

INFORMIEREN. AGIEREN. VORBEUGEN.



[Ladungssicherung im Transporter >](#)  
[< Dreckige Geschäfte](#)

## Vom Smartphone bis zum Tablet-PC

### Mobile Kommunikationsmittel im Visier von Kriminellen



Smartphones sind mobile Kleincomputer

© Robert Kneschke, fotolia

Smartphones sind nicht nur zum Telefonieren da. Aufgrund ihrer zahlreichen Zusatzfunktionen sind sie eigentlich mehr mit Computern als mit Handys zu vergleichen. Deswegen muss man sie genauso gut schützen. Sie sind ein attraktives Ziel für Angreifer, denn multifunktionale Handys werden häufig im beruflichen Umfeld genutzt, um auf sensible Daten von Unternehmen zuzugreifen. Internetkriminelle interessieren sich aber auch für persönliche Daten, beispielsweise die Log-in-Daten für das E-Mail-Konto, das Online-Banking und den Facebook-Account.

Eine Infizierung erfolgt wie bei einem normalen Computer: per E-Mail oder über manipulierte Webseiten. Wie eine im Januar 2012 veröffentlichte

[Studie zum Thema Informationssicherheit bei mobilen Endgeräten](#) belegt, hat sich in Deutschland in den vergangenen beiden Jahren die Anzahl persönlicher mobiler Datenträger, die auf Unternehmensnetzwerke zugreifen, mehr als verdoppelt. Auf 52 Prozent dieser Geräte sind Kundendaten gespeichert. Der Studie zufolge sind 76 Prozent der befragten deutschen Unternehmen besorgt über den Verlust und die Sicherheit von sensiblen Informationen, die auf den Endgeräten der Mitarbeiter hinterlegt sind. Das können geschäftliche E-Mails sein, aber auch Kundendaten oder Netzwerkzugangsdaten. Über die Manipulation des Fernzugriffs auf Unternehmensdaten können sogar Daten aus dem Firmennetzwerk kopiert und entwendet werden.

## So können Sie sich schützen

Tipps vom Bundesamt für Sicherheit in der Informationstechnik:

- ▶ Halten Sie die Zugangsdaten unter Verschluss. Geben Sie die PIN und Codes nur unter Sichtschutz gegenüber Dritten ein und wechseln Sie regelmäßig Ihre Passwörter.
- ▶ Lassen Sie Ihr Smartphone nicht aus den Augen, um unbefugte Zugriffe und Manipulationen zu vermeiden.
- ▶ Halten Sie Ihr Smartphone-Betriebssystem stets auf dem aktuellen Stand. Installieren Sie die vom Hersteller empfohlenen Anwendungs-Updates regelmäßig. Weitere Informationen zu den aktuellen Betriebssystemversionen und den Programm-Updates Ihres Smartphones erhalten Sie üblicherweise auf der Webseite des Herstellers.
- ▶ Apps sind kleine Zusatzprogramme oder Spiele, die die Nutzer selbst im sogenannten Appstore oder einem anderem Marketplace herunterladen und auf dem Handy installieren können. Installieren Sie Apps nur aus vertrauenswürdigen Quellen. Informieren Sie sich gezielt über den Anbieter der Applikation im Internet und beachten Sie die Kritiken, die andere Nutzer der Applikation geschrieben haben. Installieren Sie nur Apps, die Sie regelmäßig nutzen. Einige Hersteller bieten Nutzern die Möglichkeit, sich anzeigen zu lassen, auf welche Daten und Funktionen die zu installierende App Zugriffsrechte hat. Prüfen Sie in diesem Fall kritisch, ob die Zugriffsrechte zum Erfüllen der Funktionalität wirklich nötig sind. Es könnte sich dabei um potentielle Trojanersoftware handeln.
- ▶ Deaktivieren Sie drahtlose Schnittstellen (z.B. WLAN oder Bluetooth), wenn diese nicht benötigt werden.
- ▶ Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht. Seien Sie vorsichtig bei ungesicherten oder Ihnen unbekanntem WLAN-Angeboten. Wählen Sie sich nur bei bekannten WLAN-Betreibern ins Internet ein.
- ▶ Überprüfen Sie regelmäßig in den Einstellungen Ihres Smartphones den Akku-Verbrauch. Dort wird meist auch angezeigt, welche Applikationen Rechenzeit und Netzwerkverkehr verursacht haben. Bei Auffälligkeiten deinstallieren Sie im Zweifelsfall die verdächtige Applikation.
- ▶ Lassen Sie bei Verlust des Smartphones die SIM-Karte umgehend sperren.

## Achtung: Manipulierte Apps

Das Google Smartphone-Betriebssystem Android ist bereits zum Ziel der Programmierer von Viren und anderen Schadprogrammen geworden.

Es gibt Programme, die ohne das Wissen der Benutzer teure Premium-SMS verschicken. Andere Schadprogramme spähen beispielsweise Daten und Passwörter aus oder blenden regelmäßig Werbebanner auf dem Telefondisplay ein. Auf das Telefon gelangen sie dabei zurzeit fast ausschließlich über manipulierte Apps.

## So können Sie sich schützen

- ▶ Brandneue Apps meiden! In der Regel werden Schadprogramme spätestens nach einigen Wochen oder Monaten entdeckt – bei den neusten Angeboten ist das Risiko deshalb höher als bei etwas älteren Programmen, die schon von vielen Nutzern heruntergeladen und ausprobiert wurden.
- ▶ Das Betriebssystem des Smartphones regelmäßig mit Updates auf den neuesten Stand bringen! Einige Geräte machen das



- ▶ automatisch, sobald sie mit dem Internet verbunden sind. Andere müssen dafür per Kabel mit dem PC verbunden werden.
- ▶ Virens Scanner: Solche Scanner sollen Schädlinge auch schon vor der Installation erkennen. Allerdings erkennen die meisten Scanner nur Viren, die bereits bekannt sind. Das Virens Scanner-Modul ist also bei der aktuell eher geringen Bedrohungslage nur von begrenztem Nutzen. Die Anbieter der Apps arbeiten hier noch an besseren Lösungen.
- ▶ Internetseitenfilter: Damit Sie am Smartphone nicht Opfer einer betrügerischen Internetseite werden, bieten manche Apps wie zum Beispiel Lookout einen Internetseitenfilter. Er funktioniert genauso wie auf dem PC: Wenn man im Internet-Browser des Handys eine gefährliche Internetseite aufruft, blockiert die App mit einem Warnfenster den Aufruf der Seite.

#### **Folgende Artikel könnten Sie auch interessieren:**

-  [Bankgeschäfte und Einkaufen im Netz](#)
-  [Warnsystem als Handy-App](#)
-  [Betrug beim Online-Gaming](#)

[Alle Artikel dieser Kategorie](#)

## **Weitere Infos für Polizisten**



So sieht die Gewerkschaft der Polizei die Lage

### **Reisechaos vor Fußballspielen**

Gefahren, Störungen und Straftaten in Zusammenhang mit Fußballspielen...[\[mehr erfahren\]](#)

---



Betrüger stellen Fake-Stellenangebote ins Netz

### **Gefälschte Stellenanzeigen**

Eine neue Betrugsmasche scheint von den USA und Großbritannien auch...[\[mehr erfahren\]](#)

---



## High Tech-Unterstützung für die Polizei

Der Laufroboter „Spot“ ist das Aushängeschild des Innovation Lab der...[\[mehr erfahren\]](#)

---



Wie sicher sind funkfähige Kredit- und Girokarten?

## Kontaktloses Bezahlen

Das Bezahlen an der Kasse soll mit funkfähigen Kredit- und EC-Karten...[\[mehr erfahren\]](#)

---



Geldautomaten im Visier von Hackern

## Cyber-Betrugsmasche „Jackpotting“

Um möglichst unerkant an große Summen Bargeld zu gelangen, lassen...[\[mehr erfahren\]](#)

---

© Verlag Deutsche Polizeiliteratur

---

## Cookie Einstellungen



- Statistiken
- Essentiell

Wir nutzen Cookies auf unserer Website, die in unserer [Datenschutzerklärung](#) beschrieben sind. Wir verwenden anonyme Statistiken, um unsere Website zu verbessern. Bitte unterstützen Sie unsere wichtige Präventionsarbeit und akzeptieren Sie alle Cookies. Vielen Dank!

AblehnenAlle akzeptieren