Sicheres Smartphone

Mit diesen zehn Sicherheitstipps machen Sie Ihr Smartphone ein gutes Stück sicherer. Kombiniert mit ein wenig Vorsicht, ist Ihr Gerät nur noch schwer zu knacken. ● VON LUCA DIGGELMANN

Egal, ob Android-Gerät oder iPhone: Sicherheit ist hier genauso wichtig wie am PC – oder sogar noch wichtiger, denn es lagern mittlerweile viele persönliche Daten auf den kleinen Begleitern. Die folgenden Sicherheitstipps sollten Sie daher unbedingt berücksichtigen.

1. Zugriffskontrolle

Das absolute Minimum der Smartphone-Sicherheit ist ein Sperrcode. Dieser sorgt dafür, dass unbefugte Personen keinen Zugriff auf Ihre Daten erhalten, sollten Sie beispielsweise Ihr Smartphone verlieren. Sowohl bei Android als auch bei iOS werden Sie beim ersten Systemstart dazu aufgefordert, einen Sperrcode einzurichten. Falls Sie den Schritt verpasst haben, können Sie den Code auch später noch hinzufügen.

UNTER ANDROID

Öffnen Sie die *Einstellungen* und suchen Sie nach *Displaysperre*. Wählen Sie die gewünschte Methode aus. *Wischen* ist unsicher und sollte nicht verwendet werden. Bei *Muster* putzen Sie besser öfters Ihr Display, da sonst Ihr Sperrcode durch Fingerabdrücke sichtbar wird. *PIN* und *Passwort* sind die sichersten Varianten. Passwort ist jedoch ohne biometrische Unterstützung (etwa durch einen Fingerscanner) eher mühsam, Bild 1.

UNTER IOS

Öffnen Sie die *Einstellungen* und scrollen Sie zu *Touch ID & Code* respektive *Face ID & Code*, je nach Modell. Dort finden Sie alle Optionen rund um den Sperrcode und die biometrischen Hilfen, die das jeweilige iPhone anbietet. Setzen Sie unter *Code aktivieren* einen Sperrcode und schalten Sie falls gewünscht *Touch ID* (Fingerscanner) oder *Face ID* (Gesichtserkennung) ein, Bild 2.

Biometrische Hilfen wie Fingersensoren oder Gesichtsscanner sind eine einfache Variante, Ihr Smartphone gut abzusichern, ohne dabei auf eine angenehme Bedienung verzichten zu müssen. Die Einrichtung variiert aber je nach Gerät. Durchforsten Sie am besten Ihre Einstellungen oder konsultieren Sie die Bedienungsanleitung Ihres Geräts.

Bild 1: In Android haben Sie eine grosse Auswahl an Displaysperren

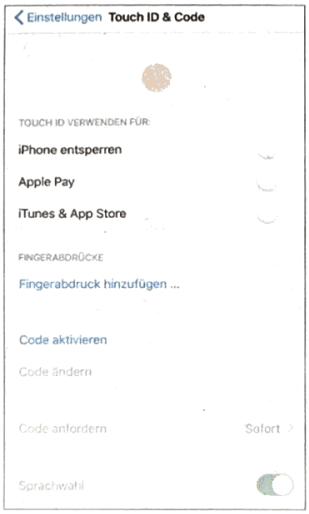

Bild 2: Bei neuen iPhones gehören Touch ID und Face ID dazu

2. WLAN

Öffentliche Wi-Fi-Hotspots sind praktisch, aber auch riskant. Sie wissen nie wirklich, wer einen Hotspot betreibt und wer sich alles im Netz tummelt. Das macht es für Hacker extrem einfach, Daten abzugreifen. Verbinden Sie sich nur dann mit öffentlichen Hotspots, wenn es nicht anders geht. Halbprivate Netze wie Hotelnetzwerke mit Passwort sind etwas sicherer, aber dennoch nicht sicher genug für kritische Anwendungen wie zum Beispiel E-Banking.

Ähnliches gilt für die Funktechnik Bluetooth. Lassen Sie Bluetooth ausgeschaltet, solange Sie es nicht verwenden. Das Sicherheitsrisiko ist aufgrund der kurzen Übertragungsdistanz zwar sehr klein, aber der Aufwand, Bluetooth jeweils kurz auszuschalten, ist noch kleiner.

3. App-Zugriffe

Eine App, die QR-Codes liest, braucht wahrscheinlich Zugriff auf die Kamera, nicht aber Ihre Kontakte. Prüfen Sie bei Apps immer genau, welche Berechtigungen die App benötigt und ob diese auch Sinn ergeben.

Seit einiger Zeit fragen Android-Apps erst nach Rechten, wenn sie diese brauchen. Allerdings behaupten einige Apps auch einfach, sie würden dringend Zugriff auf alle Ihre Kontakte benötigen, um überhaupt starten zu können. Denken Sie hier sorgfältig nach: Was kann die App genau und wie hängt das mit den angefragten Berechtigungen zusammen.

Falls Sie im Nachhinein Zugriffsrechte ändern möchten, können Sie das problemlos tun. Unter Android öffnen Sie die *Einstellungen* und navigie-

Foto: Shutterstock/Pim pic

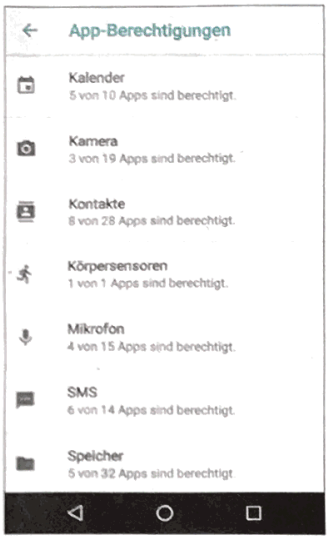

Bild 3: In diesem Menü können Sie unter Android einer App die Rechte absprechen oder gewähren

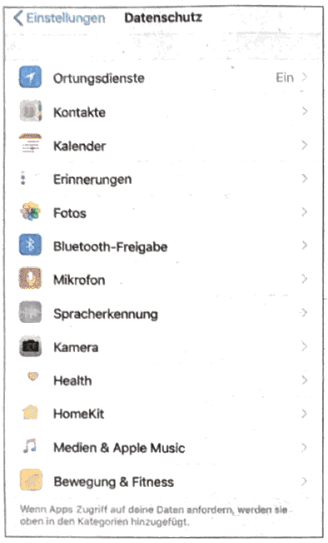

Bild 4: Auch auf dem iPhone lassen sich die Berechtigungen von Apps problemlos anpassen

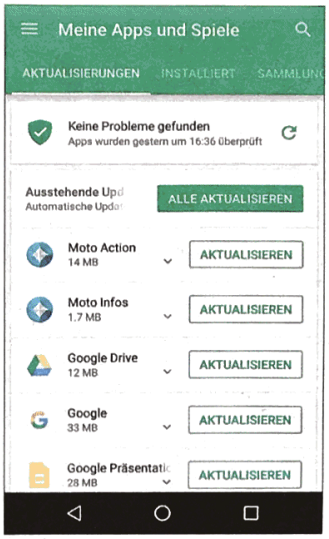

Bild 5: Selbst wenn es mühsam ist – laden Sie Updates fürs System und für Apps regelmässig herunter

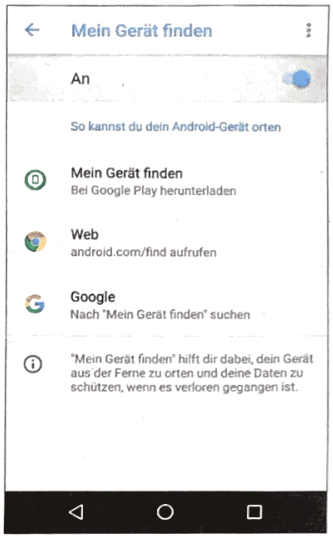

Bild 6: Aktivieren Sie bereits im Voraus die Ortungsfunktion, nach dem Diebstahl geht das nicht mehr

ren Sie zur Option *Apps* und *App-Berechtigungen*, Bild 3. In iOS öffnen Sie stattdessen *Einstellungen/Datenschutz*, Bild 4.

4. Fremde App-Stores

Die einfachste Methode, sich Malware auf einem Smartphone einzufangen, ist über Apps von fremden Quellen. Soll heissen: Apps, die nicht aus dem Google Play Store oder dem Apple App Store stammen. Unter Android können Sie das Ausführen von Apps, die nicht von Google Play stammen, komplett deaktivieren. Die Option dazu finden Sie in den *Einstellungen* unter *Sicherheit*.

Das heisst nicht, dass Apps aus den offiziellen Stores nicht verseucht sein können, das Risiko, sich etwas einzufangen, ist jedoch massiv kleiner.

In iOS braucht es einen Hack, um Apps aus Fremdquellen überhaupt erst installieren zu können (siehe dazu auch nächster Abschnitt).

5. Root-Zugriff

Der Root-Zugriff (Zugriff mit weitreichenden Rechten aufs ganze System) bietet diverse Vorteile wie mehr Einstellungsmöglichkeiten und andere Freiheiten. Allerdings hebelt man so auch das eingebaute Sicherheitssystem des Smartphones aus. Standardmässig hat kein Anwender Root-Zugriff auf sein Smartphone. Das Gerät muss dazu gehackt werden. Falls Sie das getan haben oder tun wollen: Ein Smartphone mit Root-Zugriff braucht viel mehr Aufmerksamkeit im Bereich Sicherheit. Eine Sicherheits-Software lohnt sich hier. Beachten Sie dazu auch unsere Kaufberatung auf S. 52.

6. Webbrowser

Während Google und Apple im Store veröffentlichte Apps prüfen, gilt das nicht für Websites, die Sie mit dem Webbrowser ansteuern. Entsprechend ist es für Angreifer leichter, Sie über eine infizierte Webseite zu attackieren als über eine App im Store. Verwenden Sie also falls möglich Apps und besuchen Sie nur Webseiten, die Sie als sicher kennen. Falls Sie regelmässig auf unseriösen Webseiten unterwegs sind, lohnt sich eine Sicherheits-Software.

7. 2F-Authentifizierung

Nutzen Sie für so viele Dienste wie möglich eine Zwei-Faktor-Authentifizierung. Dabei erhalten Sie bei einem Login auf einem neuen Gerät einen Code per SMS, App oder E-Mail, den Sie zusätzlich angeben. So verhindern Sie unberechtigten Zugriff, sogar wenn Ihr Passwort geknackt wurde.

8. Updates, Updates, Updates

Laden Sie Updates so häufig und schnell wie möglich. Das gilt sowohl für Betriebssystem-Updates als auch für App-Updates, Bild 5.

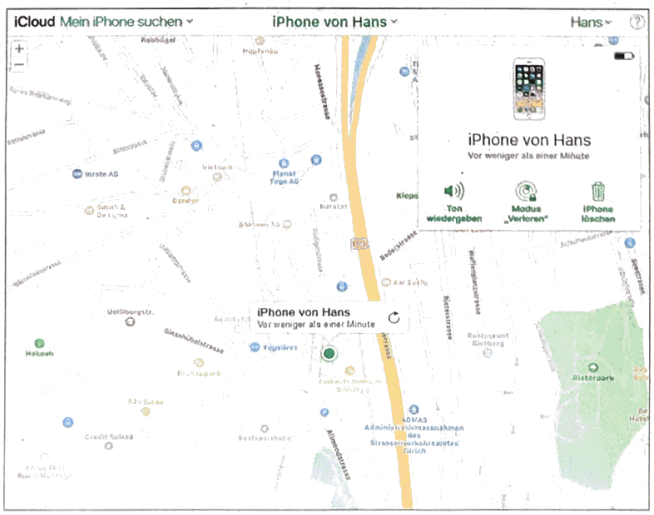

Bild 7: Über die iCloud-Webseite können Sie Ihr verlorenes iPhone orten

9. Umgang mit Daten

Smartphone-Speicher sind knapp bemessen, unlimitierte Daten bezahlbar und das Mobilfunknetz hierzulande exzellent. Das sind alles gute Gründe, seine Daten in die Cloud zu verfrachten, also in einen Onlinespeicher. 200 GB Onlinespeicher gibt es für rund 20 Franken pro Jahr und die Preise sinken. Das ist mehr als genug für die meisten Nutzer. Und wenn Ihnen jemand das Handy klaut, ist das Gerät schnell vom Cloud-Speicher getrennt.

Wichtige Dokumente sollten Sie sowieso nicht auf dem Smartphone aufbewahren, sondern besser in der Cloud. Die Gefahr, dass das Smartphone geklaut wird, verloren geht oder ins Wasser fällt, ist zu gross. Gehen Sie dieses Risiko nicht ein.

10. Notfallplan

Bereiten Sie unbedingt vorab einen Notfallplan vor. So wissen Sie sofort, was zu tun ist, sollte Ihr Smartphone gestohlen werden oder verloren gehen. Präventiv sollten Sie zudem eine Backup-Routine einrichten. Am besten per Cloud-Speicher.

Unter Android verwenden Sie die Funktion *Mein Gerät finden* in *Einstellungen/Sicherheit & Standort*. Geht Ihr Smartphone verloren, können Sie auf einem beliebigen Rechner die Webadresse android.com/find aufrufen und Ihr Gerät orten, Bild 6. Auf der gleichen Webseite sperren Sie übrigens Ihr Android-Smartphone aus der Ferne oder löschen sämtliche Daten darauf.

In iOS verwenden Sie die Option *Mein iPhone suchen* unter *Einstellungen/iCloud*. Um ein verlorenes iPhone zu suchen, öffnen Sie *Mein iPhone suchen* auf einem anderen Apple-Gerät oder über die Website icloud.com. Wie bei Android können Sie das Gerät orten, klingeln lassen, sperren oder zurücksetzen, Bild 7.