

Die verletzbare Firmenzentrale in der Westentasche

Heute ist beinahe jedes fünfte verkaufte Handy ein Smartphone. Doch der Dauerspaß mit den iPhones oder den Androids verwischt die Grenzen zwischen privater und beruflicher Nutzung und bietet so ungeahnte Einflugschneisen auf Firmenrechner.



Glaubt man einer Prognose der Marktforscher von Gartner, dann werden in wenigen Jahren die beiden mobilen Betriebssysteme Symbian und Android weltweit einen Marktanteil von zusammen 60 Prozent erreicht haben. „Die Einführung von neuen Betriebs-systemen – wie Apples iOS4, BlackBerrys OS6, Nokias Symbian 3 und 4 und Microsofts Windows Phone 7 – beflügelt das starke Wachstum im Smartphone-Markt und treibt Innovationen voran“, prophezeit Analystin Roberta Cozza.

Der sorglose Umgang mit mobilen Alleskönnern öffnet Hackern und Wirtschaftsspionen jedoch häufig den direkten Zugang auf Firmenrechner. Das kann in einer Bruchlandung enden, wenn der Sesselnachbar in der Hotellobby mit wenigen Klicks remote und unerkannt Einblick in die Unternehmenskommunikation gewinnt, Geschäftsprozesse anstößt oder Termine für den Vorstand vergibt. Und: Die stetig steigende Zahl unterschiedlicher Endgeräte erhöht den Komplexitätsgrad der IT-Sicherheit für die Administratoren. Hinzu kommt, dass Mitarbeiter Unternehmensdaten sowie Applikationen auf ihr Handy laden. Diese unterliegen dann nicht mehr der direkten Kontrolle ihres Administrators. „Die Wahl der passenden Architektur ist dabei ein kritischer Erfolgsfaktor, um den Aufwand für das Management in einem wirtschaftlich vertretbaren Rahmen zu halten“, lautet der Tipp von Berlecon-Beraterin Melanie Flug. Ein enger Austausch zwischen IT-Verantwortlichen und -Nutzern schon in der Konzeptionsphase sei daher unerlässlich, damit der Datenaustausch zwischen den mobilen Endgeräten und der

Unternehmens-IT später nicht so leicht von Dritten angezapft werden kann.

Denn das kann fatale Folgen haben: Viele der programmierten Helferlein scheren sich nicht um den Schutz sensibler und persönlicher Daten. So haben es Wissenschaftler von Intel Labs, Duke University und Pennsylvania State University in einer Untersuchung zum „Realtime Privacy Monitoring on Smartphones“ bei Android-Apps herausgefunden.

Zwei Drittel der analysierten Programme geben demnach persönliche Informationen an Dritte weiter, ohne dass die Nutzer dem zugestimmt hätten. Die Hälfte der Apps überträgt zum Beispiel Lokalisierungsdaten an Werbeunternehmen beziehungsweise Ad-Server. Rund ein Viertel der Anwendungen leitet zudem die Geräte-ID, die IMEI-Seriennummer (International Mobile Station Equipment Identity), Daten auf der SIM-Card sowie die Telefonnummer weiter. Nur weil die Nutzer einen neuen Bildschirmhintergrund installiert haben.

Um den Schnüfflern auf die Schliche zu kommen, haben die Wissenschaftler nun eine eigene App entwickelt: TaintDroid. Aber das Programm verhindert nicht die Prozesse, sondern schlägt nur Alarm. Ein Weckruf, der auch den Business-Bereich wachrütteln sollte. Denn: Die universelle und für alle Einsatzszenarios geeignete mobile Unternehmenslösung gibt es nicht.

Plattformen: Stärken und Schwächen

Windows Phone 7

- + Kommunikation mit Windows-Software
- + In Hubs zusammengefasste Bereiche erleichtern die Datenverwaltung
- + SSL-Verschlüsselung
- Sicherheits- und Management-Lösungen
- Keine Unterstützung für externe Speicher

Apple

- + Multitasking des iOS 4
- S/MIME wird nicht unterstützt – deshalb für den Einsatz in sicherheitskritischen Bereichen nicht geeignet
- Verteilung der Software muss manuell für jedes einzelne Gerät erfolgen

BlackBerry

- + BlackBerry Enterprise Server

- + Geringer Datenverkehr
- Umlaute
- Veralteter Webbrowser (keine Multimedia-Elemente)

Symbian

- + IMAP-Anbindung
- In die Jahre gekommenes System

Android

- + Dynamik der großen Entwicklerszene
- + Umgang im IMAP
- Eigentlich nicht reif für den professionellen Einsatz

webOS (Palm)

- + Multitasking
- Kann beim IMAP-Handling nicht vollständig überzeugen