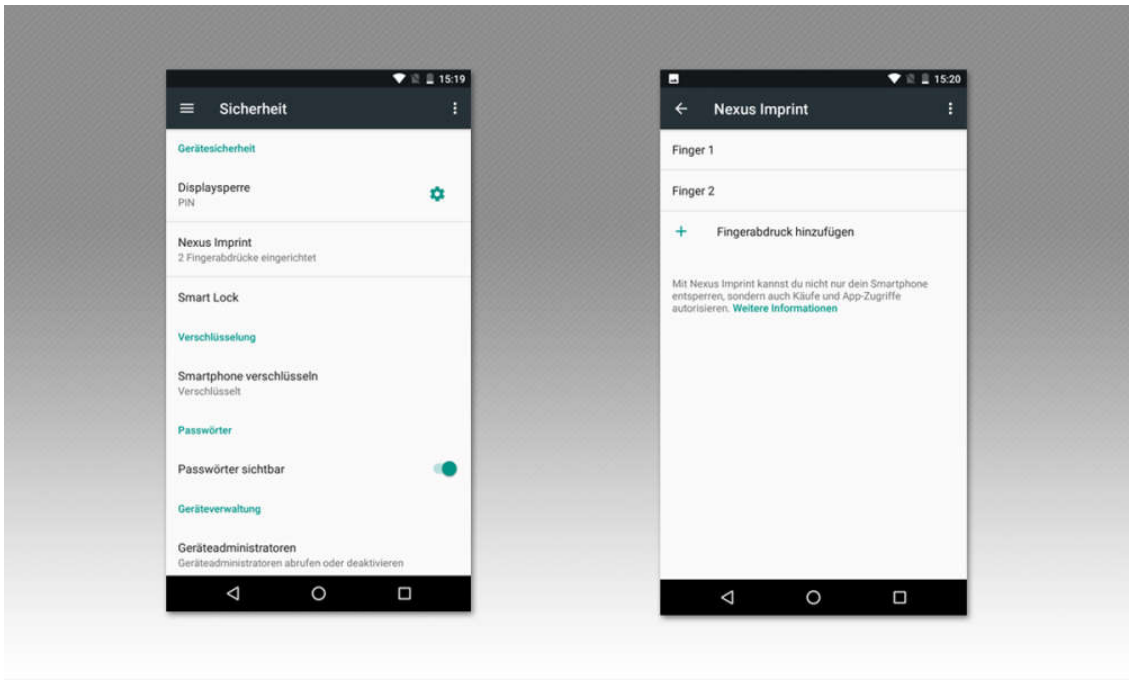
Smartphone-Sicherheit 10 goldene Regeln



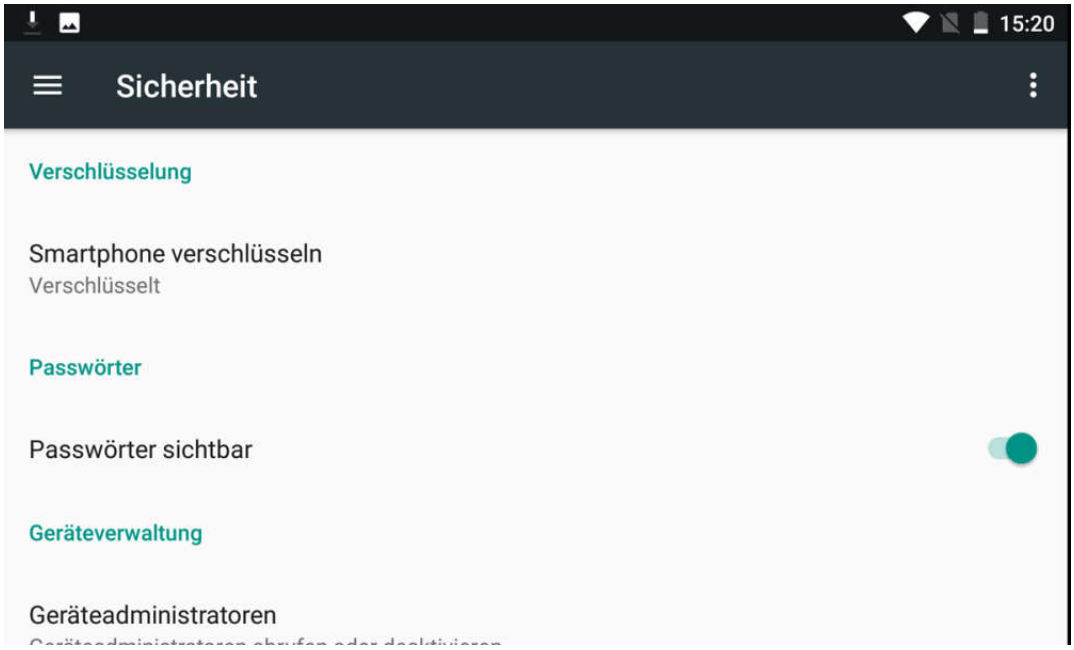
© Screenshot WEKA / PC Magazin

Regel 1: Handy verriegeln

Mit einer Code-Sperre lassen sich alle Handys vor unbefugtem Zugriff schützen. Deshalb ist die Einrichtung dieser Sperre eine der wichtigsten Regeln für die Smartphone-Sicherheit. Erst nach Eingabe des Codes stellt das Gerät seine Funktionen und Informationen zu Verfügung.

Immer mehr Geräte können Sie außerdem per Fingerabdruck, Gesichtserkennung oder ein Wischmuster entriegeln. Diese Methoden sind bequemer, aber auch weniger sicher als die Code-Sperre, die im besten Fall auf einer Zahlen-und Buchstabenkombination mit einer Länge von sechs Zeichen beruht. Aber auch einfachere Kombinationen wie das gängige Muster aus vier Zahlen sind ein akzeptabler Schutz.

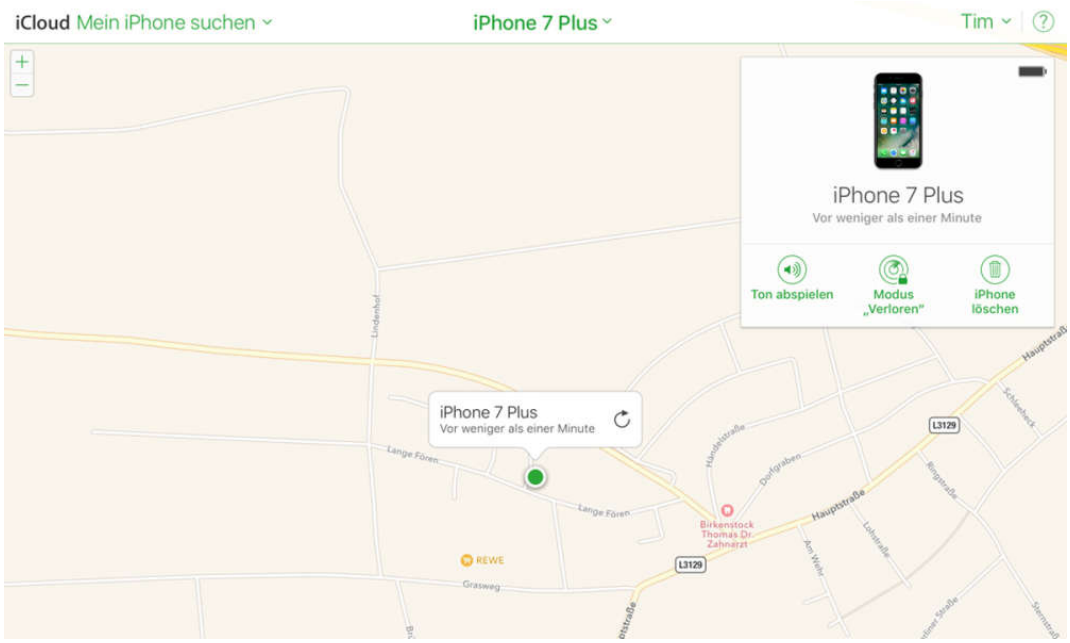
Manche Smartphones sperren sich erst einige Zeit nach der letzten Verwendung wieder. Komfortabel, das Handy in einem kurzen Zeitraum immer wieder verwenden und dann ausschalten. Stellen Sie den Zeitraum bis zum verriegeln aber aus Sicherheitsgründen so niedrig ein wie möglich.



© Screenshot WEKA / PC Magazin

Regel 2: Daten verschlüsseln

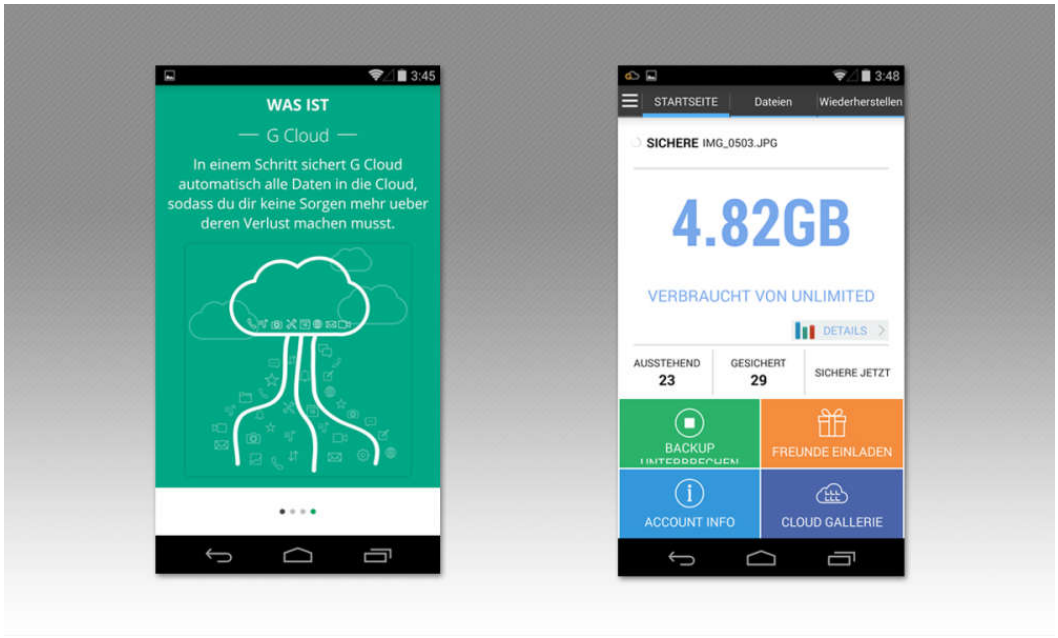
Trotz Sperre mit einem Code, Fingerabdruck oder ähnlichem kann ein technisch versierte Angreifer die auf Ihrem Smartphone gespeicherten Daten auslesen – solange diese nicht verschlüsselt sind. Viele Smartphones bieten eine entsprechende Funktion, aber sie ist nicht immer ab Werk eingeschaltet. Überprüfen Sie die entsprechende Einstellung deshalb baldmöglichst. Bedenken Sie, dass die anfängliche Verschlüsselung einige Zeit benötigt, während das Gerät arbeitet. Am besten aktivieren Sie die Funktion, wenn Sie das Handy einige Stunden nicht benötigen und verbinden es währenddessen mit dem Stromnetz.



© Screenshot WEKA / PC Magazin

Regel 3: Suchfunktion aktivieren

Weil Ihr Smartphone einen Aufenthaltsort fast immer genau kennt können Sie es im Verlustfall online aufstöbern. Lässt es sich auf diese Weise nicht wieder beschaffen, dann können Sie die darauf gespeicherten Daten zumindest aus der Ferne löschen. Bei Apples iPhone hört die entsprechende Funktion auf den Namen „Mein iPhone suchen". Android-Benutzer verwenden zum Beispiel Googles Android Geräte-Manager, der ein kostenfreies Google-Benutzerkonto voraussetzt. In beiden Fällen muss die Funktion schon eingeschaltet sein, wenn das Handy verloren geht, beziehungsweise gestohlen wird. Eine nachträgliche Aktivierung ist nicht mehr möglich. Unterbindet der neue Besitzer die Internetverbindung, scheitert die Ortung.



© Screenshot WEKA / PC Magazin

Regel 4: Regelmäßige Backups

Eine an einem sicheren Ort gespeicherte Kopie der persönlichen Daten ist im Schadensfall Gold wert. Am besten automatisieren Sie die Sicherung der Daten auf Ihrem Handy – dann geht sie nicht mehr vergessen.

Am leichtesten fällt das Backup, wenn das Handy seine Daten einfach in der Cloud speichert. Zum Beispiel bietet Apple jedem iPhone-Besitzer 5 Gigabyte kostenlosen Speicherplatz in der iCloud. Dort kann das iPhone Backups via Internet speichern. Die entsprechende Funktion finden Sie in den Einstellungen unter „iCloud“. Hersteller von Android-Handys haben teilweise eigene Online-Backup-Lösungen entwickelt. Alternativ bedienen Sie sich des App-Angebotes auf Google Play, zum Beispiel in Form der kostenlosen App G Cloud Backup.

© Screenshot WEKA / PC Magazin

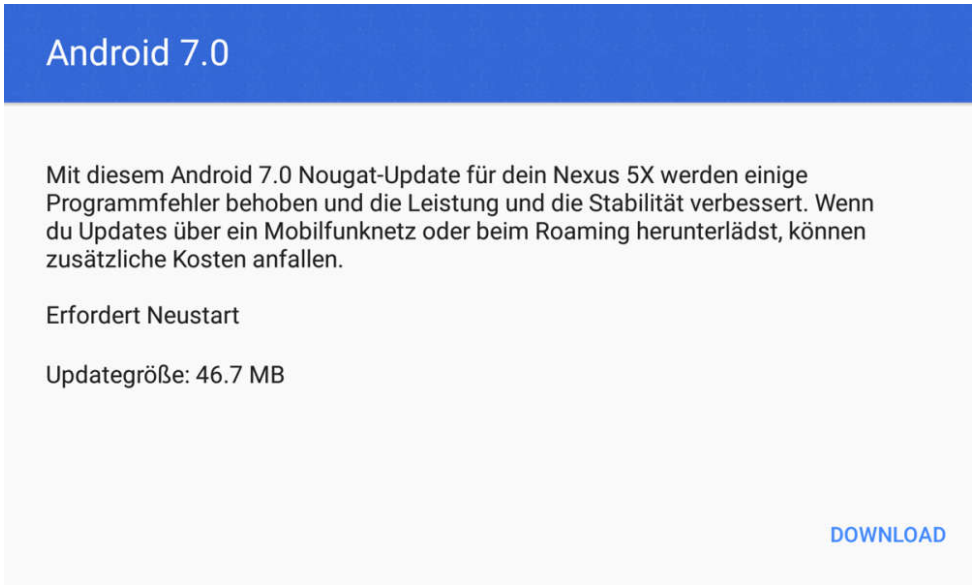
Regel 5: Google Play

Installieren Sie ausschließlich Apps und Spiele aus vertrauenswürdigen Quellen. Im Klartext: laden Sie neue Software nur aus den offiziellen App Stores wie Google Play und Apple AppStore herunter. Hier sorgen die Store-Betreiber für die Einhaltung qualitativer und sicherheitstechnischer Mindeststandards. Das heißt nicht, dass hier alle Downloads gänzlich sorglos genutzt werden können. Aber das Risiko ist deutlich geringer als bei Apps, die Sie aus weniger prominenten Quellen herunterladen. Die Regel "Saubere Software" gilt besonders für Android-Benutzer, denn hier ist das Angebot an alternativen Software-Quellen besonders groß.

© PanGu

Regel 6: Kein Root, kein Jailbreak

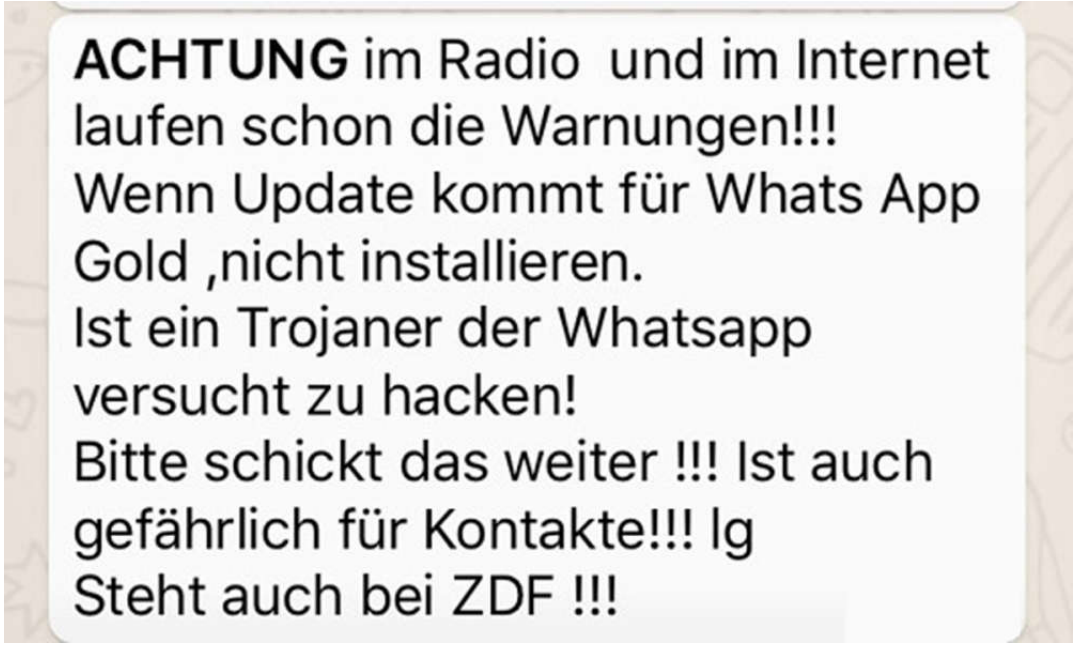
Als "Rooten" (Android) beziehungsweise "Jailbreaken" (Apple iOS) bezeichnet man die Prozedur, mit der man sich mehr oder weniger trickreich Administrationsrechte auf dem eigenen Smartphone verschafft. Erst dadurch lässt sich manche App (vollumfänglich) nutzen. Während Apple das Jailbreaken durch Schutzmaßnahmen stark erschwert, ist das Rooten von Android-Geräten vergleichsweise leicht. Da ist es kein Wunder, dass viele Android-Apps ausdrücklich einen Root-Zugang erfordern. Das Problem: mit dem Root-Zugang beziehungsweise Jailbreak hebeln Sie zahlreiche Sicherheitsvorkehrungen Ihres Handys aus. Überlegen Sie deshalb gründlich, ob neue Apps und Funktionen dieses Risiko wert sind und verzichten Sie besser darauf.



© Screenshot WEKA / PC Magazin

Regel 7: Updates sofort installieren

Installieren Sie Updates, sobald Ihnen diese zum Download angeboten werden. Natürlich kann es einmal eine Ausnahme geben, zum Beispiel wenn Sie gerade nur per mobilem Internet unterwegs sind und auf Ihr Datentransfervolumen achten müssen. Sobald Sie aber wieder in einem WLAN sind sollten Sie Ihr Handy ans Stromnetz hängen und das Update einspielen. Häufig werden über Updates erst kürzlich entdeckte Sicherheitslücken geschlossen, die aber bereits aktiv ausgenutzt werden. Deshalb schützen Updates besonders gut vor aktuellen Bedrohungen.

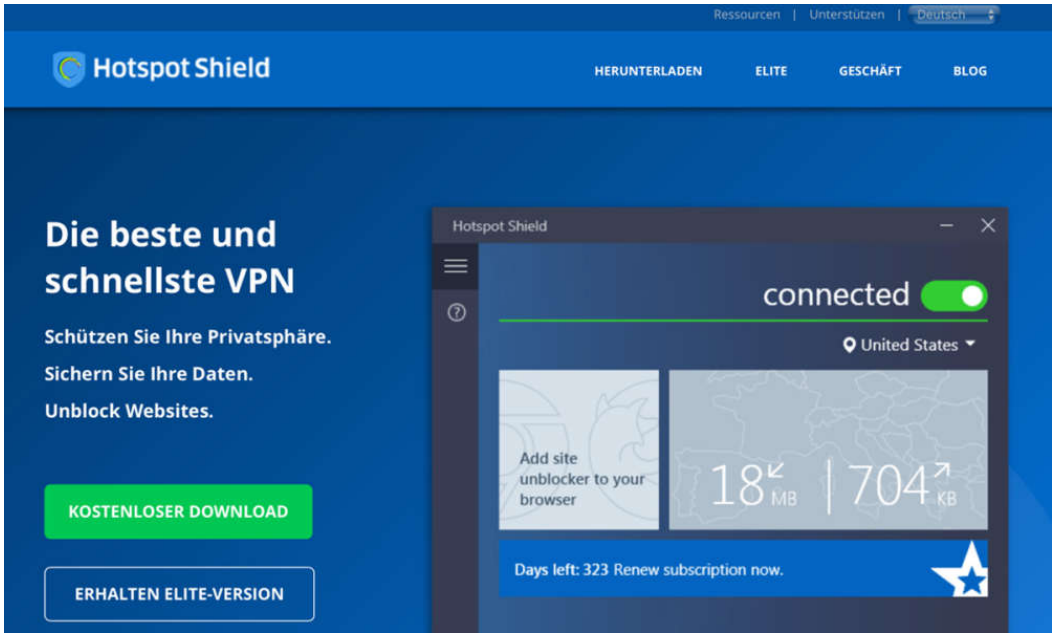


© Screenshot WEKA / PC Magazin

Regel 8: Social Engineering erkennen

Zu den gefährlichsten Angriffsmethoden zählt das Social Engineering. Dabei werden zwischenmenschliche Beziehungen ausgenutzt, um Sie zum Beispiel zur Preisgabe persönlicher Informationen wie etwa Zugangsdaten zu bringen. In diese Kategorie fallen zum Beispiel Phishing-E-Mails, mit denen der Absender versucht, Sie auf eine nachgemachte Website zu befördern, zum Beispiel auf eine Kopie von PayPal oder einer Bank. Dort sollen Sie dann, häufig unter dem Vorwand einer Sicherheitsüberprüfung, Ihre Zugangsdaten eingeben. Auch Kurznachrichten, zum Beispiel solche, die Sie auf „Ihr persönliches, kostenloses Upgrade auf WhatsApp Gold“ hinweisen, fallen in diese Kategorie. Hier sollen Sie aber zur Installation eines Schadprogramms gebracht werden. Dasselbe gilt für vermeintliche Notrufe von Freunden, die angeblich auf einer Auslandsreise bestohlen wurden und nun dringend Geld benötigen. Diese Angriffe basieren auf entwendeten Adressbüchern.

Schützen können Sie sich, indem Sie gegenüber unbekannten Absendern und außergewöhnlichen Anfragen besonders skeptisch sind. Außerdem sollten Sie persönliche Informationen nicht herausgeben. Klicken Sie in verdächtigen E-Mails und Kurznachrichten enthaltene Links nicht an, sondern besuchen Sie die Website des vermeintlichen Absenders, indem Sie die Adresse direkt in den Browser eingeben. Suchen Sie den telefonischen Kontakt zum Absender, wenn Sie sich nicht sicher sind, dass die Nachricht wirklich von ihm stammt.

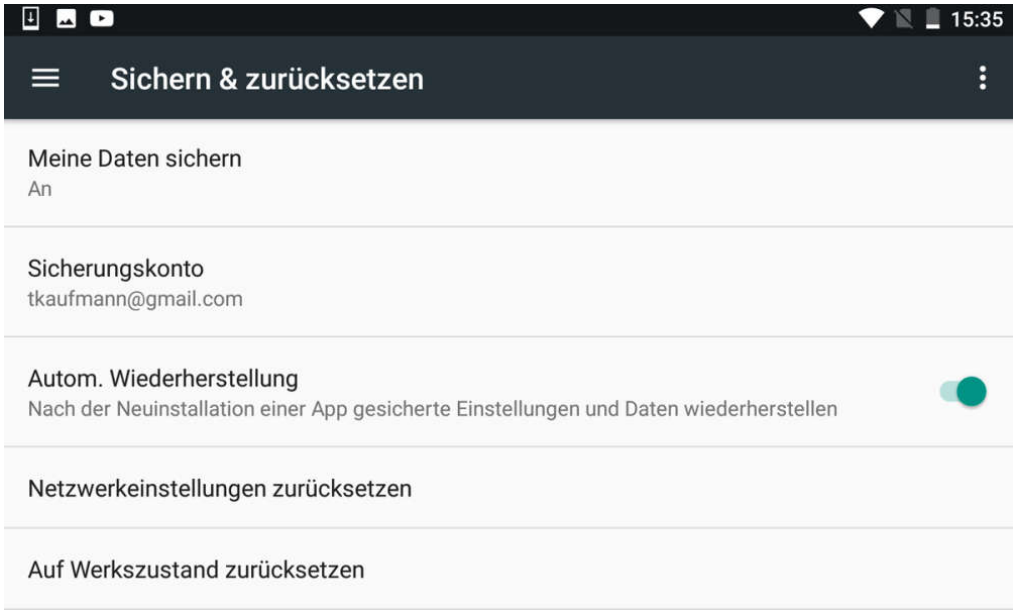


© Screenshot WEKA / PC Magazin

Regel 9: Vorsicht vor fremden WLAN

Im Restaurant, Hotel, im Zug und an immer neuen Orten ersetzen WLAN die teure Mobilfunkverbindung ins Internet. Grundsätzlich ist das gut. Bedenken Sie aber, dass der Betreiber des Funknetzwerks und von ihm mit der Administration beauftragte Personen Zugriff auf die übermittelten Daten haben. Das gilt auch dann, wenn die Verbindung per WPA verschlüsselt ist.

Nutzen Sie öffentliche Netzwerke deshalb nicht, um sensible Websites zu besuchen, auf denen Sie Ihre Zugangsdaten eingeben müssen. Auch diese könnten nämlich ausgespäht werden. Die Sicherheit lässt sich durch den Einsatz eines virtuellen privaten Netzwerks (VPN) deutlich erhöhen. Dabei werden alle Daten auf Ihrem Computer verschlüsselt, bevor sie durch das WLAN wandern. Auch auf Smartphones sind VPN-Verbindungen möglich. Ein Lesetipp hierzu ist unser VPN-Anbieter Vergleich mit Hide my Ass, Cyberghost & Co. im Test.



Regel 10: Beim Verkauf zurücksetzen

Die Sorgfaltspflicht gegenüber dem eigenen Smartphone endet erst dann, wenn es Ihnen nicht mehr gehört. Ist es dann noch in funktionsfähigen Zustand, sollten Sie es auf die Werkseinstellungen zurücksetzen. Weil dabei auch Ihre persönlichen Daten gelöscht werden ist das die beste Methode, um persönliche Daten in Sicherheit zu bringen. Lässt sich das Handy nicht mehr bedienen, dann kann das Zurücksetzen unmöglich sein. In diesem Fall wissen Sie sich aber nun dank Regel Nummer 2 (Daten verschlüsseln) auf der sicheren Seite, wenn Sie das Gerät entsorgen.