So schützen Sie Ihr Mobilgerät vor Viren und anderen Schädlingen

Verena Ottmann, Arne Arnold

Sobald eine Android-Sicherheitslücke bekannt wird, veröffentlicht Google in der Regel ein Update, dem die anderen Hersteller kurze Zeit später folgen sollten. Doch was tun, wenn ein Hersteller nicht liefert?

Es ist der wirksamste Schutz vor Sicherheitslücken, das Betriebssystem Ihres Mobilgeräts möglichst aktuell zu halten. Falls der Hersteller Ihres Modells keine Updates mehr bereitstellt, lässt das vermuten, dass das Gerät bereits älter ist oder überhaupt schlecht mit Updates versorgt wurde und wird. Dann sollten Sie erwägen, sich ein neueres Gerät mit aktuellem Android und besserer Update-Politik anzuschaffen.

Beispielsweise ergaben unsere Recherchen, dass vor allem Geräte mit Android 4.1 bis 4.4 anfällig für Sicherheitslecks sind – und diese Betriebssystem-Versionen waren im April 2017 noch auf 30,1 Prozent aller Smartphones installiert!

Alternativ können Sie Ihrem alten Mobilgerät auch ein Custom-ROM wie Lineage OS aufspielen, um das Risiko durch Schädlinge zu reduzieren. Allerdings sollten dafür technisches Grundverständnis und eine gewisse Risikobereitschaft vorhanden sein, weil Sie hierbei in die Tiefen Ihres Systems eindringen und nicht jedes Custom- ROM den gewünschten Erfolg bringt.

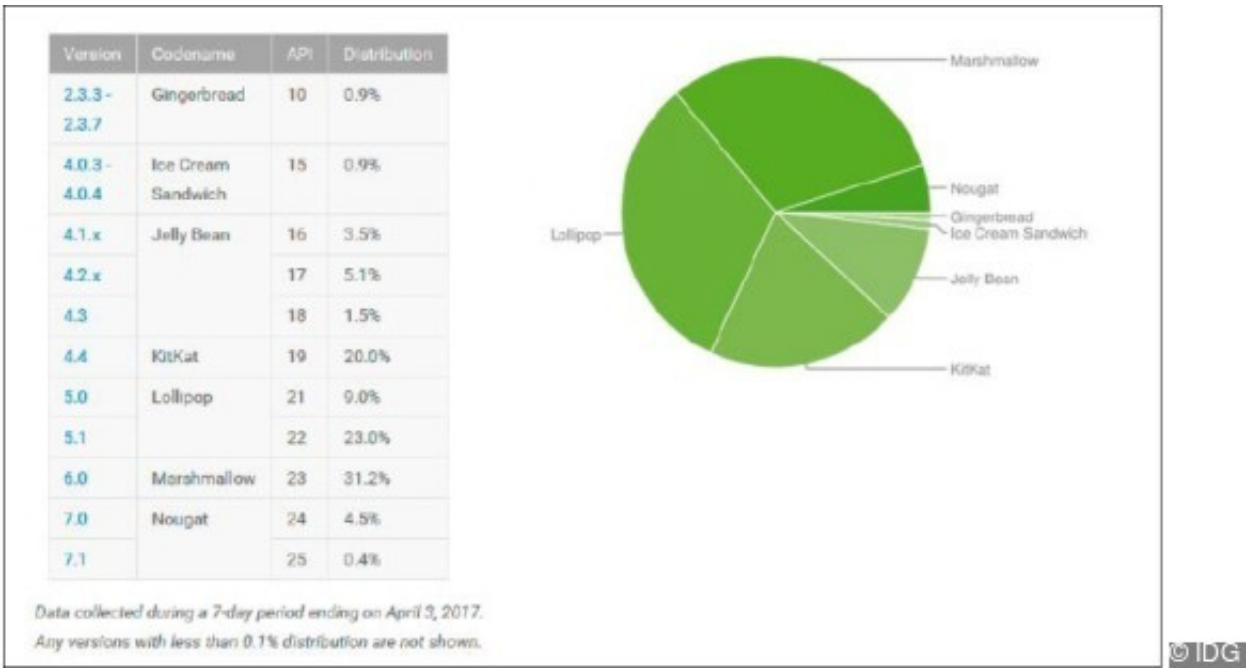
Im Folgenden geben wir Ihnen noch weitere Tipps, wie Sie das Sicherheitsrisiko für Ihr Mobilgerät möglichst gering halten können.

Übrigens: Hat sich beispielsweise ein Erpresservirus auf Ihrem Smartphone breitgemacht, sollten Sie vorsichtshalber die Log-in-Passwörter zu allen Ihren Diensten ändern, angefangen bei Bezahldiensten wie Paypal über Ihr

Mailkonto bis hin zu Shopping-Sites wie Ebay und Amazon.

LineageOS 14.1: Download, Installation, Funktionen - so geht's

Die Goldenen Regeln gegen Malware



Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	0.9%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.9%
4.1.x	Jelly Bean	16	3.5%
4.2.x		17	5.1%
4.3		18	1.5%
4.4	KitKat	19	20.0%
5.0	Lollipop	21	9.0%
5.1		22	23.0%
6.0	Marshmallow	23	31.2%
7.0	Nougat	24	4.5%
7.1		25	0.4%

Data collected during a 7-day period ending on April 3, 2017.
Any versions with less than 0.1% distribution are not shown.

IDG

Vergrößern **Das größte Sicherheitsrisiko ist eine veraltete Android-Version. Im April 2017 liefen noch 30,1 Prozent aller Mobilgeräte mit Android 4.1 bis 4.4.**

Die meisten schädlichen Apps stammen nicht aus dem offiziellen Google Play Store. Man hat sie also sehr wahrscheinlich aus anderen Quellen – etwa über einen Link oder Mailanhang – als APK-Datei aufs Smartphone geladen und installiert. Die Schädlinge stecken oft in beliebten Programmen wie Spielen, Videoplayern, Messengern oder Antiviren-Apps. Von außen ist den Anwendungen dabei nicht anzusehen, dass ihr Code korrumpiert wurde. Erst nach der Installation zeigen sie dann ihr wahres Gesicht. Um dem entgegenzuwirken, sollten Sie sich an einige grundsätzliche Regeln halten:

1. Laden Sie nur im Ausnahmefall Apps aus anderen App-Stores als dem Google Play Store herunter. Deaktivieren Sie am besten die entsprechende Option in den Einstellungen unter „Sicherheit –> Unbekannte Quellen“. So gelangen keine Apps aus Drittanbieter-Stores mit ungewolltem Gepäck auf

Ihr Mobilgerät.

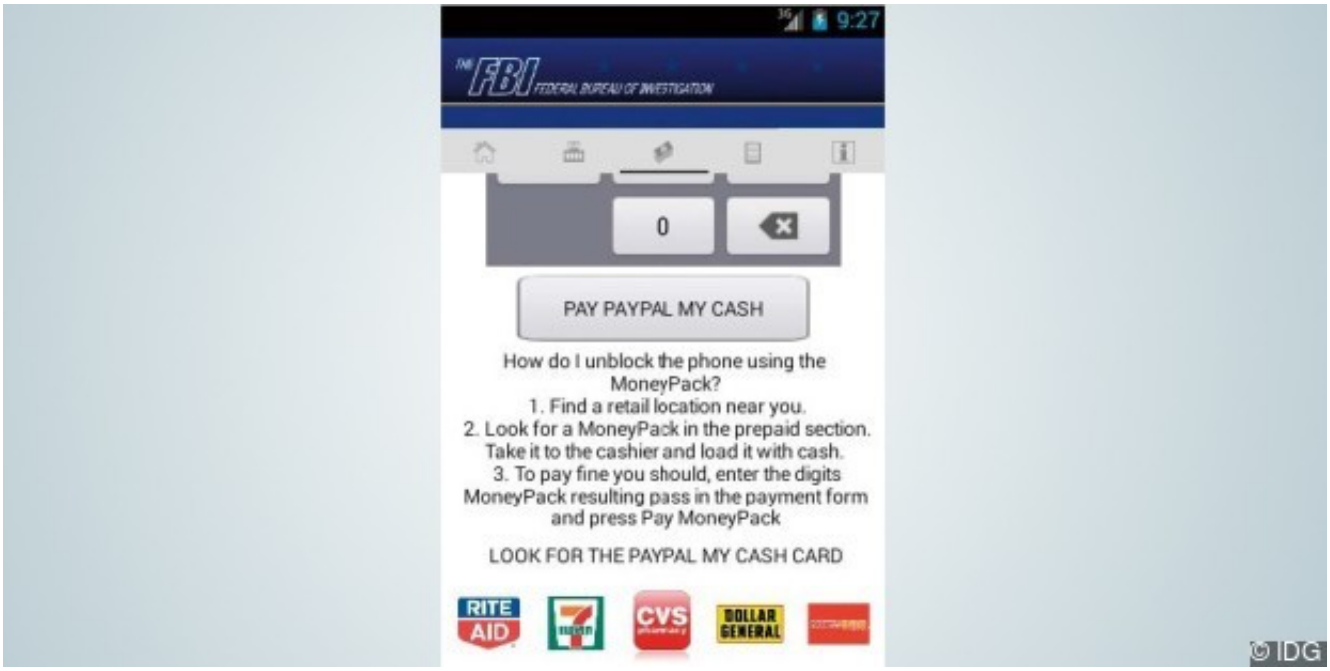
2. Zeigen Sie ein gesundes Misstrauen gegenüber APK-Dateien. Es wird schon seinen Grund haben, dass die dazugehörige App (noch) nicht offiziell erhältlich ist. Beispielsweise hatten Hacker vor dem offiziellen Release von Pokémon Go virenverseuchte APK-Dateien des Spiels in Umlauf gebracht.

3. Klicken Sie nicht unbedacht auf Links in Mails, deren Absender Sie nicht kennen. Eventuell steckt ein Download dahinter, der automatisch startet und Ihnen eine korrumpierte App aufs Smartphone lädt. Was für Mails am PC gilt, gilt auch für Mails auf dem Mobilgerät!

4. Glauben Sie keinen Angeboten, die zu gut erscheinen, um wahr zu sein. Viele Schädlinge sind etwa in Porno-Playern versteckt. Aber: Niemand schenkt Ihnen etwas im Internet, vor allem keine Porno-Angebote! Im Zweifelsfall bezahlen Sie die angeblichen Gratisinhalte mit Ihren Daten oder gar dem Zugriff auf Ihr Smartphone.

Relevant: Android-Sicherheitslücken - So schützen Sie sich

Sicherheitssuite schützt Ihr Mobilgerät



Vergrößern **Wer unbedacht APK-Dateien aus dubiosen Quellen herunterlädt und auf seinem Mobilgerät installiert, kann sich leicht einen Erpresservirus oder Ähnliches einfangen.**

Können Sie sich der APK-Dateien aus dubiosen Quellen noch durch besonnenes Verhalten erwehren, hilft Ihnen eine Antiviren-App von Avira, AVG, Symantec und anderen dabei, auch Angebote aus dem offiziellen Google Play Store vor dem Download zu überprüfen. Aber nicht nur das: Die Apps scannen das Android-Dateisystem auf bekannte Malware und lassen meist einen Echtzeitscanner im Hintergrund laufen, der neue Dateien durchleuchtet und gegebenenfalls löscht.

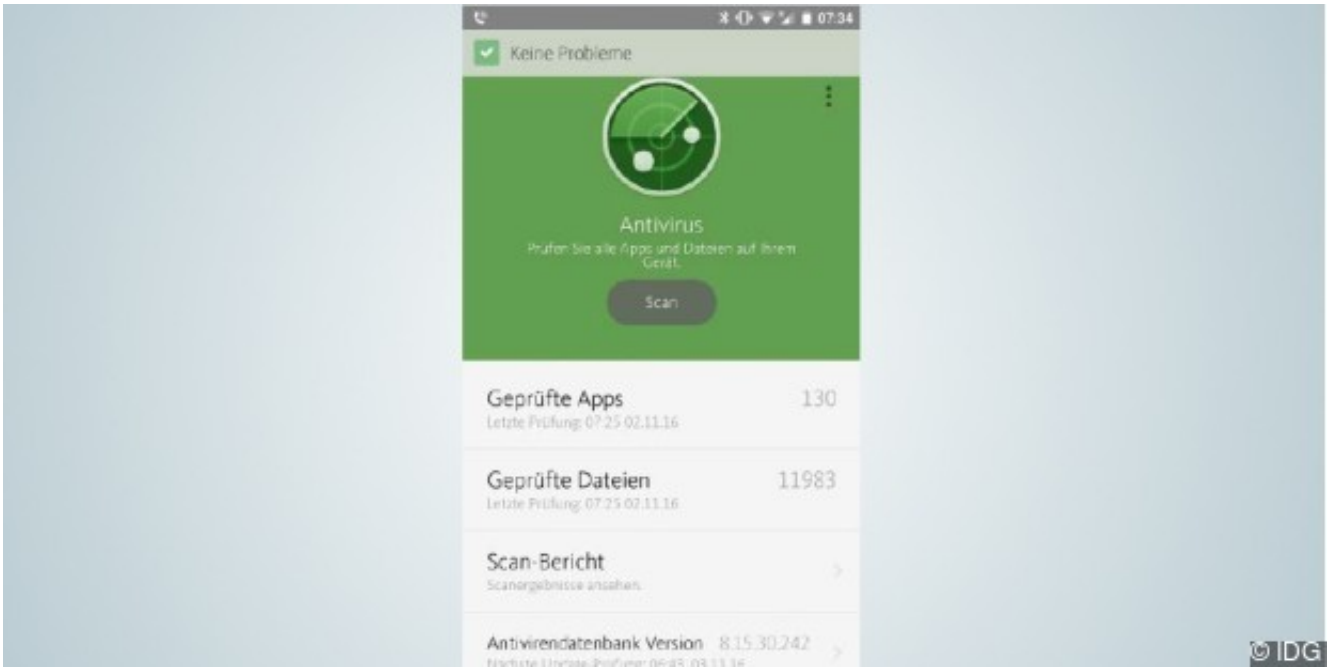
Darüber hinaus existieren im Internet zahlreiche Websites, die entweder versuchen, unbemerkt Malware zu installieren, oder die über gefälschte Formulare Ihre Log-in-Daten ergaunern wollen. Für dieses Angriffsmuster bieten Ihnen mobile Sicherheitslösungen die Funktion „Safe Browsing“. Dabei arbeitet ein Echtzeitscanner im Hintergrund, der Ihre Aktionen im Internet überwacht. Wenn Sie versuchen, auf eine verdächtige Webseite zuzugreifen, erhalten Sie eine Warnmeldung, und das Laden der Webseite wird unterbrochen.

Ein wenig anders gehen die Sicherheitssuiten bei der Analyse der installierten Apps vor. An dieser Stelle dient als Referenz eine zentrale

Datenbank, die von den Herstellern gepflegt wird. Nach der Installation der Sicherheits-App wird ein Scan all Ihrer installierten Apps gemacht. Die Liste wird an eine Datenbank in der Cloud übergeben und geprüft, ob sich unter den Apps verdächtige Anwendungen finden. Falls ja, erhalten Sie eine Aufforderung zum Entfernen. Viele Lösungen bieten auch einen Hinweis auf kritische oder zu viele Berechtigungen. Damit Ihr Smartphone oder Tablet den sicheren Zustand beibehält, wird jede weitere App vor der Installation untersucht und nur installiert, wenn es sich nicht um Malware handelt.

Neben diesen klassischen Sicherheitsfunktionen haben die Anbieter die Lösungen um weitere Funktionen ergänzt – dies geht vom „Task Killer" über das Verwalten von App-Berechtigungen bis hin zur Sperrung des Endgeräts beim SIM-Kartenwechsel.

Smartphone-Backup erstellen



Vergrößern **Die Sicherheits-Apps – hier die Lösung von Avira – scannen das mobile Endgerät auf verdächtige Dateien und Anwendungen.**

Um gegen jede Art von Schädling gerüstet zu sein, sollten Sie die Daten Ihres Mobilgeräts regelmäßig sichern. Dann können Sie Ihr Smartphone oder Tablet jederzeit ohne Bedenken zurücksetzen, da Sie ja das Backup haben. Legen Sie die Sicherungsdatei Ihrer Smartphone-Daten aber

unbedingt auf dem PC oder in der Cloud ab. Eine Sicherung auf dem Mobilgerät selbst bringt Ihnen bei Virenbefall gar nichts!
Backup über den PC: Möchten Sie das Backup über den PC erstellen, können Sie dazu die Software verwenden, die der Hersteller Ihres Geräts dafür anbietet, etwa Samsung Smart Switch oder LG Backup. Besser sind jedoch Drittanbieter-Programme wie der „ My Phone Explorer “. Das Tool erstellt Backups von Handydaten sowie von Apps und Einstellungen.

So geht's: Verbinden Sie Ihr Mobilgerät per USB, Bluetooth oder WLAN mit dem PC. Entscheiden Sie sich für USB, muss Ihr Smartphone beim Anschließen im Modus „Nur laden" stehen und USB-Debugging aktiviert haben. Steht die Verbindung, können Sie über „Datei –> Einstellungen –> Multi-Sync" auswählen, was Sie alles sichern möchten. Aber: Ein komplettes Image-Backup des Handys lässt sich mit dem My Phone Explorer nicht anlegen.

Backup in der Cloud: Bevorzugen Sie ein Backup in der Cloud, ist dies beispielsweise mit Dropbox möglich. Mithilfe der App „ Autosync Dropbox – Dropsync “ wählen Sie einen lokalen Ordner und einen Ordner in der Dropbox aus und aktivieren die Synchronisierung per Haken. Die übrige Konfiguration nehmen Sie in den Einstellungen vor. Besonders komfortabel ist die Option „Instant Upload". Sobald in einem überwachten Ordner eine neue Datei auftaucht, wird diese sofort in die Dropbox geladen. Sollen mehr als ein Verzeichnis oder Dateien größer als 10 MB synchronisiert werden, ist jedoch ein Upgrade auf die Proversion der App erforderlich.

Die Backup-App „ iDrive “ bietet ebenfalls eine Möglichkeit an, um alle auf einem Android-Gerät befindlichen Daten in der Cloud zu sichern. Dabei werden die Daten auf Wunsch auch verschlüsselt und mit einem Passwort geschützt.

Und auch Google selbst bietet diverse Backup-Möglichkeiten, die Sie im Menü „Sichern & zurücksetzen" finden.