

KASPERSKY lab

W H I T E P A P E R

Mobile Unsicherheiten



Wer IT-Fachleute nach aktuellen Sicherheitsrisiken befragt, hört wahrscheinlich neben Viren, Würmern und Trojanern in erster Linie Botnetze, Rootkits und Phishing. Explizit von Bedrohungen für mobile Geräte werden die wenigsten sprechen – doch das kann ein Fehler sein.

Olympiastadion Peking, 8. August 2008, 21 Uhr Ortszeit. Die Eröffnungsfeier der Olympischen Spiele ist in vollem Gange, das „Vogelnest“-Stadion ist mit 91.000 Zuschauern ausverkauft, dazu kommen noch die Künstler und die Athleten der Teilnehmerländer in der Arena. 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. Gelangt der Trojaner ins System, versucht er, den Mechanismus zu deaktivieren, der die Installation unsignierter Anwendungen verhindert. Nachdem sich dann das infizierte Smartphone mit dem Internet verbun-

In den ersten drei Monaten des Jahres 2008 waren mobile Viren sehr aktiv.

Alexander Gostev
Senior Virenanalyst, Kaspersky Lab

den hat, übermittelt InfoJack.a private Daten, etwa die Seriennummer des Geräts, die Betriebssystemversion sowie installierte Anwendungen, an eine chinesische Website. Innerhalb weniger Minuten verbreitet sich der Schädling via Bluetooth unter den Smartphones der Zuschauer, Politiker und Journalisten.

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. Blickt man etwa auf die Liste der Top-Ten-Bedrohungen des SANS-Instituts (www.sans.org), sieht man, dass die mobilen Schädlinge immerhin Platz vier belegen – noch vor Spyware und Social Engineering.

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 den mobilen Schädlingen kann man sich schützen. So wurde vor kurzem Kaspersky Mobile Security 7.0 veröffentlicht, ein Rundum-Schutz für mobile Geräte. Doch dieses Paket der zweiten Generation deckt mehr ab als ähnliche Programme. Die Software schützt nicht nur vor mobilen Schädlingen wie 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, liegen auch Firmeninterna plötzlich brach.

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 auf dem mobilen Gerät geöffnet werden. Das klappt nicht nur mit dem internen Handy-Speicher, sondern auch mit Dateien auf Speicherkarten. Außerdem wichtig: Auch neue Programme werden 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.

Entdeckt der Wächter gefährliche Objekte, können diese gelöscht oder in Quarantäne verschoben werden. Wer nicht das ganze System, sondern nur einen einzelnen Ordner untersuchen will, kann das über die Registerkarte „Untersuchung“ und „Ordner scannen“ machen. Updates der Signatur-Datenbanken erfolgen automatisch, User müssen sich darum nicht explizit kümmern. Die mobilen Aktualisierungen sind per WAP oder HTTP (GPRS, EDGE, WLAN) verfügbar, daneben können die Updates auch bei der Synchronisierung mit dem PC geladen werden.

Anti-Spam für SMS und MMS

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. Bei eingehenden Nachrichten neuer Kontakte, die noch nicht klassifiziert sind, schlägt die Software die Übernahme in eine der beiden Listen vor. Diese akzeptieren nicht nur komplette Telefonnummern, sondern auch Wildcards, etwa * für mehrere beliebige Zeichen und + für ein beliebiges Zeichen. Ebenfalls sehr praktisch: Der Inhalt des Postausgangs, also alle Nummern, denen bereits eine Kurznachricht geschickt wurde, kann in einem Rutsch in die Whitelist übernommen werden.

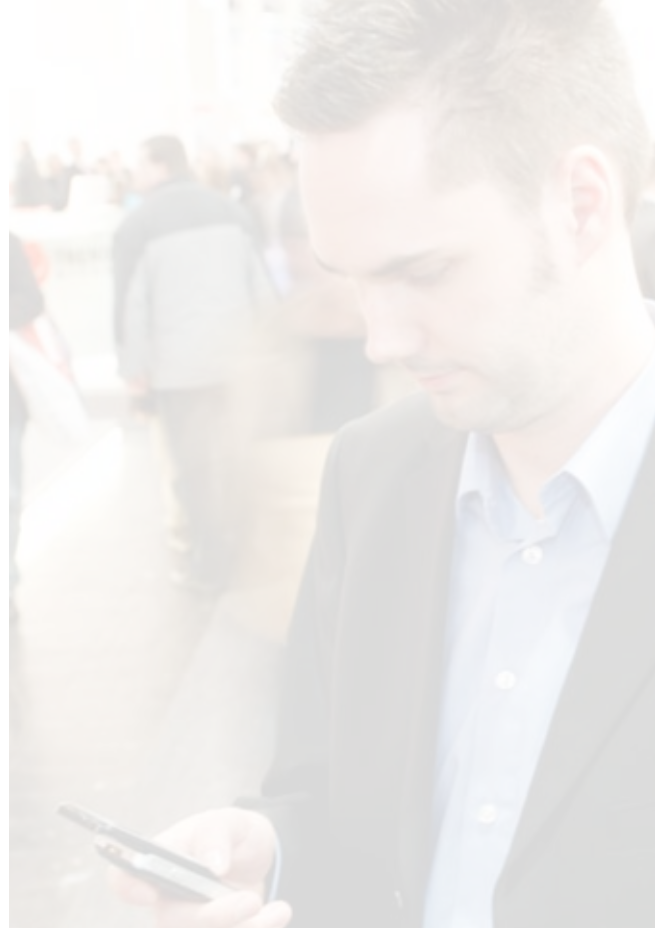
Firewall To Go

Neben Virenschutz ist eine zentrale Komponente die Firewall, die – wie vom PC bekannt – Netzwerkangriffe abwehrt. Der Anwender wählt dafür ein passendes Schutzniveau der integrierten IP-Firewall aus. Je nach Wahl werden bestimmte Verbindungen erlaubt oder verboten. So ist es auch möglich, den gesamten Netzwerkverkehr zu stoppen. Sowohl eingehende wie auch ausgehende Verbindungen sind dann nicht mehr möglich. Standard ist die Einstellung „Mittel“. Dabei werden alle eingehenden Verbindungen blockiert, ausgehende Verbindungen sind nur über die Standard-Programme möglich.

Datenschutz bei Handy-Verlust

Doch die beste Schutz-Software nützt nichts, wenn die Geräte verloren gehen oder gestohlen werden. Datensicherheit bei Verlust ist deshalb fester Bestandteil einer Rundum-Schutzlösung wie Kaspersky Mobile Security 7.0: Mit dem so genannten SMS-Block können Nutzer bei Verlust ihres Geräts eine geheime Kurzmitteilung versenden, die den Zugriff auf das Gerät solange vollständig 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.

Beide Funktionen können aber nur dann Schutz bieten, wenn das Gerät eingeschaltet ist und die SIM-Card nicht ausgetauscht wurde. Damit die Daten auch mit einer anderen SIM-Karte sicher sind, gibt es die Funktion SIM-Watch. Sie verweigert ohne die ursprüngliche SIM-Card den Zugriff auf die Daten des Geräts. Bei Ersatz der alten SIM-Card durch eine neue wird dem Anwender zudem die neue Telefonnummer des Geräts zugeschickt, ohne dass der Dieb es bemerkt. Dann lassen sich die Daten wieder per SMS-Clean löschen, im besten Fall kann der Dieb sogar aufgespürt werden.



Kaspersky Lab

Kaspersky Lab reagiert im weltweiten Vergleich von Antivirus-Herstellern meist am schnellsten auf IT-Sicherheitsbedrohungen wie Viren, Spyware, Crimeware, Hacker, Phishing-Attacken und Spam. Die Produkte des global agierenden Unternehmens mit Hauptsitz in Moskau haben sich sowohl bei Endkunden als auch bei KMUs, Großunternehmen und im mobilen Umfeld durch ihre erstklassigen Erkennungsraten und minimalen Reaktionszeiten einen Namen gemacht. Neben den Stand-Alone-Lösungen des Security-Experten ist Kaspersky-Technologie Bestandteil vieler Produkte und Dienstleistungen führender IT-Sicherheitsunternehmen. Mit den Kaspersky Hosted Security Services bietet das Unternehmen darüber hinaus Dienstleistungen im Bereich Malware- und Spam-Schutz sowie Content-Kontrolle für Unternehmen jeder Größe an.

Kontakt

Kaspersky Labs GmbH
Steinheilstr. 13
85053 Ingolstadt

Telefon: +49 (0)841 981 89 0
Telefax: +49 (0)841 981 89 100

info@kaspersky.de
www.kaspersky.de