Impressum

Herausgeber:
Initiative D21 e.V. und Bayerisches Staatsministerium der Justiz und für Verbraucherschutz

Redaktion:
Martin Falenski (Initiative D21) – V.i.S.d.P.

Gestaltung:
Ulrike Miller, www.miller-partners.com

Kontakt:
Initiative D21, Reinhardtstraße 38, 10117 Berlin
kontakt@initiative21.de, www.initiative21.de

Bayerisches Staatsministerium der Justiz und für Verbraucherschutz
Prielmayerstraße 7, 80335 München
poststelle@stmjv.bayern.de, www.justiz.bayern.de

Bildnachweis:
dreamstimes.com
Stand März 2013

Aufbruch Bayern

Sicherheitsvorkehrungen – Checkliste

Geben Sie auf Ihr Gerät und Ihre Daten acht und treffen Sie Sicherheitsvorkehrungen. Die Installation eines so genannten Prozessmonitors (zum Beispiel „Android Assistent"), also eines Programmes, das die Aktivitäten Ihres Gerätes auf einen Blick anzeigt, ist ein zusätzlicher Schutz. Führen Sie sich immer vor Augen, dass ein Verlust des Gerätes erhebliche Möglichkeiten des Missbrauchs Ihrer Daten mit sich bringen kann.

- ☑ **Zugangsschutz:** Aktivieren Sie den Zugangsschutz (Tastatursperre und Gerätesperrcode) und geben Sie die Entsperrcodes nicht an Dritte weiter. Achten Sie auch auf Sichtschutz bei der Eingabe von Daten.
- ☑ **Schnittstellendeaktivierung:** Deaktivieren Sie unbedingt Schnittstellen wie die WLAN- oder die Bluetoothfunktion, wenn Sie sie nicht brauchen. Dritte können sonst über diese unbemerkt auf Ihr mobiles Gerät zugreifen.
- ☑ **Sicherheitsupdates:** Achten Sie darauf, dass Ihr Betriebssystem und Ihre Anwendungen immer auf dem neuesten Stand sind. Richten Sie für sichere Anwendungen automatische Updates ein.
- ☑ **Apps:** Installieren Sie nur vertrauenswürdige Apps (zum Beispiel aus dem „Apple App-Store" für iOS-Geräte oder aus „Google Play" für Android-Geräte). Achten Sie darauf, welche Rechte Sie dem Anbieter mit dem Download der jeweiligen App einräumen.
- ☑ **Datensicherung:** Sichern Sie in regelmäßigen Abständen mit einem Synchronisationsprogramm Ihre Daten auf einem anderen Gerät (zum Beispiel „iTunes" für iOS oder „MyPhoneExplorer" für Android).
- ☑ **Sicherheitssoftware:** Installieren Sie eine Sicherheitssoftware über den App-Store (zum Beispiel „avast! Mobile Security" für Android).
- ☑ **Drittanbietersperre** (oder auch „WAP-Sperre"): Lassen Sie Drittanbieter bei Ihrem Zugangsprovider (Vodafone, BASE, o.ä.) sperren, wenn Sie nicht vorhaben, das mobile Endgerät für Bezahlvorgänge zu nutzen. So vermeiden Sie Kosten, die unbemerkt durch so genannte „Mehrwertdienste" entstehen können.
- ☑ **Datensparsamkeit:** Speichern Sie so wenig persönliche Daten wie möglich auf Smartphone oder Tablet, vor allen Dingen keine Passwörter oder PIN-Codes.

Darüber hinaus sollte man bei der Nutzung von „Hotspots" Vorsicht walten lassen und auf keinen Fall sensible Daten wie Passwörter eingeben. Und wenn das Gerät einmal gegen ein anderes ausgetauscht werden soll, achten Sie auf die vollständige Löschung der Daten auf dem Gerät und entfernen Sie die SIM-Karte.

Und: Geht das Gerät einmal verloren, unbedingt die SIM-Karte bei Ihrem Diensteanbieter (Vodafone, BASE, o.ä.) sperren lassen.

Einige Gerätehersteller bieten für den Notfall auch eine sogenannte Remote-Funktion an („remote" = engl. „fern"), mithilfe derer man den Inhalt des Geräts auch aus der Ferne löschen kann.

Links/weiterführende Informationen:

- **www.vis.bayern.de:** Verbraucherportal der Bayerischen Staatsregierung zu allen wichtigen Verbraucherthemen wie zum Beispiel Rechte der Verbraucher. Die Sicherheit im Netz bildet im Bereich Daten und Medien einen eigenen Schwerpunkt.
- **www.bsi-fuer-buerger.de:** Informationsseite des Bundesamtes für Informationssicherheit über die Gefahren des Internets und wie man ihnen am besten begegnet.
- **www.polizei-beratung.de:** Informationsseite der Polizeilichen Kriminalprävention der Länder und des Bundes mit ausführlichen Hinweisen zu den Gefahren im Internet.
- **www.internet-sicherheit.de:** Seiten des Instituts für Internetsicherheit der Westfälischen Hochschule mit vielen Sicherheitstipps.
- **www.dsin.de:** Homepage des Vereins Deutschland sicher im Netz unter anderem mit Hinweisen zum Thema Mobile Geräte.
- **www.heise.de:** Portal des Nachrichtenverlags heise mit aktuellen Sicherheitshinweisen speziell für Android und iPhone.

Gut zu wissen!

Gefahren des mobilen Internets

Smartphones und Tablets

INITIATIVE D21

Bayerisches Staatsministerium der Justiz und für Verbraucherschutz

Einführung

Liebe Leserin, lieber Leser,

immer mehr Bürgerinnen und Bürger gehen mobil ins Internet. Über die Hälfte aller Onliner nutzen Smartphones, Tablets & Co., um ihre Mails abzurufen, online einzukaufen oder um sich in sozialen Netzwerken mit anderen auszutauschen. Mittlerweile entsprechen diese sogenannten „mobile devices" dabei kleinen Computern, mit denen gearbeitet oder kommuniziert wird und auf denen vertrauliche Daten gespeichert werden. Daher müssen für sie die gleichen Sicherheitsanforderungen wie für normale PCs gelten. Treffen Sie die nötigen Vorkehrungen, um Ihr Gerät und Ihre Daten zu schützen! Dieser Flyer soll Ihnen dabei eine kleine Hilfestellung sein.

Ihre

Dr. Beate Merk, MdL

Bayerische Staatsministerin der Justiz und für Verbraucherschutz

Allein innerhalb des Jahres 2012 stiegen die Nutzerzahlen bei mobilen Endgeräten in Deutschland um 13%, mittlerweile sind zwei von fünf Deutschen mobil im Netz unterwegs.

Arten mobiler Endgeräte

Im Wesentlichen gibt es zwei Arten mobiler Endgeräte:

- **„Tablet"** (engl. für „Tafel") oder auch „Tablet-PC" = flacher, tragbarer, sehr leichter und durch die besondere Speichertechnologie sehr schneller Computer mit einem berührungsempfindlichen Bildschirm („Touchscreen").
- **„Smartphone"** = modernes, mit Computerfunktionen ausgerüstetes leistungsstarkes Handy.

Betriebssysteme und Software

Neun von zehn Smartphones und Tablets laufen mit den Betriebssystemen Android und iOS, die restlichen 10% verteilen sich im Wesentlichen auf Symbian, RIM und WindowsMobile.

- **Android:** Von Google entwickeltes Betriebssystem auf der Basis von Linux; weltweit am verbreitetsten. Wird von verschiedenen Endgeräte-Herstellern verwendet. Das System ist quelloffen, das heißt, die Programmstruktur ist für jeden einsehbar und kann je nach Bedarf modifiziert und angepasst werden.
- **iOS:** Vom Unternehmen Apple in seinen mobilen Geräten iPhone und iPad verwendetes Betriebssystem.

Auf den Betriebssystem-Oberflächen laufen die Anwendungen, die sogenannten „Apps". Die Palette reicht von Nachrichtenangeboten über Spiele bis hin zu Anwendungen, mit denen man zum Beispiel aus der Ferne die Heizung seines Hauses regeln kann. Die oft kostenfreien Apps bekommt man in den sogenannten „App-Stores", die entweder von den Betriebssystem-Entwicklern (Bsp. „Google Play" oder „iTunes") oder den Endgeräteherstellern angeboten werden. Viele Apps gibt es nur für die Betriebssysteme Android und iOS. Die Zahl der weltweit existierenden Apps wird auf weit über eine Million geschätzt.

Überblick: Gefahren des mobilen Internets

Die mobile Internetnutzung bringt eine Vielzahl von Vorteilen mit sich. Leider sind die Gefahren aber größer als bei der Nutzung stationärer PCs. Die mobile Nutzbarkeit macht die Geräte angreifbarer. Am gefährdetsten sind dabei Android-Handys, da sie am verbreitetsten sind und das quelloffene Betriebssystem Manipulationen erleichtert.

- In **Hotspots** (frei zugänglichen WLAN) können Dritte Daten mit einfachsten Mitteln mitlesen. Dies ist besonders gefährlich bei sensiblen Anwendungen wie Online-Banking.
- Viele mobile Geräte sind nicht durch besondere **Schutz-Programme** wie zum Beispiel Viren-Scanner gesichert; daher sind sie besonders anfällig für Viren und andere Schadsoftware. Es gibt auch noch weitaus weniger Angebote als für PCs.
- **Anwendungen** für Mobilgeräte räumen zum einen dem Anbieter oftmals umfangreiche Zugriffs- und Leserechte für das Endgerät ein. Zum anderen können sie aber auch recht einfach manipuliert werden, so dass sich in vermeintlich sicheren Anwendungen Schadsoftware verbergen kann.
- Da die Geräte in der Regel **permanent online** sind, können durch die Mobilfunkanbieter - und zum Teil auch durch die App-Anbieter – Bewegungsprofile des Nutzers erstellt werden.

Wenn Sie das Gefühl haben, das Gerät wird *langsamer* oder es *verhält sich anders als sonst*, kann dies ein Indiz dafür sein, dass im Hintergrund unerwünschte Prozesse laufen.