Hannes A. Czerulla

Gesprengte Ketten

Custom-ROMs installieren und Android-Geräte rooten

Custom-ROMs lassen sich mittlerweile ebenso leicht aufs Smartphone oder Tablet flashen wie Root-Rechte unter Android zu ergattern sind. Technisches Detailwissen und tagelange Recherche in Foren sind kaum noch nötig: Software-Tools erledigen die Arbeit fast automatisch und unterstützen die meisten Mobilgeräte.

Die Android-Version auf vielen Smartphones ist hoffnungslos veraltet, weil die Hersteller keine Updates mehr herausbringen. Stattdessen haben sie die Systeme mit Apps und Funktionen zugemüllt, nach denen man nie verlangt hat und die man nicht deinstallieren kann. Der Nutzer darf weder sein Wunschbetriebssystem installieren noch stehen ihm Administratorrechte zu, um tiefer ins System einzugreifen.

Doch diese Probleme lassen sich lösen: mit Flash und Root. Flashen nennt man das Installieren eines Custom-ROM (siehe Seite 114) auf dem Smartphone oder Tablet. Beim Rooting eignet man sich Administratorrechte an, um Funktionen zu nutzen, die Androids Sicherheitssystem eigentlich untersagt. Beide Prozeduren waren sehr mühselig und erforderten Fachwissen, um Androids Sicherheitsmaßnahmen zu umgehen. Die meisten Methoden nutzen offene Sicherheitslücken und ungepatchte Bugs aus. Die benötigten Programme musste man sich in unübersichtlichen Foren zusammensuchen; für jedes Smartphone-Modell und jede Android-Version brauchte man andere Methoden und Software.

Mittlerweile gibt es Programme, die alles fast automatisch erledigen. Sie sind mit diversen Gerätetypen kompatibel, laden Treiber und Zusatzsoftware im Hintergrund herunter und wählen für jedes Mobilgerät automatisch die korrekte Methode zum Flashen und Rooten – einfacher geht es nicht.

Was ist was

Um ein Custom-ROM oder gar ein anderes Betriebssystem wie Sailfish OS oder Ubuntu aufs Gerät zu bekommen, sind grundsätzlich

drei Arbeitsschritte nötig: Bootloader entsperren, Custom Recovery installieren und das neue ROM aufspielen.

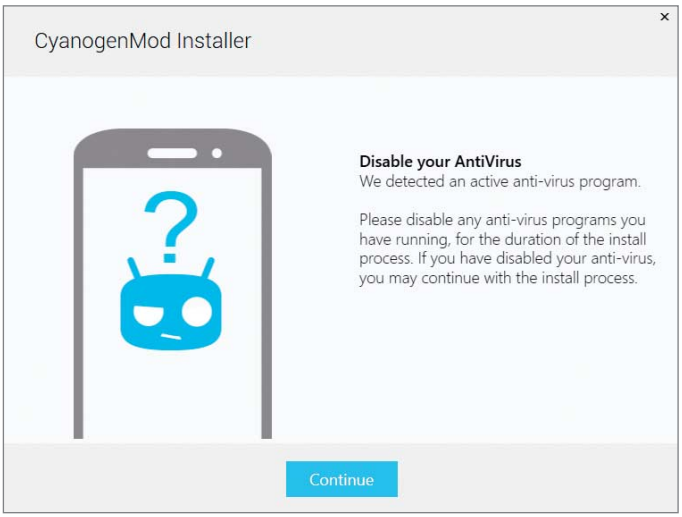
Der Bootloader ist ein Programm, das während des Boot-Vorgangs vor dem eigentlichen Betriebssystem geladen wird. Es initialisiert Teile der Hardware, lädt den Android-Kernel und reicht schlussendlich die Verantwortung für den Systemstart weiter. Smartphone- und Tablet-Hersteller nutzen den Bootloader aber auch, um dem Nutzer den Zugriff auf die Systempartition zu verweigern. Bevor man ein Custom-ROM installieren kann, muss man zuerst diese Sperre entfernen – man spricht von einem „Bootloader Unlock“. Bei einigen Geräten wie der Nexus-Reihe ist der Unlock mit einem einfachen Befehl erledigt. Hersteller wie HTC, Motorola und Sony stellen sogar selbst Werkzeuge zum Entsperren zur Verfügung und beschneiden im Gegenzug die Garantie. Geräte mit Lock bekommt man nur mit zusätzlicher Software geknackt. Entsperrt man den Bootloader, gehen alle Daten auf dem Gerät verloren. Zuvor sollte man also erst alles sichern und vorsichtshalber die SD-Karte herausnehmen.

Im zweiten Schritt wird ein sogenanntes Custom Recovery installiert. Dabei handelt es sich um ein Minibetriebssystem, das ein beschädigtes Betriebssystem im Notfall wiederherstellt, aber beispielsweise auch offizielle System-Updates vom Hersteller installiert. Die von den Hardware-Herstellern installierten „Stock Recoverys“ können nur wenig. Mehr Funktionen haben Custom Recoverys, sie installieren unter anderem Custom-ROMs. Die zwei populärsten Custom Recoverys sind ClockworkMod Recovery (CWM) und TeamWin Recovery Project (TWRP), deren Funktionen fast identisch sind. Der größte Unterschied ist, dass sich TWRP per Touchscreen bedienen lässt und eine grafische Bedienoberfläche mitbringt; CWM ist rein textbasiert und lässt sich in den meisten Varianten nur mithilfe der Lautstärketasten und des Einschaltknopfes steuern.

Ist das Custom Recovery auf dem Gerät, wird der dritte Schritt zum Custom-ROM – das eigentliche Flashen – meist zum Kinderspiel. Custom Recoverys installieren ROMs fast automatisch direkt vom internen Speicher des Mobilgeräts. Will man später ein anderes ROM aufspielen oder zur ursprünglichen Android-Version zurückkehren, erledigen die Recoverys auch diese Aufgabe.

Rooting

Rooting ist der kleine Bruder des Flashings. Anstatt das gesamte Betriebssystem auszutauschen, geht es nur darum, Administratorrechte freizuschalten, um das System nach Gutdünken anzupassen oder Apps mit Spezialfunktionen zu nutzen. Nach erfolgreichem Rooting bleibt in Android erst mal alles beim Alten, auch alle Daten bleiben erhalten.

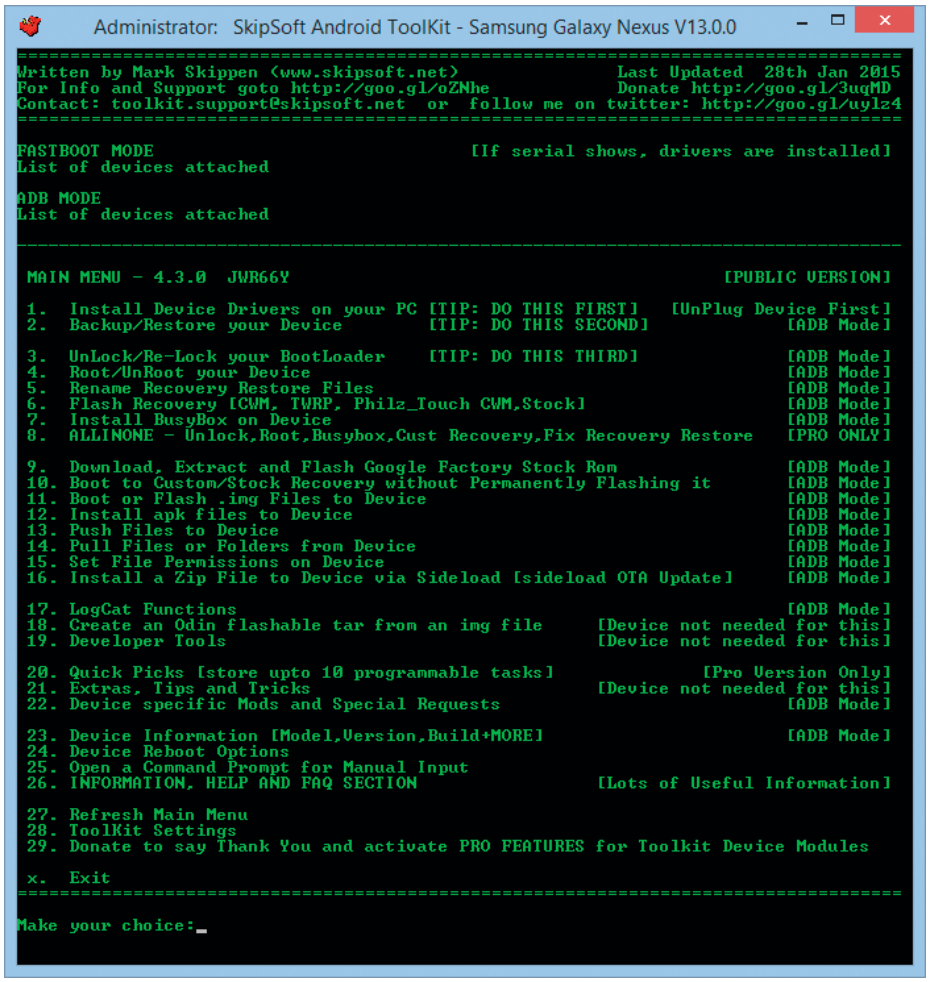


Virenscanner halten Flashing-Programme wie den CyanogenMod Installer fälschlicherweise für schädlich.

Einziger sichtbarer Unterschied ist eine App namens SuperSU oder Superuser. Sie wird während des Rootings aufs System gespielt und verwaltet künftig alle Root-Rechte – ähnlich wie die Benutzerkontensteuerung von Windows. Fordert eine App Admin-Rechte an, fragt SuperSU beziehungsweise Superuser den Nutzer nach Erlaubnis. Solange man diese Frage nicht leichtfertig abnickt, stellt Rooting kein Sicherheitsrisiko dar.

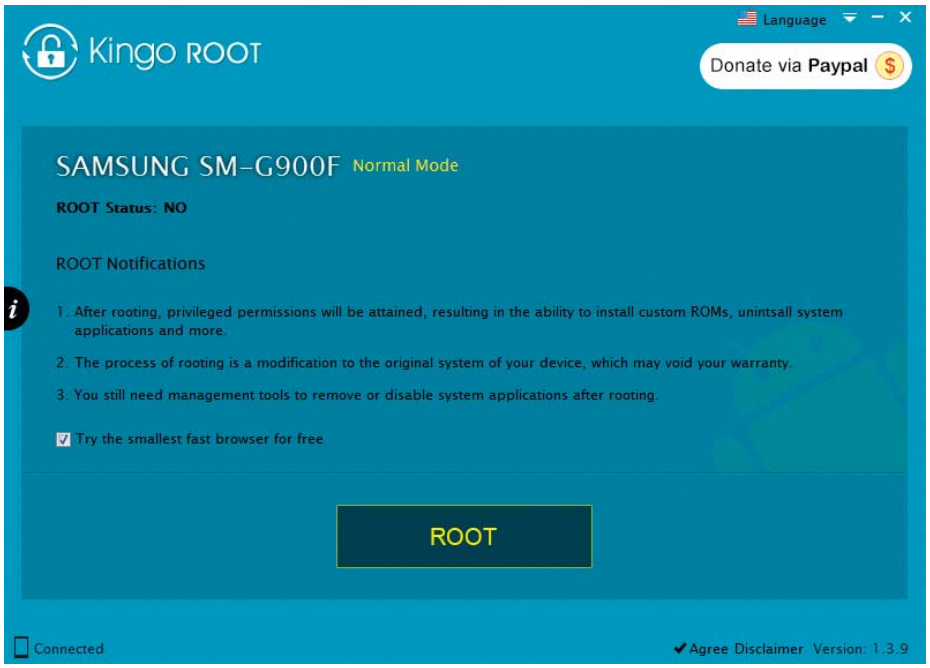
Einige Apps wie WhatsApp zeigen eine Warnmeldung, wenn sie Rooting auf dem Gerät bemerken. Schließt man die Meldung, funktioniert aber alles wie gewohnt. Nur wenige Programme wie die TAN-App der Sparkassen verweigern aus Sicherheitsgründen die Arbeit auf gerooteten Geräten.

Egal, ob man rootet oder flasht: Die meisten Hersteller erklären mit den Modifikatio-



Falls das SkipSoft Unified Android Toolkit mit einem Gerät kompatibel ist, übernimmt es alle zum Rooten und Flashen nötigen Aufgaben.

Das WinDroid Universal Android Toolkit kombiniert eine eingängige Benutzeroberfläche mit großem Funktionsumfang.



Kingo Root entsperrt den Root-Zugriff mit einem Klick. Vorher sollte man aber die Installation des Browsers abwählen.

nen die Garantie und Gewährleistung für ungültig.

In den Startlöchern

Bevor es losgehen kann, müssen Sie Vorbereitungen auf dem Android-Gerät treffen, damit die Flash- und Rooting-Tools vom PC oder Mac aus mit dem Android-Gerät kommunizieren können. Zuerst müssen Sie den USB-Debugging-Modus aktivieren. Diese Einstellung ist eigentlich für Entwickler gedacht und dient dazu, dass der Desktop-Rechner tieferen Zugriff in die Geräte-Software erhält als normalerweise per USB. Sie finden die Option in den Android-Systemeinstellungen unter dem Menüpunkt „Entwickleroptionen“. Sollte dieser Punkt nicht im Menü stehen, müssen Sie ihn freischalten. Dafür wählen Sie im Hauptmenü den untersten Punkt „Über das Telefon“ beziehungsweise „Über das Tablet“ und tippen dort siebenmal auf den Punkt „Build-Nummer“.

Einige Tools funktionieren nur in Kombination mit Android-Apps, die nicht in Google Play verfügbar sind, da sie gegen dessen Richtlinien verstoßen. So lädt man die jeweilige App als apk-Datei via Browser herunter und installiert sie manuell. Damit Android das erlaubt, aktivieren Sie in den Systemeinstellungen des Mobilgeräts im Untermenü „Sicherheit“ die Option „Unbekannte Quellen“. Als letzter Schritt empfiehlt sich ein Backup der persönlichen Daten wie Browser-Lesezeichen und Chat-Nachrichten. Auf ungerooteten Geräten lassen sich Apps samt Daten am einfachsten mit der App Helium sichern. Auf dem PC müssen Sie temporär den Virenschutz deaktivieren, da viele Programme die Root- und Flash-Tools fälschlicherweise als Malware identifizieren. Abgesehen vom CM Installer sind alle im Folgenden vorgestellten Programme nur auf Englisch erhältlich.

CyanogenMod Installer

Einer der einfachsten Wege, das Wunsch-ROM aufs Mobilgerät zu bekommen, führt über den CyanogenMod Installer. Eigentlich ist er nur dazu gedacht, das Custom-ROM CyanogenMod zu installieren. Dabei macht er aber auch den Weg für andere Custom-ROMs frei. Denn bevor er CyanogenMod aufs System spielt, entsperrt er vollautomatisch den Bootloader und installiert ClockworkMod Recovery. Im Test konnte der Installer zwar mit moderneren Geräten nichts anfangen. Dennoch ist das Programm einen Versuch wert, da der Aufwand so gering ist. Es besteht – wie bei unserem Testgerät – die geringe Gefahr, dass das Mobilgerät nach der Installation in einer Bootschleife festhängt. Andere Flashing-Tools können das Gerät dann meist retten.

Der CM Installer besteht aus einem winzigen Windows-Programm und einer Android-App. Beide laden Sie über die Webseite get.cm herunter, wo auch eine kurze Anleitung steht. Installieren und starten Sie zuerst die Android-App. Sie nimmt den Nutzer bei der Hand und führt ihn durch jeden einzelnen Installationsschritt.

Verbinden Sie zunächst Mobilgerät und PC oder Mac via USB und aktivieren Sie in Android den PTP-Modus. Weiter geht es auf dem Desktop-Rechner. Sobald der CM Installer dort das Gerät erkannt hat, wählt er automatisch die korrekte Flash-Methode und lädt die nötigen Programme und die passende CyanogenMod-Version herunter. Danach spielt er ein Custom-Recovery auf und flasht das ROM. Zwar erscheinen während des Prozesses immer wieder Menüs und Meldungen auf dem Mobildisplay; der CM Installer wählt aber alles Nötige selbst aus.

Nach ein paar Minuten startet das Android-Gerät neu und braucht wahrscheinlich etwas länger zum Booten als sonst. Falls das Gerät auch nach einer halben Stunde noch in der Boot-Schleife hängt, sollten Sie den Akku entnehmen oder den Einschaltknopf länger als zehn Sekunden gedrückt halten. Das zwingt das Gerät zum Neustart. Hat alles geklappt, läuft nun CyanogenMod auf dem Gerät.

Wenn Sie ein anderes Custom-ROM bevorzugen, können Sie dieses nun mithilfe des installierten Custom Recovery aufspielen. Schieben Sie das von Ihnen bevorzugte ROM als Zip-Datei in ein Verzeichnis des internen Flash-Speichers des Mobilgeräts, wo Sie es leicht wiederfinden. Schalten Sie nun das Gerät aus und booten Sie ins Recovery. Am leichtesten gelangen Sie über den Bootloader dorthin: Drücken Sie im ausgeschalteten Zustand ein paar Sekunden lang gleichzeitig die Power- und die untere Lautstärketaste. Bei Samsung-Geräten muss zusätzlich der Home-Button gedrückt werden. Navigieren Sie über die Lautstärketasten durch die Menüs und bestätigen Sie Ihre Auswahl mit dem Power-Knopf. Wählen Sie „Recovery“, um ClockworkMod Recovery aufzurufen. Wählen Sie dort „install zip\choose zip from\ sdcard“ und suchen Sie das Verzeichnis mit Ihrem ROM. Das Hauptverzeichnis des internen Flash-Speichers heißt hier „sdcard\0“. Starten Sie die Installation, indem Sie die Zip-Datei auswählen.

Sollte das heruntergeladene ROM zur Hardware inkompatibel sein, bricht die Installation automatisch ab. War sie erfolgreich, sollten Sie nach der Installation im Hauptmenü des Recovery nacheinander die Menüpunkte „wipe data\factory reset“ und „wipe cache partition“ auswählen. Im Untermenü „Advanced“ wählen Sie zusätzlich „wipe dalvik cache“. Das restlose Löschen

des Zwischenspeichers verhindert viele Fehler, die gelegentlich nach der Installation eines neuen ROM auftreten. Nun ist das neue Betriebssystem installiert und Sie können das Gerät neu booten.

SkipSoft Unified Android Toolkit

Von der puristischen Aufmachung des SkipSoft Unified Android Toolkit sollte man sich nicht täuschen lassen: Es ist eine Art Schweizer Taschenmesser fürs Knacken von Android-Geräten. Das Windows-Programm funktioniert zwar über ein einfaches Textfenster und nimmt nur Befehle per Tastatur entgegen. Auf diesem Weg flasht es aber ROMs, rootet Geräte und speichert vollständige Backups. Alle Google-Modelle ab dem Galaxy Nexus werden unterstützt, viele Samsung-Geräte sowie das OnePlus One. Im neongrünen Hauptmenü wählen Sie als Erstes Ihr Smartphone, Tablet oder Ihre Android-Settop-Box aus. Das Toolkit arbeitet modulweise und installiert automatisch nur die fürs ausgewählte Gerät nötigen Programmteile.

Als Erstes werden die ADB-Treiber (Android Developer Bridge) zur Kommunikation mit dem Gerät per USB eingerichtet. Alle Funktionen sind bis ins Detail in den jeweiligen Menüs erklärt. Das ist zwar viel Lesestoff, spart einem aber die mühselige Recherche in einschlägigen Foren. Es fängt damit an, dass die Software mehrere ADB-USB-Treiber für jedes Mobilgerät bereithält. Backups lassen sich in zig Varianten anfertigen: nur die Apps, deren Daten oder ein komplettes Image des Systems per NANDroid-Backup. Auch zum Rooten bietet das Android Toolkit je nach Gerät und Android-Version mehrere Methoden. Auf Wunsch entfernt das Toolkit den Root-Zugriff auch wieder (Unroot). Custom-ROMs im Zip-Format installiert die Software unkompliziert via Sideload; sie werden also direkt vom PC auf das Android-Gerät geflasht. Falls der Bootloader noch nicht entsperrt ist, erledigt das Toolkit auch diese Aufgabe.

WinDroid Universal Android Toolkit

Das kostenlose WinDroid Universal Android Toolkit kann nicht ganz so viel wie das von SkipSoft, ist aber übersichtlicher und bietet eine selbsterklärende grafische Bedienoberfläche. Vor allem unterstützt WinDroid mehr Geräte: Außer den Nexus-Modellen von Google krempelt es auch Smartphones von HTC, Motorola, Oppo, Xiaomi, dem Tablet Nvidia Shield und sogar einigen Smartwatches um. Samsung-Modelle stehen nicht auf der Liste, und nicht für alle Mobilgeräte stehen alle Funktionen zur Verfügung.

Auf Wunsch entsperrt die Software den Bootloader, installiert Custom-Recoverys, richtet Root-Zugriff ein und flasht Custom-ROMs. Die passende Methode für das jeweilige Mobilgerät wählt die Software selbstständig. Custom-ROMs flasht das Toolkit aus Images (.img) oder Zip-Dateien. Für Images wählen Sie „Flash Recovery“, für Zip-Dateien „Sideload“. Unter dem Reiter „Commands“ stehen Spezialbefehle wie der Neustart des Geräts direkt in den Bootloader oder das Recovery. Von hier aus lassen sich auch App-Dateien vom PC aus installieren. Eine Backup-Funktion fehlt.

Rooting-Tools

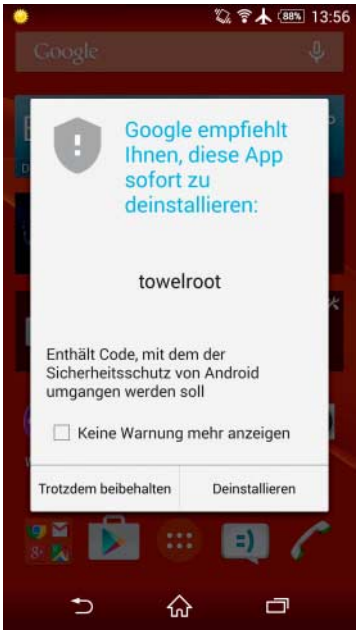
Nicht immer braucht man die Funktionsvielfalt der großen Toolkits. Zum Rooten, reichen einfachere und kleinere Programme. Da beim Rooten individuelle Sicherheitslücken ausgenutzt werden, bedarf fast jedes Modell und jede Firmware-Version eines anderen Wegs. Glücklicherweise gibt es sogenannte One-Click-Root-Tools. Sie laufen vom PC aus und unterstützen mehrere Android-Geräte gleichzeitig.

Besonders viele Modellvarianten unterstützt Kingo Root. Die Bedienoberfläche könnte kaum einfacher sein: Es gibt außer etwas Infotext nur eine Schaltfläche mit der Aufschrift „Root“. Bevor Sie darauf klicken, sollten Sie unbedingt den Haken in der kleinen Checkbox darüber entfernen; andernfalls wird zusätzlich ein Browser installiert. Nacheinander versucht Kingo Root mehrere Root-Methoden am verbundenen Gerät – das kann einige Zeit dauern. Einige Geräte starten während des Rootings mehrmals neu. Die dabei installierte Kingo-Root-App kann man im Anschluss löschen. Unsere Erfolgsquote war mittelprächtig: Nexus-Smartphones wurden problemlos gerootet, ein Samsung Galaxy S5 nicht. Generell hat Kingo Root Schwierigkeiten mit moderneren Modellen. Läuft darauf bereits Android 5, sind die Erfolgsaussichten gering. Schließt man ein bereits gerootetes Gerät an, kann Kingo Root das Rooting auch entfernen.

Towelroot kommt ohne PC aus und besteht nur aus einer Android-App, die Sie auf der Seite des Entwicklers herunterladen können (siehe c’t-Link) – ein Klick auf das Lambda-Symbol startet den Download. Der Download im Mobil-Browser direkt auf das Android-Gerät schlug bei uns mehrmals fehl. Daher empfehlen wir, die apk-Datei auf den PC herunterzuladen und von dort aus aufs Mobilgerät zu ziehen. Ist Towelroot installiert und gestartet, tippen Sie auf „make it ra1n“ und warten ab. Startet das Android-Gerät neu, ist das Rooting fehlgeschlagen. Towelroot unterstützte die wenigsten unserer Testgeräte, weil es eine Linux-Sicherheitslücke ausnutzt, die neuere Android-Versionen bereits geschlossen haben. Aber je älter das Modell, umso besser sind die Erfolgsaussichten.

Die Alternative zu Towelroot heißt Framaroot. Es handelt sich ebenfalls um eine einfachst zu bedienende App, die für jedes Gerät mehrere Rooting-Methoden anbietet, die nach Charakteren aus Herr der Ringe benannt sind. Probieren Sie einfach alle Methoden nacheinander durch.

Towelroot ist eine App mit einem Button und einer einzigen Funktion: Rooting.



Bei den hier vorgestellten Programmen können Sie Googles Warnungen getrost ignorieren.

Wenn alles nichts hilft

Sollten Sie mit keinem der Universal-Tools erfolgreich sein, benötigen Sie eine alternative, auf Ihr Gerät zugeschnittene Methode. Damit wird es komplizierter, denn die wenigsten funktionieren mit nur einem Klick. Unter Umständen müssen Sie sich mit Befehlen der Android Debug Bridge befassen oder ROMs per Fastboot flashen, Androids eigenem Protokoll für Sideloads. Umfangreiche Listen dieser Alternativen und weitere Hilfe finden Sie beispielsweise im Forum der englischsprachigen Seite XDA-Developers. Dort treffen sich Entwickler, Frickler, Nutzer und Ahnungslose und sind meist recht auskunftsfreudig. Die deutschsprachige Alternative Android-Hilfe.de ist zwar nicht ganz so umfangreich; auf die meisten Fragen zum Thema Rooting, Flashing und Co. findet man aber auch dort kompetente Antworten. (hcz@ct.de)

c't Alle Programme unter: ct.de/yajh