Virenschutz gratis: 1 Jahr ESET Mobile Security

c't Android

c't 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

www.ctspecial.de

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

Werden Sie zum Hardware-Profi!

Jetzt für nur **12,90 €** bestellen.

shop.heise.de/ctguide service@shop.heise.de
Auch als eMagazin erhältlich unter: 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

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-Smartwartches 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-Stativaufsatz 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 dekompilieren
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?

Das 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 zerfasert 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-CPUs 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

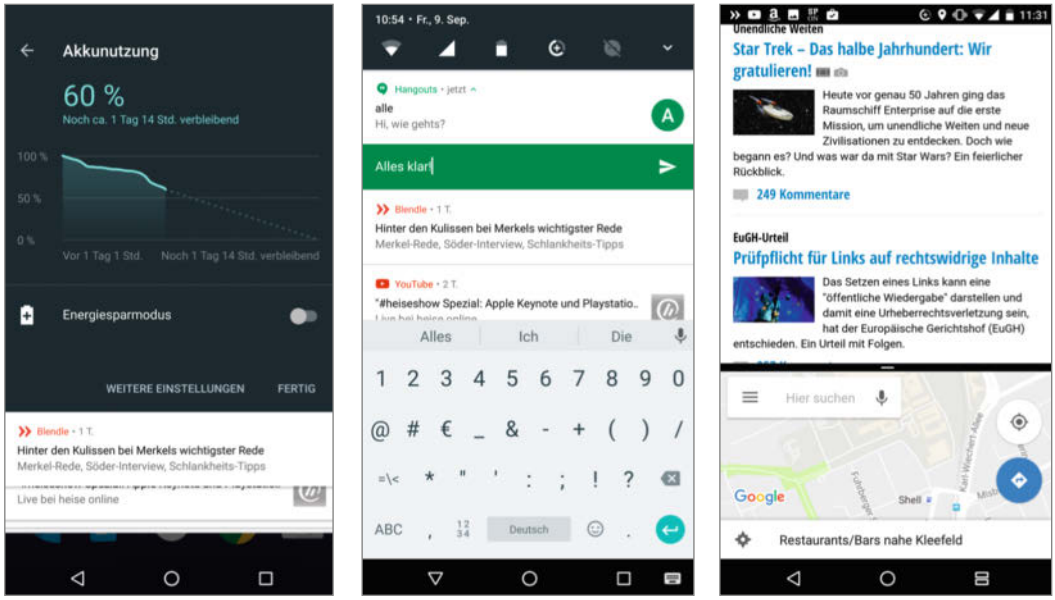
Lange erwartet ist die Möglichkeit, zwei Apps parallel auf dem Bildschirm anzuzeigen – das klappt anders als bei iOS nicht nur auf Tablets, sondern auch auf Smartphones. Läuft ein Programm im Vordergrund, startet ein langer Druck auf den Taskwechsler die geteilte Ansicht. Nun kann man sich je nach Bildschirmorientierung 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.

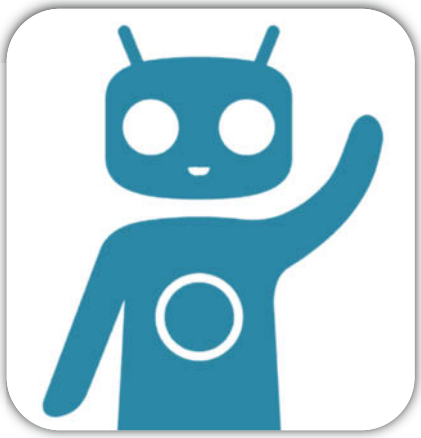
Allerdings hängt es vom App-Entwickler ab, wie gut er die Möglichkeiten nutzt. WhatsApp erlaubt zwar das direkte Antworten an den Kontakt, zeigt aber nur noch die zuletzt empfangene Nachricht. Prinzipiell bietet Android aber einen guten Kompromiss aus Kürze und Funktionsumfang und macht das übersichtlicher 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 lahmt. 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) c't



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 neue 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) c't

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

ESET Mobile Security & Antivirus für Smartphones und Tablets

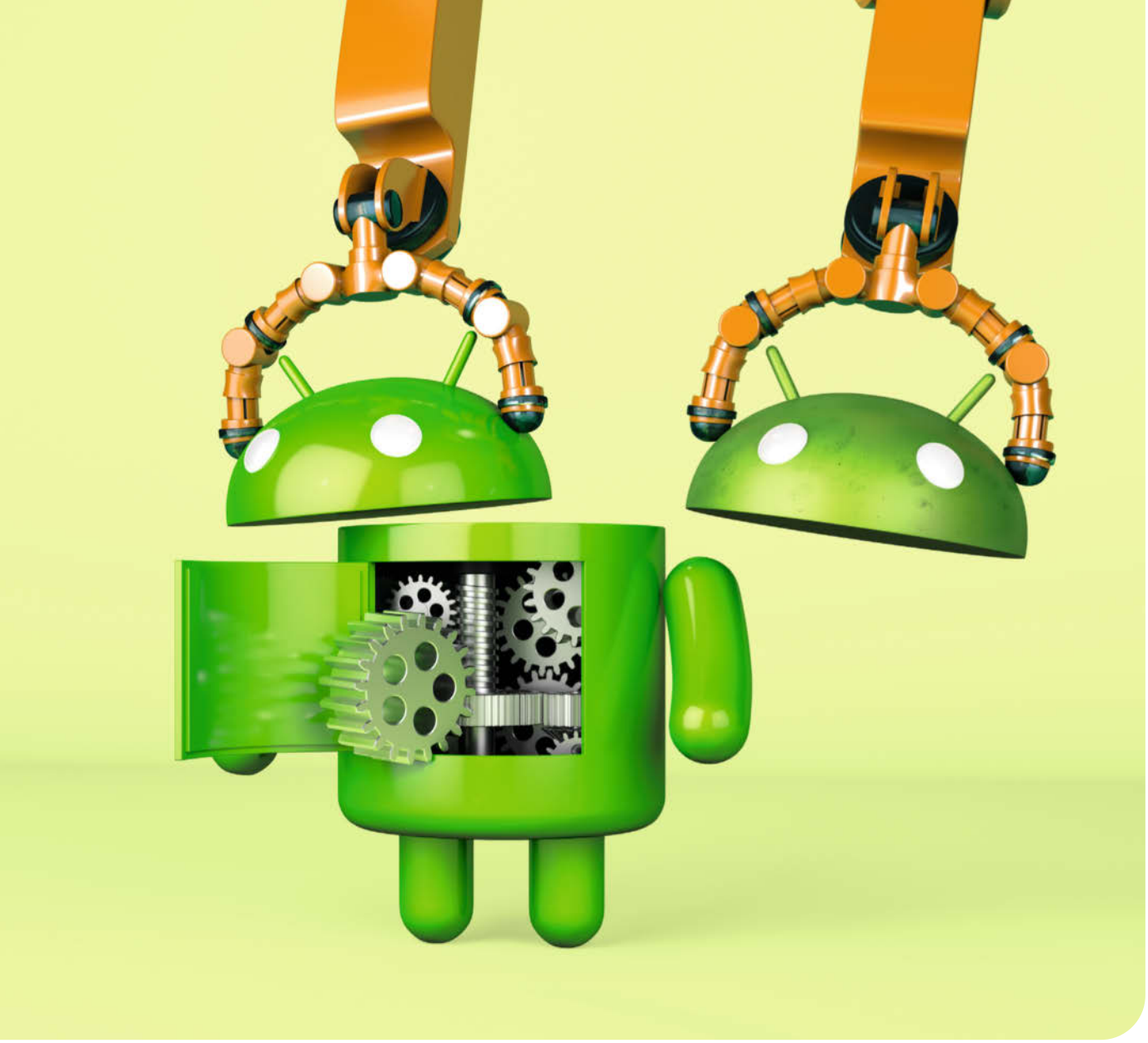
Aktion: Eset Mobile Security ist eine Art Allround-Security-Werkzeugset für Android-Geräte. Die Sicherheits-Suite schützt unter anderem vor Phishing und hilft, gestohlene oder verlorene Smartphones wiederzufinden.

Auf 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 Virenscanner, 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 eingehefteten Registrierungscode. Dieser ist bis zum 31. Juli 2017 gültig. Leser der digitalen Ausgabe erhalten den Aktivierungscode nach Zusendung einer Kopie des Kaufbelegs per E-Mail an android@ct.de. (tir) c't

Download: *www.ct.de/wqu6*



Alexander Spier, Christian Wölbert

Updates und Sicherheitspatches im Check

Immer wieder nagen 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.

Android-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 allerneuesten 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 4.4.4 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

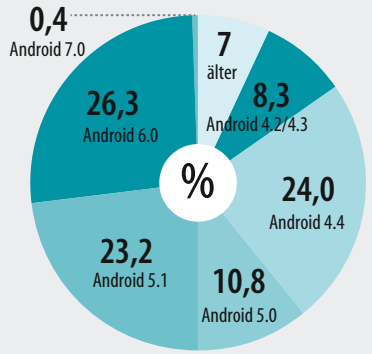
Die von uns in den vergangenen Jahren immer wieder bemängelte Zwei-Klassen-Gesellschaft bei System-Updates besteht weiterhin. Sieht man von den Nexus-Geräten von Google ab, dauert es wie gehabt meistens mehrere Monate, bis Android-Updates von den Herstellern ausgeliefert werden und neue Features zur 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) c't

Tests für Sicherheitslücken: ***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

heise shop
shop.heise.de

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

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.

Ein 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 Virenscanner 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 Virenscanner 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 warnten 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 Virenscanner 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 Virenscannern 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 Virenscanner.

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.