Vorlage

App-Berechtigungen

Apps benötigen für ihre Funktion bestimmte „Berechtigungen“. Mit ihnen wird der Zugriff auf die Daten und die Gerätefunktionen des Smartphones geregelt. Allerdings fordern viele Apps deutlich mehr Zugriffsrechte, als sie für ihre Funktion eigentlich benötigen. Dies trifft besonders auf kostenlose Apps zu: Um die Produktionskosten ausgleichen zu können, versuchen die Anbieter der Apps möglichst viele persönliche Daten ihrer Nutzer zu sammeln. Die gesammelten Daten können für personalisierte Werbung genutzt werden, an der die Anbieter dann verdienen. Eine App ist daher zwar häufig kostenlos, aber nicht gratis – denn oft „bezahlt“ man mit den eigenen privaten Daten.

Man sollte stets bei einem Download oder der Installation kontrollieren, auf was die App tatsächlich zugreift. Ein Spiel braucht sehr wahrscheinlich keinen Zugang zum Telefonbuch. Ebenso wenig benötigt eine Foto-Bearbeitungs-App eine dauerhafte Internetverbindung. Wenn eine App eine Internetverbindung braucht, ohne dass es sinnvoll erscheint, sendet sie wahrscheinlich Daten an Dritte. Man sollte direkt online nach der App suchen – falls es sich um eine Datenkrake handelt, wird das wahrscheinlich in den Foren bekannt sein. Selbst wenn die Berechtigung bei der Installation nicht einzustellen ist, kann man mittlerweile nachträglich bestimmen, worauf die App zugreifen darf.

Die wichtigsten App-Berechtigungen sind folgende:

Kalender

Die Berechtigung kann zum Beispiel für Apps wie Gmail sinnvoll sein, um wichtige Termine aus den Emails im Kalender zu speichern. Diese Berechtigung kann aber auch gefährlich werden, wenn eine bösartige App nicht nur die Tagesabläufe ausspäht, sondern auch die Termine ändert oder gar löscht.

Kamera

Nicht nur Kamera-Apps, auch Anwendungen wie Taschenlampen-Apps benötigen diesen Zugriff, um beispielsweise den LED-Blitz zu verwenden. Allerdings könnten schädliche Apps die Möglichkeit, jederzeit Fotos und Videos aufzunehmen, auch dazu nutzen, den Nutzer auszuspionieren.

Kontakte

Messenger-Apps wie WhatsApp benötigen den Zugriff, um alle verfügbaren Kontakte anzeigen zu können. Beachtet werden sollte, dass eine bösartige App alle Kontaktdaten von Freunden und Bekannten speichern und verkaufen könnte.

Körpersensoren

Verschiedene Fitness-Apps benötigen Zugriff auf die Sensorendaten, um nutzvolle Ergebnisse für das Training präsentieren zu können. Andere Apps sollten allerdings keinen Zugriff hierauf haben, denn sie könnten die gesundheitliche Verfassung des Nutzers für andere Zwecke ausspähen.

Mikrofon

Apps für Videochats, zum Diktieren und ähnliche Anwendungen benötigen diesen Zugriff, um zu funktionieren. Die Möglichkeit, auf das Mikrofon zugreifen und dadurch Audiomitschnitte erstellen zu können, kann aber das Smartphone für eine Malware-App zu einem perfekten Abhörgerät machen.

SMS

Messanger-Apps wie WhatsApp nutzen diese Berechtigung, um Verifizierungscodes zu lesen. Eine Malware-Anwendung kann aber im schlimmsten Fall auf Kosten des Nutzers Nachrichten versenden und sogar per SMS gebührenpflichtige Dienste abonnieren. Das Bezahlen per SMS sollte daher sicherheitshalber beim Provider deaktiviert werden.

Speicher: Fotos/Medien/Daten

Dateimanager-Apps, Social-Media-Apps oder Bildbearbeitungsprogramme können einen berechtigten Anspruch für den Zugriff auf Fotos, Medien oder Daten haben, um richtig zu funktionieren. Es gibt aber auch Apps, bei denen im schlimmsten Fall damit gerechnet werden muss, dass sie private Dateien für fremde Zwecke (z.B. für Werbung) sammeln.

Standort

Navigations-Apps wie „Google Maps“ benötigen diesen Zugriff, um individuelle Routen und Wegbeschreibungen anzeigen zu können. Andere Apps können mit den Standortdaten die Nutzer aber auch gezielt orten und ein Bewegungsprofil erstellen.

Telefon

Kommunikations-Apps wie Skype benötigen diesen Zugriff, damit Nutzer direkt aus der Anwendung heraus ihre Kontakte anrufen können. Eine betrügerische App könnte allerdings ohne Erlaubnis kostenpflichtige Nummern anrufen und enorme Kosten verursachen.

Berechtigungen ändern

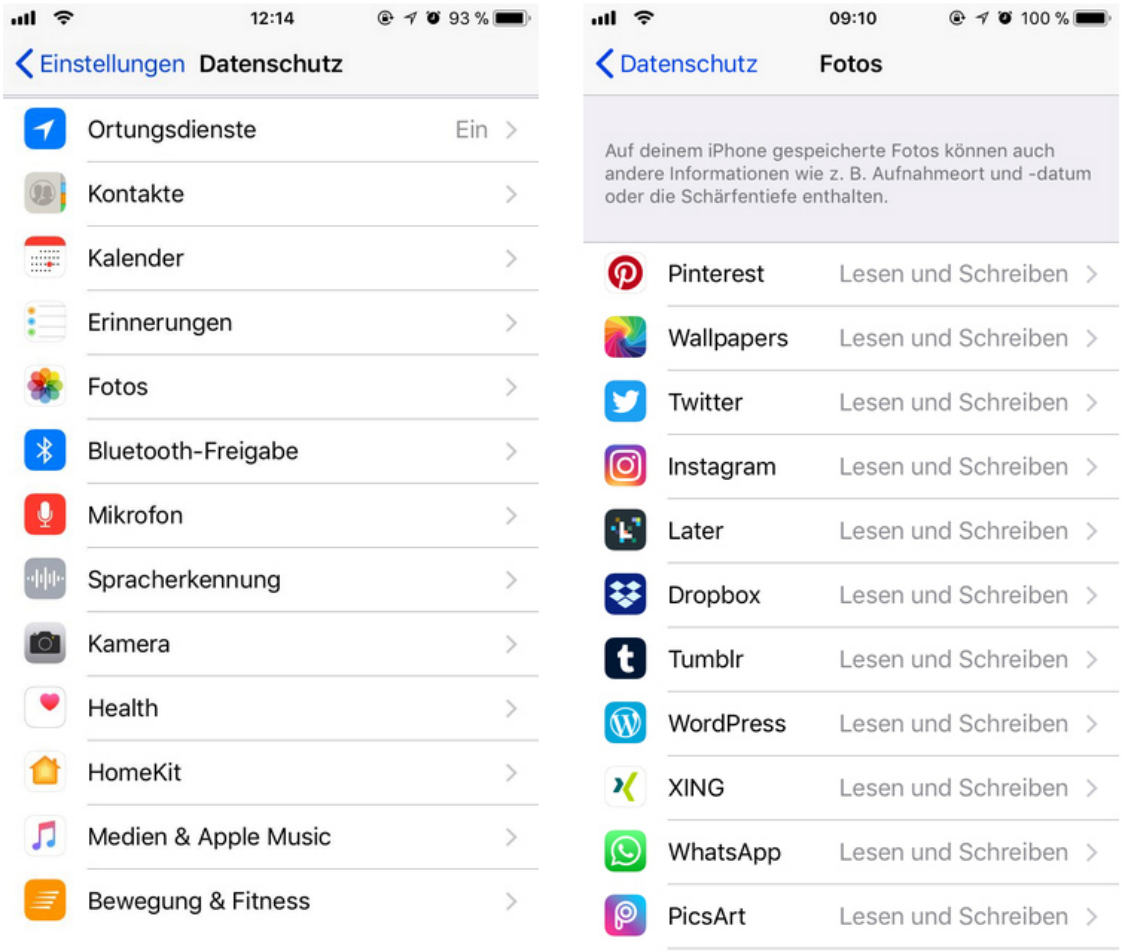
Die Berechtigungen für bereits installierte Apps können in den Einstellungen eines Smartphones geändert werden. Je nach Betriebssystem des Smartphones – iOS/Apple oder Android – müssen hierfür unterschiedliche Schritte unternommen werden.

Vorlage

Hinweis zu den im Folgenden dargelegten Beschreibungen und Bildern: Einzelne Details können je nach Gerätegeneration und Software-Version leicht variieren und von den aufgeführten Darstellungen abweichen.

iOS/Apple

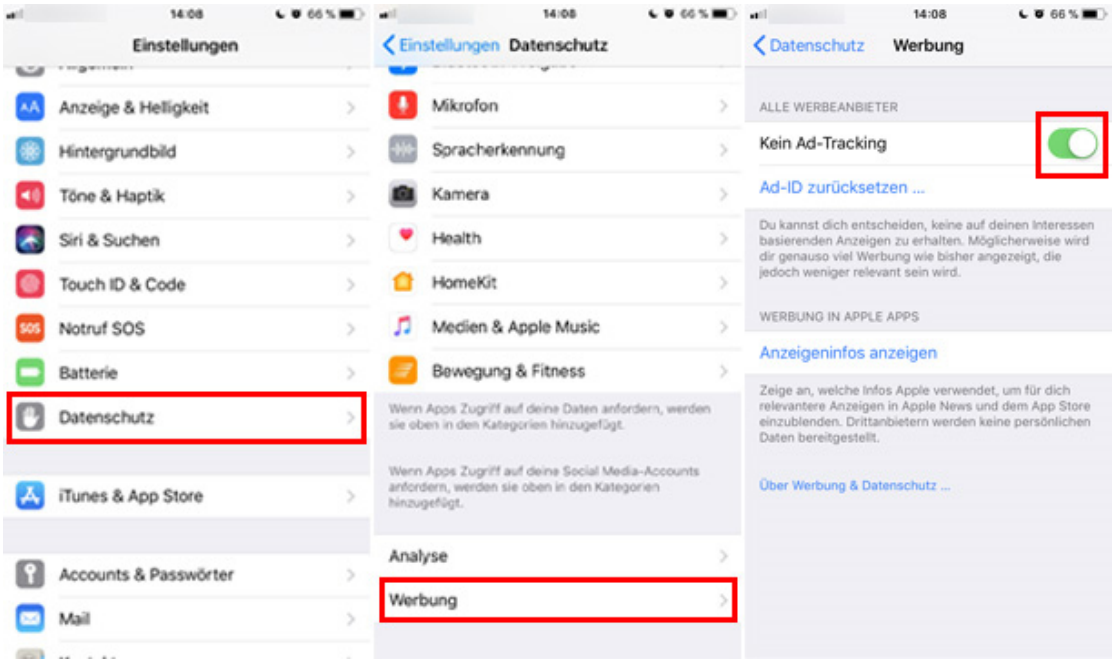
Um die Berechtigungen ändern zu können, muss unter „Einstellungen“ der Menüpunkt „Datenschutz“ geöffnet werden: Hier sind alle Berechtigungen zu finden, die aktiviert bzw. deaktiviert werden können. Hierfür einen Berechtigungstyp wie z.B. „Kamera“ oder „Mikrofon“ öffnen und die Berechtigungs-Einstellungen für die gespeicherten Apps vornehmen.



(Bild: Screenshot Berechtigungen iOS/Apple)

Außerdem kann das Anzeigen von Werbung generell ausgeschaltet werden. Hierfür auf den Button „Werbung“ gehen und mit dem Schieberegler „Kein Ad-Tracking“ aktivieren. Wenn außerdem noch „Ad-ID zurücksetzen“ aktiviert wird, kann das Gerät nicht mehr für Werbung identifiziert und verfolgt werden.

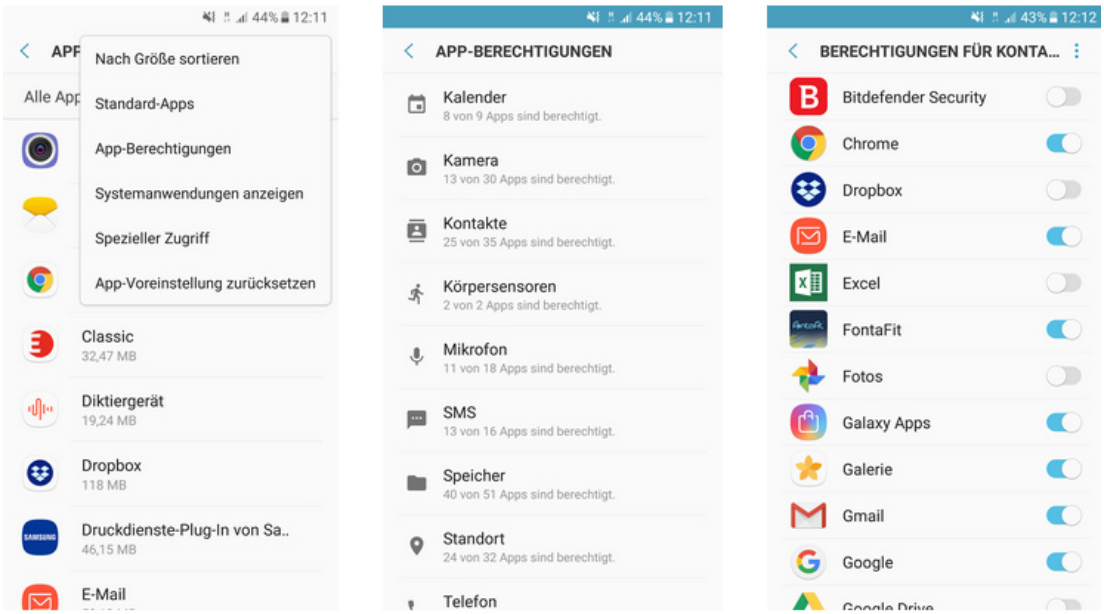
Vorlage



(Bild: Screenshot Ad-Tracking und Ad-ID)

Android

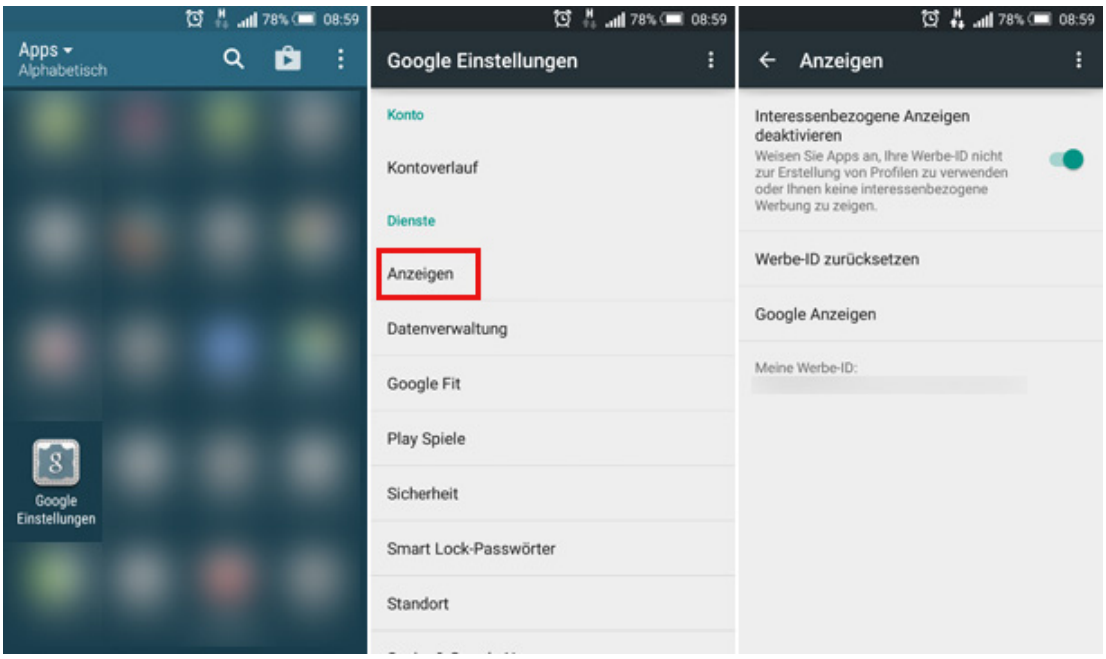
Um die Berechtigungen ändern zu können, muss unter „Einstellungen“ der Menüpunkt „Apps“ geöffnet werden. Hier dann das Untermenü „App-Berechtigungen“ öffnen und einen Berechtigungstyp wie z.B. „Kamera“ oder „Mikrofon“ öffnen. Hier sind alle Apps versammelt, die auf die Funktion zugreifen können. Nun den Schieberegler entsprechend positionieren: Ist er farbig dargestellt, ist die Berechtigung aktiv, ist er grau, ist die Berechtigung deaktiviert.



(Bild: Screenshot Berechtigungen Android)

Vorlage

Außerdem kann die Möglichkeit, Werbung anzuzeigen, ausgeschaltet werden. Hierfür unter „Einstellungen“ auf den Menüpunkt „Anzeigen“ gehen und den Regler „Interessenbezogene Anzeigen deaktivieren“ auf aktiv setzen. Wenn außerdem noch „Werbe-ID zurücksetzen“ aktiviert wird, kann das Gerät nicht mehr für Werbung identifiziert und verfolgt werden.



(Bild: Screenshot Interessenbezogene Anzeigen und Werbe-ID)