

# *Mobile Unsicherheiten*

**Wer IT-Fachleute nach aktuellen Sicherheitsrisiken befragt, hört Begriffe wie Viren, Würmer und Trojaner. Von Bedrohungen für mobile Geräte werden die wenigsten sprechen – doch das kann ein Fehler sein.**

Olympiastadion Peking, die Eröffnungsfeier der Olympischen Spiele ist in vollem Gange, das „Vogelnest“-Stadion ist mit 91.000 Zuschauern ausverkauft. Ein gefundenes Fressen für den Trojaner InfoJack.a. Er attackiert Geräte mit dem Betriebssystem Windows Mobile.

Der Schädling stammt von einer chinesischen Website und ist als heimliche Beigabe in verschiedene legale Smartphone-Programme wie etwa Google Maps geschlüpft. Innerhalb weniger Minuten verbreitet sich der Schädling via Bluetooth unter den Smartphones der Zuschauer, Politiker und Journalisten. Nachdem sich das infizierte Smartphone mit dem Internet verbunden hat, übermittelt InfoJack.a private Daten, wie die Seriennummer des Geräts, die Betriebssystemversion sowie installierte Anwendungen, an eine chinesische Website.

Mobile Schädlinge zum ersten Mal im Fokus der Weltöffentlichkeit? Nein, denn der Macher des Trojaners wurde einige Monate vorher von chinesischen Behörden geschnappt, die Webseite wurde offline genommen. Glück gehabt.

## **Die mobilen Schädlinge kommen**

Den Big Bang gab es also bisher noch nicht. Doch Computer-Schädlinge für Handys, Smartphones und PDAs sind im Kommen. Den Trend bestätigt Alexander Gostev, Senior Virenanalyst bei Kaspersky Lab: „In den ersten drei Monaten des Jahres 2008 waren mobile Viren sehr aktiv.“ Dabei verteilen sich die neuen Schädlinge ziemlich gleichmäßig auf die vier wichtigsten Angriffsziele mobiler Viren: auf die Plattformen Symbian, Windows Mobile, J2ME und iPhone.

Doch auch vor mobilen Schädlingen kann man sich schützen. So wurde vor kurzem Kaspersky Mobile Security 8.0 veröffentlicht, ein Rundum-Schutz für mobile Geräte. Doch dieses Paket der dritten Generation deckt mehr ab als andere Programme. Die Software schützt nicht nur vor mobilen Trojanern oder Würmern, sondern sichert auch gegen Netzattacken ab und bekämpft SMS-Spam. Zudem werden bei Verlust oder Diebstahl des Smartphones die darauf gespeicherten Daten vor fremdem Zugriff geschützt. Das ist besonders wichtig, denn meist findet man geschäftliche E-Mails auch in Kopie auf dem Smartphone. Ist das Gerät weg, sind auch Firmeninterna plötzlich weg.

## **Schneller Anti-Virus**

Zur Grundausstattung gehört wie auch bei Security-Software für Computer ein Echtzeitschutz für das Dateisystem des mobilen Geräts. Dabei werden von Kaspersky Mobile Security alle eingehenden Objekte, die über drahtlose Verbindungen empfangen werden (Infrarot-Port, Bluetooth), EMS- und MMS-Nachrichten, bei der Synchronisierung mit

dem PC und beim Aufrufen von Dateien über den Browser untersucht. Wird ein Schädling gefunden, fängt der mobile Schutz das Objekt ab.

Außerdem hat der Schutzmechanismus alle Dateien im Blick, die geöffnet werden. Das klappt auch mit Dateien auf Speicherkarten. Natürlich werden auch neue Programme auf Schädlingsbefall geprüft. Auf der Registerkarte „Untersuchung“ können ein Viren-Scan gestartet, die Parameter dafür eingestellt, der Echtzeitschutz-Modus bearbeitet und ein Zeitplan für den Start einer automatischen Untersuchung konfiguriert werden.

### **Anti-Spam und Firewall**

Spam-Probleme bei E-Mails kriegt man trotz des immensen Aufkommens mittlerweile ganz gut in den Griff. Bei Handy-Spam gibt es allerdings noch keine einheitlichen Lösungen. Die unerwünschten Nachrichten trudeln bei Mobiltelefonen via SMS und MMS ein. Kaspersky Mobile Security macht Schluss damit: Spam versendende Telefonnummern sowie unerwünschte Wörter oder Phrasen können auf eine Blacklist gesetzt werden. Alle Einträge aus dem Adressbuch des Anwenders landen dagegen auf der Liste mit vertrauenswürdigen Absendern.

Eine weitere zentrale Komponente ist die Firewall, die Netzwerkangriffe abwehrt. Der Anwender wählt dafür ein passendes Schutzniveau aus. Je nach Einstellung werden bestimmte Verbindungen erlaubt oder verboten.

### **Datenschutz bei Handy-Verlust**

Doch die beste Schutz-Software nützt nichts, wenn die Geräte verlorengehen oder gestohlen werden. Datensicherheit bei Verlust ist deshalb fester Bestandteil von Kaspersky Mobile Security 8.0: Mit dem so genannten SMS-Block können Nutzer bei Verlust ihres Geräts eine geheime Kurzmitteilung versenden, die den Zugriff auf das Gerät blockiert, bis das vorher festgelegte Passwort eingegeben wird. Zudem kann über die Funktion SMS-Clean eine Kurzmitteilung an das Gerät geschickt werden, die den Speicher komplett löscht.