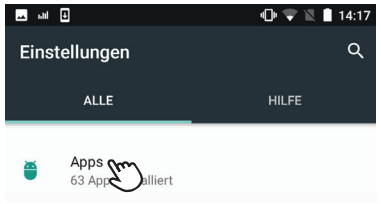
Smartphone, Android & Berechtigungen

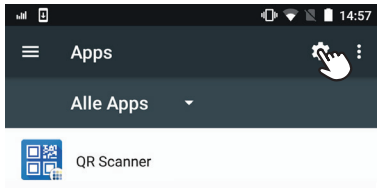
Wir nutzen unser Smartphone für private Gespräche, ob in Text, Wort oder Bild, speichern unsere Kontakte und organisieren unsere Termine damit.

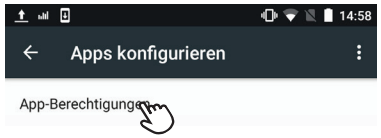
Der Zugriff auf all diese sensiblen Daten wird durch sogenannte Berechtigungen geregelt. Das bedeutet beispielsweise, dass jeder App, die die Kamera benötigt, hierfür zunächst die entsprechende Zugriffsberechtigung erteilt werden muss.

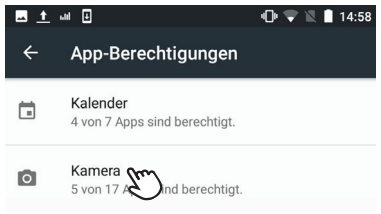
Berechtigungen deaktivieren

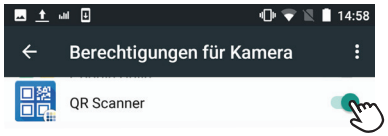
Beim Öffnen einer App werden Sie häufig dazu aufgefordert, Berechtigungen zuzustimmen um die App vollständig nutzen zu können. Nach der Zustimmung können Sie jeder App die Berechtigung wieder entziehen. Wie Sie diese deaktivieren, wird Ihnen in folgender Bilderstrecke Schritt für Schritt erklärt:

1. 

2. 

3. 

4. 

5. 

Kontakt

Karlsruhe Institut für Technologie (KIT)

Institut für Angewandte Informatik und
Formale Beschreibungsverfahren (AIFB)

Forschungsgruppe Security • Usability • Society (SECUSO)

Prof. Dr. Melanie Volkamer
Kaiserstraße 89, Gbd. 05.20
76133 Karlsruhe

Telefon: +49 721 608 450 45
E-Mail: kontakt@secuso.org

www.secuso.aifb.kit.edu
facebook.com/secuso
twitter.com/secusoresearch

Herausgeber

Karlsruher Institut für Technologie (KIT)

Präsident Professor Dr.-Ing. Holger Hanselka
Kaiserstraße 12
76131 Karlsruhe
www.kit.edu

Der Inhalt des Faltblatts basiert auf Forschungserkenntnissen, welche von der Forschungsgruppe SECUSO an der TU Darmstadt erarbeitet wurden und seit 2018 am KIT weiterentwickelt werden. Die Finanzierung des Faltblatts erfolgt im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts KASTEL.

Karlsruher Institut für Technologie

aifb

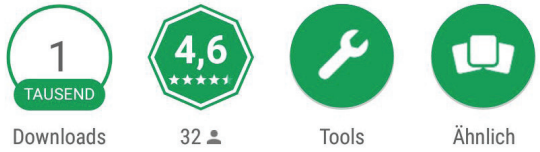
Android-Apps

Was Sie bei der App-Wahl und Installation beachten sollten

INSTITUT FÜR ANGEWANDTE INFORMATIK UND FORMALE BESCHREIBUNGSVERFAHREN (AIFB)

Taschenlampe (Privacy Friendly)
SECUSO Research Group
USK ab 0 Jahren

INSTALLIEREN



Die App ermöglicht es das eingebaute Kameralicht als Taschenlampe zu verwenden.

WEITERLESEN

SECUSO
SECURITY · USABILITY · SOCIETY

KASTEL

Privatsphäre und Smartphone – Passt das?

Haben Sie sich schon einmal gefragt, was Ihr Smartphone mit Ihrer Privatsphäre zu tun hat? Dieser Abschnitt vermittelt einen Überblick zu häufigen Missverständnissen.

Ich habe doch nichts zu verbergen?

Auch wenn die Veröffentlichung einzelner personenbezogener Daten an sich nicht dramatisch erscheint, kann eine Sammlung und vor allem die Auswertung vieler dieser Daten von anderen missbraucht werden: Beispielsweise nutzen Hacker gesammelte Daten, um mehr über Sie zu erfahren. Sie können so gezielte Angriffe (sog. Spear-Phishing) gegen Sie durchführen, indem Ihnen sehr persönlich wirkende E-Mails geschickt werden. Ebenso wird mit dem über Sie gesammelten Wissen versucht, Ihre Kauf- und Wahlentscheidung zu beeinflussen.

Zusätzlich gilt es zu bedenken, dass die genaue Kenntnis über Ihren aktuellen Aufenthaltsort jederzeit in die Hände von Kriminellen gelangen kann und damit eine ernsthafte Gefährdung darstellen kann (z.B. Einbrecher).

Bin ich nicht zu unwichtig, um interessant zu sein?

Es ist sehr leicht Daten im großen Stil zu sammeln und zu verarbeiten, insbesondere da vieles öffentlich geteilt wird. Auch wenn es Ihnen unwahrscheinlich vorkommt, dass gerade Sie „interessant" sein sollten, werden Ihre Daten, z. B. wen Sie wann anrufen, dennoch gesammelt.

Wenn mein Smartphone sicher ist, ist es meine Privatsphäre doch auch?

Privatsphäre und Sicherheit des Gerätes haben nicht zwingend etwas miteinander zu tun. Insbesondere auch weil viele Ihrer Daten ganz offiziell von Apps durch Firmen und Werbenetzwerke gesammelt und weiterverkauft werden.

Apps aus dem App-Store sind doch aber alle sicher?

Das Vermeiden von inoffiziellen App-Stores ist prinzipiell eine gute Schutzstrategie. Dennoch sind die offiziellen Stores nicht gegen Schadsoftware immun. Die Stores enthalten Millionen von Apps, daher können nicht alle individuell von Hand geprüft werden. Darüber hinaus können Apps, die technisch gesehen keine Schadsoftware sind, dennoch Ihre privaten Daten sammeln und weitergeben.

Wer nichts eingibt, ist doch sicher vor Datensammlern?

Aufgrund der Funktionsweise von Smartphones haben Apps oft nicht nur auf die direkte Eingabe von Daten Zugriff, sondern auch auf persönliche Daten, die darauf gespeichert sind (z. B. Bilder). Auf diese kann ohne Ihr Wissen im Hintergrund zugegriffen werden.

Aber manchen Firmen kann man doch vertrauen?

Wird eine vertrauenswürdige Firma Opfer eines Hackerangriffs, sind alle dort hinterlegten Daten betroffen. Sie sollten vorsichtig sein und überlegen, welche Daten wirklich für die Funktionen der App benötigt werden, auch wenn Sie der Firma vertrauen.

Ich kann ohnehin nichts dagegen tun, oder?

Auch wenn einige Dienste und Apps für Ihre Grundfunktionen den Zugriff auf private Daten benötigen, so gibt es für viele Anwendungen auch privatsphäre-freundliche Alternativen (siehe Regeln).

Die wichtigsten Regeln zur Auswahl von Apps

1. Regel: Informieren Sie sich darüber, welche Zugriffsberechtigungen eine App anfordert. Überlegen Sie, ob die angeforderten Berechtigungen für die gebotene Funktionalität angemessen sind. Im besten Fall werden nur solche Berechtigungen angefordert, die für Funktionen der App notwendig sind. So benötigt eine Foto-App Zugriff auf die Kamera, nicht aber auf Ihre Kontakte. Werden Berechtigungen gefordert, die nicht zur Funktionalität der App passen, sollten Sie ggf. auf eine Installation verzichten oder die Berechtigungen verweigern.

Informationen dazu finden Sie direkt im PlayStore, indem Sie am unteren Ende der App-Beschreibungsseite auf „Berechtigungsdetails" drücken.

2. Regel: Versuchen Sie Apps zu finden, die genau die Funktionalität bieten, die Sie benötigen und keine darüber hinaus. Dies erhöht die Chance, dass die App keine unangemessenen Berechtigungen fordert. Das minimiert das Risiko für ungewollte Datenweitergaben.

3. Regel: Bevorzugen Sie Apps mit einer großen Nutzerbasis. Prüfen Sie die Anzahl der Downloads sowie die Anzahl der Bewertungen einer App. Eine hohe Sterne-Bewertung ist nur verlässlich, wenn es auch hinreichend viele (>100) einzelne Bewertungen gibt.

Beide Informationen finden Sie direkt unter dem Button zum Installieren.

4. Regel: Lesen Sie aufmerksam die Bewertungstexte anderer Nutzer zur App. Schenken Sie insbesondere auch den negativen Ihre Aufmerksamkeit. Achten Sie hierbei insbesondere auf Hinweise zu Verletzungen der Privatsphäre, wie z. B. unangemessene Berechtigungen oder Beschreibungen von auffälligen oder verdächtigen Verhaltens der App.

Sie finden diese Informationen direkt unter den Sterne-Bewertungen.

5. Regel: Prüfen Sie, ob die App noch aktiv entwickelt wird, d. h. wann das letzte Update der App erschienen ist. Nur aktive Entwickler können auch auf bekanntwerdende Sicherheitslücken reagieren.

Berühren Sie im PlayStore die App Beschreibung, sodass alle Informationen angezeigt werden, und scrollen Sie ganz nach unten zum Eintrag „Aktualisiert am".

6. Regel: Informieren Sie sich über den Entwickler der App. Besuchen Sie die Webseite des App-Entwicklers. Diese finden Sie in Android am unteren Ende der App Beschreibung. Folgende Punkte sprechen für die Vertrauenswürdigkeit des Entwicklers:

- Der Entwickler hat bereits verschiedene Apps im Angebot und bedient damit eine breite Nutzerbasis.
- Der Entwickler kommt aus einem Land, welches Datenschutzgesetze hat.
- Der Entwickler ist eine große Firma, deren guter Ruf für diese einen hohen Wert hat.
- Der Entwickler stellt eine eigene Datenschutzrichtlinie entweder auf seiner Webseite oder im App Store zur Verfügung.

7. Regel: Hat der Entwickler der App auch andere Apps oder Programme im Angebot, schauen Sie sich auch auf den Beschreibungsseiten dieser um. Achten Sie auch hier auf die oben genannten Punkte.

8. Regel: Prüfen Sie mithilfe einer Suchmaschine, ob es womöglich Medienberichte über den Entwickler oder die App selbst gibt, z. B. Testberichte von unabhängigen Medien oder auch Berichte über erfolgreiche Hackingangriffe

9. Regel: Prüfen Sie regelmäßig Ihre installierten Apps, ob Sie diese noch benötigen. Deinstallieren Sie ungenutzte Apps. Dies verhindert, dass diese im Hintergrund laufen und Daten sammeln können.

Halten Sie das App-Icon länger gedrückt bis oben rechts „Deinstallieren" erscheint und schieben Sie es darauf.

10. Regel: Versuchen Sie eventuell sensible Daten wie persönliche Fotos regelmäßig von Ihrem Smartphone auf ein anderes Gerät (z. B. PC, Laptop) zu sichern und vom Smartphone zu löschen. So schränken Sie den Zugriff auf Ihre Fotos auch für Apps mit Zugriffsberechtigung darauf ein.