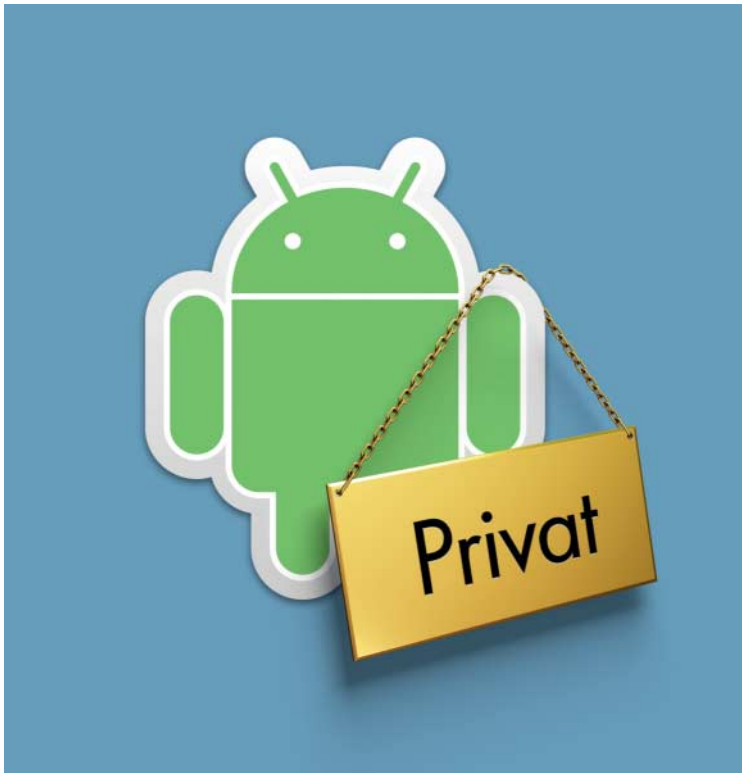


Verschwiegener Androide

Privacy-Checkliste Android

Auf Smartphones lagern immer mehr persönliche und vertrauliche Daten. Anders als der heimische PC kommen die Telefone aber überall mit hin und sammeln selber viele Daten. Was Sie tun müssen, damit Android nicht alles ausplaudert.

Von Alexander Spier

Gerätesperre einrichten

Egal ob vor Dieben oder neugierigen Kollegen, der einfachste Weg, Ihre Daten zu schützen, ist das Einrichten einer wirksamen Gerätesperre. Dank der immer häufiger vorhandenen Fingerabdruckscanner ist das schneller und komfortabler geworden. Ersetzt wird der Zugangscode durch den Abdruck nicht, der Finger erleichtert nur das Entsperren und macht es angenehmer, komplizierte Passwörter oder längere PINs zu wählen.

Ob mit oder ohne Scanner, unter „Einstellungen/Sicherheit/Displaysperre“ (Android 5: „Einstellungen/Gerät/Sperrbildschirm“) legten Sie fest, ob Wischmuster, PIN oder Passwort den Zugang einschränken. Diese sollten trotz registriertem Fingerabdruck merkbar bleiben, denn nach jedem Neustart des Geräts muss man weiterhin erst den Zugangscode eingeben. Wischmuster sind zwar einfacher zu merken, zu einfache Varianten können aber durch die Schlieren auf dem Display erkannt werden. Um es Beobachtern schwerer zu machen, sollte man zudem „Muster sichtbar machen“ deaktivieren.

Die Speicher von Geräten mit Android 6 oder 7 sind von Haus aus verschlüsselt, so kommt nur der Nutzer mit dem richtigen Zugangscode an die Daten. Bei älteren Smartphones kann die Verschlüsselung nachträglich aktiviert werden, was aber unter Umständen die Geschwindigkeit des Geräts verringert.

App-Berechtigungen einschränken

Statt den Apps gesammelte Daten wieder zu entreißen, sollten Sie besser das Sammeln gleich unterbinden. Ab Android 6.0 ist das relativ simpel: Möchte eine App auf Kamera, Kontakte, Standort, Speicher und so weiter zugreifen, muss sie vorher fragen. Einmal gewährte Rechte können Sie unter „Apps“ wieder entziehen. Dazu klicken Sie auf das Zahnrad rechts oben und dann auf App-Berechtigungen, wo die Programme sortiert nach Zugriffsrechten aufgeführt sind.

Einige Apps verweigern nach dem Rechteentzug allerdings die Arbeit. Zudem werden längst nicht alle Berechtigungen erfasst. Vor der Installation sehen können Sie sie nur, indem Sie im jeweiligen Play-Store-Eintrag ganz runter bis zu den „Berechtigungsdetails“ scrollen.

Läuft das Smartphone unter Android 5.1 oder früher, gibt es keine direkte Möglichkeit, einer App Rechte zu verweigern. Nur wenige Hersteller wie Huawei und alternative Android-ROMs erlauben das. Der SRT AppGuard für knapp 4 Euro rüstet eine Rechteverwaltung nach, indem er die jeweilige App mit veränderten Rechten neu installiert. Er ist nur über die Webseite des Herstellers erhältlich und muss von Hand per APK-Datei installiert werden.

Synchronisierung abschalten

Sobald Sie ein Google-Konto auf dem Smartphone eingerichtet haben, synchronisiert Google Kontakte, Kalenderdaten und vieles weitere in seine Cloud. Eine Möglichkeit, zum Beispiel Termine ausschließlich auf dem Gerät zu speichern,

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover

bieten lange nicht alle Smartphones. Dann hilft einzig das Abschalten der Synchronisation mit Google: Bevor Sie zum Beispiel Kontakte anlegen, gehen Sie in die Android-Einstellungen, rufen sie „Konten“ auf und tippen sie „Google“ an und je nach Android-Version auf den Kontennamen. Nun können Sie alle Kategorien abwählen, die Sie nicht automatisch mit Ihrem Google-Account synchronisieren möchten.

Auch einige andere Apps tragen sich unter Konten ein und erlauben selektives Abschalten der Synchronisation. Allerdings heißt ein fehlender Eintrag nicht, dass die App keine Daten verschickt: Möglicherweise lässt sich das Verschicken nur nicht abschalten. Zum Nachteil wird das Abschalten beim Neueinrichten oder wenn das Gerät nicht mehr zugänglich ist: Nicht anderweitig gesicherte Daten sind dann verloren.

Google-Backup deaktivieren

Bei der Einrichtung des Smartphones bietet Google an, Android-Einstellungen und App-Daten in der Cloud zu sichern. Das kann zwar beim Wiederherstellen praktisch sein, doch werden dabei auch sensible Informationen wie WLAN-Passwörter gesichert. Nachträglich lässt sich das Backup unter „Einstellungen/Sichern & zurücksetzen“ wieder deaktivieren. Gelöscht sind die Daten dann aber noch nicht. Dafür gehen Sie in den Einstellungen auf den Punkt Google, rufen dort „Persönliche Daten & Privatsphäre“ und dann das „Google Dashboard“ auf. Unter Android finden Sie alle für diesen Account registrierten Geräte. „Sicherungsdaten löschen“ entfernt sämtliche Geräte-Backups aus dem Google-Account.

Die Nachteile halten sich in Grenzen. Zum einen ist das Backup rudimentär, zum anderen nutzen viele Apps die Möglichkeit erst gar nicht. Gekaufte Inhalte wie Apps sind ohnehin an den Account geknüpft und können wieder aus dem Play Store installiert werden.

Standortverlauf abschalten

Google interessiert es brennend, wo ein Nutzer sich mit seinem Smartphone aufhält, unabhängig ob eine Google-App läuft. Das soll für bessere Suchergebnisse, Verkehrsinfos und auf den Ort bezogene Empfehlungen sorgen. Der Standortverlauf ist zum Beispiel in Google Maps über „Meine Zeitachse“ einsehbar. Abschalten können Sie ihn unter anderem in den Maps-Einstellungen über die Kategorie „Persönliche Inhalte“ oder in den Android-Einstellungen unter „Standort/Google-Standortverlauf“. Im folgenden Menü können alle mit dem Account verknüpften Geräte einzeln oder komplett deaktiviert werden, einige tauchen dort aber nur mit ihren kryptischen Modellnummern auf.

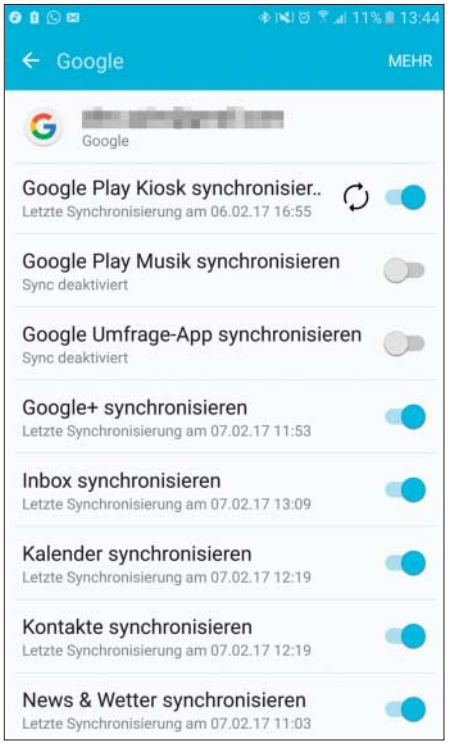
Den bisherigen Standortverlauf können Sie unter „Persönliche Inhalte“ ganz oder teilweise löschen. Dort beschränken Sie auch die Anzeige von Kontakten und Fotos im Standortverlauf, allerdings hebt das nicht die Verknüpfung der Daten durch Google auf.

Google-Tastatur vom Netz abklemmen

Googles Android-Tastatur Gboard (ehemals Google Keyboard) kann beim Schreiben zum Kontext passende Wörter vorschlagen. Dazu analysiert die App das Geschriebene und verknüpft das mit anderen Daten aus dem Account. In den Einstellungen unter „Sprache & Eingabe“ kann man Gboard das abgewöhnen: Unter „Textkorrektur“ können Sie die personalisierten und andere Vorschläge abschalten. Damit nicht versehentlich vertrauliche Informationen in der Cloud landen, stellen Sie unter „Wörterbuch“ dazu die Synchronisation von erlernten Wörtern ab. Unter „Erweitert“ verhindern Sie dazu noch das Senden von Textausschnitten zur Analyse der Eingabe.

Wie stark Google die Eingabe analysiert, wird klar, wenn man im Chat zum Beispiel „Essen gehen?“ schreibt: Dazu passend erscheint ein Suchvorschlag von Google über der Tastatur. Solche Vorschläge lassen sich unter „Suche“ abschalten.

Oder wechseln Sie gleich zu Alternativen wie dem Hacker’s Keyboard, das als einer der wenigen Android-Tastaturen ohne zusätzliche Berechtigungen und Zugriff aufs Internet auskommt.



Über die Sync-Einstellungen des Google-Kontos können Sie das Senden von Daten an Google stark einschränken.

Google-Neugier bremsen

Vieles, was Google über den Nutzer sammelt und speichert, kann über die Google-Einstellungen beeinflusst werden. Scrollen Sie unter „Persönliche Daten & Privatsphäre“ bis zur Verwaltung der Google-Aktivitäten und klicken Sie auf „Aktivitätseinstellungen“. Hier lässt sich abschalten, was Google speichert und für die Suche nutzen darf.

Die Kategorien sind allerdings teils irreführend. So lässt sich die Aufzeichnung, welche App wann und wie oft benutzt wurde, nur zusammen mit der Auswertung der eingetippten Suchbegriffe deaktivieren. Die Aufzeichnung von Aktivitäten auf Webseiten lässt sich immerhin getrennt abschalten. „Geräteinformationen“ umfasst bedeutend mehr als Details zum Gerät. Hier werden auch Kontakte, Kalender oder die abgespielte Musik erfasst.

Generell etwas schwerer können Sie es Google auch beim Anzeigenvermarkten machen, wenn Sie in den Google-Einstellungen und „Anzeigen“ die Werbe-ID regelmäßig ändern und die Anzeige von personalisierter Werbung deaktivieren.

(asp@ct.de) c't

© Copyright by Heise Medien
Persönliches PDF für alle Leser der c't aus 30625 Hannover