



Nr. III

Innsbruck, Mai 2006

AK Tirol gibt Sicherheits-Tipps im Umgang mit Handys

Allgemeine Hinweise

Aus technischer Sicht ist ein Handy wie ein PC mit eingeschränkten Funktionen aufgebaut, es verfügt über einen entsprechenden Hardware-Aufbau mit einem Prozessor und arbeitet mit einem Betriebssystem. Das momentan am weitesten verbreitete Betriebssystem ist „Symbian OS“, weiters sind etwa „Palm OS“, „Windows Mobile Smartphone“ und „Linux Smartphone“ auf dem Markt.

Es ist bekannt, dass der Datenaustausch über das Internet eine Gefahr für den PC darstellt. Im Prinzip besteht die gleiche Gefahr beim Datenaustausch mit dem Handy, dieses verfügt zudem über viele Möglichkeiten der Kommunikation: GSM, GPRS, UMTS, Infrarot, Bluetooth und WLAN, daneben besteht auch die Möglichkeit, Daten über eine Speicherkarte auf das Gerät zu importieren. Je nach Art der „Datenschnittstelle“ oder Art des Datenaustauschs bestehen unterschiedliche Risiken.

Beim Datenaustausch (etwa download von Dateien oder Programmen über GPRS, z.B. Java-Spielen oder anderen Anwendungen) besteht somit das Risiko, dass Viren, Würmer oder Trojaner das Handy schädigen. Immer mehr Fälle von Missbrauch werden bekannt und Konsumenten sind häufig mit überhöhten Telefonrechnungen konfrontiert. Mit einigen Vorsichtsmaßnahmen lässt sich diese Gefahr aber erheblich minimieren.

Diese Aufstellung soll helfen, potenzielle Gefahren richtig einzuschätzen, undefinierbare Störungen am eigenen Mobiltelefon rasch zu identifizieren und größeren Schaden zu vermeiden.

Da alle aktuellen Betriebssysteme „Multitasking-fähig“ sind, somit Programme „unsichtbar“ im Hintergrund betreiben können, können unerwünschte Anwendungen vom Benutzer unbemerkt ablaufen.

Während Viren und Würmer auch zufällig auf das eigene Handy gelangen und Schaden anrichten können, muss der Benutzer einen Trojaner erst selbst installieren bzw. aktivieren.

Diese Programme sind häufig als Hilfsapplikationen oder Spiele getarnt. Eine der bekannten Trojaner-Applikationen für Handys kopiert Einträge im Adress- oder Telefonverzeichnis, sendet diese mittels SMS an einen definierten Empfänger und löscht alle entsprechenden Einträge aus der Liste der Sendevorgänge. Möglich sind auch Manipulationen von Einträgen. Etwa kann das Kommunikationsprofil derart verändert werden, dass Verbindungen über bestimmte Mehrwertdienste umgeleitet werden, was hohe Kosten verursacht. Über GPRS können Verbindungen aufgebaut werden oder beliebige SMS oder MMS versendet werden. Schließlich kann auch der Flash-Speicher des Handys, in dem das Betriebssystem gespeichert ist, überschrieben werden.

Sicherheitstipps:

- Informieren Sie sich beim Hersteller Ihres Handys und Ihrem Provider nach Software-Updates.
- Installieren Sie nur Dateien, deren Herkunft nachvollziehbar ist, etwa über entsprechende Zertifizierungen verfügen. Akzeptieren Sie keine unsignierten Dateien, die Sie unaufgefordert erhalten. Die meisten der bisher bekannten Handy-Würmer benötigen eine manuelle Installation um aktiviert zu werden und Schaden anrichten zu können.
- Achten Sie auch auf die Quelle der Datei, laden Sie nur Applikationen von vertrauenswürdigen WAP- oder Internet Portalen, bei Hacker-Internetseiten und P2P-Netzwerken sollte man vorsichtig sein.
- Achten Sie auf Veränderungen im System, diese könnten eine Infektion als Ursache haben.
- Kontrollieren Sie regelmäßig die Telefonrechnung und den Einzelrufnummernnachweis.

- Kontrollieren Sie regelmäßig die Verbindungsprofile im Menü des Handys, es werden alle Datenaustausche verzeichnet. Allerdings ist es möglich, dass ein Virus die Einträge verändert.
- Informieren Sie sich über aktuelle Anti-Viren Programme für Handys bei Ihrem Provider oder im Fachhandel.
- Ist es bereits zu einer Infektion durch ein schädigendes Programm gekommen, kann ein Anti-Viren Programm dieses entfernen.

Besondere Hinweise für die Anwendung von Bluetooth

Bei Bluetooth-fähigen Handys bestehen besondere Risiken einer Manipulation oder einer Infizierung mit Viren usw. Die Reichweite der Signale beträgt eigentlich nur ca 10 Meter, Mobilfunkexperten ist allerdings der Nachweis einer Kommunikation mit einem Bluetooth-fähigen Handy über eine Entfernung von knapp 2 km unter Zuhilfenahme einer Richtantenne gelungen.

Etwa seit Anfang 2004 gibt es immer wieder Meldungen über Schwachstellen einiger Bluetooth-Handys. Demnach können Hacker mit einem entsprechend präparierten Laptop oder PDA ein fremdes Bluetooth-Handy manipulieren. Dadurch können etwa auf dem Handy gespeicherte Daten wie Adressen- und Telefonbucheinträge, Kalender, Visitenkarten, Codes usw. gelesen, manipuliert und im Handyspeicher und auf der SIM-Karte falsch abgespeichert werden, Telefongespräche vom Laptop oder PDA aus eingeleitet oder unterbrochen werden oder das Handy ganz blockiert werden. Diese Angriffsmöglichkeiten werden als „Blue Bug“, „Blue Snarf“ oder „Bluejacking“ bezeichnet.

Auch bestimmte Handy-Würmer befallen speziell Bluetooth-Handys. Sind diese einmal auf dem Handy aktiviert suchen sie nach anderen Bluetooth-Geräten und versenden Kopien von sich selbst an diese Geräte.

Sicherheitstipps

- Die beschriebenen Manipulationen können nur durchgeführt werden, wenn die Bluetooth-Schnittstelle aktiviert ist. Grundsätzlich sollte man die Bluetooth-Schnittstelle ausschalten und bei Bedarf aktivieren. Auch sollte diese nur in sicherer Umgebung aktiviert werden, nicht etwa auf Bahnhöfen, Flughäfen oder Messen.

- Grundsätzlich sollte man die Bluetooth-Sichtbarkeit des Handys abschalten („Hidden“). Dann können nur bereits gekoppelte Geräte mit dem Handy eine Verbindung aufbauen. Werden neue Geräte mit dem Handy gekoppelt, sollte man die Sichtbarkeit wiederum nur vorübergehend (in sicherer Umgebung) einschalten.
- Alle gekoppelten Geräte sollten im Modus „Unauthorized“ arbeiten, dann muss jeder neue Verbindungsversuch vom Benutzer bestätigt werden.
- Ist es bereits zu einer Infektion gekommen, muss man diesen durch ein Anti-Viren Programm entfernen.
- Besteht der begründete Verdacht, dass eine fremde Person eine Manipulation am Handy vorgenommen hat, so stellt dies einen strafrechtlichen Tatbestand dar und es sollte daher bei der Polizei Anzeige erstattet werden. Treten sonstige Schäden am Handy durch Viren usw. auf, so kann natürlich auch ein Schadenersatzanspruch gegenüber dem Schädiger geltend gemacht werden, wenn dieser ausgeforscht werden kann.