FAQ
Android rooten

Antworten auf die häufigsten Fragen

Von Sebastian Piecha

Warum rooten?

! Erst auf einem gerooteten Handy hat man die komplette Kontrolle über sämtliche Android-Einstellungen und Apps. Beispielsweise lässt sich erst ein gerootetes Handy komplett sichern, inklusive aller Apps und Einstellungen. Zusätzlich kann man elementare Einstellungen anpassen, um beispielsweise die CPU und Batterie zu tunen, vorinstallierte System-Apps wie Bloatware entfernen und beliebige Apps, Treiber oder auch Kernel-Module installieren, die tiefer ins System eingreifen und zum Beispiel Verbindungen zu Werbenetzwerken blockieren.

Risiken …

? Was konkret ist am Rooten gefährlich?

! Nach dem Rooten haben alle erdenklichen Android-Apps Zugriff auf das Gerät, also auch Malware. Diese können die Root-Rechte nutzen, um sich tief ins System einzubinden, um zum Beispiel Verbindungen und Eingaben abzufangen oder vertrauliche Daten unerkannt und ungehindert an den Angreifer zu verschicken.

… und Nebenwirkungen

? Wie wahrscheinlich ist es, dass ein Gerät nach einem Rooting-Versuch nicht mehr funktioniert, also zum Brick beziehungsweise hübschen Briefbeschwerer wird?

! Es kommt immer wieder vor, dass beim Rooting einzelne Smartphones vorübergehend nicht booten. Ein dauerhafter, nicht behebbarer Schaden ist selten.

Das Rooten oder Einspielen eines Custom-ROM erfordert Zeit und sollte nicht unter Druck erfolgen. Der Vorgang ist vor allem für Einsteiger nicht einfach zu überblicken, sodass Fehler beim Umsetzen passieren können und das Handy dann nicht mehr startet.

In der Regel sind das Softwareprobleme, das Handy wird also nicht nachhaltig zerstört, sondern muss lediglich neu und dann korrekt gerootet werden. Zum Beispiel gehen ROM-Updates des Herstellers auf gerooteten Geräten oft schief und wenn sie funktionieren, entfernen solche Updates die Root-Rechte, sodass ein erneutes Rooten erforderlich wird.

Zudem gibt es Speicherbereiche, die essenzielle Einstellungen enthalten (z. B. enthält die EFS-Partition bei Nexus-Geräten die IMEI). Wenn die Einstellungen einzigartig für das jeweilige Gerät sind, lassen sie sich ohne ein vorheriges Backup gar nicht oder nur mit enormem Aufwand wiederherstellen. Von Manipulationen solcher Speicherbereiche sollte man also tunlichst die Finger lassen.

Banking

? Gibt es Anwendungen, für die sich gerootete Smartphones nicht eignen?

! Falls Sie ein Android-Gerät für das Online-Banking nutzen wollen, sollten Sie das Rooten lieber unterlassen – nicht nur, weil es dann offen steht für Android-Malware, sondern weil Banken dieses Gefahrenpotenzial natürlich kennen und deshalb zumindest in ihren allgemeinen Geschäftsbedingungen in der Regel die Nutzung ihrer Banking-Apps auf gerooteten Geräten untersagen. Manche Apps können auch feststellen, ob ein Gerät gerootet ist und verweigern dann den Start.

Banken kennen natürlich das Gefahrenpotenzial des Rootings.

Garantiefragen

? Verwirkt man beim Rooting die Garantieansprüche?

! Die meisten Hersteller von Android-Smartphones verweigern die Garantie auf gerootete Geräte, sodass man im Schadensfall auf den Kosten sitzen bleibt. Dabei ist zu beachten, dass bei vielen Geräten Spuren des Rooting-Eingriffs selbst nach einer Entfernung des Root-Zugangs erhalten bleiben.

Rooting aus Systemsicht

? Was genau passiert, wenn man ein Smartphone rootet?

! Das Android-Betriebssystem ist von Linux abgeleitet und teilt daher Dateien und Prozesse in verschiedene Kategorien wie „System“ und „User“ ein und teilt diesen unterschiedliche Zugriffsrechte zu. Die Zugriffsrechte sind an User-IDs gekoppelt. Jede App, jeder Prozess und auch der Anwender haben eigene User-IDs.

Im Grundzustand kann eine App nur auf Ressourcen zugreifen, die ihr zugeordnet sind; diese sind mit ihrer User-ID markiert. Wenn eine App auf Ressourcen einer anderen zugreifen soll, braucht sie dafür zusätzliche Rechte. Das ist etwa der Fall, wenn man in der Mail-App Anhänge hinzufügen will, denn diese werden in der Regel mit anderen Anwendungen erzeugt.

Nur der Root-User hat Zugriff auf alle Elemente des Betriebssystems. Damit böswillige Software nicht auf Inhalte anderer Apps ohne Rückfrage zugreifen kann, arbeitet ein Android-OS üblicherweise ohne den `su`-Befehl (substitute user), mittels dem Anwendungen Root-Rechte erlangen können.

Einfach gesagt, wird beim Rooten das su-Kommando (das su-Binary) auf das System kopiert und dort verankert. Auf manchen Handys ist der Vorgang aufwen-

diger, weil das su-Binary alleine nicht genügt. Dort werden dann zusätzliche Skripte oder Daemons eingerichtet. All das ist in den Apps eingerichtet, mit denen man ein Android-Smartphone rootet, sodass man sich um diese technischen Details nicht mehr kümmern muss.

Sicherheitsvorkehrungen

? Wie sollte man den Vorgang absichern, um den Ursprungszustand herstellen zu können?

! Bevor Sie ein Smartphone rooten, legen Sie unbedingt Backups an. Auf Android besteht dieser Vorgang aus zwei Schritten. Im ersten sichert man User-Daten, im zweiten den gesamten Rest an Einstellungen.

Sichern Sie zunächst so viel wie möglich vom laufenden Android-System. Viele Backup-Programme berücksichtigen nur wenige Dateikategorien – das sind oft nur User-Daten sowie ein Teil der User-Konfigurationsdaten. Halten Sie Ausschau nach einer Backup-App des Herstellers, die auch Einstellungen anderer Apps sichern kann. Nachdem das erledigt ist, sichern Sie alle Geräte-Einstellungen. Richten Sie dazu zunächst ein „Custom-Recovery“ wie TWRP oder CWM ein (siehe ct.de/y6pr); für das Backup im Custom-Recovery-Modus genügen dann wenige Fingertipps.

Beachten Sie, dass manche Handys elementare Einstellungen in separaten Partitionen speichern. Das können Mobilfunk-Einstellungen sein, zum Beispiel die Frequenzen, die sie im LTE-Modus nutzen. Achten Sie darauf, sämtliche Partitionen zu sichern.

Außerdem ist es hilfreich, ein Original-ROM des Herstellers zur Hand zu haben. Wenn er keines veröffentlicht hat, sollte man vor dem Rooten zumindest Custom-ROMs etwa von LineageOS beschaffen (siehe ct.de/y6pr). Erst wenn man ein komplettes ROM in der Hinterhand hat (egal ob Original oder Custom), verfügt man über alle Elemente des Smartphones, um es bei Softwaredefekten wieder bootfähig machen zu können.

Voraussetzungen für die Rückkehr

? Was braucht man, um den Ursprungszustand wiederherstellen zu können?

! Neben der Custom-Recovery-App braucht man ein Speichermedium mit genügend Kapazität, auf das die Backups geschrieben werden können.

Wenn Ihr Smartphone einen SD-Kartenslot hat, nehmen Sie am einfachsten eine SD-Karte. Andernfalls eignen sich USB-OTG-Adapter („on the go“), um daran USB-Speichersticks anzuschließen. Diese werden als zusätzliche Verzeichnisse gemountet, um sie als Ziel für Backups verwenden zu können.

Wenn sich das Handy weder für OTG noch für SD-Karten eignet, können Sie das Backup hilfsweise zunächst auf den Handy-eigenen Speicher schreiben. Bevor Sie dann mit dem Rooting loslegen, kopieren Sie die Backups auf ein anderes Medium, zum Beispiel per `adb pull` auf den PC.

Voraussetzungen für das Rooting

? Was setzen Rooting-Tools voraus?

! Für den Rooting-Vorgang braucht man einen PC mit Windows, Linux oder macOS, der per USB am Smartphone angeschlossen ist, sowie eine Rooting-Software auf dem Desktop-PC. Die meisten veröffentlichten Anleitungen sind für Windows gedacht. Wer nach Tools sucht und dazu das Smartphone-Modell und das PC-Betriebssystem angibt, erhält jede Menge Treffer.

Viele der Tools setzen die Android Debug Bridge `adb` voraus. Damit kann man wahlweise per USB oder WLAN per Kommandozeile auf das Gerät zugreifen, um Dateien zu übertragen, auf die Shell des Smartphones zuzugreifen, ein Backup oder Restore auszuführen oder um es neu zu starten.

Probleme und Fehlermeldungen

? Das Gerät bootet nicht, was tun?

! Zunächst: Ruhe bewahren. Ein Hardware-Brick, nach dem das Smartphone tatsächlich für alle Zeiten unbrauchbar ist, kommt äußerst selten vor. Wenn ein Gerät durch den Rooting-Vorgang nicht mehr bootet, dann liegt das sehr häufig an einer Inkompatibilität oder an einem Fehler beim Rooting-Vorgang. Das kann beim Entsperren des Bootloaders, beim Aufspielen des Custom Recovery oder des Custom-ROM oder beim Rooten passieren.

Es klingt zwar lapidar, hilft aber in aller Regel: Starten Sie den Vorgang noch mal von vorne und halten Sie sich stur an die Anleitung. Falls Sie das Rooten das erste Mal versuchen, drucken Sie die Anleitung aus und haken Sie jeden einzelnen Schritt ab, um den Überblick zu bewahren. Sehr gute Anleitungen zum Aufspielen eines Custom-ROM und einer Custom Recovery finden Sie bei LineageOS und TWRP.

Bei einem neuen Modell empfiehlt es sich, ein wenig zu warten, bis die Entwickler ihre Software an das Gerät angepasst haben. Falls die Informationen dazu dennoch dürftig sind, kann man die jüngste Beta-Version des Rooting-Tools ausprobieren. Wenn es damit auch nicht klappen will, können Sie es mit einer etwas älteren Custom Recovery versuchen.

Linux und Heimdall

? Warum kann Heimdall nicht auf mein Samsung-Smartphone zugreifen?

! Auf Linux setzt man zum Rooten von Samsung-Smartphones meist Heimdall ein. Der Zugriff darauf erfolgt über ein /dev-Gerät. Dafür sind Root-Rechte erforderlich. Setzen Sie dem Heimdall-Kommando `sudo` voran und geben Sie das Kennwort ein.

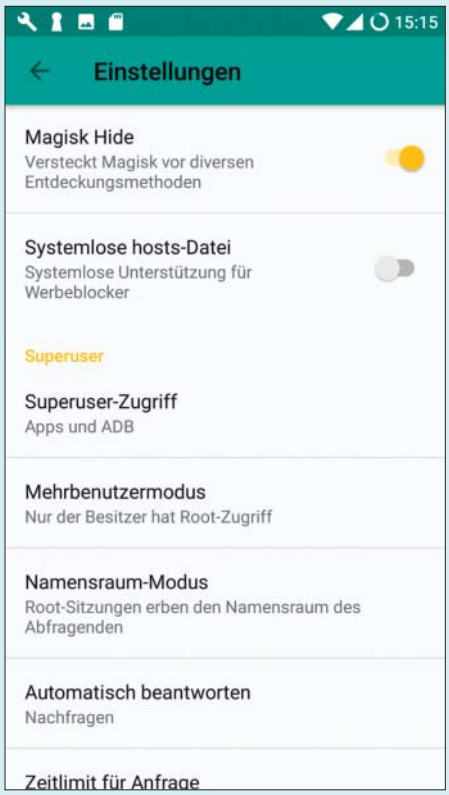
Neuere Samsung-Modelle hat der Hersteller stillschweigend geändert, sodass die Heimdall-Versionen aus den Repositories damit nicht funktionieren. Deshalb muss man Heimdall aus den aktuellen Quellen übersetzen. Den Quellcode finden Sie über ct.de/y6pr.

Wenn sich Root nicht installieren lässt

? Magisk lässt sich nicht installieren. Was tun?

! Die umfangreichste Rooting-App ist Magisk. Damit lassen sich Root-Rechte vor einzelnen Apps verstecken, damit man sie auf gerooteten Geräten ausführen kann.

Sollte sich Magisk nicht installieren lassen, hilft es, eine andere Version auszuprobieren. Versuchen Sie es zunächst mit der aktuellen, dann mit einer Beta-Version



Mit Magisk lassen sich auch Root-Rechte vor einzelnen Apps verstecken, damit man sie auch auf gerooteten Geräten ausführen kann.

und falls auch das scheitert, versuchen Sie eine ältere Version. Falls dennoch alle Rooting-Versuche zu Skriptfehlern in der Custom Recovery führen, probieren Sie es mit einem älteren Custom Recovery. Sollte auch das nicht helfen, nehmen Sie ein anderes Rooting-Tool. Eine gute Alternative unter LineageOS ist die „addonsu"-App. Auch diese finden Sie über ct.de/y6pr. Bei addonsu muss man die richtige LineageOS- und CPU-Version angeben.

Als dritte empfiehlt sich die Rooting-App SuperSU – auch diese installiert man über ein Custom Recovery.

Recovery-Installation

? Die Einrichtung des Custom-Recovery scheitert – ist mein Smartphone jetzt doch ein Brick?

! Wenn sich ein aktuelles Custom Recovery nicht installieren lässt, dann lohnt es sich, eine ältere Version auszuprobieren. Das empfiehlt sich auch, wenn die Software bei der Installation Fehlermeldungen produziert, beim Backup oder beim Installieren von Apps und Custom-ROMs oder beim Rooten.

Custom-ROMs

? Ich brauche ein Custom-ROM, um ein aktuelles Android nutzen zu können, die Einrichtung funktioniert aber nicht. Was kann ich tun?

! Es kommt vor, dass die Installation eines Custom-ROM nicht startet oder dass der Vorgang während der Ausführung ohne ersichtlichen Grund stehen bleibt. Ursache dafür ist vor allem bei einigen Samsung-Geräten eine unpassende Partitionierung. Unter anderem kann die Partitionsgröße des Android-Systems und des Custom Recovery falsch sein. Das kommt zum Beispiel vor, wenn der Entwickler die Größe der Custom-ROMs ändert.

In solchen Fällen kann es helfen, die Partitionierung neu zu erstellen und dann die Partitionen zu formatieren. Bei Samsung-Geräten erfolgt das mit Heimdall unter Angabe einer Partitionierungsdatei („pit"). Gängige Quellen für System-ROM-Partitionsdateien finden Sie über ct.de/y6pr. Auch hier gilt aber: Bevor Sie eine solche Partition einspielen, legen Sie ein Backup der aktuellen Partitionierung an. Wie man das macht, haben wir beispielhaft für das Samsung S5 beschrieben [1].

Wenn Custom-ROMs fehlen

? Ich finde kein Custom-ROM. Woran liegt das?

! Wenn die gängigen Custom-ROM-Entwickler nichts Geeignetes für ein Smartphone-Modell anbieten, kann das daran liegen, dass das Gerät selten, schlecht modifizierbar oder einfach noch sehr neu ist. Das xda-Forum ist eine beliebte Diskussionsplattform rund um das Rooting und dort sind oft Hinweise auf „brandneue" Custom-ROMs zu finden. Wir raten aber davon ab, dem nächstbesten Angebot zu folgen. Zu schnell fängt man sich ein verseuchtes oder schlecht umgesetztes System ein, dem wesentliche Funktionen fehlen. Beispielsweise kommt es vor, dass Kamera oder Bluetooth nicht funktionieren oder dass sich der Akku in Windeseile leert.

Treiber-Beschaffung

? Windows erfordert einige Treiber, um per USB auf ein Handy zugreifen zu können. Wo findet man sie?

! Treiber binden das Handy je nach dessen Betriebsart verschieden an. Man unterscheidet den Standard-Boot-Modus, den Download- oder FastBoot-Modus (bei Samsung- oder bei Nexus-Geräten) sowie den Custom-Recovery-Modus.

Viele Hersteller-Tools für das Handy bringen Windows-Treiber mit. Auch das xda-Forum ist dafür eine vertrauenswürdige Quelle. Falls Sie Linux verwenden, sind keine zusätzlichen Treiber erforderlich, auf manchen Systemen aber zusätzliche udev-Einträge [1].

Virtuelle Maschinen

? Ich will Linux in einer gesonderten virtuellen Maschine ausschließlich für das Rooting nutzen. Darüber lässt sich aber das Smartphone nicht ansprechen. Was kann man tun?

! Virtuelle Maschinen kommunizieren nur indirekt über die Virtualisierungssoftware mit der Hardware. Deshalb kann es auf solchen Systemen vorkommen, dass der Zugriff auf den Bootloader des Smartphones nicht funktioniert oder das Entsperren, das Rooten. In solchen Fällen hilft es, in der Virtualisierungsumgebung einen USB-2-Port anstatt des modernen USB-3 für die Kommunikation mit dem Smartphone einzurichten. Auch sollten Sie das Handy direkt am PC anschließen und nicht über einen USB-Hub.

Da das Handy je nach Betriebsart andere USB-Treiber verwendet, sind auch die USB-Verbindungen unterschiedlich bezeichnet. Deshalb muss man in einer virtuellen Maschine alle diese USB-Verbindungen zur Gastmaschine durchreichen.

Beispielsweise meldet sich ein laufendes Android mit seiner Produktbezeichnung. Wenn es aber im Fastboot-Modus läuft, heißt die USB-Verbindung schlicht „Android". Beide Modi haben zudem unterschiedliche Produkt-IDs. *(dz@ct.de)*

Literatur

[1] Sebastian Piecha, Root tut gut, Samsung Galaxy S5: LineageOS, Rooting und zurück zum Stock-ROM, c't 8/2018, S. 174

Tools und Custom-ROMs: ct.de/y6pr