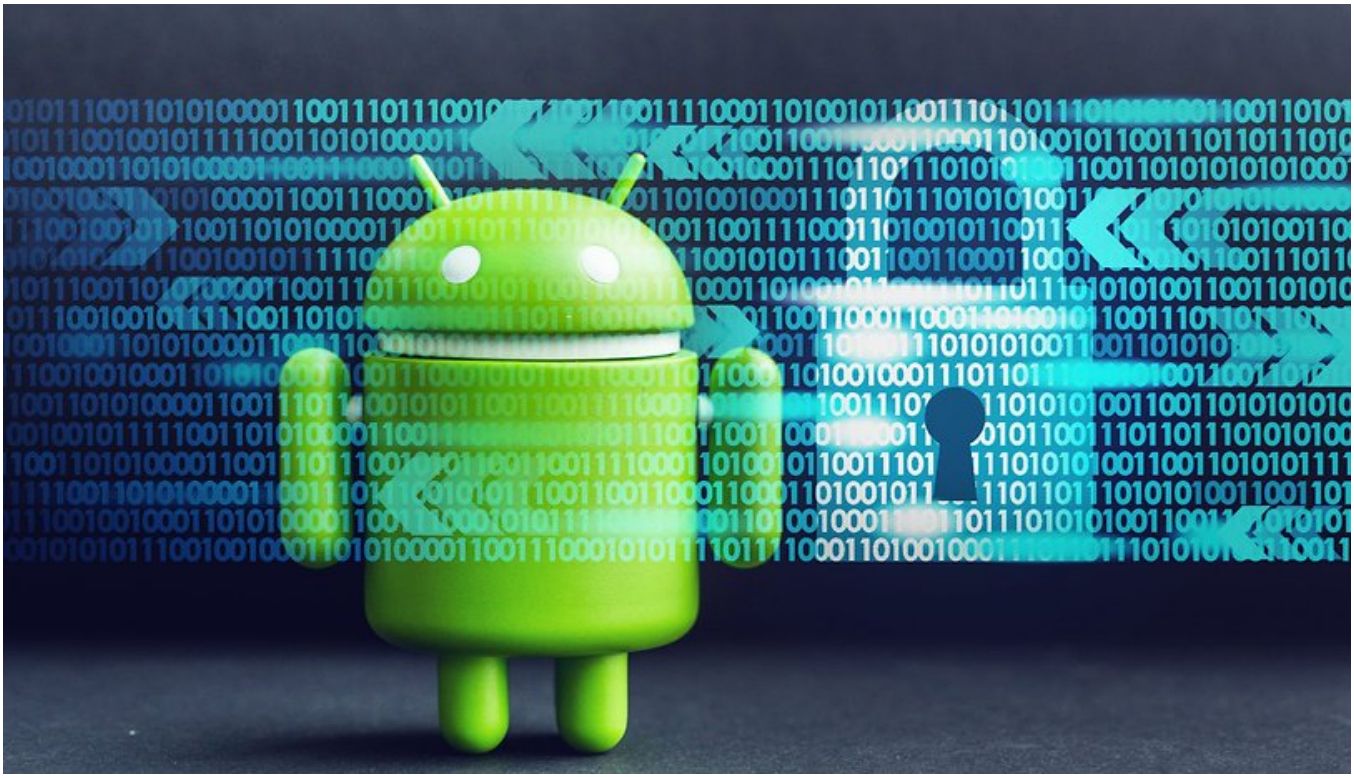
Schutz vor Android-Malware: Diese Gegenmittel helfen wirklich

Update: Infos aktualisiert



Alle paar Monate gibt es eine Sicherheitslücke bei Android, die angeblich hunderte Millionen Android-Smartphones betrifft. In den vergangenen Jahren zum Beispiel Quadrooter und Stagefright. Die Sicherheitslücken unterscheiden sich aber erheblich. Wie sicher ist Android mit seinen Hausmitteln und was hilft wirklich gegen die Gefahren aus dem Internet?

Bei Quadrooter handelte es sich um mehrere Sicherheitslücken in Qualcomm-Treibern, die im Sommerloch 2016 für Furore sorgten. 900 Millionen betroffene Android-Geräte. Gefahr! Gefahr! So stellten es zumindest die Entdecker dar. Um die Sicherheitslücke Quadrooter auszunutzen, muss es dem Angreifer jedoch gelingen, auf einem Smartphone eine entsprechend konstruierte App zu installieren und auszuführen.

Ganz anders gelagert ist die Schwachstelle Stagefright. Diese war in den

Funktionen zur Verarbeitung von Mediendateien bzw. -streams versteckt. Das Problem: Selbst ein Video einer MMS wurde durch diese Routinen geschleift. Ein Angreifer konnte also dem User eine Datei schicken und der gefährliche Code wurde ausgeführt. Ab Android 4.0 ist es aufgrund systeminterner Maßnahmen schwieriger, die Sicherheitslücke erfolgreich auszunutzen, aber es ist nicht unmöglich.

Der Unterschied zwischen den beiden Sicherheitslücken ist offensichtlich: Quadrooter erfordert einige Schritte seitens des Users, während Stagefright aus der Ferne und ohne User-Interaktion auszunutzen ist.

Welche Bordmittel gibt es gegen Sicherheitslücken à la Stagefright, Quadrooter & Co.?

Android besitzt mehrere Wege, um die Sicherheit der User zu gewährleisten. Die drei wichtigsten Maßnahmen stellen wir Euch hier im Detail vor.

Gegenmittel Eins: Installation unbekannter Apps verhindern

In den Systemeinstellungen von Android gibt es die Einstellung um Installationen von Apps unbekannter Herkunft zuzulassen. Im Auslieferungszustand ist diese Option deaktiviert, sodass Ihr nur Apps aus dem Play Store installieren könnt. Manche Hersteller haben einen eigenen App-Store vorinstalliert, beispielsweise Samsung und Huawei. Für diese gilt die Beschränkung der Option nicht.

Diese Option schützt also mit einer simplen Maßnahme gegen Malware, die über einen nicht zuverlässigen App-Store oder schlicht Internetseiten verteilt werden - konkret also gegen den Hauptangriffsvektor von Malware. Denn aus dem Play Store fliegen solche Apps sehr schnell raus, und Nachrichten über Malware im Play Store sind selten geworden. Unbekannte Quellen müssen aber für App-Stores von Amazon oder auch für Alternativen wie F-Droid aktiviert sein. Was also tun?

Gegenmittel Zwei: Apps mit Googles Virenscanner überprüfen

Google hat eine zweite Schutzlinie gezogen, die keine Kompatibilitätsprobleme hat, dafür aber die Sicherheit vor schadhaften Apps bietet: Apps überprüfen. Ab Android 4.2 ist diese Einstellung vorhanden und mittlerweile als Google Play Protect Bestandteil der Google-Play-Services. Standardmäßig ist diese auch aktiviert und das solltet Ihr auch so belassen. Mit dieser Einstellung erlaubt Ihr, dass Apps vor der Installation auf mögliche Malware-Funktionen überprüft werden. Ist dies der Fall, verweigert Android die Installation. So zumindest die Theorie.

Quadrooter hatte damit übrigens keine Chance. Google bestätigte gegenüber AndroidCentral schon wenige Tage nach der Entdeckung, dass eine Malware, die auf Quadrooter setzt, nicht installiert werden könne - sofern die entsprechende Einstellung gesetzt ist. Androids Sicherheitschef Adrian Ludwig wiederum äußerte sich ganz ähnlich zur Malware Gooligan, einer im Dezember 2016 bekannt gewordenen Malware, die Google-Konten angreift. Was steckt hinter diesen Entwarnungen?

Mehr Videos zu aktuellen Technik-Themen findest Du auf unserer Video-Seite.

Im Android Security Report war bereits 2016 zu lesen, dass mit dieser Technik die Bedrohungslage für Android-User signifikant reduziert werden konnte. Vor allem Malware-Apps konnte Google mit dem Feature den Nährboden entziehen.

Und diese Maßnahme ist seit den ersten Versionen mehrfach verbessert worden. Grundsätzlich funktioniert die App-Überprüfung, indem der Fingerabdruck (Hashwert) einer APK berechnet wird. Dieser wird mit Googles Datenbank abgeglichen, die mögliche Gefahren enthält. Google scannt nicht nur Apps im Play Store, sondern auch APKs, die über das Web zugänglich sind. Dieser simple Weg ist schon recht effektiv, denn rund 90 Prozent aller außerhalb des Play Stores installierten Apps sind Google bereits bekannt und auf mögliche Sicherheitsprobleme gescannt worden.

Ich vertraue Googles Maßnahmen und halte Android für sicher.

Zusätzlich ist es Google möglich, aus Apps einzelne Features zu extrahieren und diese einem ganz ähnlichem Verfahren zu unterziehen. Damit kann Google gefährliche Features erkennen und den User bei Bedarf warnen und sogar die Installation einer solchen App verhindern. Inzwischen scannt Google sogar im Laufe des Betriebs die installierten Apps und kann somit auch vor nachträglichen Manipulationen an einer installierten App warnen. Im Extremfall gibt es sogar die Möglichkeit, Apps vom Smartphone zu entfernen, auch dann, wenn sich diese als Geräteadministrator eingenistet haben.

Vor den allerneuesten Malware-Attacken kann Google mit der App-Überprüfung allerdings nicht schützen. Doch spätestens nach wenigen Stunden, höchstens Tagen dürften beinahe alle Android-User vor der Installation von Malware-Apps geschützt sein - wie im Fall Quadrooter. Im Play Store kommen übrigens ähnliche Maßnahmen zum Einsatz. Außerdem analysiert Google das Verhalten der dort registrierten Entwickler und kann unlautere Absichten von App-Entwicklern unterbinden.

Von diesen Informationen beruhigt, wagte ich die Probe aufs Exempel. Warum nicht einmal versuchen, diesen Schutz zu prüfen? Also aktiviere ich die unbekannten Quellen, installiere (als Gegenprobe) mehrere Virenscanner aus dem Play Store und begebe ich mich (recht einfallslos) auf die Suche nach Super Mario Run für Android - viele Downloads sollen ja voll mit Malware sein. Das Resultat? Die Installation klappt problemlos, mehrere Virenscanner warnen vor einer Bedrohung bzw. Gefahr. Beim genauen Hinsehen habe ich mir offenbar eine Adware eingefangen, die "unerwünschtes Verhalten" an den Tag legen kann. Offenbar handelt es sich aber nicht um eine ausgefuchste Malware mit Gefahren für meine Daten oder Handyrechnung. Eine Warnung seitens Google erhalte ich nicht.

Mein kleines Experiment zeigt: Googles App-Überprüfung lässt durchaus dubiose Apps durch. Unklar ist, ob es sich hierbei um eine bewusste Entscheidung handelt: Denkbar ist, dass Google bestimmte Formen von Adware nicht als Gefahr einstuft, sondern konkrete, gefährliche Funktionen

in Apps finden will, bevor der Alarm losgeht.

Google hat Android nur einen Basisschutz vor Malware verpasst.

Gegenmittel Drei: Aktuelle Sicherheitspatches

Doch Android basiert auf Linux und so gibt es noch eine dritte Schutzschicht für User: Denn der sicherste Schutz ist immer noch ein aktuelles und vollständig gepatchtes Betriebssystem. Die tatsächlich extrem gefährliche Sicherheitslücke Stagefright hat bei Google zu einem Umdenken geführt: Seither gibt es die monatlichen Sicherheitsupdates für Android. Inzwischen sind 18 dieser Patchsammlungen erschienen. Zum Verständnis muss man wissen, dass Google diese Patches nicht nur für die aktuellste Android-Version bereitstellt, sondern die Patches (soweit erforderlich) auch für ältere Android-Versionen bis Android 4.4 veröffentlicht. Daher kann es also sein, dass ein Smartphone mit Android Oreo temporär auf einem sichereren Stand ist als eines mit Pie. Relevant für die Einschätzung der Sicherheit ist der Stand der Sicherheitspatches.

Bei der Debatte um Updates für Android muss es heute nicht nur um Android-Versionen, sondern auch um die Sicherheitspatches gehen.

Allgemeines Gegenmittel: Eigenverantwortung ist unersetzlich

Eine vielleicht vierte Schutzmauer ist natürlich der User selbst: Wer all die obigen Sicherheitsmaßnahmen ausschaltet bzw. ignoriert, den APK-Download aus einer SMS in gebrochenem Deutsch installiert und dann wie wild Codes an anonyme Nummern verschickt, der hat gegen alle Sicherheitsregeln verstoßen, die man sich nur ausdenken kann.

Es heißt also, vorsichtig zu agieren und nicht jede angebliche Warnung per E-Mail, SMS oder WhatsApp ernst zu nehmen: Kopf einschalten und verantwortlich handeln ist immer eine gute Idee (nicht nur bei der Smartphone-Sicherheit).

Warnungen aus dubiosen Quellen schlage ich immer aus.

Braucht es Sicherheits-Apps für Android?

Mein kleines, oben skizziertes Experiment war eindeutig. Mehrere von mir installierte Virenscanner warnen mich vor der von mir verwendeten Adware. In Googles Sicherheitsbericht ist mehrfach von potenziell gefährlichen Anwendungen die Rede, die Antiviren-Hersteller sprechen hingegen von potenziell unerwünschten Apps, was eine geringere Schwelle ist und so mehr Apps betreffen kann.

Vor dieser Adware wäre ich übrigens geschützt geblieben, hätte ich nicht die unbekannten Quellen aktiviert. Ein weiterer bedenkenswerter Aspekt ist, dass es natürlich noch weitere Gefahren für Android-User gibt. Beim Blick auf die Beschreibungen der verschiedenen Security-Suites im Play Store fällt auch auf, dass die Viren-Scanner-Funktionen nur ein kleiner Bestandteil sind. Viel nützlicher sind hier die Datenschutzfunktionen oder der Schutz vor Angriffen via Webbrowser und E-Mail. Es gibt also durchaus Argumente für einen Virenscanner.

Sicherheits-Apps sind nur in wenigen Fällen notwendig.

Empfehlenswerte Sicherheitseinstellungen im Überblick

Kurz zusammengefasst hier die Liste der empfehlenswerten Maßnahmen und Einstellungen. Zunächst zu den wichtigen Systemeinstellungen:

- *Sicherheit > Unbekannte Quellen*: Am besten nicht erlauben bzw. direkt nach einer Installation wieder verbieten
- *Google > Sicherheit > Google Play Protect*
    - *Gerät nach Sicherheitsbedrohungen durchsuchen*: Eingeschaltet lassen
    - *Erkennung schädlicher Apps verbessern*: Hilft Google, noch nicht gescannte Apps zu erkennen. Wahlweise aktivieren.

Ein Virenscanner erscheint vor allem dann empfehlenswert, wenn Ihr häufig Apps aus unbekannten Quellen verwendet. Außerdem: Installiert Sicherheitsupdates, soweit sie für Euer Smartphone erscheinen. Liefert Euer Hersteller keine Updates oder nur unzuverlässig? Oder nur sehr zögerlich? Schreibt dem Hersteller, dass er seine Update-Politik überdenken sollte.

Die Android-Bordmittel sind für mich ausreichend.

Fazit: Android ist sicher, aber nicht zu hundert Prozent

Zurück zur Ausgangsfrage: Waren von Quadrooter wirklich 900 Millionen Geräte betroffen? Theoretisch verwundbar für die Sicherheitslücke: Ja. Aber die Schutzmaßnahmen seitens Google dürften diese Zahl schnell reduziert haben. Gerade in Europa werden die meisten Smartphones mit Google-Diensten verkauft, sodass vor allem asiatische Smartphones ohne Google-Addons übrig bleiben. Und wer keine Apps aus unbekannten Quellen zulässt, war eh aus dem Schneider (und somit eigentlich nicht für die Sicherheitslücke anfällig).

Dies bedeutet aber auch: Quadrooter bedrohte bei weitem nicht hunderte Millionen Smartphones, sondern eine weit geringere Anzahl an Usern. Fraglich ist natürlich, ob die App-Überprüfung alle Quadrooter-Exploits wirklich abfangen kann. Dies müsste ein umfangreicherer Test mit entsprechend präparierten Apps zeigen. Ich bin aber gewillt Googles Entwarnung für belastbar zu halten: Die dahingehenden Äußerungen Googles sind sehr konkret und deutlich.

Stagefright hingegen ist nur mit einem Sicherheitspatch zu stopfen. Hier waren also tatsächlich die meisten Smartphones verwundbar, sodass zeitweise die Netzbetreiber die MMS-Zustellung deaktivierten. Google wiederum empfiehlt Messenger-Apps, Mediendaten nicht automatisch zu verarbeiten. Das perfide an Stagefright: Wer eine alte Android-Version ohne die Anzeige eines Sicherheitspatchlevels hat, ist noch immer von der Sicherheitslücke betroffen. Stand heute sprechen wir vor allem von Usern, die Android 4.3 und älter einsetzen, aber auch Kitkat- und Lollipop-

Smartphones sind wahrscheinlich noch immer verwundbar.

Google hat aus Stagefright gelernt und mit den monatlichen Sicherheitspatches den richtigen Weg eingeschlagen. Die Verbreitung der Updates muss allerdings immer noch weiter verbessert werden. Hier sind vor allem die Hersteller gefragt, die Updates auch an die User zu verteilen.

- Die harte Realität: Darum wird Android nie sicher sein
- Tipps zur Sicherheit und zum Datenschutz auf Android-Smartphones

Die Informationen in diesem Artikel wurden im August 2019 auf den neuesten Stand gebracht. Ältere Kommentare wurden nicht gelöscht.

Dir gefällt, was Du hier liest? Dann abonniere unseren Telegram-Kanal: AndroidPIT News 📲!