ChannelPartner

Link: https://www.channelpartner.de/a/android-rooting-gefahren-und-moeglichkeiten,3042391

Sicherheitsrisiko durch verseuchte Apps

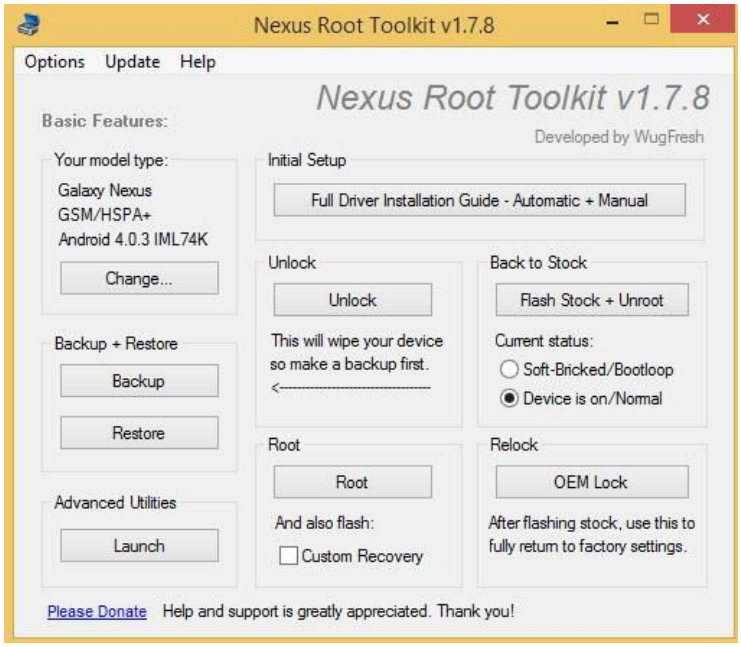
Android-Rooting: Gefahren und Möglichkeiten

Datum: 23.05.2014
Autor(en): Thomas Joos

Viele Android-Anwender "rooten" oder "jailbreaken" ihr Android-Gerät. Der Anreiz sind mehr Funktionalität, alternative Firmware und Zugriff auf Apps von Quellen wie Cydia. Missbraucht wird das häufig für die Verbreitung von Viren und Trojanern. Wir zeigen auf, was die Vorteile sind und auf was Sie achten sollten.

Android[1] baut auf einem **Linux**[2]-Kernel auf. In den Standardeinstellungen haben Anwender nur begrenzten Zugriff auf die Einstellungen und Möglichkeiten des Gerätes. Der Begriff "Root" stammt aus dem Linux/OpenSource-Bereich und soll Anwendern die Möglichkeit verschaffen, umfassende Rechte auf ihrem Gerät zu erhalten.

Ein Benutzer mit Root-Rechten ist auf dem Gerät nicht eingeschränkt, sondern hat umfassende Schreib- und Leserechte in allen Bereichen. Das wirkt sich bei Android in den verschieden **Apps**[3] und Einstellungsmöglichkeiten auf. Daher gibt es für viele Endgeräte im Internet Anleitungen, wie sich Geräte rooten lassen.



Rooting: Tools wie das Nexus Root Tookit helfen beim rooten von verschiedenen Smartphones und Tablets; im Beispiel bei den Nexus-Geräten.

Neben der Möglichkeit auf externe App-Stores zugreifen zu können, bieten gerootete Geräte noch die Möglichkeit, mehr Einstellungen auf dem System vornehmen zu können. Viele Apps, die Systemzugriff benötigen, funktionieren erst, wenn das entsprechende Gerät gerootet wurde. Das gilt häufig auch für Apps, die auf Systemdateien zugreifen wollen. Generell ist eine solche Vorgehensweise nur für Anwender sinnvoll, welche die Funktionen überhaupt erst nutzen, die das Rooting bietet. Nur um ein gerootetes Gerät zu besitzen, macht der Vorgang sicherlich keinen Sinn.

Für Profis sind die wichtigsten Vorteile beim Rooting zunächst flexiblere Möglichkeiten bei der Installation von Apps aus verschiedenen Quellen. Außerdem lassen sich mehr Systemeinstellungen auf dem Gerät ändern und zusätzliche Funktionen integrieren. Beispiele dafür sind die Installation von Custom-ROMs wie CyanogenMod, oder der Anpassung des Kernels für eine Beschleunigung der Geräte. Natürlich lässt sich auch die Oberfläche viel umfassender anpassen.

Gefahren und Probleme beim Rooting

Neben den Vorteilen gehen Anwender aber auch viele Risiken und Gefahren ein. Diese sind beim Rooting nicht zu unterschätzen. Wer Raubkopien auf seinen Endgeräten installiert, macht sich strafbar. Unabhängig davon, ob der entsprechende Anwender überhaupt weiß, ob eine bestimmte App legal ist oder illegal kopiert wurde, ist es dennoch strafbar. Fehlerhafte Einstellungen, die durch das Rooting erst möglich werden, können Geräte irreparabel beschädigen.

[Hinweis auf Bildergalerie: **Apps rund ums Fliegen im Security-Check**] gal1

Eine weitere Gefahr sind Viren- und Trojaner-verseuchte Apps aus den externen App-Stores oder anderen Quellen im Internet. Häufig bekommen Anwender nichts von diesen Trojanern mit. Die Schädlinge können Geräte nicht nur beschädigen, sondern auch enorme Kosten verursachen.

Für Firmenanwender sind gerootete Geräte besonders problematisch. Zunächst können viele Mobile Device Management (MDM)-Systeme von Unternehmen gerootete Geräte erkennen und aussperren. Das heißt, im schlimmsten Fall haben Sie nach einem Rooting-Vorgang keinen Zugriff mehr auf das Firmennetzwerk und erhalten dadurch mehr Nachteile als Vorteile durch das Rooting. Außerdem verbieten viele Unternehmen schlicht und ergreifend die Verbindung von gerooteten Geräten mit dem Netzwerk. Wer eine Verbindung dennoch durchführt und dabei erwischt wird, oder noch schlimmer, Schaden im Netzwerk verursacht, bereut sicherlich das Rooting. Viele MDM-Anwendungen können gezielt gerootete Geräte aussperren. In einem solchen Fall lohnt sich das Rooting sicherlich nicht.

Kein Support bei Rooting-Problemen

Eine weitere Gefahr ist der Support, den der Hersteller für gerootete Geräte häufig nicht mehr gewährt. Viele Hersteller erkennen, dass ein Gerät gerootet wurde, auch wenn es nach einem Problem wieder zurückgesetzt wurde. Software-Aktualisierungen oder neue Android-Versionen funktionieren häufig mit gerooteten Systemen nicht, oder versetzen diese in einen inkonsistenten Zustand.

Wenn Sie einmal ein Geräte gerootet haben, müssen Sie entweder den Rooting-Vorgang bei neuen Versionen wiederholen, oder zumindest genau darauf achten, wie Sie Aktualisierungsvorgänge durchführen. In jedem Fall macht ein gerootetes Gerät die Aktualisierung von Android und Apps komplizierter, beziehungsweise erfordert einiges an Kontrolle und Mehraufwand. Anfänger sind hier in den meisten Fällen überfordert.

Beim eigentlichen Rooting-Vorgang kann bereits einiges schief gehen. Funktioniert die Anpassung der Software nicht, startet das Android-Gerät häufig nicht mehr, oder stürzt ab. Diese Fehler werden auch als Soft-Bricks bezeichnet. Schlimmer sind Hard-Bricks, bei denen die Hardware des Gerätes zerstört wird. Während Sie bei Soft-Bricks mit Softwareanpassungen noch etwas machen können, sind Hard-Bricks meistens tödlich für gerootete Smartphones. Die meisten Hersteller gewähren dann auch keine Gewährleistung mehr, was bei besonders neuen und teuren Top-Geräte sehr ärgerlich werden kann.

Unabhängig davon, sollten sicherheitskritische Apps wie Home-Banking oder Verbindungen mit Firmennetzwerken möglichst nicht auf gerooteten Geräten verwendet werden. Vor allem ungeübte Anwender setzen sich so einer verhältnismäßig hohen Gefahr aus - insbesondere wenn auch noch externe Apps aus unbekannten Quellen installiert wurden. Viren und Trojaner aus nicht seriösen Quellen gehören zu den größten Gefahren von gerooteten Smartphones bei Android.

Vorteile des Rooting

Viele Einstellungen in **Android**[4], zum Beispiel wenn es um VPNs geht oder eine effiziente Datensicherung, erfordern gerootete Geräte. Hier müssen Anwender und verantwortliche IT-Mitarbeiter einfach abwägen, ob sich Risiken/Nutzen in ein richtiges Verhältnis setzen. In den meisten Fällen lohnt sich das Rooting nur, wenn der entsprechende Anwender genau weiß, was auf dem Gerät durchgeführt wird. Außerdem sollten auch hier nur bekannte Apps installiert werden. Auch Profi-Android-Anwender sollten möglichst unseriöse App-Stores meiden. Selbst bei **Cydia**[5] besteht die Gefahr, sich Viren einzufangen. Der Einsatz eines Virenscanners auf gerooteten Geräten ist da nur ein kleines Hilfsmittel, da auch diese Apps nicht alle Angriffe erkennen können.

Ein großer Vorteil beim Rooting ist die Möglichkeit, die komplette Oberfläche des Systems ändern zu können. Selbst die Android-Version lässt sich austauschen. Es gibt, neben CyanogenMod, weitere Custom ROMs, mit eigenen Schwächen und Stärken. Manche Entwickler legen vor allem Wert auf eine Beschleunigung der Geräte, andere auf mehr Akkulaufzeit und wieder andere auf komplett neue Oberflächen.

Vor einem Rooting-Vorgang gehört daher auch etwas Recherchearbeit dazu. Nicht alle Geräte lassen sich gleich rooten, und nicht alle Versionen der Custom-ROMs arbeiten mit allen Android-Versionen auf allen Geräten zusammen. Anwender, die Ihr Gerät rooten wollen, sollten genau durchlesen, ob das Rooten möglich ist, und das Custom-Rom, welches installiert werden soll, auch kompatibel mit dem entsprechenden Endgerät ist.

Custom-ROMs versus Rooting

Beim Rooting nehmen Sie im Grunde genommen nichts anderes vor, als sich erhöhte Rechte für Ihr Android-Gerät zu geben. Auf Basis dieser Rechte können Sie dann mehr Einstellungen ändern, Funktionen hinzufügen und Apps installieren, die offiziell nicht freigegeben sind.

Custom-ROMs ersetzen das installierte Android mit einer neuen Version. Das kann eine aktuellere Version sein, zum Beispiel für Geräte, die nicht mehr offiziell vom Hersteller unterstützt werden, oder eine Version mit angepasster Oberfläche. Um ein Custom-ROM zu installieren, brauchen Sie Root-Rechte. Viele Custom-ROMs, wie das bekannte **CyanogenMod**[6], führen beiden Vorgänge selbständig durch. Erst wird das Gerät gerootet, danach das Custom-ROM installiert.

Wann lohnt sich das Rooting am meisten?

Am meisten profitieren Anwender beim Rooting dann, wenn Sie ein altes Gerät einsetzen, für das es keine neue Android-Version mehr gibt. Sollen hier neue Funktionen installiert werden, muss häufig ein Custom-ROM ran. Prominentestes Beispiel ist **CyanogenMod**[7]. Dieses Custom-ROM baut meistens auf der aktuellsten Android-Version auf, und kann daher auch neue Funktionen schnell und einfach bereitstellen. Da bei alten Geräten die Risiken nicht ganz so hoch sind, dafür der Nutzen aber umso höher, kann sich das Rooten und das Installieren eines Custom-ROMs lohnen. Allerdings gilt auch hier, dass sich diese Vorgänge nur dann lohnen, wenn ein praktischer Hintergrund vorliegt, also eine neue Android-Version installiert werden muss, warum auch immer.

Nur damit generell eine neue Android-Version installiert wird, lohnt sich das Rooting selten. Sollen aus einer neuen Version aber Funktionen genutzt werden, zum Beispiel die Benutzerverwaltung aus Android 4, oder Sicherheitslücken geschlossen, macht eine Aktualisierung von Endgeräten durchaus Sinn. Da bei diesen Geräten häufig ohnehin die Garantie/Gewährleistung ausgelaufen ist, und diese Geräte selten noch einen echten Wert besitzen, lohnt sich eine Aktualisierung.

Das Installieren von Custom-ROMs, und das damit verbundene Rooting, kann die Sicherheit von Android-Geräten aber auch erhöhen. Vor allem bei billigen und alten Geräten findet keine Aktualisierung der installierten Android-Version mehr statt. Dadurch werden auch keine Sicherheitslücken mehr geschlossen. Installieren Sie aber auf einem solchen alten Gerät die aktuelle CyanogenMod-Version, wird auch die neue Android-Version installiert. Diese ist natürlich wesentlich sicherer als veraltete Versionen. Wenn Geräte mit SIM-Locks versehen sind, sich also nur SIM-Karten einzelner Anbieter nutzen lassen, können Sie mit dem Rooting diesen Lock entfernen und auch andere SIM-Karten nutzen.

Stable, Nightly Build, AOSP und Stock

Wer sich mit dem Thema Rooting und Custom-ROMs auseinandersetzt, stößt häufig auf einige Begriffe die wenig bekannt sind. Vor allem bei CyanogenMod spielen hier Nightly Builds und Stable Builds eine wichtige Rolle. Bei den Stable Builds handelt es sich um getestete und freigegebene Versionen, die funktionieren sollten. Diese Version ist aber häufig nicht mit den neuesten Features ausgestattet, dafür aber weitgehend frei von Fehlern.

Nightly Builds enthalten alle aktuell verfügbaren Funktionen, sind aber noch nicht umfassend getestet. Hier können noch Fehler enthalten sein, die sich in unstabilen Verhalten äußern, oder das System komplett zum Absturz bringen können. Nightly Builds sollten nur Anwender installieren, die genau wissen, was Sie tun und notfalls ein Gerät noch reparieren können, zumindest auf Seiten der Software. Natürlich macht auch hier die Installation nur dann Sinn, wenn eine Funktion aus diesem Build genutzt werden soll.

Viele Custom-ROM-Anbieter bieten die Möglichkeit, zwischen AOSP und Stock zu wählen. AOSP (Android Open Source Project) ist der offizielle und frei zugängliche Source-Code von Android. Setzen Sie aber auf ein Custom-ROM mit Stock-Software, wurden Änderungen an diesem Code vorgenommen. Auch hier sollten Anwender gründlich überlegen, ob sich eine Aktualisierung lohnt.

Die Installation eines Custom-ROMs läuft häufig in mehreren Stufen ab. Sie müssen Ihr Gerät zuerst rooten. Danach übertragen Sie das ROM auf Ihr Endgerät und starten einen Wiederherstellungsvorgang. Durch diesen Vorgang wird die neue Version installiert. Achten Sie aber darauf, dass dabei alle Daten auf dem Gerät gelöscht und alle Einstellungen angepasst werden. Die Installation eines Custom-ROMs entspricht im Grunde genommen einem Reset des Gerätes und einer anschließenden Neuinstallation von Android in angepasster Form.

Sicherung von gerooteten Geräten

Ein Vorteil von gerooteten Geräten ist die Möglichkeit, mehr Daten sichern zu können. Mit Apps wie**Titanium Backup**[8] können Sie nicht nur die Daten auf Ihrem Android-Gerät sichern, sondern auch alle Einstellungen, Android selbst, die installierten Apps, Daten dieser Apps und auch hier die meisten Einstellungen. Der Vorteil dieser Sicherung liegt auf der Hand, die Wiederherstellung eines solchen Gerätes umfasst ebenfalls alle diese Einstellungen. Titanium Backup kann auch Apps zwischen SD-Karten und dem internen Speicher hin- und her verschieben. Auch zeitgeplante Sicherungen werden unterstützt. Die Software lässt sich ausschließlich nur auf gerooteten Geräten nutzen. Wer häufig mit seinem Gerät experimentiert, sollte sich die App ansehen.

Fazit

Ob sich das Rooten eines Gerätes lohnt, lässt sich nicht definitiv verneinen oder empfehlen. Grundsätzlich gehen Anwender ein Risiko beim Rooting ein. Das Gerät funktioniert unter Umständen nach dem Vorgang nicht mehr, Viren werden durch unseriöse Apps eingeschleust, und fehlerhafte Einstellungen können das Gerät zerstören.

Auf der anderen Seite bietet das Routing auch einige Vorteile. Es gibt mehr Einstellungen, alte Android-Versionen von nicht mehr unterstützten Geräten lassen sich aktualisieren und viele Apps nutzen, die ohne Rooting nicht funktionieren. Beispiele dafür sind Datensicherungs-Apps oder Apps für VPN-Verbindungen.

Allerdings sollte kein Gerät gerootet werden, nur damit es gerootet ist. Es sollte schon ein Sinn hinter dem Vorgang stehen, wie das Entfernen eines SIM-Lock, der Einsatz einer notwendigen App oder eine neue Android-Version, die sicherer und stabiler ist.

Ungeübte Anwender sollten besser auf das Rooten verzichten oder zumindest mit einem alten Gerät beginnen, dass ansonsten nicht mehr verwendet wird. Bei neuen Android-Geräten, die häufig auch noch teuer sind, mach das Rooting selten Sinn. Ausnahme ist auch hier die Verwendung einer Custom-Rom wie CyanogenMod. (cvi)

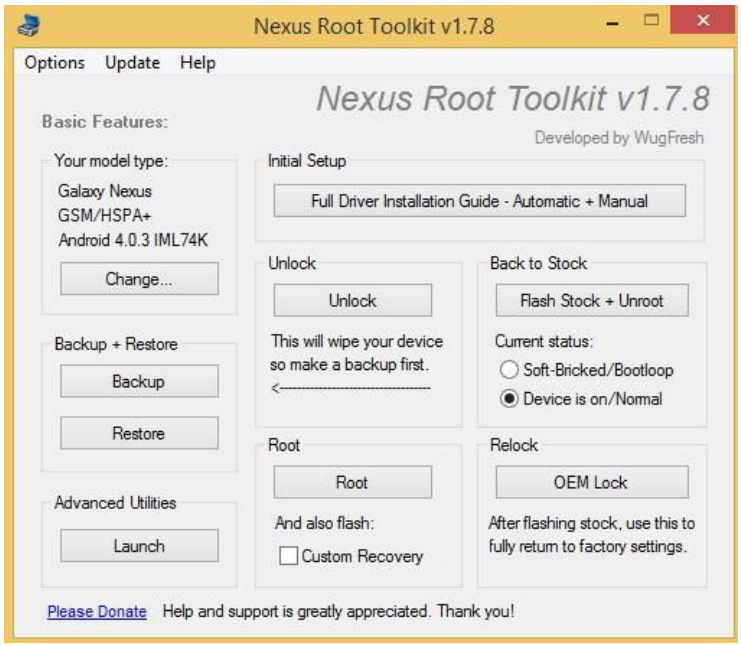
Links im Artikel:

[1] **https://www.tecchannel.de/pc_mobile/apps/2054261/**
[2] **https://www.tecchannel.de/pc_mobile/linux/2039904/empfehlenswerte_linux_distributionen_fuer_desktop_pcs/index.html**
[3] **https://www.tecchannel.de/pc_mobile/apps/2028765/top_10_liste_die_beliebtesten_android_apps/index.html**
[4] **https://www.tecchannel.de/pc_mobile/apps/2028765/top_10_liste_die_beliebtesten_android_apps/index.html**
[5] **https://play.google.com/store/apps/details?id=com.saurik.substrate**
[6] **http://www.cyanogenmod.org/**
[7] **http://www.cyanogenmod.org/**
[8] **https://play.google.com/store/apps/details?id=com.keramidas.TitaniumBackup&hl=de**

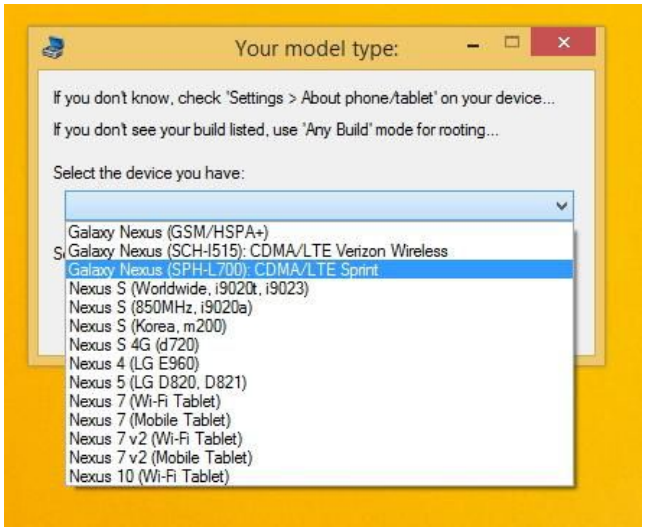
Bildergalerien im Artikel:

[gal1] **Apps rund ums Fliegen im Security-Check**

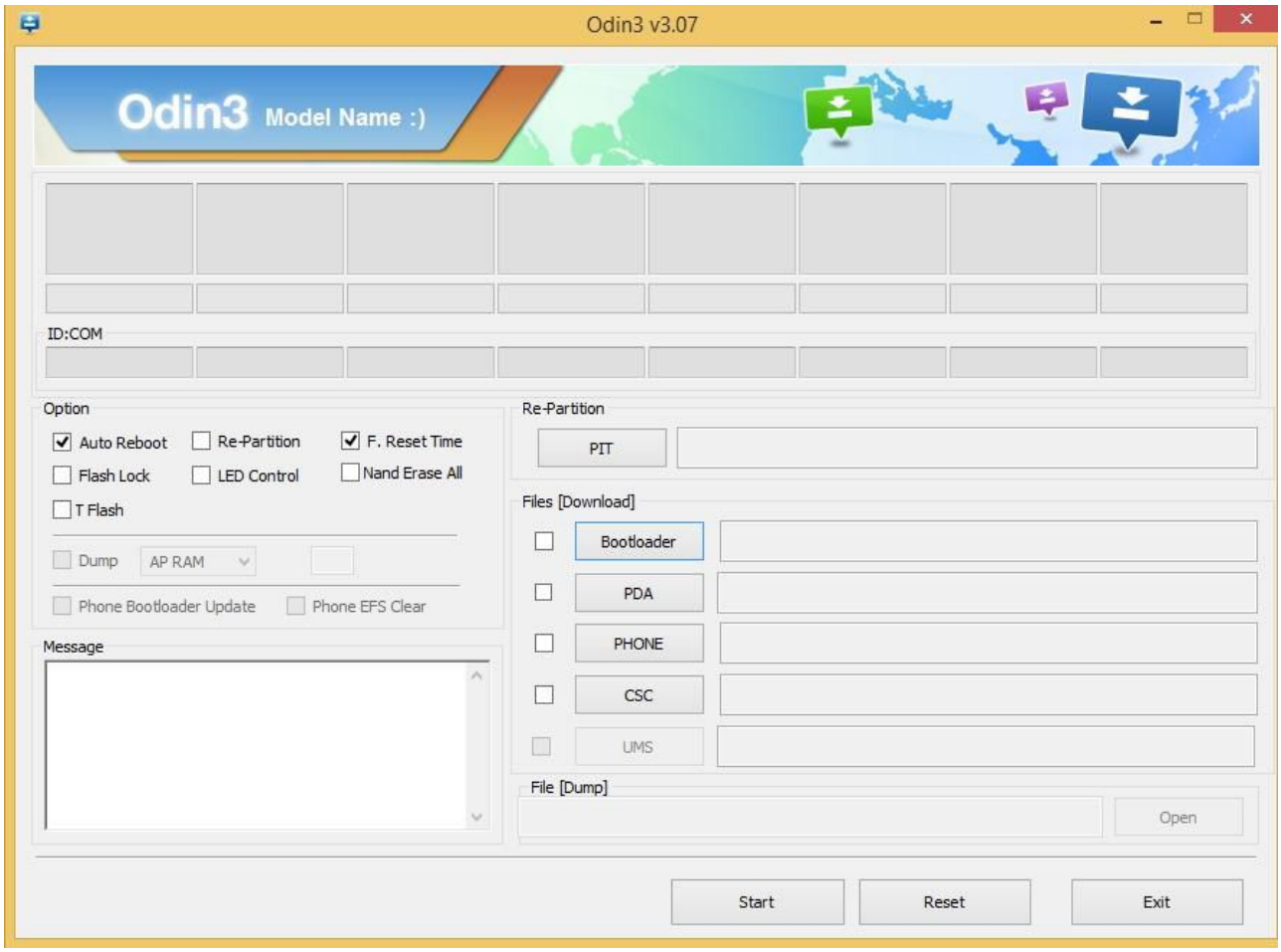
Android Rooting
Tools wie UnLock Phone können dabei helfen Android-Geräte zu rooten. Allerdings müssen Sie hier besonders aufpassen, da es in diesem Bereich ebenfalls viele Schädlinge gibt.



Android Rooting
Das Nexus Root Tookit hilft beim rooten von verschiedenen Nexus-Smartphones und -Tablets.

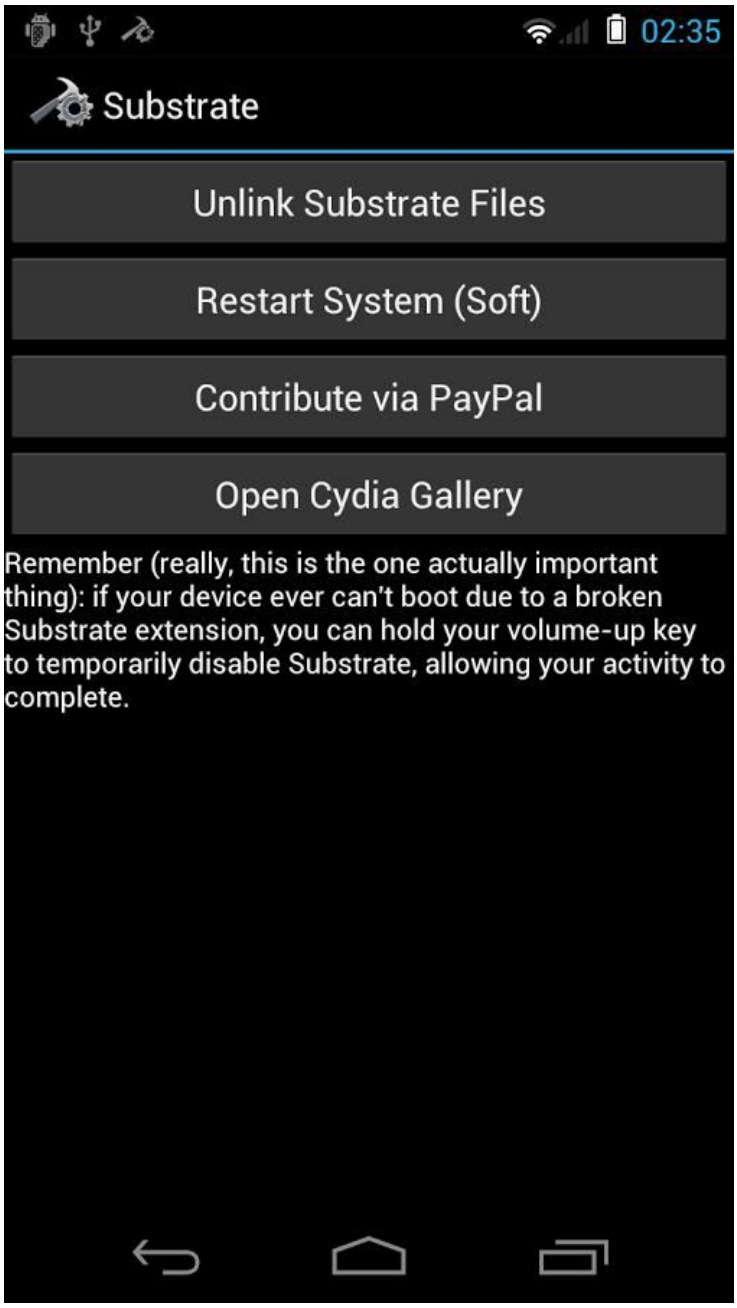


Android Rooting
Hier lassen sich die verschiedenen Nexus-Geräte auswählen.



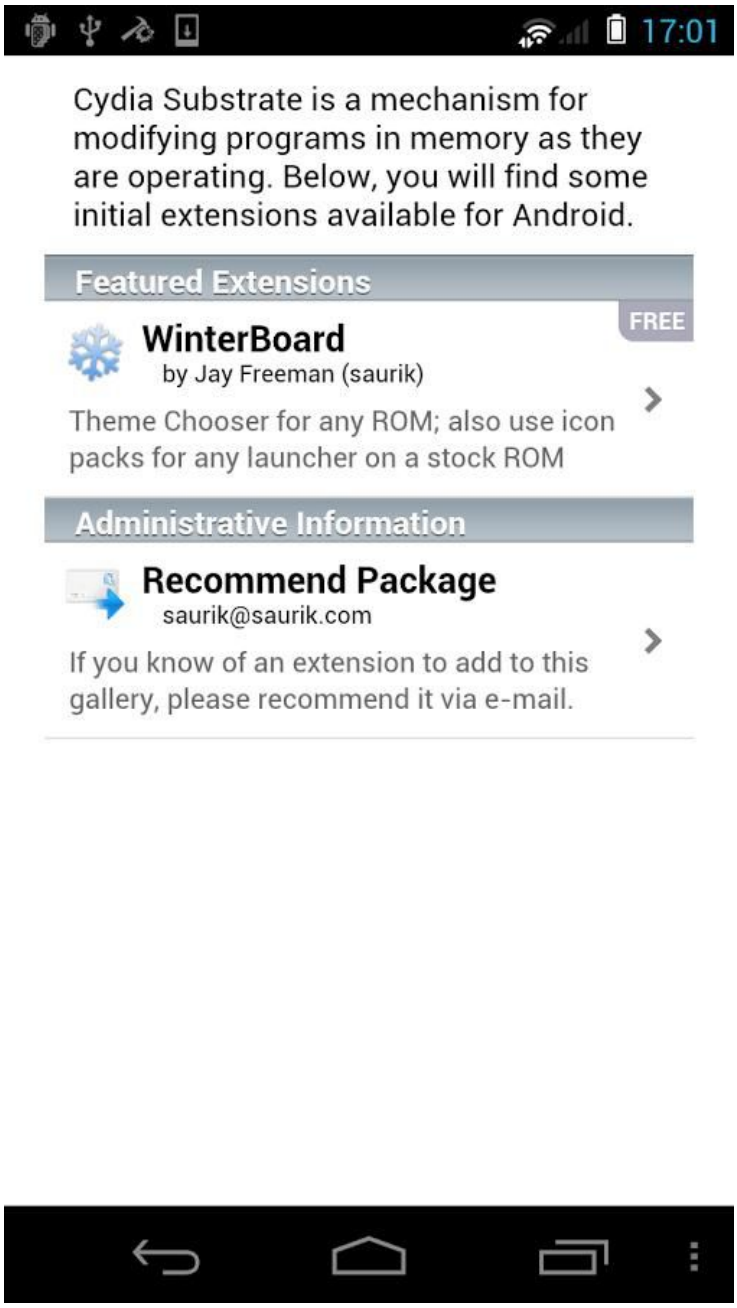
Android Rooting

Zum Rooten von Samsung-Smartphones über einen PC wird häufig das Tool Odin verwendet.



Android Rooting

Bei alternativen App Stores wie Cydia besteht die Gefahr, sich Viren einzufangen.



Android Rooting

Natürlich gibt es auch deutlich mehr Möglichkeiten und Einstellungen durch die Apps auch Stores wie Cydia.