegung entfällt.

Große DOCX-Dateien konnte WPS Office im Test nicht immer laden. Word-Elemente, die die App nicht kennt, gehen beim Speichern unwiederbringlich verloren. Beim Import von Excel-Tabellen stellt sie Diagramme zwar dar, platziert Beschriftungen aber falsch. Bedingte Formatierungen unterstützt WPS Office nicht, zeigt diese in Excel-Tabellen aber ebenso wie Datenbalken und Sparklines an. Animationen in PowerPoint-Präsentationen werden nicht nur angezeigt, sondern lassen sich sogar problemlos ändern.

- ↑ großer Funktionsumfang
- ↓ Probleme mit komplexen Word-Dokumenten



## Polaris Office

Der Einsatz von Polaris Office erfordert ein Konto beim Hersteller, das bei der kostenlosen Variante 15 GByte Platz auf dessen Cloud-Speicher bereitstellt. Dazu gibt es ein monatliches Datenvolumen von 1 GByte – eine 10 MByte große Datei kann man damit bis zu 100 Mal bearbeiten. Bei Erreichen des Limits schaltet Polaris die App bis zum nächsten Monat in einen Lesemodus.

Die Pro-Version ohne Beschränkung kann man für monatlich 6 Euro oder jährlich 60 Euro mieten. Sie ist auf bis zu 10 Mobilgeräten und bis zu 5 PCs nutzbar. Im Test konnte die Windows-Version von Polaris Office allerdings nicht überzeugen (siehe c't 8/16, S. 52).

Die App bearbeitet in Texten Kopf- und Fußzeilen, fügt Seitenzahlen ein und unterstützt Tabellen, Kommentare, Hyperlinks und Lesezeichen; Fußnoten bleiben der Pro-Version vorbehalten. Bilder kann man einrahmen oder durch Effekte wie Neon-Licht verfremden. Auf Wunsch liest Polaris Office Texte vor, was erstaunlich gut und verständlich gelingt.

In Tabellen funktioniert die Auswahl von Rechenfunktionen ähnlich wie in der Excel-App, es fehlt jedoch jegliche Beschreibung. Bedingte Formatierungen heben Zellen je nach Wert farbig hervor oder erzeugen Datenbalken oder Symbole wie in neueren PC-Versionen von Excel.

Folien lassen sich komfortabel gestalten, Seitenübergänge einzeln animieren. Beim Vorführen ist man nicht auf das Smartphone-Display beschränkt – Polaris Office streamt Präsentationen wahlweise auf ein TV-Gerät mit angeschlossenem Chromecast-Stick.

Im Test hinterließ die App trotz des großen Funktionsumfangs einen schalen Beigeschmack: Beim Versuch, umfangreichere Dokumente zu laden, stürzte sie immer wieder ab.

- ↑ einige exklusive Funktionen
- ↓ mangelnde Stabilität



## Office-Apps für Android-Smartphones

Produkt	Docs To Go 4.0	FreeOffice Mobile 2012	Google Docs 1.6	Microsoft Office 16.0	Polaris Office 7.2.8	WPS Office 9.7.3
Hersteller	Dataviz, www.dataviz.com	SoftMaker, www.softmaker.de	Google, www.google.de	Microsoft, www.microsoft.de	Polaris Office Corp., www.polarisoffice.com	Kingsoft Software, www.kingsoftstore.com
<b>Allgemein</b>						
Systemvoraussetzungen	Android 4.0 und höher	Android 2.2 und höher	Android 4.1 und höher	Android 4.0 und höher	Android 4.0 und höher	Android 4.0 und höher
Sprache	Deutsch	mehrsprachig (17 Sprachen)	Deutsch	Deutsch	Deutsch	Deutsch
Speicherbedarf	36,4 MByte	56 MByte	354 MByte	259 MByte	143 MByte	115,0 MByte
Cloud-Speicher	Dropbox, Google Drive, Box, OneDrive	Dropbox, Evernote, Google Drive, OneDrive	Google Drive	Dropbox, OneDrive, SharePoint	Amazon Cloud Drive, Box, Dropbox, Google Drive, OneDrive, Polaris Cloud, Sugar-Sync, ucloud, WebDAV	Box, Dropbox, Google Drive, beliebige WebDAV-Server
<b>Textbearbeitung</b>						
Dateiformate	doc, docx	doc, docx, odt, rtf, tmd u. a.	gdoc, doc, docx	doc, docx	doc, docx, gdoc	doc, docx
Dokumentvorlagen	–	✓	–	✓	✓	✓
Stilvorlagen	–	✓	✓	✓	✓	✓
Nummerierungen/ Aufzählungen	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓	✓/✓
Tabellen	✓	✓	✓	✓	✓	✓
Bilder	–	✓	✓	✓	✓	✓
Kopf-/Fußzeilen	–/–	✓/✓	–/–	✓/✓	✓/✓	✓/✓
Fußnoten anzeigen/ editieren	✓/✓	✓/✓	✓/–	✓/✓	✓/✓	✓/–
Verzeichnisse anzeigen/ erzeugen	✓/–	✓/✓	✓/–	✓/–	✓/–	✓/–
Suchen/Ersetzen	✓/✓	✓/✓	✓/✓	✓/–	✓/✓	✓/✓
Rechtschreibprüfung	✓	✓	✓	✓	–	✓
Änderungen nachverfolgen	–	✓	✓	✓	–	✓
Besonderheiten	–	Änderungen nachverfolgen, automatische Sicherung, Feldvariablen, Autokorrektur, Fotos über Kamera einfügen, PDF-Export	Fotos über Kamera einfügen	Dokumentvorlagen, Dateifreigabe	Bildeffekte, Dokumentvorlagen, Fotos über Kamera einfügen, Diagramme, Freihandzeichnungen, Kommentare, Lesezeichen, PDF-Export, Text vorlesen	Lesezeichen, Feld-Variablen für Seite und Datum
<b>Tabellenkalkulation</b>						
Dateiformate	xls,.xlsx	pmd, pmdx, sdc, xls,.xlsx u. a.	gsheet,.xlsx	xls,.xlsx	gsheet, xls,.xlsx	xls,.xlsx
Fenster fixieren	✓	✓	–	✓	✓	✓
Zellformate (Kategorien)	10	10	10	10	10	12
Rechenfunktionen	111	330	290 <sup>2</sup>	446	231 <sup>2</sup>	296 <sup>2</sup>
Sortieren	✓	✓	–	✓	✓	✓
Suchen/Ersetzen	✓/–	✓/✓	✓/✓	✓/–	✓/✓	✓/✓
Diagramme anzeigen/ erzeugen	✓/–	✓/–	✓/✓	✓/✓	✓/✓	✓/✓
Besonderheiten	–	Änderungen nachverfolgen, Autokorrektur, Formelanzeige, PDF-Export	Kommentare, Notizen	Dokumentvorlagen, Dateifreigabe	Bildeffekte, Dokumentvorlagen, Fotos über Kamera einfügen, Freihandzeichnungen	zusätzliche Tastaturbelegung zur Zahlen- und Formel-Eingabe, Pivot-Tabellen
<b>Präsentation</b>						
Dateiformate	ppt, pptx	ppt, pptx, prd	gslides, pptx	ppt, pptx	gslides, ppt, pptx	ppt, pptx
Gliederungsansicht	✓	✓	–	–	–	–
Seitenvorschau	✓	✓	✓	✓	✓	✓
Folien duplizieren	✓	✓	–	–	–	✓
Animationen	–	✓ <sup>1</sup>	–	✓	✓	✓
Notizen	✓	✓	✓	✓	✓	✓
Besonderheiten	–	automatische Sicherung, Änderungen nachverfolgen, Autokorrektur, Designs, PDF-Export	Designs, Kommentare, Chromecast-Übertragung	Dokumentvorlagen, Dateifreigabe	Bildeffekte, Dokumentvorlagen, Fotos über Kamera einfügen, Freihandzeichnungen, Chromecast-Übertragung	Freihandzeichnungen, übers WLAN abspielen
<b>Bewertungen</b>						
Textbearbeitung	⊖	⊕⊕	○	⊕⊕	○	⊕
Tabellenkalkulation	⊖	⊕⊕	○	⊕⊕	○	⊕
Präsentation	⊖⊖	⊕⊕	⊖	⊕⊕	○	○
Bedienung	○	⊕⊕	⊕	⊕⊕	⊕	⊕
Unterstützung von MS-Office-Dateien	⊖	⊕	⊖⊖	⊕⊕	⊖	⊖⊖
Preis	kostenlos, 12 € (Premium)	kostenlos	kostenlos	kostenlos	kostenlos, 6 €/Monat oder 60 €/Jahr (Pro)	kostenlos
<sup>1</sup> nur Darstellung, nicht editierbar <sup>2</sup> nur englischsprachig						
⊕⊕ sehr gut    ⊕ gut    ○ zufriedenstellend    ⊖ schlecht    ⊖⊖ sehr schlecht    ✓ vorhanden    – nicht vorhanden    k. A. keine Angabe						

Christian Kausche

# Kostenlose Filemanager ohne Werbe-Overkill

Viele der bisher beliebten Filemanager wie Astro oder ES Datei Explorer nerven inzwischen nur noch mit ihren Werbeeinblendungen. Zeit für die Suche nach einem neuen Lieblings-Tool zur Dateiverwaltung unter Android.

Filemanager helfen beim lästigen Verwalten von Dateien und umgehen die eine oder andere Schwäche einiger Apps. Sie öffnen Video-, Musik-, Bild- und Textdateien, auch lassen sich Dateien mittels der Suche schnell finden. Doch die bisherigen Lieblinge der Redaktion sind seit einigen Updates mit Werbung zugekleistert oder stopfen die Benachrichtigungsliste mit nutzlosen Hinweisen voll.

Natürlich reagieren die Entwickler lediglich auf die mangelnde Zahlungsbereitschaft der Nutzer – rund 5 Euro für Astro Pro, 3 Euro für ES File Explorer –, schließlich können sie ihren Lebensunterhalt nicht alleine von guten Play-Store-Bewertungen bestreiten. Doch bei allem Verständnis haben wir uns auf die Suche nach kostenlosen und werbefreien Filemanagern gemacht. So kommt auch der Gelegenheitsnutzer zu seinem Tool, ohne sich im Tracking- und Profiling-Netz der Werbeindustrie zu verheddern.

Dutzende Filemanager existieren im Play Store, doch nur wenige glänzen durch großen Funktionsumfang, einfache Bedienbarkeit und weitgehende Werbefreiheit. Drei blieben schließlich übrig: Der schon von Windows bekannte Total Commander, die Fairphone-2-Nutzer bekannte Open-Source-App Amaze File Manager sowie die App namens Dateimanager+ vom Hersteller Flashlight+Clock.

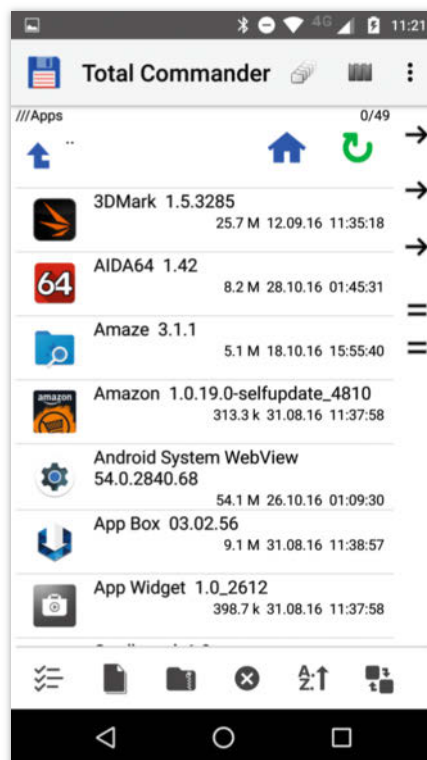
Gut gefiel uns auch der FX File Explorer von NextApp, doch die kostenlose Version beherrscht keine Cloud-Zugriffe. Der beliebte „Datei Manager“ von Cheetah Mobile fiel aus dem Test, weil auch er inzwischen viel Werbung einblendet. Zudem lässt die Pro-Version an Bedienbar- und Übersichtlichkeit zu wünschen übrig. Letzteres gilt auch für den „Dual File Manager XT“, bei dem die Werbung wegkaufbar ist, sowie die retro-charmanten Ghost Commander und Far On Droid.

## Übersichtlich

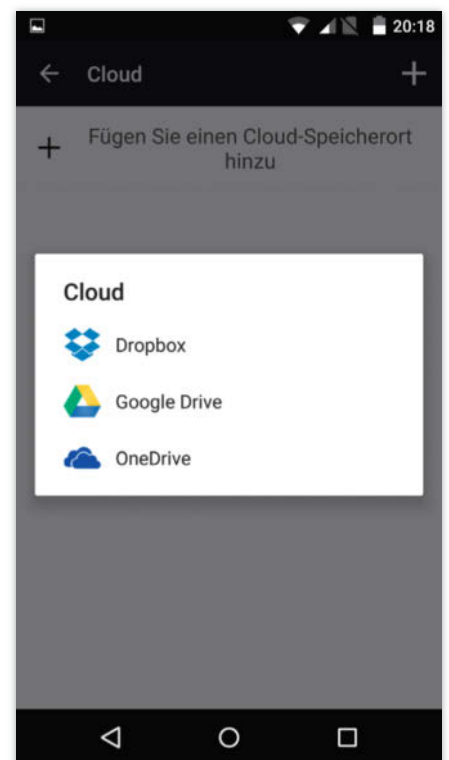
Amaze File Manager und Total Commander punkten mit zwei Fenstern und einem Home-Schalter, der den Anwender jederzeit zurück auf die Startübersicht führt. Amaze packt alle relevanten Ordner und Speichermedien ins Hamburger-Menü – das ist das Hauptmenü, das sich beim Tipp auf die drei Striche oben links öffnet. Noch anders der Dateimanager+: Er startet mit einer eher kleinen Liste von Ordnern und Medien, die sich nach und nach mit den meistbenutzten Ordnern füllt. Amaze und Total Commander spen-

dieren individuelle Farbgestaltungsmöglichkeiten der Bedienoberfläche, Ersterer auf moderne Art, Letzterer etwas altbacken.

Die Grundfunktionen wie Kopieren, Verschieben und Umbenennen erledigen alle drei einwandfrei. Auch öffnen sie alle Dateitypen mit einem internen Modul oder per externer App, etwa Musik-, PDF-, Bild- und Videodateien; für Textdateien haben sie einen Editor. Ein Manko beim Total Commander: Textdateien lassen sich nur auf komplizierte Weise über das Kontextmenü eines Ordners erstellen.



Alle drei haben ähnlich umfangreiche und nützliche App-Manager.



Dateimanager+ und Total Commander können viele Cloud-Dienste nutzen.

Die bei allen vorhandene Suche lässt sich beim Total Commander mit Parametern wie Dateigröße oder Bearbeitungsdatum verfeinern und bei Amaze als regulärer Ausdruck formulieren. Alle drei suchen standardmäßig im aktuellen Ordner samt dessen Unterzeichnissen. Um alle Medien auf einen Rutsch zu durchsuchen – internen Speicher, SD-Karte, USB-Stick –, wechselt man ins Root-Verzeichnis „/“; bei Amaze und Total Commander geht das einfach, beim Dateimanager+ etwas umständlich. Der Suchvorgang dauert dann allerdings sehr lange. Einen speziellen Modus mit mehr Möglichkeiten auf gerooteten Geräten bieten Amaze und Total Commander.

Alle drei Filemanager haben einen App-Manager, mit dem man beispielsweise Apps deinstalliert oder (bei Amaze und Total Commander) zum Play-Store-Eintrag der App springt. Auch können sie Apps sichern, wobei allerdings nur die APK-Datei kopiert wird, keine Konfigurationen oder sonstige Dateien. Kurios: Der App-Manager von Total Commander kann Apps nicht direkt starten, sondern nur über den Play Store.

## SD/USB und Cloud

MicroSD-Karten erkennen alle drei Filemanager sofort. Alle Dateioperationen funktionieren wie erwartet; bei neueren An-

droid-Versionen muss man der App einmalig den Zugriff gewähren. Bei allen drei geschieht das über denselben, etwas umständlich zu bedienenden Standard-Dialog von Android. Dasselbe gilt auch für USB-Medien, falls das Smartphone sie unterstützt. Der Total Commander benötigt dazu ein Plug-in, die anderen erkennen Sticks und Platten sofort. Welche Dateisysteme sie unterstützen, hängt vom Smartphone ab. Üblich ist FAT32, oft geht exFAT. Alleine Total Commander rüstet per Plug-in NTFS und HFS+ nach.

Dateimanager+ und Total Commander greifen auch auf Daten in der Cloud zu: Ersterer hat etwa FTP und SFTP eingebaut, ebenso Clients für Dropbox, Google Drive und Microsoft OneDrive. Letzterer benötigt dazu die Installation der entsprechenden Plug-ins. Amaze beherrscht hingegen nur SMB.

Anders herum erlauben Dateimanager+ und Amaze File Manager den Zugriff von außen aufs Smartphone: Sie haben einen FTP-Server eingebaut, der bei beiden sinnvollerweise nicht ständig läuft, sondern erst aufgerufen werden muss. Er zeigt die lokale IP samt Portnummer an, die man auf einem im gleichen LAN eingebuchten PC eintippt und dann Dateien lesen, löschen und aufs Gerät laden kann. Bei Amaze ist die Portnummer fest, Dateimanager+ er-

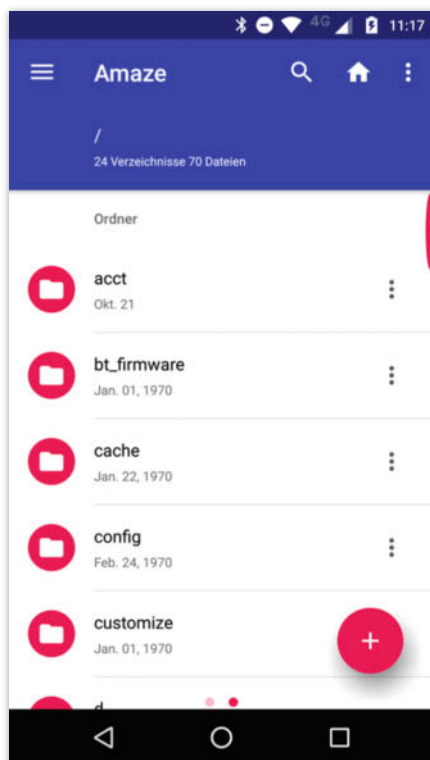
laubt eine individuelle oder zufällige Portnummer.

Dateimanager+ und Total Commander kommen mit weiteren Sonderfunktionen wie einem Musik-Player. Der des Total Commander hat einen individuell einstellbaren Equalizer mit Presets, er eignet sich durchaus generell zum Abspielen von Musikdateien. Des Weiteren lässt er sich mit Plug-ins beispielsweise um den Zugriff auf Cloud-Dienste erweitern.

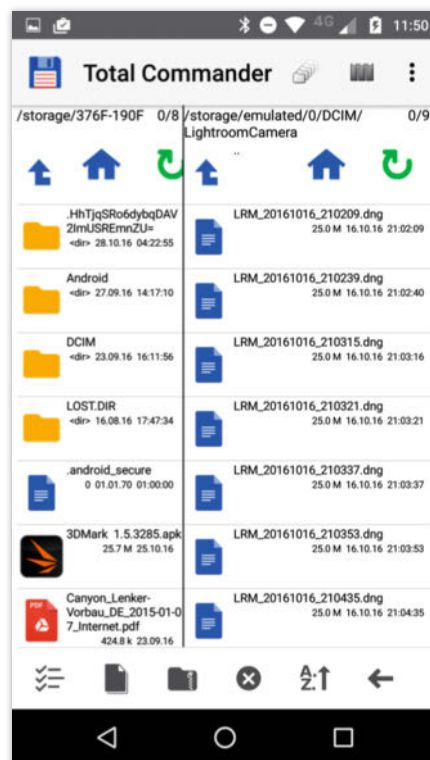
Wer sein Android-Gerät ohne Google-Account nutzt und daher keinen Zugang zum Play Store hat, findet die Installations-APKs von Amaze und Total Commander auch auf der Homepage der Entwickler.

## Fazit

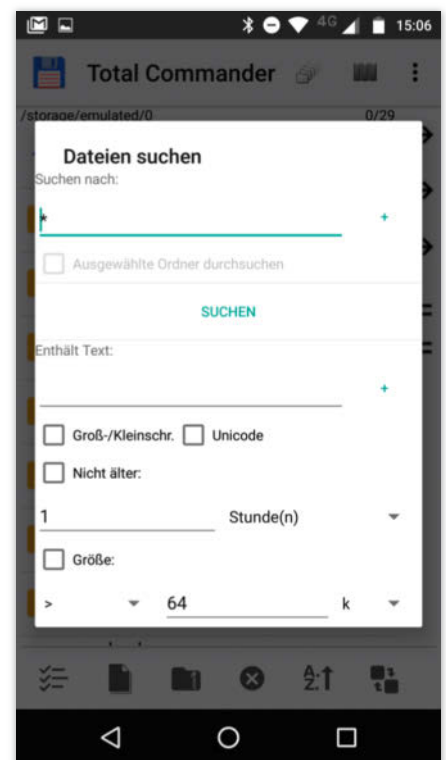
Alle drei Apps erfüllen ihren Zweck, unterscheiden sich aber in der Bedienbarkeit und dem Umfang der Sonderfunktionen. Für Minimalisten und Einsteiger eignet sich der Amaze File Manager. Fortgeschrittene finden beim Dateimanager+ interessante Funktionen wie die Cloud-Anbindung. Für Experten ist der Total Commander die beste Wahl, erfordert aber auch die langwierigste Einarbeitung etwa in die vielen Konfigurationsmöglichkeiten. Welche Sonderfunktionen Sie hier nutzen möchten, bestimmen Sie durch die Plug-ins selbst. (jow) **ct**



Beim Amaze deuten zwei Pünktchen unten das zweite Fenster an.

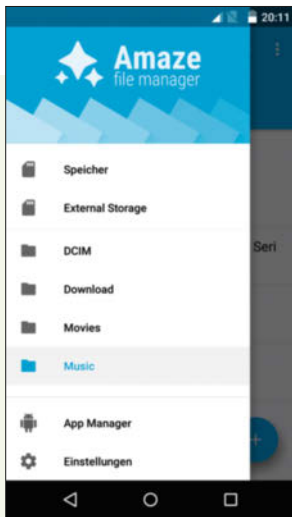


Total Commander zeigt auf Wunsch zwei Verzeichnisse nebeneinander.



Die vielseitigsten Suchparameter bietet Total Commander an.



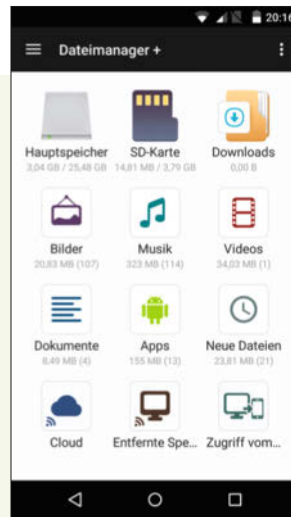


## Amaze File Manager

Dank umfangreichen Hamburger-Menüs, Home-Knopf und zwei Ordnerfenstern behält der Nutzer im Amaze File Manager stets die Übersicht. Die zwei Fenster stellt er nicht gleichzeitig nebeneinander dar, sondern der Nutzer wischt hin und her; zwei Punkte am unteren Fensterrand zeigen an, welches gerade aktiv ist. Angelegte Lesezeichen erscheinen direkt im Hamburger-Menü; durch langes Drücken löscht und ändert man sie. Wird das Menü zu voll, lässt sich der obere Teil scrollen. Zudem kann man auf dem Android-Home-screen Start-Icons anlegen, die direkt einen Ordner öffnen: lange auf den Ordner drücken und im Drei-Punkte-Menü oben rechts „Schnellwahl“ tippen. Auch für Dateien klappt das. In den Einstellungen lässt sich wählen, dass Amaze den Suchstring als regulären Ausdruck interpretiert.

Langes Drücken auf eine Datei oder einen Ordner startet den Markierungsmodus, über den man mehrere Dateien und Ordner auf einen Schlag etwa kopiert oder komprimiert. Für einzelne Dateien und Ordner öffnet man das Kontextmenü mit den drei Punkten rechts. Unter Android 4.4 beobachteten wir einen Fehler: Das Ausschneiden/Einfügen einer Datei von SD-Karte auf den internen Speicher misslang, danach war die Datei weg.

- modern, übersichtlich
- zwei Fenster
- auch ohne Zugang zu Google Play erhältlich
- wenige LAN/Cloud-Protokolle



## Dateimanager+

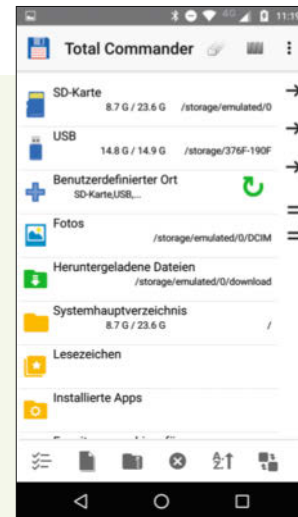
Auf der Startansicht zeigt Dateimanager+ Icons für wichtige Ordner, die erkannten Speichermedien und die Sonderfunktionen wie App-Manager und Cloud-Zugriffe.

Das Hamburger-Menü enthält eine Leiste mit Symbolen, über die man – ungewohnt kompliziert – zwischen drei Registerkarten umschaltet: meistbenutzte Ordner, Lesezeichen und Ordner-/Dateiverlauf. Wählt man darüber oder von der Startansicht aus einen Ordner an, ist das Menü allerdings nicht mehr sichtbar, sondern dort erscheint die Zurück-Schaltfläche. Darüber oder über die Home-Schaltfläche muss man erst zurück zur Startansicht springen, damit das Hamburger-Menü wieder auftaucht.

Ein Zugriff aufs Stammverzeichnis „/“ ist möglich, wenn man auf „Hauptspeicher“ geht und sich dann über den „Hoch“-Knopf oben rechts durch die Verzeichnisstruktur „/storage/emulated“ hangelt und eine Fehlermeldung zwischendurch ignoriert.

Die Funktionen wie Umbenennen oder Kopieren ruft man nicht über das Kontextmenü einer Datei oder eines Ordners auf, sondern man drückt lange. Das startet den üblichen Modus zum Markieren mehrerer Objekte, und erst dort erscheinen die gewünschten Funktionen auch für einzelne Objekte. Darunter findet man auch das Anlegen von Lesezeichen.

- viele Cloud-Dienste eingebaut
- teils hakelig
- wenige Konfigurationsoptionen

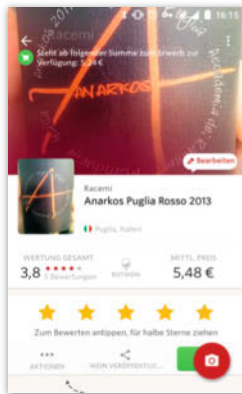


## Total Commander

Total Commander stammt von den gleichen Entwicklern wie die gleichnamige Windows-Version des Tools. Er arbeitet wie der Amaze File Manager mit zwei Fenstern; anders als dort kann man aber eine gleichzeitige Ansicht beider Fenster aktivieren, wahlweise auch nur im Querformat. Das jeweils aktive Fenster erscheint dann etwas verbreitert. Vor allem mit verkleinerter Schrift oder auf Tablets erweist sich das als praktikabel. In der Startansicht legt man Schnellzugriffe auf viel genutzte Ordner an und sammelt wichtige Dateien im Ordner Lesezeichen. Der merkwürdigen Speicherverwaltung von Android geschuldet, zeigt Total Commander den internen Speicher als „SD-Karte“ und die SD-Karte auf machen Geräten als „USB“ an.

Zusätzliche Funktionen lassen sich per Plug-ins vom Entwickler und von Drittherstellern nachrüsten: der Zugriff auf andere Rechner per FTP, SFTP, SMB und WebDAV etwa, die Kopplung zweier Smartphones per WLAN oder das Anbinden von Cloud-Diensten. Eines der beiden USB-Plug-ins liest auch Medien in Apples HFS+-Format. Der Download der Plug-ins findet im Google Play Store statt, zwischendurch wird man aber auf eine Seite mit abgelaufenem SSL-Zertifikat geführt.

- zwei Fenster, optional gleichzeitig
- vielseitige Cloud-Anbindung
- viele Suchparameter
- auch ohne Zugang zu Google Play erhältlich
- etwas altbackene Oberfläche



## Gute Weine finden

Die riesige Auswahl an Weinen fordert selbst Kenner heraus. Vivino-Nutzer scannen das Etikett und sehen sofort die Bewertung der Community.

Nach eigenen Angaben hat Vivino über 22 Millionen Nutzer und eine dementsprechend große Datenbank zu bieten. Stichproben im Weinladen und Supermarkt zeigten im Test, dass etliche Weine abgedeckt sind. Die ortsbezogene Suche listet das Angebot von Supermärkten und Restaurants in der Nähe auf. Schließlich kann man sich mit anderen Vivino-Nutzern verbinden und in der App Erfahrungen austauschen.

Das Basisangebot von Vivino ist kostenlos. Ein Abo für 5 US-Dollar im Monat gewährt unter anderem Zugriff auf die Parker-Punkte des gleichnamigen Weinkritikers und seiner Redaktion. Die Vivino-Redaktion stellt auch selbst Listen aus Weinen zusammen und vermittelt zum Kauf an Händler weiter.

Weinliebhaber stehen vor dem Problem, sich zu merken, was schmeckt. Vivino bietet eine gute Alternative zum Flaschensammeln. Nicht zuletzt sind die Nutzerbewertungen äußerst hilfreich.

Vivino nutzt Technik des OCR-Spezialisten Abbyy. Daher reicht es, ein Weinetikett oder die Weinliste eines Restaurants zu fotografieren – den Rest erledigt die App. Im Nu erscheinen die Herkunftsdaten des Tropfens, sein Durchschnittspreis und die mittlere Bewertung der Vivino-Community. Weiter unten schlüsselt die App die Einzelbewertungen auf und zeigt größtenteils englischsprachige, aber auch deutsche Kommentare zum Wein. (akr)



## Video-Selfies mit Effekt

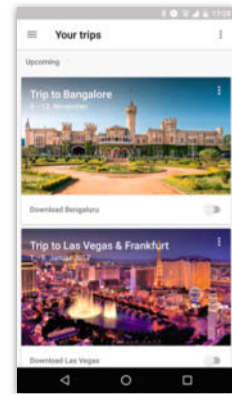
Die Video-Selfie-App MSQRD, spricht Masquerade, wendet erstaunlich realistische Masken in Echtzeit an.

Unter den Spaß-Apps ist MSQRD in aller Munde, nicht nur wegen seiner hochwertigen Live-Effekte, sondern auch weil Facebook das Start-up Anfang März '16 gekauft hat. Die Technik hielt sogar schon in das soziale Netzwerk Einzug. In-App-Käufe gibt es nicht – der Hersteller stellte MSQRD als Showcase der Technik vor.

Die App bietet einen Foto- und einen Video-Modus, zeigt nach dem Start das Bild der Frontkamera und bietet darunter eine Reihe Masken zur Auswahl an. In der Android-Version sind es bisher knapp 20, mehr sollen folgen. Unter den Effekten sind Affen-, Tiger- und Hundemasken, Clowns-, Totenkopf- und Tattoo-Make-up, ein alte Frau und ein Mann mit Schnurrbart. Auf dem iPhone gibt es zusätzlich IronMan, Darth Maul, den Joker aus „The Dark Knight“, Taucherbrillen, die Anonymous-Maske von Guy Fawkes und vieles mehr. Auch Face-Swapping, also der automatische Austausch zweier Gesichter vor der Kamera ist möglich.

Nach einem Fingertipp auf die Stopp-Taste oder nach maximal 30 Sekunden Aufnahme ist Schluss. Das Video landet im Telefonspeicher, lässt sich direkt auf Facebook veröffentlichen und an WhatsApp oder andere Programme weiterreichen.

Die App erkennt zuverlässig Merkmale wie Augen- und Mundpartie. Abgesehen von starren Masken setzen alle Effekte die Mimik dahinter erstaunlich gut um. (akr)



## Sicher am Ziel

Die Google-App „Trips“ stellt alle wichtigen Informationen für geplante Reisen zusammen – und sogar meist automatisch.

Sobald im Gmail-Postfach eine Buchungsbestätigung von Flügen oder Hotels auftaucht, legt Trips automatisch eine Reise an. In Reitern bietet sie praktische Informationen unter anderem zu Nahverkehr, Sehenswürdigkeiten, Museen, Restaurants und anderen Attraktionen an. Für viele Städte finden sich auch fertige Tagespläne mit mehreren Besichtigungsstationen. Abgerundet wird das mit grundsätzlichen Hinweisen zum Zielland – beispielsweise landestypischen Gepflogenheiten, Notrufnummern und Währungskurs. Auf Wunsch kann Trips alle Infos zur Reise vorab herunterladen.

Wer Google Trips ohne Gmail nutzen möchte, kann Reisen auch manuell hinzufügen, muss dann aber auf die Kontaktdaten des Hotels und die Flugzeiten verzichten. Ersteres lässt sich umgehen, indem man das Hotel einfach in Google Maps favorisiert, danach taucht es auch in Trips auf. Auf die eingebundenen Flugzeiten sollte man sich aber nicht blind verlassen: In unserem Test bekam die App weder eine Änderung der Abflugzeit eine Woche vor Reisebeginn noch einen Wechsel des Gates eine Stunde vor Abflug mit – ohne manuelle Kontrolle beim Check-in hätten wir den Flug also verpasst.

Davon abgesehen fanden wir Google Trips und insbesondere dessen Offline-Modus sehr praktisch. Ein Haken: Die App ist bislang nur in englischer Sprache verfügbar. (spo)

### Vivino

#### App für Wein-Liebhaber

Hersteller	Vivino, <a href="http://www.vivino.com">www.vivino.com</a>
Systemanf.	Android (var.), iOS ab 7.0, Windows ab 8
Preis	Basis <b>kostenlos</b> , Premium 5 US-\$ im Monat

### MSQRD

#### Video-Selfie-App

Hersteller	Masquerade, <a href="http://msqrd.me">msqrd.me</a>
Systemanf.	Android ab 4.3, iOS ab 8.4
Preis	<b>kostenlos</b>

### Google Trips

#### Reiseplanungs-App

Entwickler	Google, <a href="http://www.google.com/trips">www.google.com/trips</a>
Systemanf.	Android 4.1, iOS 8.0
Preis	<b>kostenlos</b>

# Für Wissenshungrige

## Ausgewählte Fachliteratur

shop.heise.de/fachliteratur



### Nitesh Dhanjani **IoT-Hacking**

In Zukunft werden Milliarden »Dinge« über das Internet miteinander verbunden sein. Hierdurch entstehen jedoch auch gigantische Sicherheitsrisiken. In diesem Buch beschreibt der international renommierte IT-Sicherheitsexperte Nitesh Dhanjani, wie Geräte im Internet of Things von Angreifern missbraucht werden können.

ISBN 9783864903434  
[shop.heise.de/iot-hacking](http://shop.heise.de/iot-hacking)

34,90 € >



### Peter A. Henning **Smart Home Hacks**

Machen Sie aus Ihrem Haus oder Ihrer Wohnung ein SmartHome! Dieses Buch zeigt den Weg, wie Sie mit Hausautomationssystemen individuelle bedarfsge- rechte Lösungen entwickeln und gewährt Einblicke in die Unterschiede und Vorteile verschiedener Konzepte.

ISBN 9783960090120  
[shop.heise.de/smart-home-hacks](http://shop.heise.de/smart-home-hacks)

BEST-  
SELLER

32,90 € >

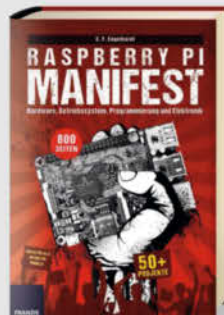


### E. F. Engelhardt **Internet of Things Manifest**

Bringen Sie Geräte unterschiedlicher Hersteller unter einen Hut, schließen Sie Datenvoyeure aus, sparen Sie Geld und Energiekosten mit dem Handbuch zur digitalen Weltrevolution.

ISBN 9783645604857  
[shop.heise.de/iot-manifest](http://shop.heise.de/iot-manifest)

49,90 € >



### E. F. Engelhardt **Raspberry Pi Manifest**

Erfahren Sie in 50 Projekten, wie Sie den Minicomputer für Ihre Zwecke nutzen: von der Spielekonsole bis zum Netzwerkdrucker, von SmartTV bis Navi, für jeden ist etwas dabei.

ISBN 9783645604932  
[shop.heise.de/raspi-manifest](http://shop.heise.de/raspi-manifest)

29,90 € >



### Charles Platt **Make: Elektronik**

Tauchen Sie ein in die faszinierende Welt der Elektronik und verstehen Sie ihre Gesetze mit einfachen Anwendungen hin zu komplexen Projekten mit Schritt-für-Schritt-Anleitungen und großem Theorie- und Praxisteil.

ISBN 9783864903687  
[shop.heise.de/make-elektronik](http://shop.heise.de/make-elektronik)

34,90 € >



### Dr. Christian Pätz **Z-Wave**

Lernen Sie die Z-Wave-Technologie kennen und einzusetzen: Funk- & Antennentechnik, Aufbau, Zusammenspiel und Management der einzelnen Geräte, Tipps, Erfahrungen, die rechtliche Situation und Lösen praktischer Probleme.

ISBN 9783738601947  
[shop.heise.de/zwave-buch](http://shop.heise.de/zwave-buch)

19,99 € >



### Cord Elias **FPGAs für Maker**

Erfahren Sie Schritt für Schritt, wie Sie als Maker und Elektronikbastler eigene Chips entwerfen, simple und später anspruchsvollere Schaltungen realisieren können oder wie VHDL funktioniert. Erlernen Sie so den selbstständigen Umgang mit FPGAs.

ISBN 9783864901737  
[shop.heise.de/fpga](http://shop.heise.de/fpga)

36,90 € >



### Simon Monk **Der Maker-Guide für die Zombie-Apokalypse**

Bereiten Sie sich vor: mittels 20 Survival-Projekten mit einfacher Elektronik, Arduino und Raspberry Pi werden Sie Ihren eigenen Strom erzeugen, unverzichtbare Bauteile vor dem Zombie-Zugriff retten und lebensrettende Elektronikschaltungen bauen, um Untote aufzuspüren.

ISBN 9783864903526  
[shop.heise.de/zombies](http://shop.heise.de/zombies)

24,90 € >

BEST-  
SELLER



# und Maker!

## Zubehör und Lesestoff

shop.heise.de/hardware



### Fibaro Motion Sensor

Erfassen Sie mit dem Motion Sensor für Z-Wave Smart Home Bewegungen, Temperaturen, Helligkeiten und Erschütterungen.

Die Smart Home-Zentrale löst daraufhin Aktionen via Z-Wave-Funk-Protokoll aus.

[shop.heise.de/motion-sensor](http://shop.heise.de/motion-sensor)

49,90 € >



### 7" Touchscreen-Display

Nutzen Sie Ihren Raspberry als Schaltzentrale eines All-in-one-PCs, Tablets, Infotainment-Systems oder Embedded-Projekts. Separat im

heise shop erhältlich: Original-Gehäuse in schwarz oder weiß.

[shop.heise.de/touchscreen](http://shop.heise.de/touchscreen)

74,90 € >



### Fibaro Wallplug

Der Wallplug macht jede Steckdose zum intelligenten Z-Wave Smart Home-Gerät. Die RGB-LED Ring-Beleuchtung informiert über den

Zustand und den Stromverbrauch des Geräts. Die Funktion kann je nach Smart-Home-Zentrale frei konfiguriert werden.

[shop.heise.de/wallplug](http://shop.heise.de/wallplug)

54,90 € >



### Fibaro Swipe-Tablet

Steuern Sie Ihr intelligentes Heim durch Hand- und Fingergesten. Spielen Sie Musik ab und schalten Sie

den Fernseher ein, steuern Sie Ihre Alarmanlage und die Fensterrolläden durch einen Fingertipp.

[shop.heise.de/swipe-tablet](http://shop.heise.de/swipe-tablet)

129,90 € >



TOP  
PRODUKT

### Sensoren- & Aktoren-Kit

Die perfekte Zubehör-Sammlung für Ihre Projekte mit Microcontrollern: 38 Drehschalter,

Sound-Sensoren, Button-, Buzzer- & LED-Module, Touch- & Sound-Sensoren und vieles mehr.

[shop.heise.de/sensoren-set](http://shop.heise.de/sensoren-set)

49,90 € >



### Arduino Uno R3

Endlich ist das Original wieder im heise shop erhältlich!

Der vielseitige Microcontroller als Steuereinheit für Ihre Home Automation, Multikopter, Messungen oder Bastelprojekte.

[shop.heise.de/arduino-uno](http://shop.heise.de/arduino-uno)

19,90 € >



### Raspberry Pi Z-Wave-Set + Sonderheft

Das c't Sonderheft Smart Home 2016 zusammen mit Raspberry Pi 3, RaZberry2-Modul, Gehäuse, Steckernetzteil und SDHC-Speicherkarte mit Z-Wave-Software - ideale Grundlage für Ihre Heimautomation-Projekte.

[shop.heise.de/smarthome-set](http://shop.heise.de/smarthome-set)

109,90 € >



### Raspberry Pi 3-Starterset + Sonderheft

Sichern Sie sich unseren Verkaufsschlager und steigen Sie ein in die Welt der Mikrocomputer mit dem c't Sonderheft Raspberry Pi und dem kompletten Starterpaket: Raspberry Pi 3, Netzteil, Gehäuse, SDHC-Card mit NOOBS.

[shop.heise.de/raspi-set](http://shop.heise.de/raspi-set)

68,90 € >

BEST-SELLER



### Z-Uno Z-Wave-Modul

Erstellen Sie mit dieser Arduino-Entwicklerplatine Ihr eigenes Z-Wave-Gerät! Kombinieren Sie die Einfachheit eines Arduino-Boards mit den Möglichkeiten des Z-Wave Home-Automation-Funkprotokolls.

[shop.heise.de/z-uno](http://shop.heise.de/z-uno)

57,90 € >



### RaZberry2 Z-Wave-Modul

Verwandeln Sie Ihren Raspberry Pi in ein professionelles Z-Wave-Gateway für das Smart Home. Einfach zu erlernen und zu bedienen: die Software Z-Way, basierend auf dem JavaScript-Interface JSON.

[shop.heise.de/razberry](http://shop.heise.de/razberry)

54,90 € >



Alle aktuellen Zeitschriften, ausgewählte Fachbücher, eBooks und digitale Magazine für Heise Medien- oder Maker Media-Abonnenten oder ab einem Einkaufswert von 15 € versandkostenfrei.

Bestellen Sie ganz einfach online unter [shop.heise.de](http://shop.heise.de) oder per E-Mail: [service@shop.heise.de](mailto:service@shop.heise.de)

heise shop

[shop.heise.de](http://shop.heise.de)



Bild: gioiak2-Fotolia.com

Jo Bager

# Zeiterfassung für PC und Smartphone

**Organisation klappt nur mit Kontrolle: Das gilt auch für Arbeitszeiten. Wer diese kontrollieren oder abrechnen will, muss den Zeitaufwand für seine Tätigkeiten genau dokumentieren. Die richtigen Anwendungen erledigen das fast von selbst.**

**M**ist! Das mit dem Positionspapier für den Chef hat länger gedauert als gedacht. Jetzt schiebe ich aber erst mal die Anfrage von der netten Kollegin dazwischen, und dann schaue ich noch schnell, ob Peter Glaser bei Facebook wieder ein paar niedliche Katzenfotos gepostet hat. Dann mache ich das Papier halt erst morgen fertig: Die beste Planung hilft nichts, wenn man sich nicht daran hält, sich verzettelt, überschätzt oder aus der Arbeit herausgerissen wird.

Zeit-Controlling hilft, die größten Zeitfresser zu finden und künftig besser zu pla-

nen. Freiberufler, die ihre Arbeitskraft vermieten, sollten ohnehin minutiös festhalten, wann sie welche Aufgabe für welchen Arbeitgeber bearbeiten. Das Gleiche gilt für Mitarbeiter von Unternehmen, die für verschiedene Abteilungen tätig sind.

Es gibt Zeiterfassungs-Software en masse. Wir haben für diesen Artikel exemplarisch drei Anbieter herausgepickt, die die Bandbreite der Lösungen repräsentieren: Toggl, Kimai und Chrometa. Alle drei lassen sich reibungslos und flexibel in den Arbeitsalltag integrieren. Dazu zählt, dass ihre Software für viele verschiedene Plattformen verfügbar ist.

## Toggl

Toggl stellt außer einer Web-Oberfläche auch Desktop-Anwendungen für Windows, Mac OS und Linux, Apps für Android und iOS sowie eine Chrome-Erweiterung zur Verfügung. Der Betreiber unterhält zudem ein offenes API für seinen Dienst, wodurch Toggl auch in anderen Anwendungen und Web-Diensten die Zeit messen kann.

In allen Toggl-eigenen Clients läuft die Bedienung ähnlich simpel ab. Klickt man beispielsweise auf das Icon der Chrome-Erweiterung, um eine neue Arbeitszeit zu er-



fassen, öffnet sich ein kleines Fenster. Mit einem Klick auf „start new“ beginnt man die Erfassung eines neuen Arbeitsabschnitts. Diesem gibt man einen Namen und fügt optional Tags an. Falls man in Toggl bereits Projekte angelegt hat, kann man dem Timer auch gleich ein Projekt zuweisen. Der Timer beginnt bereits zu laufen, sobald man auf Startknopf klickt: Die für die Benutzung von Toggl aufgewandte Zeit wird also mit erfasst.

Mit der Chrome-Erweiterung lässt sich bei fast hundert Web-Diensten ein Timer starten – von Salesforce über Todoist bis zu Gmail. In Google Docs etwa bettet sie ein Icon gut sichtbar in die Menüleiste ein. Wo auch immer man Toggl nutzt: Der Dienst synchronisiert den Timer auf allen Clients.

Toggl hat viele kleine nützliche Funktionen, die den Anwender bei der täglichen Arbeit unterstützen und helfen, die Zeiterfassung feinzutunen. So können die Desktop-Apps und die Chrome-Erweiterung sich dem Anwender mit kleinen Warnmeldungen in Erinnerung rufen, falls

**Mit der TimeTrapp-App erfasst man die Zeit für einen Kimai-Server und lässt sich einen Überblick über Projekte geben.**

der mal vergisst, Zeiten zu erfassen. Beide Clients enthalten zudem einen optionalen Pomodoro-Timer.

Im Web-Dashboard laufen die erfassten Zeiten zusammen, hier generiert Toggl aus den erfassten Daten aussagekräftige Statistiken. Per Web-Frontend lädt man auch weitere Team-Mitglieder ein. Beim günstigsten von vier Preismodellen können Teams von bis zu fünf Benutzern Toggl kostenlos nutzen. Schon in der kostenlosen Version lassen sich beliebig viele Projekte anlegen und für etliche Zwecke ausreichende Reports generieren, die Toggl auch als PDF-Dateien exportiert. Die nackten Zahlen exportiert Toggl als CSV-Datei für andere Anwendungen. Wer die Zeiten von größeren Teams erfassen und Sub-Projekte anlegen will, der muss ein kostenpflichtiges



The screenshot shows the 'Zusammenfassung' (Summary) screen of the TimeTrapp app. It displays a date range from '01.06.2016' to '28.06.2016' and a red 'Aktualisieren' (Refresh) button. Below this is a table of time tracking data.

Zusammenfassung		
Von	01.06.2016	
Bis	28.06.2016	
<b>Aktualisieren</b>		
Gesamte Zeit	00:31	8.53
TestProjekt	00:00	0.00
testen	00:00	0.00
GTD	00:31	8.53
testen	00:17	8.53
GTD Artikel	00:14	0.00
testen und schreiben		

# FÜR ROOTINIERS.

IX. WIR VERSTEHEN UNS.

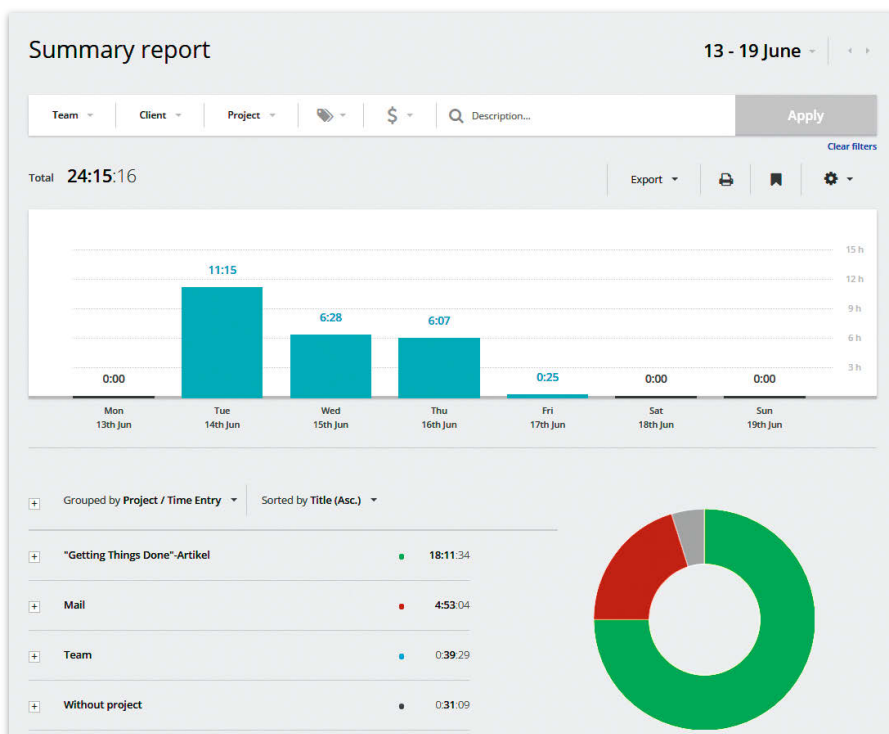


**Jetzt auch für Android! Das Mini-Abo testen:**  
3 Hefte + 16GB-Stick nur 13,50 Euro [www.iX.de/digital](http://www.iX.de/digital)

Sie wollen Zugriff auf alle Fakten? Nehmen Sie ihn sich – iX ab sofort auch als Android-App. Testen Sie 3 aktuelle Ausgaben jetzt komplett papierlos auf Ihrem Android/iOS-Tablet & -Smartphone per HTML5 oder PDF zum Vorzugspreis. **Jetzt zugreifen: [www.iX.de/digital](http://www.iX.de/digital)**







**Im Web-Dashboard fasst Toggl die Timer-Informationen zusammen und bereitet sie zu aufschlussreichen Statistiken auf.**

Abonnement abschließen; die Preise starten bei 9 US-Dollar pro Nutzer und Monat.

## Kimai

Kimai arbeitet so ähnlich wie Toggl. Der entscheidende Unterschied: Der Kimai-Server ist als Open-Source-Anwendung verfügbar. Man kann die Server-Anwendung auf seinem eigenen Webspace installieren, sodass kein Dritter die Abrechnungsdaten zu Gesicht bekommt.

Das System setzt PHP 5.4 und eine MySQL-Datenbank voraus (4.3 oder höher) – Zutaten, die die meisten Shared-Web-space-Pakete enthalten. Der Download besteht aus einer Zip-Datei, die man entpackt und auf den Server hochlädt. Ruft man anschließend die entsprechende Kimai-URL im Browser auf, führt ein Installer durch die weitere Einrichtung.

Insbesondere wenn man mit dem Smartphone Zeiten erfassen will, ist es sinnvoll, die mobile Erweiterung zu installieren – eine weitere Zip-Datei, deren Inhalte man in den Webspace hochlädt. Noch ein wenig komfortabler lässt sich die Zeit unter Android, iOS oder Windows 10 mit der App TimeTrapp erfassen. Sie kostet je nach Plattform zwischen 1 und 2 Euro.

Kimai kommt nicht so chic daher wie Toggl, bietet aber viele Funktionen. So ist

das System für den Mehrbenutzerbetrieb ausgelegt. Kimai ermöglicht es, Budgets und Auslagen zu verwalten, um die Gesamtkosten von Projekten im Blick zu behalten. Erfasste Zeiten lassen sich flexibel filtern. Zeit-Reports exportiert Kimai als PDF-, XLS oder CSV-Datei mundgerecht für andere Anwendungen. Der Server kann aber auch gleich selbst komplette Rechnungen in Form von Microsoft-Word-Dateien auswerfen.

## Chrometa

Die Arbeit mit Chrometa verläuft anders als mit Toggl und Kimai. Sobald die Client-Software des Dienstes eingerichtet ist, muss man nichts mehr tun, um die Arbeitszeit zu erfassen – das macht der Dienst nämlich automatisch. Ein Hintergrundprogramm, das für Windows und Mac OS verfügbar ist, schneidet mit, welche Anwendungen mit welchen Dokumenten sich auf dem PC im Vordergrund befinden; bei E-Mails registriert Chrometa die Betreffzeile. Diese Informationen übertragen die Chrometa-Clients zum Anbieter. Der Windows-Client hat in unseren Versuchen zudem zuverlässig mitgekriegt, wenn man mal den PC verlassen hat, und anschließend gefragt, ob er die Zeit erfassen und welchem Projekt er sie zuordnen soll.

Der Anbieter stellt außerdem Apps für Android und iOS zur Verfügung. Sie erfassen automatisch, wie viel Zeit der Anwender für Anrufe benötigt. Sonstige Zeiten kann man mit den Apps von Hand erfassen und einem Projekt zuweisen. Es gibt auch eine Hand voll Integrationen in Fremd-anbieter-Anwendungen, etwa in die Projektmanagement-Software Basecamp oder den Speicherdienst Box.com.

Die erfassten Zeiten und die zugehörigen Anwendungen und Dokumententitel laufen im Web-Office des Anbieters zusammen: dort entsteht so ein minutengenaues Plan der PC- und Smartphone-Nutzung. Hier kann im Unterschied zu Toggl und Kimai ein wenig Handarbeit gefragt sein, um im Web-Frontend die Zeiten verschiedenen Projekten zuzuordnen. Dabei hilft Chrometa dem Anwender durch Filter. Damit lassen sich etwa die Zeiten, die für die Bearbeitung von Dokumenten bestimmter Formate anfallen oder die von ausgewählten Anwendern stammen, schnell zusammenfassen lassen, um sie einem bestimmten Projekt zuzuordnen. Hinterlegt man bei Chrometa Regeln, kann der Dienst Zeiten, die mit den Clients erfasst und zum Anbieter hochgeladen werden, automatisch bestimmten Projekten zuordnen, zum Beispiel auf Basis der Dokumententitel.

Chrometa ist für Einzelanwender und Teams verfügbar; die Preise starten bei 12 US-Dollar pro Monat und Nutzer. Auch wenn der Anwender den Chrometa-Client jederzeit pausieren kann, um private Dinge zu erledigen: Der Dienst greift tief in die Privatsphäre ein; die zum Anbieter übertragenen Titel von Dokumenten und Websites sowie die Betreffzeilen von E-Mails zeichnen ein recht genaues Bild, woran der Einzelne arbeitet. In Unternehmen sollte Chrometa nicht ohne Zustimmung des Betriebsrats und des Datenschutzbeauftragten genutzt werden.

## Kontrolle ist besser

Wer seine Arbeit auf Zeitbasis abrechnet, muss seine Leistungen erfassen. Ein Arbeitszeit-Protokoll eignet sich auch, um den Erfolg oder Misserfolg von Selbstoptimierungsmaßnahmen zu überprüfen. Es gibt ein riesiges Angebot an Zeit-Loggern. Falls Sie mit den hier vorgestellten Lösungen nicht klarkommen, finden Sie unter dem c't-Link Sammlungen mit weiteren Apps und Diensten.

(jo) **ct**

Listen mit weiteren Zeiterfassungsdiensten: [www.ct.de/waa2](http://www.ct.de/waa2)

# CeBIT Security Plaza 2017

Gebündeltes Sicherheits-Know-how  
20. - 24. März 2017 – Halle 6, Stand B16



Foto: © voyager624 – Fotolia.com

**Der Publikumsmagnet  
für IT-Sicherheit**

## Buchen Sie jetzt das Rundum-sorglos-Paket für Ihren Messeauftritt auf der CeBIT 2017!

### Ihre Vorteile

- **Rundum-sorglos-Paket** inkl. Planung, Organisation, hochwertiger Standbau, Standbewachung, umfassende PR- und Marketingkampagnen
- **Messeauftritt mit Ausstellungsfläche** inkl. Monitor und Firmenlogo, Strom, WLAN
- Sie profitieren von dem **starken Gesamtauftritt der Security Plaza (über 800 qm)** als zentrale Anlaufstelle zu aktuellen IT-Sicherheitsthemen
- **Vortragsmöglichkeiten** auf der Security Plaza-Forumsbühne
- Möglichkeit zum **intensiven Dialog** im angenehmen Ambiente mit Ihren Kunden in der **Transfer Lounge / Cateringbereich**

heise Events veranstaltet 2017 bereits zum 7. Mal die Security Plaza. Wir bieten Ihnen mit der Plaza das perfekte Zusammenspiel zwischen Ausstellungsfläche, Produktvortrag auf der Forumsbühne und einem großzügigen Catering- und Networkingbereich.

**Werden Sie unser Gast und Teil der Security Plaza 2017!**

Unsere Partner 2017:



Eine Veranstaltung von:



In Kooperation mit:



Weitere Informationen unter: [www.heise-events.de/security\\_plaza](http://www.heise-events.de/security_plaza)





Lutz Labs, Alexander Spier

# Schnelle MicroSD-Karten mit 32 und 128 GByte

Mit Speicherkarten im Micro-SD-Format erweitert man ganz einfach den Speicher seines Smartphones oder der Action-Kamera. Welche der kaum fingernagelgroßen Kärtchen schnell sind und ob sie am PC ebenfalls eine gute Figur machen, klärt unser Test.

Der Speicher im Smartphone kann eigentlich nie groß genug sein, und die Action-Kamera läuft ohne Speicherkarte gar nicht. Also ab in den nächsten Elektronik-Laden und einfach eine Speicherkarte kaufen? So einfach ist das nicht: Wer Videos in hoher Auflösung aufnehmen will und nicht stundenlang auf die Befüllung der Karte am heimischen PC warten möchte, informiert sich besser vor dem Kauf.

16 verschiedene Speicherkarten mussten im c't-Labor ihre Eignung für Smartphone und PC beweisen. Dabei waren Karten von Kingston, Lexar, Samsung, SanDisk, Toshiba und Transcend – Samsung

und SanDisk nahmen sogar mit zwei Serien teil. Von allen Karten haben wir uns Modelle mit 32 und 128 GByte besorgt; alle unterstützen mindestens eine Schreibrate von 10 MByte/s (Class 10).

Viele 32-GByte-Kärtchen kosten kaum noch 10 Euro, die vierfache Kapazität geht ab 35 Euro über den Ladentisch. Besonders schnelle Karten sind aber weit teurer: Knapp 200 Euro kostet die SanDisk Extreme Pro mit 128 GByte. Noch größere Karten haben zwar einige Anbieter noch im Angebot, doch steigt bei diesen der Preis pro GByte noch einmal stark an. Karten mit 16 GByte oder weniger lohnen sich hingegen kaum noch.

## Größen und Geschwindigkeitsklassen

Die SD Card Association, Hüter des SD-Standards, spezifiziert drei verschiedene Kapazitätsklassen: SD (bis 2 GByte), SDHC (High Capacity, bis 32 GByte) und SDXC (Extended Capacity, bis 2 TByte). SDHC-Karten funktionieren beispielsweise in einem SDXC-Lesegerät, aber nicht umgekehrt.

Neben den Kapazitätsklassen gibt es verschiedene Geschwindigkeitsklassen für den Flash-Speicher und mehrere Übertragungsverfahren. Flotte Karten verwenden Übertragungsverfahren für maximal 104 (UHS-I) oder 312 MByte/s (UHS-II);



diese sind an Logos mit den römischen Ziffern I oder II identifizierbar. Karten ohne diese Logos übertragen höchstens 25 oder gar nur 12,5 MByte/s. UHS-II-Karten nutzen eine zweite Kontaktreihe. Steckt man sie in einen Nicht-UHS-II-fähigen Kartenleser, können die Karten nur einen der langsameren Standards nutzen.

Die Geschwindigkeit des Flash-Speichers geben die Hersteller gerne mit einer eingekreisten Zahl an. Karten mit den Geschwindigkeitsklassen 2, 4 und 6 sollte man meiden, Class 10 setzen die meisten Smartphones als Minimum voraus.

## Geschwindigkeitsabfall

SD-Karten unterstützen anders als SSDs keinen Trim-Befehl. Durch diesen teilt das Betriebssystem der SSD mit, dass gelöschte Daten nicht mehr benötigt werden; der Controller kann daraufhin aufräumen und mehr freie Speicherbereiche zur Verfügung stellen. Bei SD-Karten aber bleibt der Inhalt gelöschter Dateien erhalten. Das ist gut, falls man versehentlich ein Foto gelöscht hat, aber schlecht für die Performance der Karte. Denn bei hohem Füllstand stehen dem Controller der SD-Karte nur wenige freie Blöcke zur Verfügung; bei weiteren Schreibanforderungen muss der Controller eventuell erst Blöcke lesen, die freien Teile mit den zu schreibenden Daten auffüllen und sie wieder zurückschreiben – und das dauert.

In Zukunft soll es (Micro-)SD-Karten mit erweitertem „Discard“-Befehl geben, der ähnlich wie Trim funktioniert – aber das wird noch dauern.

Bis dahin bleibt nur, SD-Karten gelegentlich zu formatieren, am besten mit dem Format-Utility der SD Card Association. Wie Windows lässt auch der SD Formatter (siehe c't-Link am Ende des Artikels) eine Schnellformatierung zu, bietet aber auch zwei andere Methoden an: Full Erase und Full Overwrite. Das Dateisystem lässt sich nicht auswählen, das Tool formatiert immer mit exFAT.

## FAT32 versus exFAT

Billige Smartphones nennen in den Datenblättern immer noch MicroSDHC und damit 32 GByte als Maximum. Erst bei teureren Smartphones ist MicroSDXC Usus.

Doch mit der eingebauten Technik hat das häufig nichts zu tun. Grund sind vielmehr Lizenzkosten, die Microsoft für das moderne exFAT-Dateisystem verlangt. Karten mit mehr als 32 GByte sind in der Regel mit exFAT formatiert, denn das sieht der SDXC-Standard vor. Legt man eine so formatierte Karte in ein Gerät ohne exFAT-Unterstützung ein, behauptet Android, die Karte sei defekt und müsse formatiert werden. Lässt man sich darauf ein, formatiert das System die Karte ohne Murren mit FAT32 und der vollen Kapazität. Einzige relevante Einschränkung dabei: FAT32 unterstützt keine Dateien über 4 GByte Größe.

## Leistungsaufnahme

MicroSD-Karten benötigen im Ruhezustand nur wenig Energie. Exakte Angaben müssen wir schuldig bleiben, da wir lediglich die Kombination aus USB-Adapter und Speicherkarte messen können, nicht aber

die Speicherkarte allein. Einige Richtwerte gibt es jedoch: UHS-II-Karten benötigen zwischen 300 und 400 mW, UHS-I-Karten nur 10 bis 20. Betreibt man die schnellen Karten im UHS-I-Modus, etwa im Smartphone, sinkt auch deren Ruhestrombedarf auf dieses Niveau. Zudem gilt: Je schneller die Karten lesen und schreiben, desto mehr Energie benötigen sie dafür. Die UHS-II-Karten genehmigen sich beim Schreiben bis zu 1,5 Watt, die langsameren Karten liegen allesamt unter 1 Watt.

## MicroSD-Karten im Smartphone

Viele Android-Smartphones besitzen MicroSD-Slots zur Speichererweiterung. Das Auslagern von Daten und Programmen kann jedoch problematisch sein: Das System muss damit rechnen, dass etwas fehlt, weil die Speicherkarte entfernt wurde. Zudem ist freier Zugriff auf die Speicherkarte für alle Apps ein Sicherheits- und Datenschutzrisiko, weshalb mit jeder neuen Android-Version die Rechte für Apps restriktiver gehandhabt wurden. Ein aktuelles Android lässt das Speichern von Apps auf die SD-Karte erst gar nicht zu. Programme dürfen lediglich ihre Daten, etwa Bilder, Bücher oder Kartenmaterial auslagern. Viele Smartphone-Hersteller bauen die Funktion aber nachträglich ein.

## Speichererweiterung

Seit Android 6 können Speicherkarten als interner Speicher genutzt werden. Sämtliche vorher darauf gespeicherten Inhalte gehen bei der dafür notwendigen Forma-

## Micro-SD-Karten – Benchmarks

	Sequenzielle Transferraten lesen <sup>1</sup> [MByte/s] besser ►	Sequenzielle Transferraten schreiben <sup>1</sup> [MByte/s] besser ►	IOPS schreiben/lesen <sup>2</sup> besser ►
Kingston microSDHC 32GB	42/41/44	15/14/14	220/1242
Kingston microSDXC 128GB Kit	58/70/83	26/15/16	100/630
Lexar 1000x (32 GByte)	65/83/172	55/35/36	407/4140
Lexar 1000x (128 GByte)	65/81/137	59/42/43	627/2412
Samsung microSDXC Evo (32 GByte)	43/43/44	25/21/21	940/1697
Samsung microSDXC Evo (128 GByte)	42/42/44	26/19/20	323/407
Samsung microSDXC Pro Plus (32 GByte)	65/81/88	81/53/64	973/1646
Samsung microSDXC Pro Plus (128 GByte)	59/78/86	79/43/65	765/2348
SanDisk Ultra microSDHC (32 GByte)	66/84/89	62/18/18	384/2670
SanDisk Ultra microSDXC (128 GByte)	65/84/88	77/31/43	468/2043
SanDisk Extreme PRO microSDHC (32 GByte)	67/86/89	84/59/72	724/2115
SanDisk Extreme PRO microSDXC (128 GByte)	65/82/247	114/51/68	202/2529
Toshiba Exceria M302-EA microSDHC (32 GByte)	62/76/89	27/23/24	61/1375
Toshiba Exceria M302-EA microSDXC (128 GByte)	59/74/89	32/23/26	67/996
Transcend microSDHC Premium Kit (32 GByte)	65/82/89	24/19/17	343/1830
Transcend microSDXC Premium Kit (128 GByte)	64/81/89	37/23/27	340/545

<sup>1</sup> gemessen mit Motorola Moto G3 (AndroBench 5), Motorola Moto Z (AndroBench 5) und Lexar-USB-Adapter am PC (WinSat) <sup>2</sup> gemessen mit Lexar-USB-Adapter (UHS-II) am PC (WinSat)



## Kingston microSDHC

Kingston kann, anders als die Hersteller der meisten anderen Karten in diesem Test, nicht auf eigenen Flash-Speicher zugreifen; das Unternehmen kauft ihn bei Toshiba, SanDisk oder Micron. Bei der 32-GB-Byte-Karte liegt nicht einmal ein SD-Adapter dabei – alle anderen Hersteller liefern mindestens einen solchen mit, wenn nicht gar einen USB-Adapter.

Beim Lesen kommen beide Kingston-Karten gerade einmal über 40 MByte/s, beim Schreiben schafft die 32-GB-Byte-Karte nicht einmal die Hälfte – das liegt zwar oberhalb der versprochenen Leistung, aber am unteren Ende dieses Vergleichstests. Die 128-GB-Byte-Karte ist zwar am PC etwas schneller, aber im Smartphone sinkt die Schreibleistung ebenfalls auf rund 15 MByte/s.

- ↑ günstig
- ↓ kein SD-Adapter bei 32 GByte
- ↓ sehr langsam



## Lexar 1000x

Die SD-Karten von Lexar waren die ersten im Micro-Format, die das schnelle UHS-II-Interface unterstützen. Mit passendem UHS-II-Kartenleser machen sie am PC vor allem beim Lesen eine gute Figur, die 128-GB-Byte-Karte ist jedoch etwas langsamer. In Smartphones können beide die Geschwindigkeit nicht erreichen, die ihr Speichercontroller ermöglicht. Hier liegen sie allenfalls im Mittelfeld, sind aber keineswegs langsam.

UHS-II-Karten und vor allem passende Lesegeräte sind noch recht selten. Da Lexar einen schnellen USB-Adapter beilegt, relativiert sich der Preis etwas. Insgesamt aber können die UHS-II-Karten mit dem schnellsten Vertreter dieser Gattung, der SanDisk Extreme Pro, nicht mithalten.

- ↑ flott am PC
- ↑ USB-Adapter im Lieferumfang
- ↓ teuer



## Samsung microSDXC Evo

Bei Samsung ist die Auswahl einer passenden SD-Karte schwer: Es gibt nicht nur die von uns getesteten günstigen Evo- und die teuren Pro-Plus-Karten, sondern auch noch ein paar Serien dazwischen. Die Evos gehören aber nicht nur zu den günstigsten Karten im MicroSD-Format, sondern auch zu den langsamsten. Die 32-GB-Byte-Karte schafft beim Schreiben gerade einmal 15 MByte/s – das Kopieren eines 4 GByte großen Films dauert damit fast fünf Minuten.

Aus der Leserschaft erreichten uns in den vergangenen Monaten Hinweise, dass die Evos häufiger ausfallen würden. Im Lauf des Tests konnten wir dies nicht reproduzieren. Dennoch sollte man bei Verwendung dieser Karte besonders darauf achten, seine Daten zu sichern.

- ↑ günstig
- ↓ langsam
- ↓ Berichte über Ausfälle

tierung verloren. Bereits im internen Speicher vorhandene Mediendateien verschiebt das System auf die SD-Karte. So formatierte Karten erscheinen für System und Apps genauso wie der Systemspeicher, auch der Nutzer kann nicht sehen, wo welche Daten liegen. Da Android die Daten verschlüsselt auf der Karte ablegt, sind sie auf anderen

Smartphones oder im Kartenleser am PC nicht lesbar. Bei einem Defekt der Karte sind auch die Inhalte verloren.

## Wie schnell geht es?

Um die Geschwindigkeit der MicroSD-Karten im Smartphone zu testen, haben wir

zum einen das günstige Motorola Moto G3 und zum anderen das High-End-Modell Motorola Moto Z benutzt. Beide nutzen ein relativ unverändertes und recht aktuelles Android 6.0.

Der Androbench 5 warf als einziges Benchmark-Tool Ergebnisse heraus, die mit den Ergebnissen am PC vergleichbar

## MicroSD-Karten

Modell	microSDHC / microSDXC Kit	1000x	microSDXC Evo	microSDXC Pro Plus	Ultra microSDHC / microSDXC	Extreme PRO microSDHC / microSDXC	Exceria M302-EA microSDHC / microSDXC	microSDHC / microSDXC Premium Kit
Hersteller	Kingston, <a href="http://www.kingston.com/de">www.kingston.com/de</a>	Lexar, <a href="http://www.lexar.com">www.lexar.com</a>	Samsung, <a href="http://www.samsung.de">www.samsung.de</a>	Samsung, <a href="http://www.samsung.de">www.samsung.de</a>	SanDisk, <a href="http://www.sandisk.de">www.sandisk.de</a>	SanDisk, <a href="http://www.sandisk.de">www.sandisk.de</a>	Toshiba, <a href="http://www.toshiba.de">www.toshiba.de</a>	Transcend, <a href="http://www.transcend.de">www.transcend.de</a>
Bezeichnung	SDC10G2/32GBSP / SDC10G2/128GB	LSDMI32GCBEU1000R / LSDMI128CBEU1000R	MB-MP32DA/EU / MB-MP128DA/EU	MB-MD32DA/EU / MB-MD128DA/EU	SDSQUNC-032G-GN6IA / SDSQUNC-128G-GN6MA	SDSDQXP-032G-G46A / SDSQXPJ-128G-QN6M3	THN-M302R0320EA / THN-M302R1280EA	TS32GUSDU1 / TS128GUSDU1
Kapazität lt. Hersteller <sup>1</sup>	32 / 128 GByte	32 / 128 GByte	32 / 128 GByte	32 / 128 GByte	32 / 128 GByte	32 / 128 GByte	32 / 128 GByte	32 / 128 GByte
von Windows erkannte Kapazität	28,91 / 117,02 GByte	29,82 / 119,58 GByte	29,81 / 119,75 GByte	29,81 / 119,23 GByte	29,72 / 119,08 GByte	29,72 / 119,59 GByte	28,91 / 115,99 GByte	30,01 / 120,25 GByte
Zubehör	— / SD-Adapter	USB-Adapter	SD-Adapter	SD-Adapter	SD-Adapter	SD- / USB-Adapter	SD-Adapter	SD-Adapter
Garantie	10 Jahre	10 Jahre	5 / 10 Jahre	10 Jahre	10 Jahre	10 Jahre	5 / 10 Jahre	30 Jahre
Preis pro Gigabyte	34,4 / 31,3 Cent	75 / 65,6 Cent	28,1 / 28,1 Cent	62,5 / 62,5 Cent	34,4 / 28,1 Cent	78,1 / 153,9 Cent	28,1 / 27,3 Cent	31,3 / 37,5 Cent
Straßenpreis	11 / 40 €	24 / 84 €	9 / 36 €	20 / 80 €	11 / 36 €	25 / 197 €	9 / 35 €	10 / 48 €

<sup>1</sup> Die Hersteller rechnen mit 1 GByte = 1 000 000 000 Byte. Für Windows dagegen ist 1 GByte = 1 073 741 824 Byte, die angezeigte Kapazität daher kleiner.



## Samsung microSDXC Pro Plus

Die Karten der Pro-Plus-Serie kosten rund das Doppelte der günstigen Evos. Am PC rauschen die Daten mit rund 80 MByte/s hin und her, Unterschiede zwischen Lesen und Schreiben sind marginal. Beim Lesen in den Smartphones erreichen beide Karten Spitzenwerte, beim Schreiben allerdings fällt die Karte mit 128 GByte etwas ab.

Samsung gibt als einer der wenigen Hersteller einen Hinweis zur Haltbarkeit: 10.000 Schreibzyklen soll die Karte vertragen. Ebenfalls interessant ist, dass Samsung die Garantie von 10 Jahren auf 1 Jahr senkt, wenn die Karte in Überwachungssystemen benutzt wird – wohl aufgrund der hohen Schreibbelastungen.

- ↑ schnell
- ↓ teuer
- ↓ eingeschränkte Garantie



## SanDisk Ultra microSDXC

SanDisk kann sich – wie auch Lexar, Samsung und Toshiba – beim Flash-Speicher das Beste herausuchen: Die SanDisk-Muttergesellschaft Western Digital betreibt zusammen mit Toshiba das Ferti-gungsgespann Flash Forward.

Anders als viele UHS-I-Konkurrenten sind die Ultras auch beim Schreiben recht schnell: 60 MByte/s schafft die 32-GByte-Karte, die 128er sogar fast 80 MByte/s.

Die Schreibwerte fallen im Smartphone zwar stark ab, vor allem bei der 32er-Karte, aber die mit 128 GByte setzt sich mit fast 45 MByte/s an die Spitze der günstigeren Karten. Lediglich die beiden UHS-II-Karten und die Samsung Pro Plus sind schneller – diese kosten aber mindestens das Doppelte.

- ↑ schnell am PC
- ↑ bestes Preis/Leistungsverhältnis bei 128 GByte
- ↓ 32-GByte-Karte im Smartphone langsam



## SanDisk Extreme PRO microSDXC

Die Karten aus der Extreme-Pro-Reihe von SanDisk sind nicht direkt vergleichbar: Während die 32-GByte-Karte ein UHS-I-Interface besitzt, nutzt das 128-GByte-Modell die wesentlich schnellere UHS-II-Schnittstelle. Das wirkt sich auch auf die Leserate am PC aus: Obwohl die 32-GByte-Karte beim Lesen schon respektable 90 MByte/s schafft, zieht das 128-GByte-Modell mit 250 GByte/s einsam an die Spitze des Testfelds.

Auch im Smartphone gehören beide Karten zu den schnellsten, hier allerdings liegt die große Karte etwas hinter der kleinen. Die 128er Karte springt allerdings mit knapp 200 Euro auch preislich aus dem Rahmen.

- ↑ schnell
- ↑ UHS-II-Modell sehr schnell
- ↓ teuer bis sehr teuer

waren. Mit der vorgegebenen Blockgröße kamen einige Karten besser, andere schlechter zurecht, sodass sich die Reihenfolge im Vergleich zu den PC-Benchmarks geringfügig verschob.

Am Ende ergab sich dennoch ein klares Bild: Langsame Karten kamen in beiden Geräten auf sehr ähnliche Werte. Bei schnelleren Karten drosselten die Smartphones ab einer gewissen Datenrate, das Moto G3 deutlich früher als das Moto Z. Lesend machte das G3 bei rund 65 MByte/s dicht, schreibend schafften einige Karten immerhin über 50 MByte/s.

Im Moto Z war das Maximum bei 85 MByte/s lesend und 70 MByte/s schreibend erreicht. Am besten schnitt insgesamt die SanDisk Extreme mit 32 GByte ab, die 128-GByte-Variante konnte von ihrem schnelleren UHS-II-Interface nicht profitieren. Auch die Samsung-Pro-Karten schnitten erwartungsgemäß gut ab.

Die erreichbaren Datenraten werden sich bei anderen Geräten unterscheiden, hier spielen auch die Anbindung und der

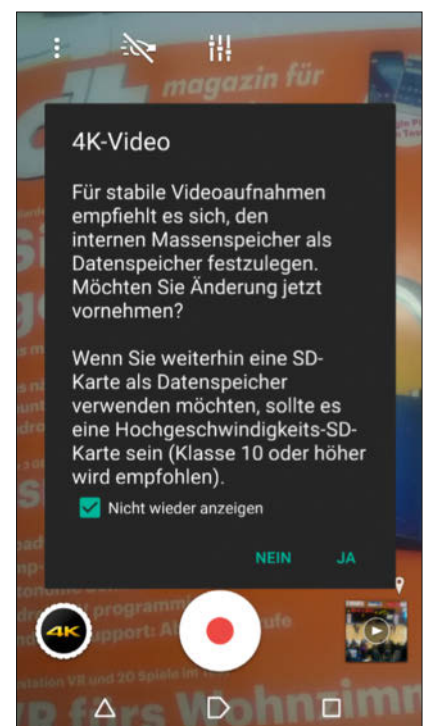
Speichercontroller eine Rolle. Smartphones mit Unterstützung für die schnellere UHS-II-Schnittstelle gibt es bislang nicht.

## Wie schnell muss es sein?

Welche Karte nun die richtige fürs Smartphone ist, hängt also unter anderem vom Gerät ab – extrem schnelle Karten lohnen sich in billigen Modellen nicht. Vor allem gilt es, nach Einsatzzweck zu wählen.

Als Datengrab und Foto-Ablage genügen langsame Karten. Die Leserate reicht zum Abspielen von Videos und zum Blättern durch die Fotosammlung aus; die

Wie dieses Sony Xperia Z2 wollen auch andere Smartphones 4K-Videos lieber auf dem internen Speicher ablegen – die Geschwindigkeit der SD-Karte spielt dabei keine Rolle.







## Toshiba Exceria M302-EA microSDXC

9 Euro für 32 GByte, gerade mal 35 Euro für 128 GByte – Toshiba stellt mit den Exceria die günstigsten Karten in diesem Test. Gemessen am Preis können die Karten durchaus überzeugen: Beim Lesen am PC reizen sie mit knapp 90 MByte/s die UHS-I-Schnittstelle fast aus, beim Schreiben allerdings ist bei knapp 30 MByte/s Schluss; in unseren Test-Smartphones sank die Schreibrate sogar auf rund 25 MByte/s.

Besonders schwach war die Leistung beim Schreiben auf zufällige Adressen: Nicht einmal 70 IOPS markieren das untere Ende. Auch bei der Nettokapazität liegt die Karte hinten: Von nominell 128 GByte bleiben unter Windows lediglich 116 GByte übrig.

- ↑ günstig
- ↓ geringe IOPS-Werte
- ↓ geringe Nettokapazität



## Transcend microSDXC Premium Kit

Auch Transcend hat verschiedene MicroSD-Serien im Angebot; wir haben uns für diesen Test die billigste ausgesucht. Diese Karten sind zwar laut Anbieter nicht für die Aufzeichnung von 4K-Videos geeignet, es gab damit aber in unserem Test keine Probleme.

Detaillierte Datenblätter hält auch Transcend nicht bereit, aber immerhin eine Information zum verwendeten Speicher – MLC – und zur Haltbarkeit der Kontakte: Bis zu 10.000 Ein- und Ausschübe sollen sie vertragen.

Anders als bei anderen Karten ist das 128-GByte-Modell beim Schreiben etwas schneller als das 32er; beim Lesen liegen beide Karten an der Spitze der UHS-I-Modelle.

- ↑ flott beim Lesen
- ↑ hohe Nettokapazität
- ↑ lange Garantiedauer

etwas längeren Ladezeiten sind kaum zu bemerken. Fotos und Full-HD-Videos speichern alle schnell genug weg. Allenfalls bei langen Serienaufnahme mit sehr hochauflösenden Kameras geraten die langsamsten bei den Schreibraten an ihre Grenzen.

Wenn man jedoch häufig genutzte Daten auslagert, sollte man sich nach einem schnelleren Modell umschauen – zum Beispiel für umfangreiches Kartenmaterial. Spätestens wenn man Apps auf die Karte auslagert, sind schnellere Modelle sinnvoll. Langsame Karten bremsen Apps aus, die mit großen Datenbanken und -mengen arbeiten. Ist aber erstmal alles in den RAM geladen, spielt die Performance der Speicherkarte keine Rolle mehr.

Bei der Verwendung als interner Speicher sind die Datenraten daher besonders wichtig, auch beim Schreiben sollten sie möglichst hoch sein. Motorola empfiehlt Karten mit UHS-I-Interface und mindestens Class 10. Die Karten in unserem Test hängen dem internen Speicher klar hinterher. Android misst bei der Einrichtung kurz die Performance und warnt ausdrücklich vor zu langsamen Karten.

Im Moto G3 ist der Abstand nicht gewaltig, bei den Schreibraten übertreffen einige Karten sogar den internen Speicher, der nur 40 MByte/s schafft. Doch weil der Speichercontroller schnell an seine Grenzen gerät, schaffen auch die besten Karten nur die Hälfte der möglichen Leserate. Mit dem schnellen Speicher im Moto Z (rund 450 MByte/s lesen, 150 MByte/s schreiben) kann keine Karte mithalten.

## Ausreichend für 4K?

Immer mehr High-End-Smartphones und auch Action-Cams können mittlerweile Videos in UHD- beziehungsweise 4K-Auflösung aufnehmen. Das frisst nicht nur viel Speicherplatz, sondern stellt auch gewisse Ansprüche an die Schreibrate, damit die Aufnahmen nicht ruckeln oder gar abbrechen. Sony beispielsweise warnt ausdrücklich, dass es bei langsamen Karten zu Problemen kommen kann und man besser den internen Speicher nutzt.

In der Regel schaffen Smartphones solche hohen Video-Auflösungen nur mit 30 Bildern pro Sekunde und ohne Zusatz-

funktionen wie Bildstabilisation oder Zeitlupeneffekte. Die vom Moto Z erzeugten Videos brachten es auf Bitraten bis 65 MBit/s, also etwa 8 MByte/s. Die langsamste Karte im Test erreichte knapp 14 MByte/s – in der Theorie also gut genug.

Um auszuschließen, dass die Daten etwa im RAM zwischengespeichert werden, ließen wir die Aufnahmen über zehn Minuten laufen und die Datei auf knapp 4 GByte anwachsen. In der Praxis hatten wir bei der Aufnahmen bei keiner Karte erkennbare Probleme. Ebenfalls konnten wir zwischendurch in schneller Folge Bilder schießen und auf der Karte speichern.

Bis das Video abgespielt werden konnte, vergingen danach aber einige Minuten. Grund dürfte weniger das Wegspeichern der Datei aus dem DRAM-Cache sein, sondern vor allem die Indexierung durch Android. Einmal erfasst, lief das Video immer auf Anhieb. Ein Unterschied zwischen den Karten und dem internen Speicher ließ sich jedoch ausmachen: Auf dem internen Speicher stand das sehr große 4K-Video deutlich früher zur Verfügung, wenn auch nicht sofort. Bei kurzen Videos war die Verzögerung minimal.

Doch selbst wenn die Karten eigentlich flott genug sind, manche Einschränkung kann man auch mit den besten Karten nicht umgehen. So weigerte sich das Samsung Galaxy S7 standhaft, unkomprimierte RAW-Bilder auf der externen Speicherkarte abzulegen. Die sind beim Galaxy S7 rund 24 MByte groß, das ebenfalls gespeicherte JPEG dazu 4 MByte. Das wäre für die schnelleren Karten eigentlich kein Problem.

## Fazit

Die schnellsten UHS-II-Karten nutzen in Smartphones bislang nichts; dort sind UHS-I-Karten manchmal sogar schneller. Für die alltäglichen Aufgaben im Smartphone eignen sich alle Testkandidaten recht gut. Sie zeichnen Videos und Fotos in ausreichender Geschwindigkeit auf. Wer das Speicher-Interface seines Top-Smartphones ausreizen möchte, greift zu einer etwas schnelleren Karte. Beim Schreiben sind die beiden SanDisk-Ultra-Karten empfehlenswert, die auch zu den günstigsten Karten gehören, auch die Pro-Plus-Karten von Samsung sind schnell, aber teurer. Zum schnellen Lesen eignen sich fast alle Karten, nur die kleine Karte von Kingston und die Evo-Serie von Samsung bremsen selbst langsame Smartphones aus. (II) **ct**



## Kamera im Griff

Der Kameragriff LG Cam Plus erweitert das Smartphone LG G5 um Fototasten und Zusatzakku.

Der Cam Plus soll das Spitzen-Smartphone LG G5 zum vollwertigen Kameraersatz machen. Es handelt sich um einen ansteckbaren wulstigen Plastikgriff mit drei Tasten, einem Drehrad und 1200-mAh-Akku. Über den proprietären Magic Slot verbindet er sich mit dem Telefon. Dazu muss man den Akku kurzzeitig entnehmen und das Gerät neu starten. USB-C-Buchse und Lautsprecheröffnung besitzt auch das Zusatzmodul und leitet entsprechende Signale weiter.

Mit dem Griff liegt das G5 tatsächlich fast wie eine Kompaktkamera in der Hand. Die drei Tasten dienen als zweistufiger Auslöser, zum Starten der Videoaufzeichnung und zum Öffnen und Schließen der Kamera-App. Das Drehrad steuert den Digitalzoom.

Der Akku des Cam Plus taugt nicht als universeller Zusatzakku. Denn er lädt das Handy nicht kontinuierlich, sondern versorgt es jedes Mal nur fünf Minuten lang mit Strom, nachdem man eine der Kamerateasten gedrückt hat – aber nicht, wenn das Gerät komplett leer ist. Wie voll der Zusatzakku ist, erfährt man nur über eine LED, die rot leuchtet, wenn der Akkustand weniger als 10 Prozent beträgt. Einzige Funktion der zugehörigen App ist es, die Firmware-Version anzuzeigen. Für den hohen Preis bietet LG Cam Plus zu wenige Vorteile. (hcz)

### LG Cam Plus

#### Kameragriff

kompatibel mit	LG G5
Maße (H × B × T) / Gewicht	7,2 cm × 6 cm × 1,6 cm / 55 g
Akku	1200 mAh
Preis	40 €



## Zeitraffkünstler

Der mechanische Stativauflauf Flow-Mow dreht Kamera oder Smartphone um die eigene Achse – und sorgt so für spannende Zeitrafferaufnahmen.

Gleichmäßige Schwenks mit einer Videokamera wollen geübt sein – erst recht, wenn die Aufnahme als Zeitraffer wiedergegeben werden soll. Der Stativauflauf Flow-Mow automatisiert das Ganze und dreht die Kamera langsam und gleichmäßig im Kreis. Dazu wird Flow-Mow entweder zwischen Stativkopf und Kamera geschraubt oder direkt mit montierter Kamera auf einen ebenen Untergrund gestellt.

Der Aufsatz kommt ohne Batterie und Elektronik aus; statt eines Motors sorgt eine Feder für den nötigen Antrieb. Flow-Mow arbeitet wie eine Eieruhr: Man zieht ihn im Uhrzeigersinn auf, die Kamera dreht sich dann gegen den Uhrzeigersinn zurück – inklusive des eieruhrtypischen Tickens.

Es gibt zwei Varianten: Der schnellere Flow-Mow 2H dreht sich in zwei Stunden um volle 360 Grad, die 12H-Version benötigt dafür 12 Stunden. Bei beiden Versionen sind Laufzeit sowie der zu drehende Winkel aufgedruckt, sodass sich Endbild und Endzeitpunkt abschätzen lassen. Im Flow-Mow 12H steckt außerdem eine Wasserwaage.

Der Hersteller gibt an, dass sich Flow-Mow für bis zu 2 Kilogramm schwere Kameras eignen. Die meisten DSLRs sind jedoch nur im Fotomodus zu gebrauchen, da sie die Videoaufzeichnung – anders als Smartphone oder Action-Cams – nach spätestens 30 Minuten selbstständig beenden.

Flow-Mow eignet sich vor allem für sonst zu statisch aussehende Zeitraffer, etwa von Wolken, Baustellen oder Ebbe und Flut. Mit nur 75 Gramm Gewicht stört er im Rucksack nicht, sodass man ihn auf gut Glück mitnehmen kann. Etwas Zeit sollte man dann allerdings ebenfalls einpacken. (jk)

### Flow-Mow

#### Zeitraffer-Stativauflauf

Hersteller	Wolf und Wolf, www.flow-mow.com
Preis	30 € (2H-Version), 60 € (12H-Version)

# Starte neu durch!

Nutze deine Chance und  
finde die besten IT-Jobs.



[www.heise-jobs.de](http://www.heise-jobs.de)

 heise  
Jobs



Christian Wölbert

# Powerbanks von 15 bis 65 Euro

Externe Akkus laden leere Smartphones und Tablets unterwegs wieder voll. Dabei kommt es nicht nur auf die Kapazität an, sondern auch auf die Geschwindigkeit. Zwei der Powerbanks pumpen dank Quick Charge sogar rund 15 Watt ins Handy.

**A**ufgrund unserer Erfahrungen der vergangenen Tests günstiger Powerbanks haben wir die billigsten Modelle für diesen Testlauf von vornherein aussortiert und nur vielversprechende Kandidaten ausgesucht: Powerbanks von bekannten Marken wie Sony oder Samsung sowie ein paar Modelle mit guter Ausstattung von kleineren Anbietern, darunter zwei Powerbanks von Anker und Ravpower, die Qualcomms Quick-Charge-Technik unterstützen, also kompatible Smartphones besonders schnell laden.

Die von den Herstellern versprochene Energiemenge unserer Testkandidaten reicht von 12 bis 96 Wattstunden (Wh). Zum Vergleich: Ein typischer Smartphone-Akku speichert 8 bis 10 Wh, ein typischer Tablet-Akku 20 bis 30. Die kleinen Powerbanks von Sony und Samsung nehmen in der Hosentasche nicht mehr Platz weg als ein Handy und wiegen auch nicht mehr, die PowerCore+ von Anker hingegen ist schwerer als ein iPad.

Die Gehäuse wirken allesamt hochwertig, die Bedienung gibt keine Rätsel auf: Die meisten Powerbanks laden angeschlos-

sene Geräte sofort nach dem Einstöpseln, nur bei Pearl und Sony muss man einen Knopf drücken, damit es losgeht. Alle Modelle haben LEDs, die den Ladestand anzeigen. Spannender sind jedoch die inneren Werte: Wie viel Energie steckt wirklich in den Powerbanks, wie schnell laden sie angeschlossene Geräte und in welcher Zeit laden sie sich selbst wieder auf?

## Energiemenge

So viel vorweg: Dieses Mal passen die Angaben der Hersteller besser zu unseren



Testergebnissen als bei den im vergangenen Jahr getesteten Billigmodellen. Alle Kandidaten lieferten im Test mindestens 80 Prozent der versprochenen Energiemenge, die von Amazon und Anker sogar über 90 Prozent.

Um die Energiemenge zu bestimmen, haben wir die Powerbanks durch eine elektronische Last mit 5 Volt und 1 Ampere entladen und die entnommene Energie an einem Leistungsmessgerät (ZES LMG95) gemessen. Wir haben uns für 1 A entschieden, weil fast alle Powerbanks auf dem Markt das schaffen und viele Handys, zum Beispiel iPhones, beim Laden auch tatsächlich genau so viel Strom anfordern.

Bei höheren Entladeströmen steigen die Verluste in Kabeln und Steckern, sodass die angeschlossenen Geräte zwar schneller laden, den Powerbanks aber insgesamt etwas weniger Energie entlocken. Zum Vergleich haben wir zwei Probemessungen mit einem Entladestrom von 1,5 A durchgeführt. Am Ende zeigte das Leistungsmessgerät eine um gut 5 Prozent geringere Energiemenge an als bei der Messung mit 1 A.

Außerdem ermittelten wir mit dem Leistungsmessgerät, wie viel Energie nötig ist, um den Akku eines iPhone 6, eines Galaxy S6 und eines iPad Air 2 komplett zu füllen: 8,5 respektive 10,5 respektive 31 Wh. Dann berechneten wir, wie oft man mit einer Powerbank-Ladung den Geräte-Akku füllen kann. Zum Beispiel betankt die Samsung-Powerbank einen iPhone-6-Akku genau zwei Mal; die PowerCore+ von Anker schafft zehn Füllungen.

## Ladegeschwindigkeit

Die Ladegeschwindigkeit hängt von der Powerbank und vom angeschlossenen Gerät ab. Wenn eine Powerbank beispielsweise 2 A bei 9 V liefert, heißt das noch lange nicht, dass jedes Mobilgerät so viel Strom bekommt. Denn die meisten Smartphones und Tablets fordern eine Spannung von rund 5 Volt, wie im klassischen USB-Standard festgelegt. Außerdem ziehen die meisten Smartphones maximal 1,5 Ampere. Ein Ladestrom von 2 Ampere liegt schon an der Grenze der Belastbarkeit von USB-Steckern.

Darüber hinaus müssen auch noch die Ladeelektronik-Chips von Powerbank und Gerät zueinander passen. Zum Beispiel liefert die Samsung-Powerbank bis zu 2 A, lädt iPads aber nur mit 1 A. Deshalb haben wir an jede Powerbank nacheinander drei Smartphones (iPhone 6, Galaxy S6, LG G5) und zwei Tablets (iPad Air 2, Nexus 9) gestöpselt und Strom und Spannung mit

einem USB-Multimeter von Drok gemessen, das zwischen Powerbank und Handy gesteckt wird.

In der Praxis kann die Leistung sogar dann schwanken, wenn man nur eine Powerbank und nur ein zu ladendes Gerät hat. Zum Beispiel ziehen einige Smartphones weniger Strom, wenn das Display eingeschaltet ist. Außerdem kommt es vor, dass der Saft erst nach dem zweiten oder dritten Einstöpseln oder nach einigen Minuten Wartezeit richtig fließt.

Wir haben deshalb jede Powerbank mehrmals an jedes Gerät gestöpselt und das optimale Ergebnis notiert. Außerdem haben wir stets gemessen, während das Handy eingeschaltet, sein Display aber ausgeschaltet war (Standby-Modus). Die Akkus der Handys waren weniger als halbvoll, denn bei hohem Ladestand nippen viele nur noch an der Powerbank.

Auch das Kabel kann bremsen. Zum Beispiel saugte das Nexus 9 aus diversen Powerbanks durch eines unserer Kabel nur 0,8 Ampere, durch andere Kabel aber 1,4 Ampere. Wenn die Ladegeschwindigkeit wichtig ist, können wir deshalb nur empfehlen, sie zu kontrollieren. Das Drok-Multimeter misst sehr präzise und kostet gerade mal 13 Euro (Test in c't 24/15, S. 130). Die Pearl-Powerbank ist die einzige im Test, die den aktuellen Ladestrom auf ihrem Display anzeigt. Praktisch, auch wenn die Skala mit 0,2-Ampere-Schritten recht grob ausfällt.

Die Powerbank von Pearl hat zwei USB-Ports und versorgt zwei Geräte gleichzeitig

mit Strom. Probleme gab es nur, als wir an der Pearl-Powerbank ein iPad und ein weiteres Gerät (z. B. das G5 oder das Nexus 9) laden wollten: Die Spannung schwankte so stark, dass das iPad alle paar Minuten meldete, dass es nicht mehr geladen wird. Mit der PowerCore+ von Anker und der Turbo von Ravpower konnten wir jeweils drei Geräte parallel laden. Die PowerCore+ hat drei normale USB-Ausgänge, die Turbo zwei normale plus einen USB-C-Ausgang.

Auch Notebooks mit USB-C-Eingang kann man mit den Powerbanks laden. Die meisten Testkandidaten versorgten das 12-Zoll-Macbook mit 5 V und rund 2 A, die von Sony und Samsung lieferten nur 0,5 A.

## Quick Charge

In den vergangenen Jahren ist die Auswahl an Smartphones mit Qualcomms Schnellladetechnik Quick Charge 2.0/3.0 stark gestiegen. Ein paar Dutzend Modelle gehören dazu, zum Beispiel Samsungs S6, S7 und Note 4, Sonys Z4 und Z5, HTC's One, Google's Nexus 6 sowie LGs G4 und G5. Das Besondere an Quick Charge 2.0/3.0 ist die im Vergleich zum USB-Standard höhere zulässige Spannung von bis zu 12 Volt statt nur 5. Quick Charge 3.0 beherrscht mehr Abstufungen als 2.0.

Von den Powerbanks im Test unterstützen zwei Modelle Quick Charge: die Turbo von Ravpower und die PowerCore+ von Anker. Sie luden das LG G5 und das Samsung Galaxy S6 mit 7 bis 9 Volt und 1,5 bis 1,8 Ampere, also ungefähr doppelt so



Der 65 Euro teuren Anker-Powerbank liegt ein Quick-Charge-Netzteil bei.



### Sony CP-F1L (10,1 Wh)

Die 16-Euro-Powerbank von Sony ist die kleinste, leichteste und günstigste im Test. Sie passt locker in die Hosentasche und reicht gerade so für eine Galaxy-S6-Ladung. Der USB-Ausgang liefert maximal 5 Volt und 1,5 Ampere, am iPad sogar nur 1 Ampere.

- ⬆️ Netzteil inklusive
- ⬇️ liefert maximal 1,5 A
- ⬇️ lädt sich selbst langsam



### Samsung EB-PN920 (17 Wh)

Die schicke, flache, 40 Euro teure Samsung-Powerbank lädt nur aktuelle Samsung-Smartphones wie das S6 und das S7 mit 9 Volt, Geräte anderer Hersteller müssen sich mit 5 Volt begnügen. Die Abmessungen entsprechen denen eines 5-Zoll-Smartphones.

- ⬆️ liefert bis zu 2 A
- ⬆️ schickes Gehäuse
- ⬇️ relativ teuer



### Anker PowerCore (33 Wh)

Unter den 10 000-mAh-Modellen ist die kleine Anker-Powerbank die kompakteste und leichteste. Außerdem ist sie am schnellsten wieder vollgeladen, denn ihr Eingang verträgt bis zu 2 Ampere. Der Preis liegt bei moderaten 24 Euro.

- ⬆️ klein und leicht
- ⬇️ nur ein Ausgang

schnell wie die Powerbanks ohne Quick Charge. Binnen einer halben Stunde konnten wir den S6-Akku von 2 auf 58 Prozent aufladen. Auch mit dem modernen USB-Typ-C-Eingang des LG G5 spielt Quick Charge einwandfrei zusammen.

Die Samsung-Powerbank ist nicht Quick-Charge-zertifiziert, beherrscht aber Samsungs hauseigene Schnellladetechnik „Fast Charge“. Das Galaxy S6 lud sie im Test mit 9 V und 1,5 A. Das LG G5 wurde mit weniger Leistung betankt (5 V, 1,7 A).

## Selbstladung

Wie lange die Powerbanks ihrerseits benötigen, um vollzutanken, haben wir mit einer Master-Slave-Steckerleiste gemessen, die mit einer Uhr gekoppelt war. Fiel der Ladestrom an der Master-Steckdose unter einen definierten Wert, schaltete diese die anderen Steckdosen aus und die Uhr blieb stehen.

Wir haben alle Powerbanks mit ihrem maximalen Ladestrom geladen. Die von Sony und Pearl nehmen nur 5 V und 1 A an und laden dementsprechend langsam. Deutlich schneller füllen sich die großen Powerbanks von Anker und Ravpower,

denn sie unterstützen auch an ihrem Eingang Quick Charge. Die beiden zogen rund 15 Watt aus einem Quick-Charge-Netzteil.

## Fazit

Viel Geld muss man nicht ausgeben für eine zuverlässige und ergiebige Powerbank: Die kleine PowerCore von Anker kostet gerade mal um die 20 Euro, sie zickte im Test weder beim Handy-Aufladen noch beim Selbstladen. Die anderen Powerbanks machten ebenfalls keine Probleme, sodass wir auch sie empfehlen können, wenn man für Extras wie ein schickes, flaches Gehäuse (Samsung) oder ein LC-Display (Pearl) mehr Geld ausgeben will. Einzige Ausnahme

waren die Probleme der Pearl-Powerbank beim parallelen Laden von einem iPad und einem weiteren Tablet oder Smartphone.

Besitzt man ein Smartphone mit Quick Charge, lohnt sich der Aufpreis für eine passende Powerbank. Es spart einfach Zeit und Nerven, wenn der Handy-Akku in nur einer halben Stunde wieder halbvoll ist. Die PowerCore+ von Anker und die Turbo von Ravpower gibt es mit geringerer Kapazität als im Test schon ab 30 Euro. Ein Quick-Charge-Netzteil ist nur beim getesteten, großen Anker-Modell inklusive – den meisten Quick-Charge-Handys liegt aber auch eins bei. (cwo) **ct**

Quick-Charge-Liste: [www.ct.de/wfvp](http://www.ct.de/wfvp)

## Errechnete Anzahl Handy-Ladungen

Modell	iPhone 6s <small>besser ▶</small>	Galaxy S6 <small>besser ▶</small>
Anker PowerCore+	10,4	8,4
RAVPower Turbo	7,2	5,8
Anker PowerCore	3,9	3,1
Pearl Revolt	3,7	3,0
Samsung EB-PN920	2,0	1,6
Sony CP-F1LAM	1,2	1,0



## Pearl Revolt (31,7 Wh)

Nur einer der beiden Ports des Pearl-Modells lädt iPads mit 2 A, aber die Ports sind nicht beschriftet. Nach dem Einstöpseln zeigt immerhin das Display den Ladestrom an. Im Test sackte die Spannung ab, als wir ein iPad und ein weiteres Gerät luden.

- ⬆️ informatives Display
- ⬇️ Probleme beim parallelen Laden



## Anker PowerCore+ (88,4 Wh)

Der 65 Euro teure Gigant liefert genug Energie für fast drei iPad-Ladungen und lädt Smartphones mit Quick Charge wie das LG G5 und das Galaxy S6 besonders schnell. Außerdem kann man bis zu drei Geräte gleichzeitig betanken.

- ⬆️ Quick-Charge-Ein- und -Ausgang
- ⬆️ Quick-Charge-Netzteil inklusive
- ⬇️ schwer und klobig



## Ravpower Turbo (61,2 Wh)

Ähnlich sperrig wie der Konkurrent von Anker, liefert aber deutlich weniger Energie: Nur für zwei iPad-Ladungen reicht es. Lädt ebenfalls drei Geräte parallel. Einzige Powerbank im Test mit USB-Typ-C-Ausgang.

- ⬆️ Quick-Charge-Ein- und -Ausgang
- ⬆️ Variante mit Netzteil erhältlich
- ⬇️ klobig

## Powerbanks

Hersteller	Sony	Samsung	Anker	Pearl	Anker	RAVPower
Modell	CP-F1L	EB-PN920	PowerCore	Revolt (PX-1859-675)	PowerCore+	Turbo (RP-PB043-1)
Kapazität / Energiemenge (Herstellerangabe)	3500 mAh / 12 Wh	5200 mAh / 19,76 Wh	10 000 mAh / 36 Wh	10 000 mAh / k. A.	26 800 mAh / 96,48 Wh	20 100 mAh / 74,3 Wh
Lieferumfang	Micro-USB-Kabel, Netzteil	Micro-USB-Kabel	Micro-USB-Kabel, Hülle	Micro-USB-Kabel	Micro-USB-Kabel, Hülle, Netzteil	Micro-USB-Kabel, Hülle
Maße	12,9 cm × 7 cm × 1 cm	14,5 cm × 7 cm × 1,1 cm	9,1 cm × 6,1 cm × 2,1 cm	14,3 cm × 6,9 cm × 1,6 cm	17,8 cm × 7,9 cm × 2,4 cm	17,3 cm × 8 cm × 2,2 cm
Gewicht	130 g	152 g	180 g	271 g	584 g	373 g
<b>Ausstattung</b>						
Zahl der USB-Ausgänge	1	1	1	2	3	3 (davon 1 Typ C)
Input / Output bei 5 V (Herstellerangabe)	1 A / 1,5 A	2 A / 2 A	2 A / 2,4 A	1 A / 2,1 A, 1 A	2 A / 3 A	2 A / 3 A, 2,4 A, 2,4 A
Ladestandsanzeige	1 LED	4 LED	4 LED	LCD	10 LED	4 LED
<b>Messergebnisse</b>						
Energiemenge	10,1 Wh	17 Wh	33 Wh	31,7 Wh	88,4 Wh	61,2 Wh
Anzahl iPhone-6-Ladungen	1,2	2,0	3,9	3,7	10,4	7,2
Anzahl Galaxy-S6-Ladungen	1,0	1,6	3,1	3,0	8,4	5,8
Anzahl iPad-Air-2-Ladungen	0,3	0,5	1,1	1,0	2,9	2,0
lädt iPhone 6 / Galaxy S6 / LG G5	5 W / 6,5 W / 6,5 W	5 W / 13,5 W / 8,5 W	5 W / 7 W / 7,5 W	5 W / 7 W / 6,5 W	5 W / 13,5 W / 16,2 W	5 W / 13,5 W / 12,6 W
lädt iPad Air 2 / Nexus 9 mit	5 W / 7 W	5 W / 7 W	10 W / 7 W	10 W / 7 W	11 W / 7 W	10 W / 7 W
lädt zwei Geräte gleichzeitig	—	—	—	✓	✓	✓
Ladedauer [h]	01:58	02:55	04:20	06:05	08:58	05:14
Besonderheiten	—	Samsung Fast Charge	—	Taschenlampe	Quick Charge	Quick Charge
<b>Bewertung</b>						
Verarbeitung	⊕⊕	⊕⊕	⊕	⊕	⊕	⊕
Ausstattung	⊖	⊕	○	⊕	⊕⊕	⊕⊕
Straßenpreis	15 €	40 €	24 €	30 €	65 €	45 €

⊕⊕ sehr gut   ⊕ gut   ○ zufriedenstellend   ⊖ schlecht   ⊖⊖ sehr schlecht   ✓ vorhanden   — nicht vorhanden   k. A. keine Angabe





Christian Wölbert

# Outdoor-Powerbanks im Vergleich

GPS saugt viel Strom, deswegen brauchen Handys insbesondere auf Wanderungen und Fahrradtouren öfters Energienachschub. Zum Glück gibt es Outdoor-Powerbanks mit robustem und wasserdichem Gehäuse.

Nach unserem großen Powerbank-Test auf Seite 126 haben wir nun noch drei spezielle Outdoor-Modelle ins Testlabor geholt: Die Powerbanks von Pearl, Varta und Ravpower haben gummierte Gehäuse und schützen ihre USB-Anschlüsse mit Kappen. Sie müssen also nicht unbedingt im Trockenen bleiben und verkraften auch mal einen Sturz.

Alle drei Hersteller werben mit einem IP-Code, der angibt, wie gut die Gehäuse die Elektronik vor Fremdkörpern und Wasser schützen. Pearl gibt IP 65 an, Ravpower IP 66, Varta IP 67. Die erste Ziffer steht für den Schutz vor Fremdkörpern – 6 bedeutet staubdicht. Die zweite Ziffer steht für den Schutz gegen Wasser – 5 bedeutet Schutz gegen Strahlwasser, 6 Schutz gegen starkes Strahlwasser und 7 Schutz bei Tauchgängen von bis zu einer halben Stunde und bis zu einer Meter Tiefe.

Also haben wir die Powerbanks von Pearl und Ravpower abgespült und die Varta-Powerbank ins Wasser gelegt. Alle drei überstanden das schadlos, auch wenn sich unter der Klappe des Varta-Modells ein paar winzige Tröpfchen sammelten. Stürze auf den Steinboden machten den drei Kandidaten ebenfalls nichts aus.

Das Ravpower-Modell wirkt etwas empfindlicher als die beiden anderen, weil die Gummierung nur die Seiten schützt, aber

nicht die Ecken. Immerhin hat es eine Öse, und ein Karabinerhaken liegt bei. Man kann es also sicher am Gürtel oder Gepäck befestigen.

## Innere Qualitäten

Auch unsere drei klassischen Tests haben wir durchgeführt: Wie viel Energie kann man den Powerbanks in der Praxis tatsächlich entlocken, wie schnell laden sie angeschlossene Geräte und wie schnell laden sie sich selbst wieder auf? Dazu haben wir sie mit 1 Ampere entladen und die entnommene Energie gemessen, an ein paar weit verbreitete Smartphones und Tablets gehängt und die tatsächliche Ladeleistung gemessen sowie die Zeit beim Selbstaufladen gestoppt. Eine detaillierte Beschreibung der Messverfahren finden Sie auf Seite 126.

Obwohl die drei ungefähr gleich groß sind, speichert das Ravpower-Modell deutlich mehr Energie als die beiden anderen: genug Saft, um ein iPhone 6 dreieinhalb Mal aufzuladen. Die beiden anderen schaffen nur rund zwei Ladungen. Die Ladegeschwindigkeit hängt stets von der Powerbank und dem jeweils angeschlossenen Gerät ab. Zum Beispiel ziehen viele Smartphones maximal 1 Ampere, auch wenn die Powerbank mehr liefern könnte. Im Test luden die Modelle von Ravpower

und Varta unser iPad mit 2,2 Ampere, das Pearl-Modell schaffte auch noch gute 1,9 Ampere. Die Powerbanks von Varta und Ravpower haben je zwei Ausgänge und laden problemlos zwei Geräte gleichzeitig.

Die größeren Unterschiede gibt es beim Laden der Powerbanks selbst: Die Pearl-Bank zieht maximal 1 Ampere und nuckelte deshalb sechs Stunden an der Steckdose, bis sie wieder voll war. Die deutlich ergiebiger Ravpower-Bank war nach knapp fünf Stunden wieder voll, die Varta-Bank nach gut drei Stunden. So schnell geht das aber nur mit einem kräftigen USB-Netzteil, zum Beispiel dem weit verbreiteten ETA-U90E von Samsung oder Apples iPad-Netzteil. Nur die Powerbank von Ravpower versorgte angeschlossene Geräte mit Strom, während sie selbst an der Steckdose hing. Ein Netzteil ist bei keinem der drei Kandidaten inklusive.

Leider gibt es bislang keine Outdoor-Powerbank mit den proprietären Ladever-

## Errechnete Anzahl Handy-Ladungen

	iPhone 6 <small>besser ▶</small>
Pearl	2,01
Ravpower	3,42
Varta	1,98



### Pearl Revolt PB-52.0d (5200 mAh)

Die Powerbank von Pearl kostet 20 Euro und ist die günstigste im Test. Für 9 Euro verkauft Pearl auch eine kleinere Variante mit 2200 mAh. Der Testkandidat liegt griffig in der Hand, das gummierte Gehäuse verkratzt nicht schnell. Die Energie reicht für zwei iPhone-Ladungen. Einzige Besonderheit in puncto Ausstattung: die eingebaute Taschenlampe, die einige Meter weit leuchtet.

- 👍 günstig
- 👎 nur ein USB-Ausgang
- 👎 wird langsam geladen



### Ravpower Outdoor Powerbank (10 050 mAh)

Angesichts der hohen Kapazität ist das Ravpower-Modell überraschend kompakt, leicht und günstig – gerade mal 26 Euro kostet es bei Amazon. Die Ausstattung ist auch gut: Es gibt zwei Ausgänge, einen Eingang mit 2 Ampere für schnelles Selbstladen sowie eine kleine LED als Notlicht. Der USB-Eingang sitzt allerdings so tief im Gehäuse, dass nur die Stecker der beiden mitgelieferten Kabel passen.

- 👍 kompakt und leicht
- 👍 gute Ausstattung
- 👎 tief sitzender USB-Eingang



### Varta Indestructible Powerpack (6000 mAh)

Die Varta-Powerbank kostet gemessen an der Kapazität relativ viel. Das liegt auch am Gehäuse: Es wirkt sehr gut verarbeitet, eine Gummischicht schützt die Seiten und die Ecken, Stürze hinterlassen kaum Kratzer. Kurze Tauchgänge sind kein Problem. Die Ausgänge liefern 1 Ampere beziehungsweise 2,4 Ampere, der Eingang verträgt 1,8 Ampere. Die Ausstattung ähnelt damit der des Ravpower-Modells.

- 👍 hochwertiges Gehäuse
- 👍 gute Ausstattung
- 👎 relativ teuer

fahren Qualcomm QuickCharge oder Samsung FastCharge. Wer vor allem möglichst schnell laden will, muss deshalb mit einer weniger robusten Powerbank vorlieb nehmen, zum Beispiel von Samsung, Anker oder Ravpower. Das Besondere an Quick beziehungsweise FastCharge ist die im Vergleich zum USB-Standard höhere zulässige Spannung von bis zu 12 Volt statt nur 5 – dadurch lädt das Handy deutlich schneller, wenn es die Technik ebenfalls unterstützt.

## Fazit

Die Powerbank von Ravpower bietet eindeutig das beste Preis-/Leistungsverhältnis. Sie speichert viel Energie, lädt zwei Geräte gleichzeitig und tankt sich selbst schnell wieder voll. Wenn man mit zwei Extra-Ladungen für ein Smartphone zufrieden ist, reicht aber auch die günstige Pearl-Powerbank völlig aus, die außerdem als helle Taschenlampe dienen kann. Die teure Varta-Powerbank hat das robustere Gehäuse, aber keine bessere Ausstattung als das Ravpower-Modell. (cwo) **ct**

## Outdoor-Powerbanks

Hersteller	Pearl	Ravpower	Varta
Modell	Revolt PB-52.0d	Outdoor Powerbank (RP-PB-044)	Indestructible Powerpack 6000
Kapazität / Energiemenge (Herstellerangabe)	5200 mAh / k. A.	10 050 mAh / 37,1 Wh	6000 mAh / k. A.
Lieferumfang	Micro-USB-Kabel	2 Micro-USB-Kabel, Karabinerhaken	Micro-USB-Kabel, Schutzhülle
Maße	11,1 cm × 5,7 cm × 2,4 cm	11,9 cm × 7,1 cm × 2,3 cm	11,5 cm × 6,1 cm × 2,8 cm
Gewicht	173 g	211 g	234 g
<b>Ausstattung</b>			
Zahl der USB-Ausgänge	1	2	2
Input / Output (Herstellerangabe)	1 A / 2 A	2 A / 1 A, 2,4 A	1,8 A / 1 A, 2,4 A
Ladestandsanzeige	4 LED	4 LED	4 LED
<b>Messergebnisse</b>			
Energiemenge	17,1 Wh	29,1 Wh	16,8 Wh
Anzahl Galaxy-S6-Ladungen	1,6	2,8	1,6
Anzahl iPad-Air-2-Ladungen	0,6	0,9	0,5
lädt iPhone 6 Plus / Galaxy S6 mit	1,4 A / 1 A	1,5 A / 1,2 A	1,5 A / 1 A
lädt iPad Air 2 / Nexus 9 mit	1,9 A / 1,4 A	2,2 A / 1,4 A	2,2 A / 1,4 A
lädt zwei Geräte gleichzeitig	—	✓	✓
Laden und Entladen gleichzeitig	—	✓	—
Ladedauer [h]	06:07	04:44	03:16
Besonderheiten	Taschenlampen-Funktion	Taschenlampen-Funktion	—
<b>Bewertung</b>			
Verarbeitung	○	⊕	⊕⊕
Ausstattung	○	⊕	⊕
Straßenpreis	20 €	26 €	27 €
⊕⊕ sehr gut    ⊕ gut    ○ zufriedenstellend    ⊖ schlecht    ⊖ sehr schlecht ✓ vorhanden    — nicht vorhanden    k. A. keine Angabe			





Stefan Porteck, Alexander Spier

# Smartwatches für jeden Geschmack

So langsam verlassen die schlaun Uhren ihre Nerd-Nische: Die neuen Geräte bieten sinnvolle Smartphone-Ergänzungen. Viele Modelle zielen auf einen konkreten Anwendungsfall ab, etwa Trekking. Das klappt unterschiedlich gut.

**S**martwatches polarisieren: Die einen tun sie als nutzlose Spielzeuge ab, die anderen sehen sie als Chance für die Uhrenindustrie. Zur zweiten Gruppe gehört Jean-Claude Biver, seines Zeichens CEO bei Tag Heuer – der einzigen Schweizer Traditionsmarke, die derzeit eine Smartwatch im Angebot hat. Schon im Herbst 2015 wagte er die Prognose, dass Apple bald zu den größten Uhrenherstellern gehören könnte. Allen Kritikern zum Trotz könnte er damit Recht behalten: Denn wie Schweizer Medien berichten, hat Apple mit nur einem Smartwatch-Modell

schon jetzt die Marke Rolex beim Umsatz eingeholt.

Deutlich zeigt sich jedenfalls, dass Uhrenhersteller das Feld nicht kampflos Technikriesen wie Samsung, LG oder Apple überlassen wollen: Nach Tag Heuer sprangen auch Casio und mit der Fossil-Gruppe gleich die Marken Fossil, Diesel, DKNY, Skagen und Michael Kors auf den Zug auf.

Dieser neue Schwung sorgt zum einen für schickeres Design – was Uhren- und Modemarken offenbar besser beherrschen als IT-Größen – und zum anderen auch dafür, dass sich die Hersteller in der

zunehmenden dritten Generation deutlicher voneinander abheben und Nischen besetzen.

Das haben wir zum Anlass genommen, fünf aktuelle Exemplare zum Test in die Redaktion zu holen. Klassisch, edel und unauffällig beschreibt die Nische der „Tag Heuer Connected“. Casio wagt mit der WSD-F10 eine Hommage an G-Shock-Modelle und hat ein robustes Paket für den Outdoor-Einsatz geschnürt. Asus und Fossil steuern Modelle bei, die den Charme klassischer Analog-Uhren versprühen und dabei preislich sehr attraktiv sind. Pebble



hat den Smartwatch-Trend einst ins Rollen gebracht, somit darf auch die neue Pebble 2 HR nicht fehlen. Nach der Übernahme durch Fitbit wird die Pebble allerdings vom Markt verschwinden. Gerne hätten wir auch die Gear S3 von Samsung im Test gehabt, sie erreichte uns aber nicht mehr zum Redaktionsschluss.

## Allzeit bereit?

Die wichtigste Aufgabe einer Uhr bleibt unbestritten die Anzeige der Zeit. Bei Analog-Uhren geht das jederzeit mit einem flüchtigen Blick aufs Handgelenk. Doch smarte Uhren haben Displays statt mechanischer Zeiger. Hier kommen OLEDs, klassische LC-Displays oder transreflektive LCDs zum Einsatz – mit jeweils eigenen Vor- und Nachteilen.

Fossil nutzt bei der Q Marshal und anderen Modellen herkömmliche LCDs mit LED-Backlight. Deren Vorteil: Die RGB-Pixel-Matrix sorgt für eine gestochen scharfe Darstellung und die Helligkeit reicht locker aus, um die Uhr auch im prallen Sonnenlicht abzulesen. Kaum ein rundes Smartwatch-LCD ist allerdings vollständig rund, sondern unten abgeflacht und von einem schwarzen Streifen bedeckt, der vermutlich die Steuerleitungen kaschiert. So haben die Q Marshal und die WSD-F10 von Casio eine Auflösung von 320 x 300 Pixeln und zählen zu den Uhren, deren Display oft als Flat-Tire – also platter Reifen – verspottet wird.

Ist das Display immer an, reicht ein dezentler Blick aufs Handgelenk, um zu sehen, wer gerade anruft oder eine Nachricht geschrieben hat. Doch saugt die LED-Hintergrundbeleuchtung merklich am ohnehin stets knappen Akku. Wer eine Laufzeit von mehr als einem Tag wünscht, stellt im Einstellungs Menü besser ein, dass sich das Display nach wenigen Sekunden abschaltet.

Besonders dekorativ sieht ein schwarzes Display am Handgelenk allerdings nicht aus. Zudem muss man es stets per Fingertipp oder einer mehr oder weniger ausladenden Drehung des Handgelenks aufwecken. Im Alltag fanden wir das bald unpraktisch und lästig.

Grundsätzlich sieht die Situation bei Uhren mit OLEDs zwar genauso aus – etwa der Apple Watch und der Zenwatch 3. Aber immer eingeschaltet sind die organischen Displays leicht im Vorteil: Sie kommen nämlich dank der selbstleuchtenden Pixel ohne ganzflächige Hintergrundbeleuchtung aus. Somit benötigen nur die Pixel Energie, die tatsächlich leuchten. Mit

einem schwarzen Zifferblatt und dunklen Zeigern kann die Uhrenanzeige somit problemlos dauerhaft aktiv bleiben, ohne dass sich das massiv auf die Akkulaufzeit auswirkt. Bei großflächig hellen und bunten Zifferblättern ist der Vorteil aber dahin.

Zu den weiteren Vorteilen der OLEDs gehören ihre satten Farben und die knackige und kontrastreiche Darstellung. Ob man das bei den Mini-Displays wirklich braucht, sei dahingestellt – nett anzusehen ist es aber allemal.

## Im Sonnenlicht

Nachteil vieler OLEDs ist die geringere Helligkeit, weshalb sie in der Sommersonne schlecht ablesbar sind. Beim Display der Zenwatch 3 fiel uns zudem die Pen-Tile-Matrix des Displays störend auf, die für etwas unscharfe und an den Rändern leicht schillernde Buchstaben und Zeiger sorgt.

Tag Heuer hat sich bei der Connected für ein transreflektives LCD entschieden, wie man es von der Pebble und der Sony Smartwatch3 kennt. Solche Displays haben zwar auch ein LED-Backlight, aber mit einem wesentlichen Unterschied: Sie reflektieren einfallendes Licht, sodass man die Anzeige auch bei ausgeschalteter Hintergrundbeleuchtung erkennen kann. Je mehr Licht aufs Display fällt, desto besser die Lesbarkeit. Die Connected und die Pebble 2HR lassen sich damit unter allen Lichtverhältnissen gut ablesen, ohne dass dafür der Akku strapaziert wird.

Einziger Makel der Technik: Ohne Backlight wirkt das Display nahezu monochrom und auch bei aktiver Beleuchtung sehen die Farben auf der Connected etwas blas-

ser aus als bei den übrigen Testkandidaten. Das transreflektive LCD der Pebble 2 HR kann mit seiner Schwarzweiß-Darstellung mit keinem der anderen Testkandidaten mithalten.

Casio sucht einen sehr kreativen Ausweg aus dem Dilemma von Ablesbarkeit und Laufzeit: Die WSD-F10 hat in einer Sandwich-Bauweise zwei Displays. In der unteren Schicht steckt ein klassisches Farb-LCD. Darüber liegt ein monochromes Segment-Display ohne Backlight, wie man es von Taschenrechnern oder einfachen Digitaluhren kennt. Letzteres aktiviert sich automatisch, sobald das Farbdisplay ausgeht. So zeigt die Casio-Uhr jederzeit gut lesbar Uhrzeit, Datum und den Wochentag an.

Besonders praktisch: Aktiviert man den Timepiece-Modus, fährt die Uhr das Android-System herunter und nutzt nur die Digitaluhr-Anzeige. So soll der Akku bis zu einem Monat lang durchhalten. Auf die smarten Funktionen muss man dann aber verzichten.

## Helfer am Handgelenk

Wenn es um den Funktionsumfang geht, wird Smartwatches oft nachgesagt, dass ihnen das Killer-Feature fehlt. Sofern die Bezahl Dienste von Google und Co. irgendwann ihren Weg nach Deutschland finden, wäre drahtloses Bezahlen, bei dem man an der Kasse nur die Uhr kurz ans Terminal halten muss, beispielsweise eine wünschenswerte Funktion. Das klappt mit den getesteten Modellen aber noch nicht.

Dafür sorgen alle Smartwatch-Systeme zuverlässig dafür, dass man das Smart-



Die Tag Heuer Connected (links) und die WSD-F10 von Casio lassen sich auch bei ausgeschaltetem Backlight gut ablesen.

phone im Alltag kaum noch aus der Hosentasche ziehen muss: Nachdem sie über Bluetooth mit der passenden Companion-App auf dem Smartphone gekoppelt wurden, empfangen sie Benachrichtigungen und Inhalte und steuern andere Smartphone-Apps fern.

Im Idealfall kommen dafür einfache Wischgesten oder die bei beiden Systemen sehr gut funktionierende Sprachsteuerung zum Einsatz. So kann man mit allen Uhren im Test navigieren, die Musik- und Video-Wiedergabe am Smartphone steuern sowie Chat-Nachrichten und E-Mails lesen und sogar beantworten sowie sich an Aufgaben und Termine erinnern lassen [1]. Bei der Pebble muss man dafür Druckknöpfe bemühen. Das wirkt zwar anachronistisch, hat wegen der erfühlbaren Knöpfe aber den Vorteil, dass man beispielsweise beim Rad- oder Autofahren nicht hinsehen muss.

Die Android-Wear-Uhren funktionieren auch mit iPhones, da Google seine Android-Wear-App für iOS anbietet. Da Apple traditionell installierten Apps keine weitreichenden Zugriffe aufs Smartphone erlaubt, kann eine Android-Uhr am iPhone merklich weniger. Der umgekehrte Weg funktioniert überhaupt nicht. Die Pebble nimmt eine Sonderrolle ein: Sie läuft als einzige mit Android-Smartphones und iPhones.

## Fazit

Die Tag Heuer Connected ist ein Allrounder für solvente Käufer, die eine hochwertige Smartwatch als Lifestyle-Objekt wollen. Abgesehen von der Akkulaufzeit verbirgt sie durch ihr Aussehen, das Always-On-Display und die unaufdringlichen Zifferblätter größtenteils ihr smartes Innenleben und geht auch als teure Herrenuhr durch. Gleichzeitig steht sie den anderen Uhren in puncto Funktionsumfang in nichts nach. Das hat mit mehr als tausend Euro aber auch seinen Preis. Gemessen an der zu erwartenden Lebensdauer dürfte der den meisten zu hoch sein. Tag Heuer bietet deshalb ein Austauschprogramm an, bei dem man die Connected gegen Zuzahlung in eine mechanische Tag Heuer umtauschen kann, die als Einzelkauf teurer gewesen wäre.

Für iPhone-Nutzer kommt eigentlich nur die Apple Watch in Frage. Zwar lassen sich auch Android-Uhren koppeln, diese bieten aber aufgrund der Einschränkungen von iOS einen reduzierten Funktionsumfang und können so nicht mit der Apple Watch konkurrieren. Preislich ist



## Asus ZenWatch 3

Mit ihrem zweifarbigen Metallgehäuse strahlt die ZenWatch 3 von Asus eine gewisse Eleganz aus. Sie ist auffällig gestaltet, geht aber als normale Armbanduhr durch. Abgesehen von der Pebble ist sie die günstigste Uhr im Vergleich und ab 230 Euro erhältlich. Dafür muss man auf Zugaben wie GPS und Herzfrequenzmesser verzichten. Dank Lautsprecher und Mikrofon kann die ZenWatch zum Telefonieren benutzt werden, solange ein Smartphone verbunden ist.

Die Uhr reagiert flott auf Eingaben; die Oberfläche ruckelt jedoch häufig leicht. Von den drei Knöpfen startet einer eine beliebige App, der mittlere dient als Menüknopf und der dritte aktiviert den Energiesparmodus, der die Helligkeit dimmt und den Flugmodus startet. Der weit hervorstehende mittlere Knopf löst beim Anwinkeln des Handgelenks häufig ungewollt aus. Der Vibrationsmotor ist laut, aber nur schwach spürbar.

Das runde AMOLED-Display punktet mit kräftigen Farben, seine Pentile-Matrix lässt die Darstellung jedoch etwas krisselig erscheinen. Die Helligkeit reicht für die meisten Situationen; die Automatik regelt zuverlässig nach. Im prallen Sonnenlicht wird das Display schwer ablesbar und für die Nacht ist es selbst auf niedrigster Stufe zu hell. Mit einer Akkuladung hält die Uhr mit dunklem Ziffernblatt knapp bis zum Abend des Folgetages durch. Dank Schnellladetechnik sind nach 15 Minuten bereits 60 Prozent des Akkus wieder voll.

- ↑ günstig
- ↑ schickes und hochwertiges Gehäuse
- ↓ Menüknopf löst ungewollt aus
- ↓ weniger scharfes Display



## Casio WSD-F10

Die WSD-F10 von Casio kommt als Hommage an frühere G-Shock-Modelle: Mit rund sechs Zentimetern im Durchmesser ist sie riesig – und das gewollt. Die Uhr ist explizit als robuste Outdoor-Uhr gedacht. So erfüllt sie diverse Kriterien der US-Militär-Norm MIL-STD-810 für militärische Ausrüstung in Bezug auf Schock- und Vibrationsresistenz. Zudem ist sie bis zu 50 Meter wasserdicht und eignet sich zum Schwimmen und Tauchen.

Mittels Drucksensor, Kompass und Beschleunigungsmesser eignet sie sich besonders für Outdoor-Aktivitäten. Der obere der drei Buttons startet die Tool-App, die die Daten der eingebauten Sensoren grafisch schön aufbereitet aufs Display holt. Der untere Button startet eine benutzerdefinierte App.

Dank des cleveren zweischichtigen Displays hielt die WSD-F10 in unseren Tests stets zwei Tage durch. Im Kinomodus – bei dem das Farb-LCD nur auf Knopfdruck erwacht – war noch eine längere Laufzeit drin. Praktisch: Die vorinstallierte Outdoor-App stellt Daten wie Luftdruck, Höhenmeter oder den Kompass auch auf dem stromsparenden Monochrom-Display dar.

Im Vergleich zu Outdoor-Uhren von beispielsweise Garmin oder Suunto relativieren sich Preis und Größe der WSD-F10, doch viele Trekker würden sich sicher einen GPS-Sensor wünschen, um sie auch autark nutzen zu können und damit den Akku zu schonen.

- ↑ clevere Display-Technik
- ↑ robust und sehr funktional
- ↓ sehr groß
- ↓ unten abgeflachtes Runddisplay
- ↓ kein GPS



## Fossil Q Marshall

Die Q Marshal von Fossil erkennt man auf den ersten Blick kaum als Smartwatch: Sie ist schlanker als viele andere Android-Smartwatches und teilt sich ihr Gehäuse-Design mit anderen Uhren des Herstellers. Darüber hinaus installiert Fossil mehrere digitale Zifferblätter, die den Look eines analogen Chronographen überzeugend imitieren. Damit eignet sie sich vor allem für Interessenten, die eine günstige und unauffällige Uhr ohne viel Schnickschnack suchen.

Es gibt die Q Marshal in mehreren Farben und mit unterschiedlichen Armbändern. Dank des Standardmaßes von 22 Millimetern lassen sich auch alternative Armbänder aus dem Fachhandel anbringen.

Das runde, aber unten abgeflachte LCD lässt sich sehr gut ablesen und bietet genügend Helligkeitsreserven für Sonnentage. Es fehlt allerdings ein Umgebungslichtsensor, der die Display-Helligkeit automatisch anpasst. Im Test mussten wir die Helligkeit deshalb häufig manuell anpassen – insbesondere weil die Uhr sonst abends auf dem Sofa oder im Bett blendete.

Obgleich der Akku mit einer Kapazität von 360 mAh nicht überdurchschnittlich groß ist, hielt sie bei mäßiger Nutzung in unseren Tests locker zwei Tage und länger durch. Selbst wenn wir das Display häufig aufweckten, waren anderthalb Tage Laufzeit kein Problem. Danach mussten wir sie auf das magnetische Drahtlos-Ladepfättchen legen.

- ⬆ schick und variantenreich
- ⬆ lange Laufzeit
- ⬇ unten abgeflachtes Runddisplay
- ⬇ kein Helligkeitssensor



## Pebble 2HR

Am Aussehen der Pebble 2HR schieden sich in unserem Test die Geister: Viele fanden sie klein und hässlich, andere lobten ihren Nerd-Charme und die kompakte Bauweise. Ihr Display punktet zwar weder mit Größe noch feiner Auflösung, trotzdem bringt sie alle relevanten Information gut aufbereitet und angenehm lesbar rüber.

Traditionell funktioniert die Pebble mit Android-Geräten und iPhones. Das Pairing mit der zugehörigen Smartphones-App klappte im Test problemlos: App starten, Pebble-Account einrichten und das Pairing mit der Uhr bestätigen. Fertig. Fortan steht eine große Auswahl an nützlichen Apps zur Verfügung. Viele davon werden direkt auf der Uhr installiert und funktionieren auch ohne Smartphone.

Der optische Pulssensor lieferte bei unseren Tests zuverlässige Ergebnisse – zumindest, solange wir das Handgelenk ruhig hielten. Bei der Messung kommt der Pebble zugute, dass sie wegen ihrer geringen Größe und der weichen Armbänder sehr eng getragen werden kann, ohne zu drücken. Erfreulich: Schlaf-, Fitness- und Pulsdaten werden nicht zwingend bei Google oder anderen Portalen in die Cloud geladen.

Mangels Touchscreen werden alle smarten Funktionen über vier Tasten aufgerufen und gesteuert. Das klappt nach kurzer Eingewöhnung so gut, dass man die Pebble in Rekordzeit blind bedienen kann.

- ⬆ Android- und iOS-kompatibel
- ⬆ jederzeit gut ablesbar
- ⬆ sehr lange Laufzeit
- ⬇ ungewisse Zukunft
- ⬇ pixeliges Schwarzweiß-Display



## Tag Heuer Connected

Von unseren Testkandidaten ist die Tag Heuer Connected die eleganteste, hochwertigste und dezenteste Uhr. Hiermit wird man nicht darauf angesprochen, ob das eine dieser „Computer-Uhren“ ist, sondern ob es eine Tag Heuer ist. Sie kommt damit einer klassischen, mechanischen Herrenuhr optisch am nächsten. Mit Saphirglas und Titangehäuse bringt sie trotz ihrer Größe nur 82 Gramm auf die Waage.

Dank des transflektiven Displays lässt sie sich jederzeit sehr gut ablesen, ohne dass man das Display extra aufwecken müsste.

Für den authentischen und vor allem unauffälligen Look sind mehrere digitale Versionen originaler Tag-Heuer-Zifferblätter vorinstalliert. Sie unterdrücken die Android-Wear-typischen Einblendungen der Benachrichtigungskarten am unteren Displaybereich und blenden stattdessen einen kleinen Message-Counter mit der Anzahl der aktuellen Benachrichtigungen ein.

Neben dem hohen Preis ist die verwendete Intel-Technik ein Wermutstropfen: Die Connected ist zwar nicht unangenehm lahm, reagiert aber beim Starten von Apps nicht so flott wie die anderen Kandidaten mit Snapdragon-Chips. Zudem scheint die Intel-CPU stärker am Akku zu saugen – mehr als ein Tag ohne Aufladen ist nicht drin. Die mitgelieferte Ladeschale sollte man deshalb auch auf sehr kurzen Reisen dabei haben.

- ⬆ sehr schick und dezent
- ⬆ jederzeit gut ablesbar
- ⬇ geringe Laufzeit
- ⬇ sehr teuer





Das Schwarzweiß-Display der Pebble kann man unter Sonnenlicht sehr gut ablesen, es ist aber kein Touchscreen.

letztere zwar ebenfalls in der oberen Region angesiedelt, besticht aber mit einem guten Display und tadelloser Verarbeitung.

Die Casio-Uhr macht keinen Hehl daraus, voll und ganz eine Outdoor-Uhr zu

sein, die bei Wanderungen, Rad- oder Trekking-Touren zuverlässig zur Seite steht. Dabei helfen die Robustheit, das clevere Always-On-Display und die vielen praktischen Infos und Tools, die Casio in die vorinstallierte App „Moment Setter“ integriert hat. Wer länger unterwegs ist, wird zu schätzen lernen, dass sie sich ohne Aufladen bis zu einem Monat als konventionelle Digitaluhr nutzen lässt. Ihre riesigen Dimensionen wird man ihr nachsehen. Ebenfalls den Preis, der dem anderer Outdoor-Uhren entspricht. Dass die WSD-F10 jedoch keinen eingebauten GPS-Empfänger hat, ist angesichts der Zielgruppe unverständlich.

Wer für wenig Geld eine alltagstaugliche Smartwatch mit normalem Funktionsumfang sucht, sollte einen Blick auf die günstigen und trotzdem schicken Modelle von Asus und Fossil werfen. Sie werden in verschiedenen Gehäuse- und Armband-Konfigurationen angeboten. Technisch unterscheiden sie sich nur unwesentlich. Beim Display bleiben beide leicht hinter den anderen Testkandidaten

zurück. Die Entscheidung zwischen Q Marshall oder Zenwatch sollte man davon abhängig machen, ob man ein rundes OLED mit etwas geringerer Schärfe wünscht oder die bessere Lesbarkeit des nicht komplett runden LC-Displays bevorzugt.

Die Pebble 2 HR wandelt ein wenig zwischen den Welten: Nicht jeder dürfte sie als vollwertige Smartwatch wahrnehmen. Andere lieben sie gerade wegen ihrer 8-Bit-Animationen und dem Retro-Charme. Tatsächlich kann sie, abgesehen vom fehlenden Touchscreen, mit den anderen Smartwatches mithalten. Zudem macht sie mit ihrem günstigen Preis und dem Pulssensor auch als Fitness-Tracker eine gute Figur. Doch nach der Übernahme des Herstellers hat die Pebble keine Zukunft mehr.

(spo) **ct**

## Literatur

[1] Achim Barczok, Jan-Keno Janssen, Stefan Porteck, Uhrenvergleich, c't 13/15, S. 108

## Smartwatches

Modell	Zenwatch 3	WSD-F10	Q Marshall	Pebble 2HR	Connected
Hersteller	Asus	Casio	Fossil	Pebble	Tag Heuer
<b>Gehäuse</b>					
Größe (L × B × H)	45 mm × 45 mm × 11 mm	62 mm × 52 mm × 16 mm	45 mm × 45 mm × 14 mm	40 mm × 30 mm × 11 mm	52 mm × 52 mm × 13 mm
Gewicht	58 g	93 g	76 g	32 g	82 g
wasserfest	max. 1 m	50 m	max. 1 m	30 m	max. 1 m
Akku / wechselbar	340 mAh / –	330 mAh / –	360 mAh / –	k. A.	410 mAh / –
Druckknöpfe (Anzahl)	3	3	1	4	1
<b>Ausstattung</b>					
Betriebssystem	Android Wear	Android Wear	Android Wear	Pebble OS	Android Wear
Steuerung	Touch, Sprache	Touch, Sprache	Touch, Sprache	Druckknöpfe, Sprache	Touch, Sprache
Display Typ / Diagonale	OLED / 1,39"	IPS-LCD / 1,34", monochromes Segment-LCD	IPS-LCD / 1,42"	transflekatives Monochrom-LCD / 1,25"	transflekatives IPS-LCD / 1,5"
Auflösung	400 × 400 Pixel (287 dpi)	320 × 300 (239 ppi)	320 × 300 Pixel (245 dpi)	144 × 168 (172 dpi)	360 × 360 Pixel (240 dpi)
Prozessor	Snapdragon Wear 2100, 1,1 GHz	Snapdragon 400, 1,0 GHz	Snapdragon Wear 2100, 1 GHz	ARM Cortex M4, k. A.	Intel-Dual-Core, 1,6 GHz
Speicher	512 MB RAM, 4 GB Flash	512 MB RAM, 4 GB Flash	512 MB RAM, 4 GB Flash	64 KB, 8 MB Flash	1 GB RAM, 4 GB Flash
Lautsprecher / Kopfhöreranschluss	✓ / –	– / –	– / –	– / –	– / –
Mikrofon / Kamera	✓ / –	✓ / –	✓ / –	✓ / –	✓ / –
Sensoren	Beschleunigung, Umgebungslicht	Beschleunigung, Höhe, Kompass	Beschleunigung	Beschleunigung, Puls, Umgebungslichtsensor	Beschleunigung
Funkstandards	Bluetooth 4.1	Bluetooth 4.0	Bluetooth 4.1	Bluetooth 4.1	Bluetooth 4.1
Akkulaufzeit	bis zu zwei Tage	bis zu drei Tage, im Uhrenmodus bis zu einem Monat	bis zu zwei Tage	7 bis 10 Tage	ein Tag
Besonderheiten	Armband austauschbar (universell)	Dual-Layer-Display jederzeit gut ablesbar	Armband austauschbar (universell)	bei Sonnenlicht und ohne eingeschaltetes Display ablesbar	bei Sonnenlicht und ohne eingeschaltetes Display ablesbar
<b>Bewertung</b>					
Display	⊖	⊕	○	⊕	⊕
Funktionsumfang	○	⊕	○	⊕	○
Laufzeit	○	⊕	○	⊕⊕	⊖
Bedienung	⊕	⊕	⊕	⊕	⊕
Preis	270 €	500 €	300 €	130 €	1350 €
⊕⊕ sehr gut   ⊕ gut   ○ zufriedenstellend   ⊖ schlecht   ⊖⊖ sehr schlecht   ✓ vorhanden   – nicht vorhanden   k. A. keine Angabe					

# IMPRESSUM

**ct Android**

23. 1. 2017

## Redaktion

Postfach 61 04 07, 30604 Hannover  
Karl-Wiechert-Allee 10, 30625 Hannover  
Telefon: 05 11/53 52-300  
Telefax: 05 11/53 52-417  
Internet: [www.ct-special.de](http://www.ct-special.de)

**Leserbriefe und Fragen zum Heft:** [android@ct.de](mailto:android@ct.de)  
Die E-Mail-Adressen der Redakteure haben die Form [xx@ct.de](mailto:xx@ct.de) oder [xxx@ct.de](mailto:xxx@ct.de). Setzen Sie statt „xx“ oder „xxx“ bitte das Redakteurs-Kürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

**Chefredakteur:** Dr. Jürgen Rink (jr)  
(verantwortlich für den Textteil)

**Konzeption:** Alexander Spier (asp)

**Koordination:** Sophia Zimmermann (ssi)

**Redaktion:** Jo Bager (jo), Achim Barczok (acb), Daniel Berger (dbe), Holger Bleich (hob), Dieter Brors (db), Hannes A. Czerulla (hcz), Jan-Keno Janssen (jkj), André Kramer (akr), Lutz Labs (ll), Urs Mansmann (uma), Stefan Porteck (spo), Jürgen Schmidt (ju), Alexander Spier (asp), Jörg Wirtgen (jow), Christian Wölbelt (cwo), Sophia Zimmermann (ssi)

**Mitarbeiter dieser Ausgabe:** Tam Hanna, Christian Kausche, Michael Spreitzenbarth, David Wischnjak

**Assistenz:** Susanne Cölle (suc), Tim Rittmeier (tir), Sebastian Seck (sbs), Christopher Tränkmann (cht), Martin Triadan (mat)

**DTP-Produktion:** Wolfgang Otto (Ltg.), Ben Dietrich Berlin, Martina Fredrich, Jürgen Gonnermann, Jörg Gottschalk, Birgit Graff, Angela Hilberg, Anja Kreft, Martin Kreft, Astrid Seifert, Edith Tötsches, Dieter Wahner, Dirk Wollschläger, Brigitta Zurhieden

**ePaper-Produktion:** Klaus Ditze (Ltg.), Nicole Tiemann

**Art Direction:** Hea-Kyoung Kim (Art Director Junior)

**Fotografie:** Andreas Wodrich, Melissa Ramson

**Titelbild und Aufmacher-Produktion:** Thomas Saur, [www.tsamedien.de](http://www.tsamedien.de)

## Verlag

Heise Medien GmbH & Co. KG  
Postfach 61 04 07, 30604 Hannover  
Karl-Wiechert-Allee 10, 30625 Hannover  
Telefon: 05 11/53 52-0  
Telefax: 05 11/53 52-129  
Internet: [www.heise.de](http://www.heise.de)

**Herausgeber:** Christian Heise, Ansgar Heise, Christian Persson

**Geschäftsführer:** Ansgar Heise, Dr. Alfons Schröder

**Mitglieder der Geschäftsleitung:** Beate Gerold, Jörg Mühle

**Verlagsleiter:** Dr. Alfons Schröder

**Anzeigenleitung:** Michael Hanke (-167)  
(verantwortlich für den Anzeigenteil),  
[www.heise.de/mediadaten/ct](http://www.heise.de/mediadaten/ct)

**Anzeigenverkauf:** Verlagsbüro ID GmbH & Co. KG,  
Tel.: 05 11/61 65 95-0, [www.verlagsbuero-id.de](http://www.verlagsbuero-id.de)

**Leiter Vertrieb und Marketing:** André Lux (-299)

**Service Sonderdrucke:** Julia Conrades (-156)

**Druck:**  
Dierichs Druck + Media GmbH & Co. KG  
Frankfurter Straße 168  
34121 Kassel

**Vertrieb Einzelverkauf:**  
VU Verlagsunion KG  
Meßberg 1  
20086 Hamburg  
Tel.: 040/3019 1800, Fax: 040/3019 145 1800  
E-Mail: [info@verlagsunion.de](mailto:info@verlagsunion.de)

**Einzelpreis:** € 9,90; Österreich € 10,90; Schweiz CHF 17,50;  
Benelux, Italien, Spanien € 10,90

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung des Verlags in irgendeiner Form reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Die Nutzung der Programme, Schaltpläne und gedruckten Schaltungen ist nur zum Zweck der Fortbildung und zum persönlichen Gebrauch des Lesers gestattet.

Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Honorierte Arbeiten gehen in das Verfügungsrecht des Verlages über. Sämtliche Veröffentlichungen in ct erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes.

Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Printed in Germany. Alle Rechte vorbehalten. Gedruckt auf Recyclingpapier.

© Copyright 2017 by Heise Medien GmbH & Co. KG

**2 x Make mit  
35 % Rabatt testen.**

**Ihre Vorteile:**

- ▶ 2 Hefte mit 35% Rabatt testen
- ▶ Zusätzlich digital lesen über iPad oder Android-Geräte
- ▶ Zugriff auf Online-Artikel-Archiv\*
- ▶ Versandkostenfrei

**Für nur 12,90 Euro statt 19,80 Euro.**  
\* Für die Laufzeit des Angebotes.

**Gegen Wissensdurst  
und Kabelbrand!**

**[www.make-magazin.de/miniabo](http://www.make-magazin.de/miniabo)**

Hier können Sie direkt bestellen und finden weitere Informationen.

**Tel.: 0541 80 009 125 E-Mail: [leserservice@make-magazin.de](mailto:leserservice@make-magazin.de)**

(Mo.-Fr. 8-19 Uhr, Sa. 10-14 Uhr)





David Wischnjak

# Android-Apps dekompilieren, um undokumentierte APIs zu analysieren

Fast jede Android-App lässt sich mit kostenlosen Tools in ihren Quelltext zurückwandeln. So kann man vom Code anderer lernen und undokumentierte Schnittstellen von Smartphones und Tablets begutachten.

**A**ndroid ist im Prinzip vorbildlich dokumentiert. Trotzdem gibt es Lücken, auf die man schnell stößt, wenn man ungewöhnlichere Ideen umsetzt. Das ist zum Beispiel der Fall, wenn man hersteller- oder gerätespezifische APIs ansteuern will – denn die sind selten gut beschrieben.

Oftmals gibt es aber bereits Apps im Google Play Store, die genau die gewünschten Funktionen ausführen. Ein Blick in deren Quellcode würde bestimmt helfen, doch nur wenige Programmierer veröffentlichen diesen. Da die meisten Android-Apps aber in Java geschrieben sind, lassen sie sich im Vergleich zu Programmen aus

nativem Code hervorragend dekompilieren, also in Quelltext rückübersetzen.

Das mehrere Jahre alte Sony Xperia SP ist so ein Fall. Am unteren Gehäuserand befindet sich eine transparente Leiste, die bei neuen Nachrichten farbig aufleuchtet oder im Takt zur abgespielten Musik pulsiert – dank RGB-LEDs sogar in beliebiger Farbe.



Für diese Android-untypische LED-Leiste hat Sony zwar ein experimentelles „Illumination Bar API“ veröffentlicht, das jedoch nur sehr eingeschränkten Zugriff auf die LEDs erlaubt. Dass mehr geht, verrät die im Play Store erhältliche App U-Disco, die jede LED einzeln ansteuert und ihre Farbe und Helligkeit verändert – wenn auch nur mit Root-Zugriff. Ein Blick in den Quelltext könnte Aufschluss geben, wie man die LED-Leiste selbst zum Leuchten bringt.

## Dekomplier-Werkzeuge

Über die Kommandozeile lassen sich Apps mit „apktool“, „dex2jar“ und „Java Decompiler“ dekompileieren, online mit der Webseite „decompileandroid.com“. Selbst auf dem Smartphone kann man installierte Apps direkt rückübersetzen, und zwar mit der App „Show Java“. Als vierte Möglichkeit bieten sich außerdem spezialisierte Reverse-Engineering-IDEs wie „jadx“ an.

Mit jadx lässt es sich besonders komfortabel arbeiten, denn im Vergleich erkannte die Software in unseren Tests beim Dekompilieren unter anderem mehr Variablenamen richtig, außerdem ist die grafische Oberfläche praktisch und übersichtlich. Zu haben ist jadx kostenlos auf GitHub, es setzt ein installiertes Java Runtime Environment (JRE) voraus. Eine Installation von jadx selbst ist nicht notwendig, das Zip-Archiv mit den Programmdateien muss nur entpackt werden.

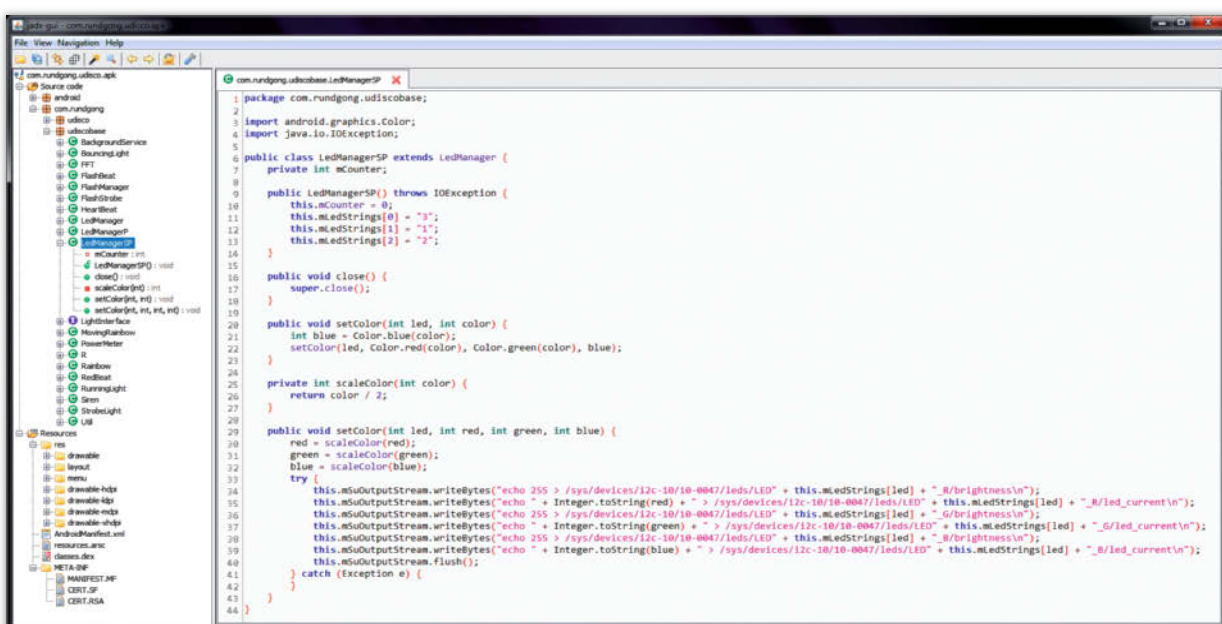
**Das Sony Xperia SP hat eine transparente Leiste mit farbig leuchtenden LEDs – wie sie angesteuert werden, ist von Sony aber nur unvollständig dokumentiert.**



Als Erstes benötigt man für das Dekompilieren die Installationsdatei der Anwendung. Da man diese nicht direkt von Google im Play Store erhält, muss man die Anwendung entweder zunächst auf einem Handy installieren und danach als APK extrahieren – das geht beispielsweise mit dem „APK Extractor“ von „meher“ – oder über Backup-Werkzeuge wie Helium auf den PC kopieren. Alternativ lassen sich die Apps auch direkt aus dem Play Store auf einen Desktop-PC herunterladen, etwa mit

dem Java-basierten Software-Paket Racoon. Man benötigt dafür wie auf dem Smartphone ein Google-Konto.

Zum Dekompilieren wird der APK-Decompiler jadx über das im Unterverzeichnis bin befindliche Skript jadx-gui (OS X, Linux) oder jadx-gui.bat (Windows) gestartet. Direkt zu Anfang erscheint ein Dateiwahl-Dialog, in dem man die APK auswählt – im Fall von Udisco ist das com.rundgong.udisco.apk. Daraufhin wird die App automatisch dekompiert und ihr Inhalt angezeigt.



Die Java-Software jadx dekompileiert Android-Apps und zeigt ihren Code an.

```

public void setColor(int led, int red, int green, int blue) {
    red = scaleColor(red);
    green = scaleColor(green);
    blue = scaleColor(blue);
    try {
        this.mSuOutputStream.writeBytes("echo 255 > /sys/devices/i2c-10/10-0047/leds/LED" + this.mLedStrings[led] + "_R/brightness\n");
        this.mSuOutputStream.writeBytes("echo " + Integer.toString(red) + " > /sys/devices/i2c-10/10-0047/leds/LED" +
            this.mLedStrings[led] + "_R/led_current\n");
        this.mSuOutputStream.writeBytes("echo 255 > /sys/devices/i2c-10/10-0047/leds/LED" + this.mLedStrings[led] + "_G/brightness\n");
        this.mSuOutputStream.writeBytes("echo " + Integer.toString(green) + " > /sys/devices/i2c-10/10-0047/leds/LED" +
            this.mLedStrings[led] + "_G/led_current\n");
        this.mSuOutputStream.writeBytes("echo 255 > /sys/devices/i2c-10/10-0047/leds/LED" + this.mLedStrings[led] + "_B/brightness\n");
        this.mSuOutputStream.writeBytes("echo " + Integer.toString(blue) + " > /sys/devices/i2c-10/10-0047/leds/LED" +
            this.mLedStrings[led] + "_B/led_current\n");
        this.mSuOutputStream.flush();
    } catch (Exception e) {
    }
}

```

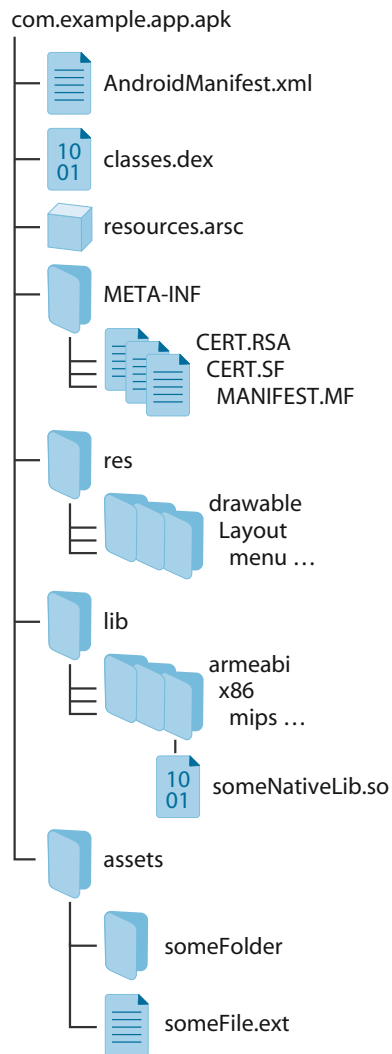
Die Methode `setColor` definiert die Stromstärke für die RGB-LEDs und erzeugt dadurch die Farbe und Helligkeit der LED-Leiste.

## Aufbau von Android-APKs

Android-Apps werden in Form von „Android Application Packages“ (APKs) verteilt. Eine solche APK ist im Grunde nur ein Zip-Archiv und lässt sich mit Packprogrammen wie 7-Zip problemlos öffnen. Im Inneren finden sich üblicherweise an oberster Stelle die Dateien `classes.dex` und `resources.arsc` sowie das `AndroidManifest.xml`. Die `classes.dex` enthält den Bytecode für die Dalvik-VM, und die `resources.arsc` ist ein komprimiertes Archiv für die Ressourcen der App wie Grafiken, String-Tabellen oder DPI-abhängige Bildschirm-Layouts. Ressourcen können sich aber auch unkomprimiert im Ordner `res` befinden.

Das Android-Manifest enthält verschiedene Meta-Daten wie den Paketnamen oder die benötigten Berechtigungen – die App kann später nur auf Schnittstellen zurückgreifen, die hier angefordert sind. Im Ordner `META-INF` befinden sich Zertifikate sowie Prüfsummen und im `lib`-Ordner vorkompilierter, nativer Code, sortiert in Unterordner nach Prozessorarchitektur. Beliebige weitere Dateien wie SQLite-Datenbanken oder Audio beherbergt der `assets`-Ordner.

Im Prinzip ist eine Android-APK ein Zip-Archiv, das unter anderem den kompilierten Java-Code sowie Meta-Informationen zum Programm enthält.



Unter „File/Preferences/Editor font“ kann man eine besser lesbare Schriftart einstellen, beispielsweise Consolas. Der Quelltext der App hat einen Java-typischen Aufbau, bestehend aus Packages mit entsprechenden Ordnern und Klassen. Im Package `android` befindet sich in der Regel nur allgemeiner Android-Code wie die Support-Library, es ist also für die LED-Ansteuerung uninteressant.

### App-OP

Ausgangspunkt ist die Klasse `MainActivity`, die sich im Package `com.rundgong.udisco` befindet. Sie enthält vor allem Code für die Bedienoberfläche. Beim Durchscrollen fällt aber eine Instanz der Klasse `LedManager` ins Auge – sie könnte sich dem Namen nach um die Ansteuerung der LEDs kümmern.

Definiert ist die Klasse `LedManager` im Package `com.rundgong.udiscobase`. Dort sind außerdem zwei ähnlich klingende Klassen `LedManagerP` und `LedManagerSP` gelistet. Bei näherer Betrachtung wird klar, dass die beiden letzteren Klassen ihre Eigenschaften von der ersten erben und dabei einige ihrer Methoden überschreiben. Genauer verrät wiederum ein Blick in die `MainActivity`, denn sie lässt sich von der Klasse `BackgroundService` eine Instanz von `LedManager` zurückgeben.

```

this.mLedManager = BackgroundService.getLedManager();

```

Diese im Package `com.rundgong.udiscobase` befindliche Klasse entscheidet in der Methode `getLedManager()`, welche der drei `LedManager`-Varianten zurückgegeben werden soll – und zwar abhängig vom Geräte-Modell. Für das Xperia SP ist die Klasse

LedManagerSP zuständig, für das Xperia P Led-ManagerP. Für unser Testgerät ist somit die Klasse LedManagerSP interessant, die wir im Listing-Kasten auf Seite 140 abgedruckt haben.

Der Zugriff auf die LEDs erfolgt direkt über Linux-Geräte Dateien mithilfe von Shell-Befehlen, ausgeführt als Superuser. Ferner ist aus dem Code der Methode setColor() zu entnehmen, dass insgesamt 18 solcher Dateien für die Ansteuerung verantwortlich sind. Jede der drei RGB-LEDs hat drei Farbkomponenten (Rot, Grün und Blau) und zu jeder von ihnen gehören wiederum zwei Dateien. Die zwei Dateien pro Farbe kommen zustande, weil sowohl die Helligkeit (brightness) als auch die Stromstärke (current) mit Werten zwischen 0 und 255 beschrieben werden müssen, wobei U-Disco die Farbe und Helligkeit offensichtlich nur über die Stromstärke kontrolliert und den brightness-Wert dauerhaft auf 255 (Maximum) setzt. Bei anschließenden Experimenten mit der LED-Leiste über das Android-Terminal hatten wir hingegen bessere Ergebnisse, wenn wir die Span-

nung konstant auf 255 setzten und stattdessen die Helligkeit variierten.

## Stolpersteine

Das Finden der gesuchten Funktionsaufrufe war in unserem Beispiel vergleichsweise leicht, denn die App U-Disco ist recht klein, gut strukturiert und in purem Java geschrieben. Außerdem war sie nicht eng verzahnt mit herstellerspezifischen Frameworks. Letzteres führt oft zu mehr Aufwand, zum Beispiel wenn man vorinstallierte System-Apps untersucht.


Aber auch im Idealfall ist rückübersetzter Java-Code selten problemlos lesbar, denn nicht alles lässt sich aus dem Bytecode wieder vollständig rekonstruieren. Bei komplizierteren Methoden erfordert es nicht selten viel Zeit, den bereits vom Compiler optimierten Code zu verstehen.

Weitere Schwierigkeiten ergeben sich, wenn der Entwickler den Code bewusst verschleiert. Ein Entwickler kann das Dekompilieren seiner Java-App zwar nicht verhindern, wohl aber die Lesbarkeit er-

schweren, indem beim Kompilieren alle Variablen, Klassen und Methodennamen zu nichtssagenden Zeichenketten umbenannt werden.

Zudem gibt es bei Android die Möglichkeit, in C/C++ geschriebene native Funktionen zu nutzen – was vor allem bei performancekritischen Anwendungen zum Einsatz kommt. Diese Programmteile liegen dann gesondert im .SO-Format vor und lassen sich nur schwer dekompilem.

Ebenfalls Probleme bereiten Android-Programme, welche nicht in reinem Java, sondern mit Xamarin/Mono oder Basic4-Android (B4A) entwickelt wurden. Während B4A-Apps durch die Übersetzung aus Basic und den zusätzlichen Wrappercode nur etwas aufgebläht und kompliziert wirken, lassen sich die mit Xamarin/Mono geschriebenen Apps nur mit Mehraufwand entschlüsseln. Dies liegt am Mono/.NET-Code, der zusätzlich einen passenden .NET-Decompiler erfordert.

(acb) 

Alle Tools und Apps: [www.ct.de/w7fg](http://www.ct.de/w7fg)

Die heise Security Tour 2017

# Komplexe Angriffe intelligent verteidigen



## Themenschwerpunkte:

- IoT: Sicherheit im Internet der Dinge
- DDoS: Schutz vor massiven Attacken
- Threat Intelligence
- Neue rechtliche Anforderungen an die IT-Sicherheit
- Social Engineering

**TERMINE:** 25. April, Köln    27. April, Hamburg    4. Mai, Wien  
9. Mai, Stuttgart    11. Mai, München

\* Die ersten 30 Teilnehmer erhalten Ihr Ticket zu 456,00 Euro (anstatt 570,00 Euro)

Weitere Infos und Anmeldung unter: [www.heisec.de/tour](http://www.heisec.de/tour)

**Sichern Sie sich schnell  
Ihr Ticket aus dem  
Early-Bird-Kontingent!\***

- 100% unabhängig
- hochkarätige Referenten
- Praxisrelevanz der Vorträge
- hervorragende Plattform zum Networking und Erfahrungsaustausch
- begleitende Ausstellung mit Informationen über die neuesten IT-Lösungen & -Produkte

Sponsoren:

 **dacoso**  
data communication solutions  
in Zusammenarbeit mit  
 **ADVA**  
Optical Networking

 **ectacom**  
**KASPERSKY**

 **Trustwave**  
Smart security on demand

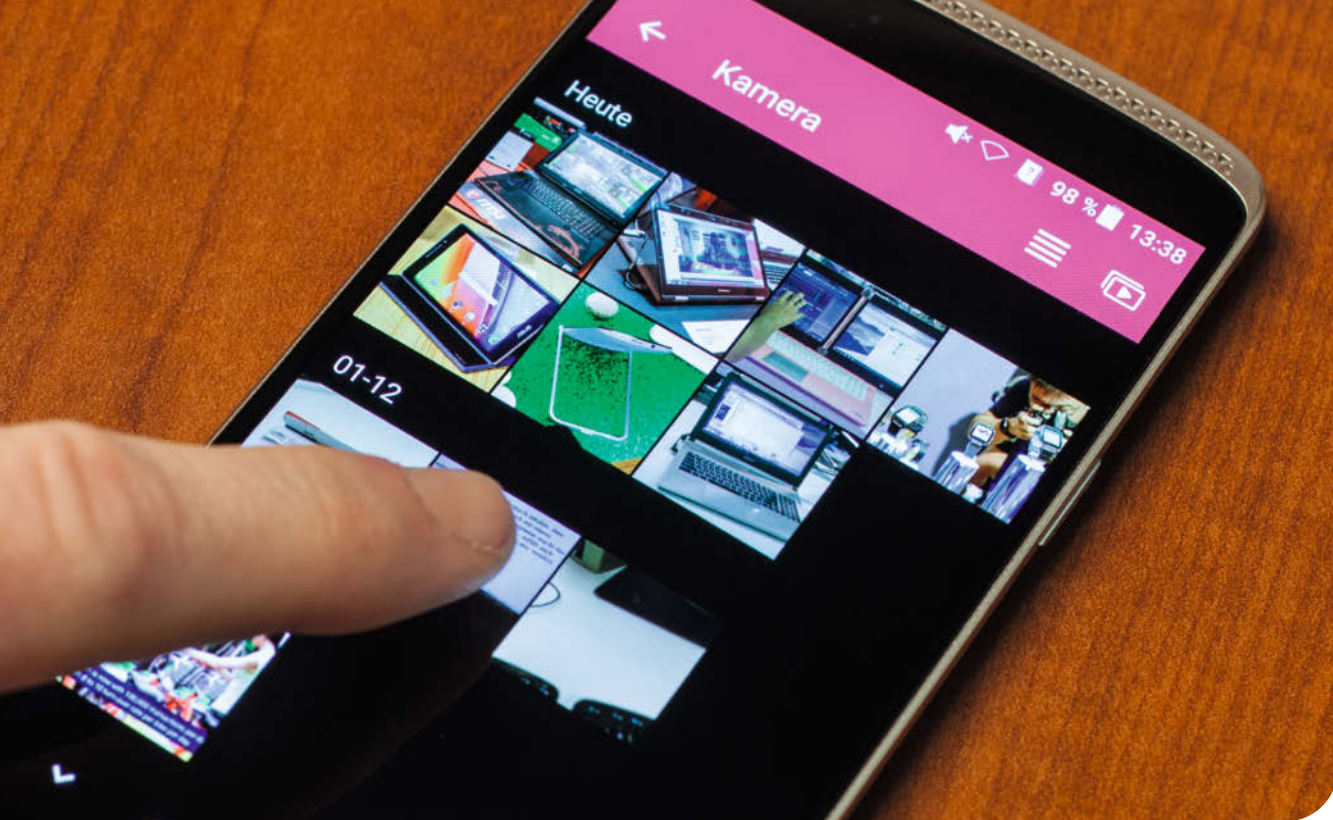
Eine Veranstaltung von:

 **heise  
Security**

Organisiert von:

 **heise  
Events**  
Conferences, Seminars, Workshops





Jörg Wirtgen

# Force Touch in eigenen Apps nutzen

Einige Android-Smartphones können die Druckstärke des Fingers messen, andere emulieren das durch eine Messung der Auflagefläche. Apps können diesen Messwert zwar auswerten, doch Android unterstützt Force Touch nicht vollständig. Wir zeigen, was Entwickler für ihre Apps herausholen können und wo sie an Grenzen stoßen.

**F**orce Touch – das ist einer der Namen der Technik, bei der ein Touchscreen die Intensität des Fingerdrucks erkennt und bei einem festen Druck eine andere Aktion auslöst als bei bloßer Berührung. Als erstes Smartphone kam damit das iPhone 6s in die Läden, nachdem Apples Smartwatch damit debütierte. BlackBerry zeigte etwas Ähnliches schon 2008 beim Storm, dort musste man das Display tatsächlich mechanisch herunterdrücken.

Im Android-Lager beherrschen derzeit zwei Geräte eine echte Druckerkenntnis, das Huawei Mate S – der Hersteller führte es sogar einige Tage vor dem Apple-Event vor – und das ZTE Axon Mini.

## Rudimentäre Unterstützung

Doch die eigene App lässt sich nicht so ohne Weiteres fit für Force Touch machen, da Android die Technik nur rudimentär unterstützt. Zwar bietet Android schon lange eine Druckstufen-Abfrage, und zwar in Form der seit API11 vorhan-

denen und seit API5 Multitouch-fähigen Funktion `MotionEvent.getPressure()`. Aber diese Methode reicht bei Weitem nicht aus, sie zwingt experimentierfreudige Entwickler zu einigem Aufwand. Selbst dann ist unter Android nicht alles möglich, was unter iOS geht.

Die Methode `getPressure()` gehört zur Klasse `MotionEvent`, die Eingaben von Touchscreen, Stift, Maus und Tastatur beschreibt. Google spezifiziert nicht genau, bei welchen Geräten `getPressure()` sinnvolle Werte liefert: Ein Beispiel in der Android-Dokumentation wertet `getPressure()` explizit nur für Stifte aus, ein anderes sammelt hingegen die Druckstärke auch für Touchscreen-Eingaben ein. Bislang nutzen vor allem Zeichenprogramme die Druckstärke. Ab welcher Stärke das der besonders feste Druck sein soll, ist in dem Android-API nicht spezifiziert.

## Einmessen

Ein paar Versuche im c't-Labor zeigten: Das Force-Touch-fähige ZTE Axon Mini meldet den gemessenen Druck tatsäch-

lich über `getPressure()` als float-Zahl zwischen 0 und 1 zurück; das ebenfalls drucksensitive Huawei haben wir leider noch nicht. Auch die Stifte beispielsweise des Samsung Galaxy Note oder des Nvidia-Tablets Shield liefern druckstärkenabhängige Werte, Samsung bis 1, Nvidia allerdings nur bis etwa 0,5.

Einige andere Smartphones wie das HTC One A9 und M9 melden einen von der Auflagefläche abhängigen Wert, was einen raffinierten und praxistauglichen, wenn auch nicht ganz präzisen Ersatz für den Druck darstellt. Nicht bei allen Modellen ist 1 das Maximum. Viele andere Smartphones wie das Note 4 liefern bei Finger-eingaben unabhängig von Druck und Fläche in `getPressure()` immer 1.

Nötig ist also eine selbstlernende Kalibrierung, die getrennt für Finger und Stift Minimum und Maximum der Druckstärke speichert. `MotionEvent` besitzt zwei Methoden zur Geräteerkennung, `getSource()` und `getToolType()`. Obwohl `getSource()` eine feinere Erkennung verspricht, erweist sich `getToolType()` als zielführender: Auf dem Nvidia Shield liefern

Stift- und Fingereingaben den gleichen `SOURCE_TOUCHSCREEN`, aber unterschiedliche `ToolTypes`. Das ist insofern kein Fehler des Tablets, da es tatsächlich keinen speziellen Stift-Digitizer hat, sondern der Stift den kapazitiven Touchscreen nutzt.

Zusätzlich muss man noch die Schwelle festlegen, über der ein Druck als fester zählt. Ganz gut funktioniert zwei Drittel der Differenz aus Maximum und Minimum. Zudem sollten Werte unter einer gewissen Grenze (beispielsweise 0,3) kein Force Touch auslösen; der Nutzer hat dann einfach noch nicht hart zugepackt. Damit die Kalibrierung flexibel nutzbar ist, implementiert man sie sinnvollerweise als statische Methode einer Hilfsklasse, beispielsweise `ForceTouchHelper.isForceTouch(MotionEvent)`.

## Abgefangen

Die Klicks auf User-Interface-Elemente empfangen Apps üblicherweise in den EventListenern `onClick()` und `onLongClick()`, doch denen gibt Android gar kein Motion-Event mit, sodass Apps nicht an die Druckstärke herankommen. Eigentlich würde man sich ja einen neuen Listener wie `onForceClick()` wünschen.

Das erfordert, sich in den `onTouch()`-Listener einzuhängen. Der wird bei jedem `MotionEvent` aufgerufen, also beim Bewegen des Fingers, beim Hochheben und Aufsetzen sowie beim Verändern der Druckstärke. Die Methode packt man in einen

neuen, selbst gebastelten Listener-Typen namens `OnForceTouchListener`:

```
public abstract class OnForceTouchListener implements
View.OnTouchListener {
    public abstract void onForceClick(View view,
        MotionEvent ev);

    public boolean onTouch(View view, MotionEvent ev)
    {
        if (ev.getAction() == MotionEvent.ACTION_DOWN
            && ForceTouchHelper.isForceTouch(ev)) {
            onForceClick(view, ev);
            return true; // Auslösen von onClick() verhindern
        }
        return false;
    }
}
```

Und den kann man nun seinen View-Elementen anhängen, die auf Force Touch reagieren sollen.

```
@Override
protected void onCreate(Bundle savedInstanceState) {
    super.onCreate(savedInstanceState);
    setContentView(R.layout.activity_main);
    ...
    TextView tvTest =
        (TextView) findViewById(R.id.textViewForceTest);
    tvTest.setOnTouchListener(new
        OnForceTouchListener(tvTest) {
        @Override
        public boolean onForceClick(View view, MotionEvent ev) {
            ((TextView)view).append("\nON_FORCECLICK\n");
        }
    })
}
```

```
});
...
```

Sieht einfach aus, funktioniert aber leider beim ZTE Axon Mini nicht. Denn dessen Drucksensor reagiert so schnell, dass er bei festen Berührungen schon vor Erreichen der maximalen Stärke ein `ACTION_DOWN`-Event mit niedrigerem `getPressure()` auslöst. Die maximale Druckstärke bekommt die App erst über ein der darauf folgenden `ACTION_MOVE`-Events (für die Änderung der Druckstärke kennt Android keinen eigenen Eventtyp) mitgeteilt.

Zur Auswertung der `ACTION_MOVE`-Events lässt man in obigem `onTouch()` einfach die `getAction()`-Abfrage weg. Damit nur ein `ForceClick` pro Berührung ausgelöst wird, benötigt man noch ein Flag:

```
@Override
public boolean onTouch(View view, MotionEvent ev) {
    if (ev.getAction() == MotionEvent.ACTION_DOWN)
        mFiredForceClick = false; // jetzt geht's wieder
    if (ForceTouchHelper.isForceTouch(ev)
        && !mFiredForceClick) {
        mFiredForceClick = true; // sperren bis nächsten
        DOWN
        onForceClick(view, ev);
        return true;
    }
    return false;
}
```

Doch nun löst das Element zusätzlich zu jedem `onForceClick()` auch `onClick()` oder `onLongClick()` aus. Das passiert, weil `onTouch()` beim `ACTION_DOWN`-Event `false` zurückgibt, wodurch View die normale Behandlung eines Klicks beginnt. Beim Aufruf von `onForceClick()` müsste also die normale Klickbehandlung stoppen – doch das geht nicht, weil die dazu nötigen Felder von View als private markiert sind.

Ein Ausweg ist, in die `onClick()`- und `onLongClick()`-Listener einzugreifen (siehe Listing unten). Das löst das Problem aber nicht vollständig, da die Event-Bearbeitung von View trotzdem die Methoden `View.performClick()` und `View.performLongClick()` aufruft; sie lösen unter anderem die Accessibility-Events zum Ansteuern von speziellen Ein- und Ausgabehilfen aus. Das ZTE quittiert zudem langes Drücken mit einer kurzen Vibration – und die spürt man nun auch, wenn man nach einem festen Druck den Finger auf dem Display lässt.

## Vollständig

Man müsste also `onTouch()` immer `true` liefern lassen. Doch dann muss man die gesamte Klick-Behandlung selbst übernehmen. Ein

```
package de.jockels.forcetouchemu;

import android.support.v4.util.SimpleArrayMap;
import android.util.Log;
import android.util.Pair;
import android.view.MotionEvent;

public class ForceTouchHelper {
    static SimpleArrayMap<Integer, Pair<Float, Float>> mValues = new SimpleArrayMap<>(10);

    public static boolean isForceTouch(MotionEvent ev) {
        // kein ForceTouch bei Multitouch
        if (ev.getPointerCount() > 1) return false;

        Integer tool = ev.getToolType(0);
        Pair<Float, Float> save = mValues.get(tool);
        if (save == null) {
            // erster Touch von diesem Tool
            mValues.put(tool, new Pair<>(ev.getPressure(), ev.getPressure()));
            // Log.v("Helper", "new tool " + tool);
            return false;
        } else {
            float p = ev.getPressure();

            // neues Minimum oder Maximum?
            if (p < save.first) mValues.put(tool, save = new Pair<>(p, save.second));
            if (p > save.second) mValues.put(tool, save = new Pair<>(save.first, p));

            // Force Touch, wenn über Minimalwert und über 66% von Max-Min
            return p > 0.3 && p > (save.first + (save.second - save.first) * 0.66);
        }
    }
}
```

Der `ForceTouchHelper` ermittelt Minimum und Maximum der Druckstärken.

Blick in die Sourcen von Android [1] – hier in die Methode `View.dispatchTouchEvent()` – zeigt, dass viele der benötigten Flags und Methoden als `private` markiert, also unerreichbar sind. Eine Sackgasse.

Selbst die sonst so mächtigen Module des Root-Rechte voraussetzenden Tweak-Tools Xposed [2] sind machtlos: Es gibt zwar tatsächlich ein Modul für Force Touch [3], doch das löst bei einem festen Druck nur den `onLongClick()` aus, immerhin in allen Apps.

Wem dieses Verhalten reicht: Das lässt sich ohne weitere Click-Probleme einfach in die eigene App einbauen:

```
public class OnForceTouchListener2 implements
View.OnTouchListener {
    boolean mFiredForceClick;
    @Override
    public boolean onTouch(View view, MotionEvent ev)
    {
        if (ev.getAction() == MotionEvent.ACTION_DOWN)
            mFiredForceClick = false;
        if (ForceTouchHelper.isForceTouch(ev)
            && !mFiredForceClick) {
            mFiredForceClick = true;
            return view.performLongClick();
        }
        return false;
    }
}
```

Weniger Konflikte fängt man sich ein, wenn man sich nur in die bisherigen `onClick()` und `onLongClick()` einhängt und dann ein Flag auswertet, das man aus den bis dahin aufgelaufenen `ACTION_MOVE`-Events erzeugt. Die Lösung fällt etwas komplexer aus, weil der `onTouch()`-Listener sich dazu in `onClick()` und `onLongClick()` einhängen muss, und weil `View` hierfür nur je einen Listener verwaltet. Die eigenen Listener muss man nun im `onTouch()`-Listener implementieren statt im `View.onXXXListener`-Aufruf (siehe Listing rechts). Doch ideal ist auch das nicht: Der feste Klick wird nun nicht sofort bei einem festen Druck ausgelöst, sondern erst entweder beim Loslassen oder beim lange Gedrücktklassen.

Etwas einfacher mag es sein, einen festen Klick für andere Arten von Views nachzurüsten, die man sowieso eher per `onTouch()` abhört statt in den Click-Events. Beispielsweise könnte man `GridView` um eine Vorschaufunktion für fest gedrückte Items erweitern.

## Geht gar nicht

Doch wie auch immer man das löst: Der App fehlt für eine vollständige Unterstützung von Force Touch zudem eine einheit-

liche Reaktion. Bei Apple funktioniert Force Touch auch dadurch intuitiv, dass Smartphone und Smartwatch den festeren Druck mit einer spürbaren Vibration zurükmelden; auch das ZTE-Smartphone vibriert kurz.

Wie man das prinzipiell implementieren könnte, zeigt ein Blick in die Android-Sourcen von `View.performClick()` und `View.performLongClick()` – man benötigt die Pendants für `sendAccessibilityEvent`, `performHapticFeedback` und `playSoundEffect`. Man müsste also nicht nur die Klasse `View` recht umfangreich verändern, sondern auch einige weitere Systemparameter ergänzen. Das könnten nur Google oder bestenfalls Entwickler von Custom-

ROMs tun, aber als App-Entwickler hat man keine Chance. Als Ausweg für App-Entwickler bleibt nur, die Accessibility-Unterstützung zu vernachlässigen und das Rütteln selbst zu erzeugen, sodass jede App im eigenen Rhythmus tanzt.

Apple blendet beim festen Druck auf ein App-Icon ein Kontextmenü ein, das die App bestimmt. ZTE macht das ähnlich, doch nur bei den mitgelieferten Apps taucht so ein Menü auf – kein Wunder, denn Android fehlt bisher eine Schnittstelle dafür. Mit Android 7.1 (API 25) kommt sie endlich: Apps können solche Shortcuts statisch oder dynamisch dem Launcher bekannt geben. Die Launcher der Google

```
package de.jockels.forcetouchemu;

import android.view.MotionEvent;
import android.view.View;
import android.widget.TextView;

/**
 * Created by jwirt on 19.01.2016.
 *
 * * onTouchListener, der ForceClicks erkennt und dann onForceClick auslöst.
 *
 * * Weil er dazu intern onClick- und onLongClick-Listener der View umbiegen muss, erzwingt
 * * die Implementierung eigene Listener, die er dann aufruft.
 *
 * * Problem: Wenn man nach einem ForceClick den Finger auf dem Display lässt, wird
 * * View.performLongClick ausgelöst, was wiederum Accessibility- und SystemSound-
 * * Aufrufe nach sich zieht. Nur der onLongClick wird unterdrückt.
 *
 */
public abstract class OnForceTouchListener implements View.OnTouchListener, View.OnClickListener,
View.OnLongClickListener {
    boolean mFiredForceClick, mFiredLongClick;
    View.OnClickListener mClick;
    View.OnLongClickListener mLong;

    public abstract boolean onForceClick(View view, MotionEvent ev);

    public boolean performForceClick(View view, MotionEvent ev) {
        mFiredForceClick = true;
        return onForceClick(view, ev);
    }

    @Override
    public boolean onTouch(View view, MotionEvent ev) {
        if (ev.getAction() == MotionEvent.ACTION_DOWN) {
            mFiredForceClick = false;
            mFiredLongClick = false;
            if (mLong==null) mLong = new View.OnLongClickListener() {
                @Override
                public boolean onLongClick(View view) {
                    if (!mFiredForceClick) OnForceTouchListener.this.onLongClick(view);
                    mFiredLongClick = true;
                    return true;
                }
            };
            if (mClick==null) mClick = new View.OnClickListener() {
                @Override
                public void onClick(View view) {
                    if (!mFiredForceClick) OnForceTouchListener.this.onClick(view);
                }
            };
            view.setOnClickListener(mClick);
            view.setOnLongClickListener(mLong);
        }

        if (ForceTouchHelper.isForceTouch(ev) && !mFiredForceClick && !mFiredLongClick)
            return performForceClick(view, ev);

        return false;
    }
}
```

Dieser `OnForceTouchListener` hängt sich selbst in die Handler ein.



Pixel und Google Nexus werten sie schon aus. Praktischerweise kann es der App egal sein, ob der Launcher nur ein langes Drücken aufs Icon verlangt oder auf eine echte Force-Touch-Geste wartet – so funktionieren die Shortcuts auch auf Geräten ohne Force Touch. Die Entwickler definieren die Shortcuts als Intent: die statischen im Manifest, die dynamischen per ShortcutManager-API [4].

## Fazit

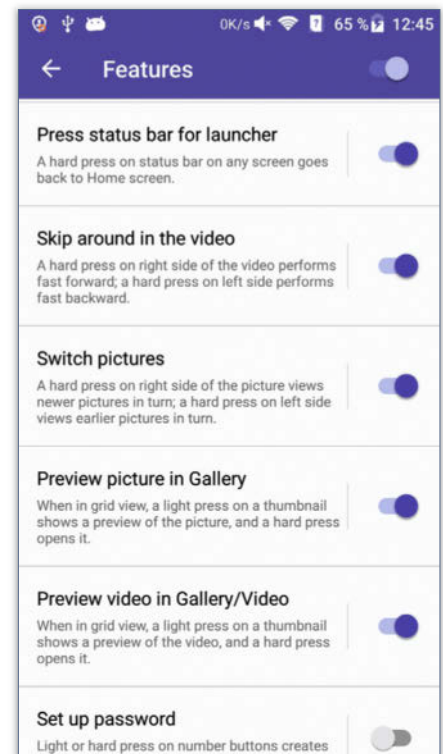
Die oben gezeigte Umsetzung der Druckstärke für eigene Android-Apps klappt so einigermaßen, ist aber noch kein echtes Force Touch: Jede App reagiert anders, es gibt kein einheitliches Feedback und keine systemweite Einstellung der Empfindlichkeit. Doch sie funktioniert nicht nur mit den zwei Force-Touch-Smartphones, sondern auch mit Smartphones und Tablets, die einen Stift oder die Druckstärkensimulation per Auflagefläche unterstützen. So kann man experimentieren, ob und wie die neue Geste bei der eigenen App in Ergänzung zum etablier-

**Das ZTE Axon Mini setzt den festen Druck in einige mehr oder weniger nützliche Zusatzfunktionen um.**

ten Langzeitklick die Bedienung vereinfacht. So richtig kann Force Touch unter Android allerdings erst durchstarten, wenn Google seine APIs erweitert. (jow) **ct**

## Literatur

- [1] Android-Sourcen, z. B. auf [http://grepcode.com/file/repository.grepcode.com/java/ext/com.google.android/android/5.1.1\\_r1/android/view/View.java](http://grepcode.com/file/repository.grepcode.com/java/ext/com.google.android/android/5.1.1_r1/android/view/View.java)
- [2] Alexander Spier, Am offenen Herzen, Android aufbohren mit Xposed, c't 7/15, S. 152
- [3] Xposed-Modul: <http://repo.xposed.info/module/com.mohammadag.systemwideforcetouch>
- [4] Shortcut-Dokumentation: <https://developer.android.com/guide/topics/ui/shortcuts.html>



# THEMEN & TESTS MIT LEIDENSCHAFT.



Mit Archiv!

JETZT KENNENLERNEN:  
**c't PLUS FÜR 18,50 €\***

- 5x c't als HEFT
- 5x c't DIGITAL\*\* und als PDF
- ZUGRIFF auf das ARTIKEL-ARCHIV
- Mit GESCHENK als DANKESCHÖN
- Nach der Testphase erwartet Sie die c't-NETZWERKKARTE mit exklusiven Vorteilen.



IHR GESCHENK:  
**Quadro XciteRC 55XXS Rocket 3D**

Klein & fein: Mit 3 Flugmodi ausgestattet ist der Quadro für Einsteiger, Fortgeschrittene und Profis geeignet. Dank dem neuesten Sechssachsgyros-Stabilisierungssystem lässt er sich sehr einfach und stabil steuern. Solange Vorrat reicht!

\*Preis in Dt. inkl. MwSt. Auslandspreise können abweichen.  
\*\*Verfügbar für Android (Tablet, Smartphone, Kindle Fire) und iOS (iPad, iPhone)

**Jetzt bestellen:**

**ct.de/plusabo**

+49 541/80 009 120

leserservice@heise.de

Bitte bei Bestellung angeben: 1CEA1702

Tam Hanna

# Nachrichtenzähler am Homescreen-Icon einblenden

Auf einigen Android-Geräten blenden Apps an ihrem Start-Icon auf dem Homescreen kleine Blasen ein. Sie informieren etwa über die Zahl neuer Nachrichten oder verpasster Anrufe. Android bietet so eine Funktion gar nicht an, doch für Entwickler gibt es eine hilfreiche Bibliothek.

Unter iOS erzeugen Entwickler den Icon-Zähler mit einem dokumentierten Aufruf. Doch in der Android-API fehlt diese Möglichkeit. Daher entstand ein Wildwuchs verschiedenartiger Lösungen, die nur auf Geräten und Launchern einzelner Hersteller funktionieren. Anwender freuen sich über die Zähler, Entwickler verzweifeln ob der Vielfalt.

Der taiwanische Entwickler Leo Lin hat sich des Problems angenommen: Seine kostenlose Bibliothek namens ShortcutBadger bietet eine gemeinsame Schnittstelle für die unterschiedlichen Zähler-Implementierungen von inzwischen neun Geräte- (Asus, HTC, Huawei, LG, Oppo, Samsung, Sony, Xiaomi, ZUK) und drei Launcher-Herstellern (ADW, Apex, Nova). Er veröffentlicht sie im Bibliotheks-Repository Maven und auf GitHub (siehe Link am Artikelende). Die Dokumentation auf GitHub beschreibt, wie Sie sie von Hand in die nötigen Konfigurationsdateien Ihres Projekts einbinden.

Noch etwas einfacher gehts inzwischen über Android Studio: Falls Sie noch nie Module von Maven benutzt haben, klicken Sie unter „File/Project Structure“ links auf

den Punkt „Project“ und hängen Sie den Zeilen mit „jcenter“ (Android Plugin Repository und Default Library Repository) „mavenCentral“ an.

Dann klicken Sie links in der Liste aufs Hauptmodul (meist app) und auf den Reiter Dependencies. Mit dem grünen Pfeil rechts fügen Sie eine „library dependency“ hinzu, im Suchfeld tippen Sie „leolin“ und wählen „ShortcutBadger“ aus. Die rund 17 KByte große aar-Datei wird beim nächsten Kompilieren automatisch heruntergeladen und in Ihr Projekt integriert.

## Angezählt

Die Bibliothek besteht aus einem statischen Objekt mit einigen wenigen Methoden. Die wichtigste ist `applyCount()` mit zwei Parametern: dem bei vielen API-Aufrufen üblichen Context (meist `this`, `getActivity()` oder `getApplicationContext()`) und der anzuzeigenden Zahl:

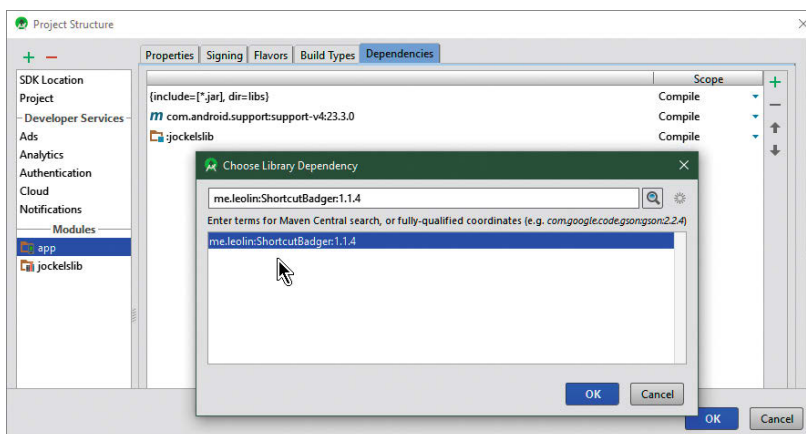
```
int count = ... //Counter ermitteln
ShortcutBadger.applyCount(this, count);
```

Die Methode `removeCount(Context)` entfernt den Zähler, wobei sie dazu einfach nur `apply-`

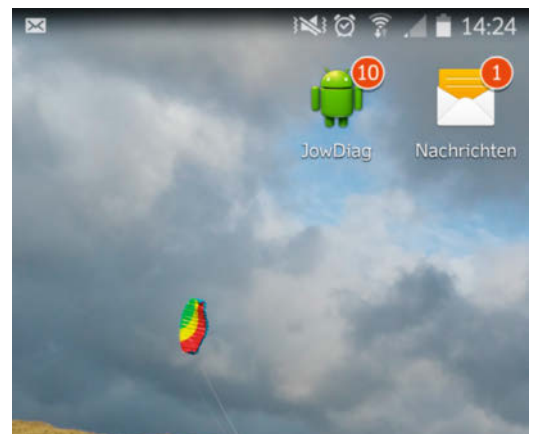
`Count(Context, 0)` aufruft. Wenn der Erfolg des Setzens interessiert: Beide Methoden liefern als Boolean zurück, ob sie einen unterstützten Zähler-Mechanismus gefunden haben. Alternativ zu diesen Methoden existieren die Exception-werfenden Varianten `applyCountOrThrow` und `remoteCountOrThrow`. Sie müssen die Bibliothek nicht initialisieren, das erledigen die Methoden automatisch.

Die Bibliothek ist darauf angewiesen, dass der Launcher die Zähler einblendet – auf den unterstützten Geräten funktioniert sie also nur mit den Launchern des Herstellers. Installiert der Nutzer einen anderen außer ADW, Apex und Nova, etwa Google Now, fehlen die Zähler. Ältere Versionen hatten tatsächlich das Start-Icon verändert und grafisch eine Zahl hineingemalt – das funktionierte auch beim Launcher von Stock-Android. Doch seit Version 1.1.0 von ShortcutBadger fehlt der Code, weil Google ihn in seinen Entwickler-Policies verbietet. Wer solchen Code trotzdem verwendet, riskiert einen Ausschluss der App und die Sperrung seines Accounts. (jow) **ct**

ShortcutBadger bei GitHub: [www.ct.de/w1un](http://www.ct.de/w1un)



Die freie Bibliothek ShortcutBadger liegt auf Maven und lässt sich mit der grafischen Oberfläche von Android Studio einfach einbinden.



ShortcutBadger blendet auf den Geräten von Asus, HTC, LG, Samsung, Sony und Xiaomi an den App-Icons kleine Nachrichtenzähler ein.



# Früher war alles besser!



Willkommen in der Welt der Classic Games, wo Computer- und Videospiele viel Kreativität und Spielspaß versprochen – und bis heute halten. Wir stellen Spiele, deren Entwickler und Plattformen vor. Bei Retro Gamer finden Sie Screenshots, Fakten, Tipps und mehr zu den Hits von damals.

## Testen Sie 2× Retro Gamer mit 30 % Rabatt!

Lesen Sie 2 Ausgaben für nur 18,- Euro\* statt 25,80 Euro\* im Handel.

Jetzt bestellen und vom Test-Angebot profitieren:  
**[www.emedia.de/rg-mini](http://www.emedia.de/rg-mini)**

Telefon: (0541) 800 09 126  
werktags von 8-20 Uhr,  
samstags von 10-16 Uhr

E-Mail: [leserservice@emedia.de](mailto:leserservice@emedia.de)  
Post: eMedia Leserservice  
Postfach 24 69  
49014 Osnabrück

\*Preis in Deutschland.



# Wenn Linux – dann richtig!



**ct Linux**

Gratis-PDF: Virtualisierung und Hochverfügbarkeit

## Root-Know-how

Praxis für den Linux-Alltag: Schneller starten  
Linux umziehen • Google Drive nutzen ...

## Einfach verschlüsseln!

USB-Sticks, Partitionen, Systeme schützen

Das versprechen Flatpak und Snap  
Docker und OpenStack erklärt

Befreit: Secure Boot loswerden  
Abgehört: WLAN knacken mit Raspi  
Durchgefallen: Linux-Notebook von Dell

# Ihr optimaler Heimserver

Bauvorschläge: leise, sparsam, schnell

www.ctspecial.de

Jetzt für  
nur **9,90 €**  
bestellen.



[shop.heise.de/linux-special](http://shop.heise.de/linux-special) ✉ [service@shop.heise.de](mailto:service@shop.heise.de)  
Auch als eMagazin erhältlich unter: [shop.heise.de/linux-special-pdf](http://shop.heise.de/linux-special-pdf)

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-  
Abonnenten oder ab einem Einkaufswert von 15 €

 **heise shop**

[shop.heise.de/linux-special](http://shop.heise.de/linux-special)