



einfache Schritte
zum Schutz Ihrer
Android-basierten
Smartphones

x2



Die *Android* Open-Source-Plattform von Google holt mit rasenden Schritten die Betriebssysteme *iOS* von Apple und *BlackBerry OS* von RIM ein und gewinnt eigene treue Anhänger. Nach lediglich 6,8 Millionen verkauften Exemplaren im Jahr 2009 erreichte die Verkaufszahl der *Android*-basierten Smartphones gegen Ende des Jahres 2010 bereits die kolossale Summe von 67 Millionen verkauften Exemplaren weltweit.

Diese wachsenden Verkaufszahlen zeigen deutlich, dass das „Zeitalter des *Android-Betriebssystems*“ heranbricht. Die Verbraucher wünschen sich zunehmend Smartphones, die nicht nur über grundlegende Kommunikations- und Messaging-Funktionen verfügen, sondern darüber hinaus auch technologisch fortschrittliche Funktionalitäten bieten. Ganz gleich, ob für geschäftliche oder private Zwecke - Apps für *Android*-basierte Smartphones lassen diesen Wunsch wahr werden.

** Der Android-Roboter in diesem E-Book wurde gemäß den Bedingungen der Creative Commons Attribution Lizenz von Google zur Verfügung gestellt.*

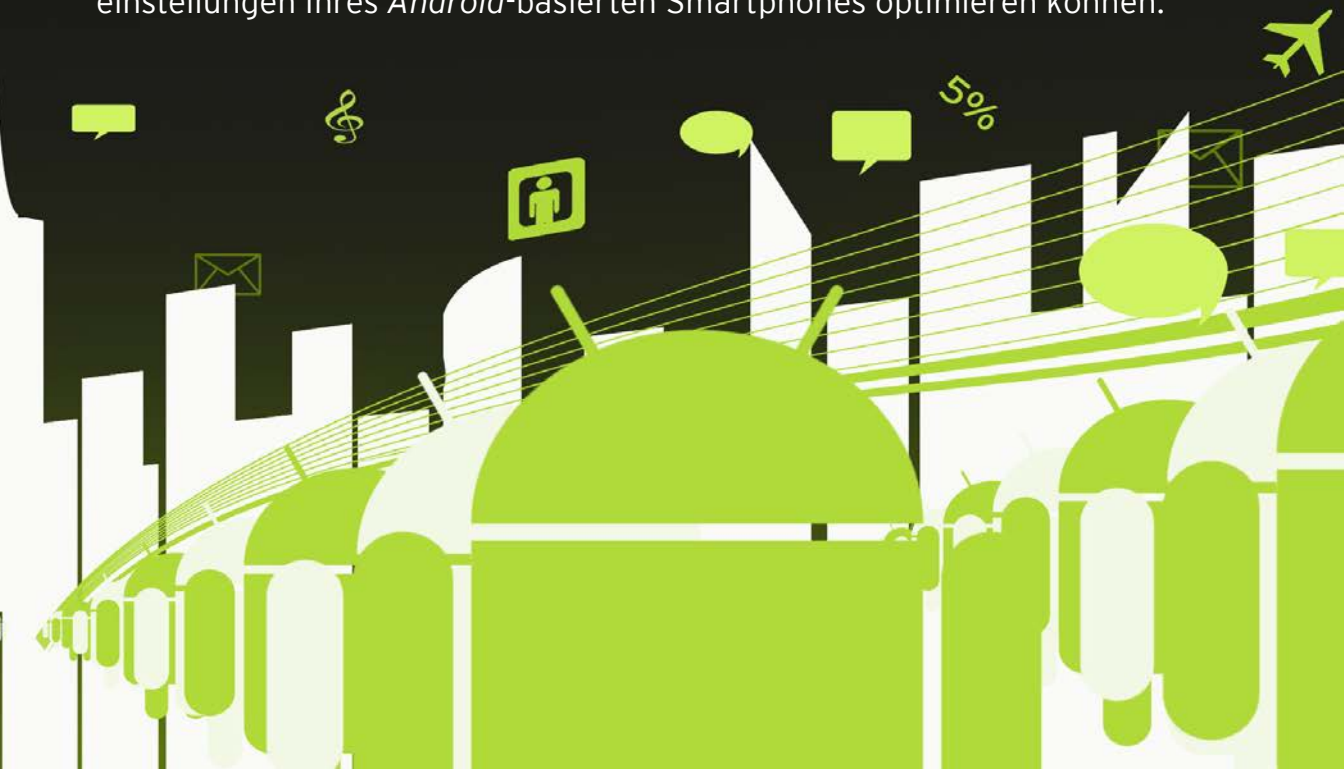




Zu den interessantesten Funktionen des *Android-Betriebssystems* gehört die Möglichkeit für Entwickler, eigene innovative und vielseitige Apps zu erstellen. Derzeit sind auf dem *Android Market* über 130.000 Apps für Anwender in 48 verschiedenen Ländern verfügbar. Die meisten dieser Apps können kostenfrei heruntergeladen werden. Dies birgt allerdings leider auch Gefahren für Anwender, die alle möglichen Arten von Apps herunterladen und testen. Mittlerweile verwenden viele Cyber-Kriminelle diese Apps, um sie für ihre eigenen Ziele mit Hilfe von Trojanern zu manipulieren.

Die Tatsache, dass *Android-Apps* auch von anderen Anbietern sowie auf den eigenen Websites der Entwickler angeboten werden, erhöht das Sicherheitsrisiko noch mehr, da auch diese Entwicklung von Cyber-Kriminellen nicht unbeobachtet blieb.

Aufgrund der vielen wertvollen Daten auf Ihrem Smartphone sollten Sie versuchen, Ihr Smartphone so gut wie möglich vor Bedrohungen zu schützen. Im Folgenden erhalten Sie einige Tipps, wie Sie die Sicherheitseinstellungen Ihres *Android*-basierten Smartphones optimieren können.



1 Verwenden Sie die integrierten Sicherheitsfunktionen Ihres *Android*-basierten Smartphones.

Sie können Ihr Smartphone möglichst effektiv schützen, indem Sie die Standort- und Sicherheitseinstellungen korrekt konfigurieren. Diese Konfiguration erfolgt unter *Einstellungen / Standort & Sicherheit*.

Außerdem ist es sinnvoll, die Pattern-, PIN- (numerisch) oder Kennwortfunktion Ihres Smartphones zu nutzen. Auch wenn die Eingabe eines Kennworts zum Aufheben des Ruhezustands zeitaufwändig erscheinen mag, trägt diese Funktion in beträchtlichem Maße zum Schutz Ihrer Daten bei, falls Ihr Smartphone einmal verloren geht.

Sollte Ihnen dieser Schutz noch nicht reichen, steht außerdem die Funktion zum Entsperren durch Fingerabdruck zur Verfügung. Dies ist wahrscheinlich die sicherste Methode, da hierdurch gewährleistet wird, dass die auf Ihrem Smartphone gespeicherten Daten ausschließlich Ihnen zugänglich sind.

Bedenken Sie stets, dass die Verwendung jeder einzelnen der oben beschriebenen Sicherheitsoptionen besser ist, als gar keine Sicherheitsvorkehrungen zu treffen. Kennwörter werden schließlich aus gutem Grund erstellt: Sie hindern Cyber-Kriminelle daran, auf Ihre Daten zuzugreifen.



2

Deaktivieren Sie die Option zur automatischen Herstellung Ihrer Wi-Fi-Verbindung.

Zusätzlich zur korrekten Konfiguration der Standort- und Sicherheitseinstellungen Ihres *Android*-basierten Smartphones kann es sinnvoll sein, die automatische Wireless-Verbindung (trotz der hiermit verbundenen Vorteile und Annehmlichkeiten) zu deaktivieren.

Die Verwendung eines kostenfreien drahtlosen Internet-Zugangs ist aus verschiedenen Gründen risikoreich. Die Verbindung mit einem offenen Netzwerk mag einfach, kostenfrei und bequem sein – sie birgt jedoch auch gewisse Risiken. Der automatische Zugriff auf offene drahtlose Netzwerke bietet praktisch jeder beliebigen Person Einlass. Die auf Ihrem Smartphone gespeicherten Daten sind über den Wireless-Router oder den Zugriffspunkt frei zugänglich. Jede Person, die sich im selben Netzwerk befindet, hat damit Einblick in Daten, die Sie möglicherweise geheim halten möchten.

Dieselben Bedrohungen, mit denen PC-Nutzer konfrontiert werden, plagen mitunter auch Nutzer *Android*-basierter Smartphones. Dies gilt für die Risiken, die die automatische Verbindung mit drahtlosen Netzwerken mit sich bringt, insbesondere mit unzureichend geschützten Netzwerken. Die Deaktivierung der automatischen Wireless-Verbindung trägt somit ebenfalls zur Abwehr mobiler Bedrohungen bei.

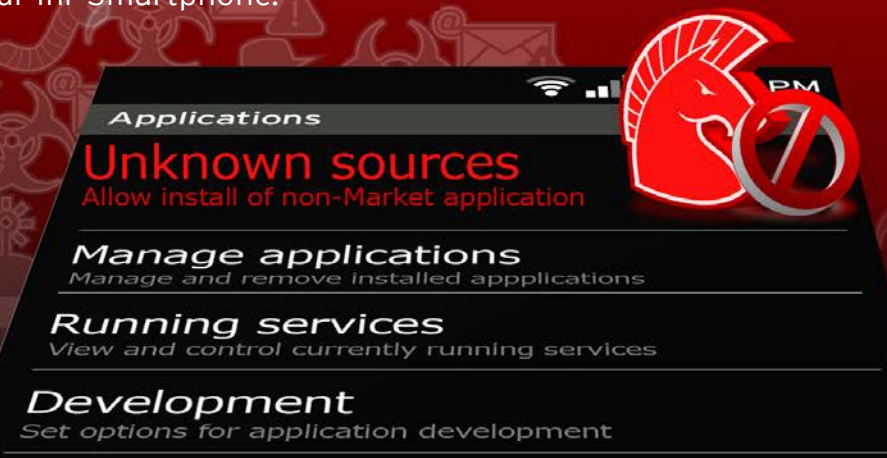


3

Ziehen Sie in Erwägung, den Download von Apps zu sperren, die nicht über den *Android Market* vertrieben werden.

Der erste *Android*-Trojaner tarnte sich als *Windows Media Player* App. Kurz darauf wurde der nächste *Android*-Trojaner in App-Stores bestimmter anderer Anbieter aus China gefunden. Obwohl wir selbst für Apps, die über den *Android Market* vertrieben werden, keine Sicherheit garantieren können, ist dieser als offizieller App-Store dennoch vertrauenswürdiger als andere.

Vor diesem Hintergrund empfehlen wir dringend, die Installation von Apps, die nicht vom *Android Market* stammen, durch Aktivierung der entsprechenden Option zu sperren. Dies bietet eine zusätzliche Schutzschicht für Ihr Smartphone.



4 Stimmen Sie Berechtigungen nur zu, wenn Ihnen dies sinnvoll und notwendig erscheint.

Die Analyse bössartiger *Android*-Apps hat ergeben, dass diese häufig zunächst eine Zugriffsberechtigung für verschiedenste Daten auf Ihrem Smartphone anfordern. Ein Beispiel hierfür ist die vor Kurzem entdeckte trojanisierte Version des *Android Market Security Tool*. Diese forderte die Berechtigung an, Textnachrichten an Nummern mit hohen Verbindungsgebühren zu senden, um den aktuellen Standort von Nutzern zu ermitteln, gespeicherte Textnachrichten anzuzeigen oder Systemeinstellungen zu ändern. Die Erteilung der Berechtigung ermöglicht es dieser App als Backdoor-Programm zu agieren. Sie erfasst und sendet Gerätedaten an einen externen Link. Darüber hinaus führt sie ohne Ihre Genehmigung weitere Funktionen aus, wie z. B. die Änderung von Anrufprotokollen, die Überwachung und/oder das Abfangen von Textnachrichten oder das Herunterladen von Videos.

Seien Sie also vorsichtig, wenn Sie die Anforderung von persönlichen Daten und/oder Gerätedaten akzeptieren oder anderen Aktionen zustimmen, die für die Ausführung bestimmter Apps gar nicht notwendig sind. Denken Sie immer zunächst über den Zweck und die Funktion einer App nach. Handelt es sich beispielsweise nicht um eine Telefonbuchanwendung, benötigt sie auch keinen Zugriff auf Ihre Kontaktliste.



5 Ziehen Sie die Anschaffung einer wirksamen App zum Schutz mobiler Geräte in Betracht.

Vorsicht beim Herunterladen und Installieren von Apps reicht nicht immer aus. Cyber-Kriminelle sind unermüdlich und denken sich ständig neue und einfallsreiche Möglichkeiten aus, um Ihnen vertrauliche Daten zu entlocken. Die Verwendung einer wirksamen Sicherheitslösung bietet daher nach wie vor den besten Schutz.

Lösungen wie *Trend Micro™ Mobile Security for Android™* bieten Ihnen jederzeit und überall zuverlässigen Schutz. Diese Lösung schützt Ihre gespeicherten Dateien sowie die Banking-Transaktionen, die Sie über Ihr *Android*-basiertes Smartphone durchführen. Sie erkennt und stoppt Malware, bevor diese Ihr Mobiltelefon erreicht - Sie können also völlig sorgenfrei arbeiten. Diese umfassende Sicherheitslösung nutzt die E-Mail- und Web-Reputation-Technologien von Trend Micro, um Ihr Smartphone wirksam vor den neuesten mobilen Bedrohungen zu schützen.



Sie möchten mehr über die neuesten Bedrohungen erfahren, die *Android*-basierte mobile Geräte, einschließlich Smartphones, gefährden? Dann lesen Sie die von uns veröffentlichten Materialien zu diesem Thema:



21:00 Uhr

TrendLabs Malware-Blog:

- [Trojanisierte Version eines Sicherheitstools als Backdoor-App \(engl.\)](#)
- [Trojanisierte App rootet *Android*-Geräte \(engl.\)](#)
- [RSA 2011: Mobile Sicherheit in der heutigen Bedrohungslandschaft \(engl.\)](#)
- [Die Konsumerisierung mobiler IT: Risiken und Vorteile \(engl.\)](#)
- [*Android*-Malware wird über App-Stores anderer Anbieter verbreitet \(engl.\)](#)
- [Bösartige *Android*-App spioniert Standort von Anwendern aus \(engl.\)](#)
- [Der erste *Android*-Trojaner schlägt zu \(engl.\)](#)

TrendWatch

- **Security Spotlight:** [Mobile Landschaft: Sicherheitsrisiken und Möglichkeiten \(engl.\)](#)
- **Security Spotlight:** [Mobiltelefone entwickeln sich zum Angriffsziel von Sicherheitsbedrohungen \(engl.\)](#)
- **Web Threat Spotlight:** [Backdoor-App tarnt sich als *Android Market Security Tool* \(engl.\)](#)

Bedrohungszyklopädie

- **Web Attack:** [Gefälschte Apps schaden *Android OS* Nutzern \(engl.\)](#)



TREND MICRO™

Trend Micro Incorporated leistet Pionierarbeit im Bereich Content-Security und bei der Bewältigung von Bedrohungen. Das 1988 gegründete Unternehmen bietet Privatpersonen und Unternehmen jeder Größe mehrfach ausgezeichnete Sicherheitssoftware, -hardware und -services. Der Hauptfirmensitz befindet sich in Tokyo. Trend Micro unterhält Niederlassungen in über 30 Ländern und vertreibt seine Produkte weltweit durch Corporate- und Value-Added-Reseller und Dienstleister. Weitere Informationen und Testversionen der Trend Micro Produkte und Services finden Sie auf unserer Website unter www.trendmicro.com.

TREND MICRO Deutschland GmbH

Central & Eastern Europe
Zeppelinstraße 1
85399 Hallbergmoos

Tel.: +49 (0) 811 88990-700
Fax: +49 (0) 811 88990-799

www.trendmicro.com

TREND MICRO (Schweiz) GmbH

Schaffhauserstrasse 104
CH-8152 Glattbrugg

Tel: +41 43 233 77 81
Fax: +41 43 233 77 83



**TREND
MICRO™**

© 2011 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro und das Trend Micro T-Ball-Logo sind Marken oder eingetragene Marken von Trend Micro, Incorporated. Alle anderen Firmen- oder Produktnamen sind Marken ihrer jeweiligen Eigentümer.