

Bild: funkschau Quelle: fotolia



Spionierende Smartphones reißen Sicherheitslücken

Durch Sicherheitslücken in Betriebssystemen und durch „schnüffelnde“ Anwendungen („Apps“) auf geschäftlich genutzten mobilen Geräten werden Unternehmen mit ständig neuen Sicherheitsrisiken konfrontiert.

sendet ohne das Wissen und Autorisierung der Nutzer die Gerätenummer – eine 40-stellige Hexadezimalzahl, die ein I-Phone zweifelsfrei identifiziert – ins Netz. Weitere 36 Anwendungen griffen sofort auf die Ortsdaten des Nutzers zu, ohne diesen darüber zu informieren und einige Apps durchforsteten sogar sogleich dessen Adressbuch – ebenfalls ungefragt.

Persönliche Daten auf dem I-Phone sind aber auch deshalb nicht sicher gegen gezielte Datenspionage geschützt, weil nach Angaben der Fachzeitschrift „iPhoneWelt“ Apples „Code-Sperre“, die die Geräte vor Zugriffen schützen soll, weitgehend wirkungslos ist. Wer Zugriff auf das Gerät bekommt, kann innerhalb von wenigen Minuten fast alle persönlichen Daten auslesen: Fotos, Telefonnummern, SMS und innerhalb von Apps gespeicherte Daten – wie beispielsweise Dokumente.

Aber auch ältere Versionen des freien, quelloffenen Betriebssystems Android, das auf vielen mobilen Geräten läuft, haben nach der neuesten Untersuchung des Instituts für Medieninformatik der Universität Ulm gravierende Sicherheitslücken. Demnach soll das Authentifizierungsprotokoll „ClientLogin“ bis zu Version 2.3.3 Fehler aufweisen, die es Hackern erlaubt, entsprechende Identifizierungen zu umgehen. So können sie nach Angaben der Medieninformatiker sehr einfach auf private Daten aus Google-Kalender, dem Telefonbuch oder aus der Mediengalerie zugreifen.

Nicht nur die I-Phone-Apps sondern auch andere Handy-Betriebssysteme haben also ihre spezifischen Risiken und „Nebenwirkungen“, die Unternehmen mit professioneller Unterstützung jedoch eindämmen und auf ein absolutes Minimum reduzieren können: „Noch bis vor kurzem galt das BlackBerry als das Multitalent für die mobile

Kommunikation in den Unternehmen“, weiß Friederike Homburg, Teamleiterin Mobilfunk von Consense, die Unternehmen bei der Auswahl, Verwaltung und Optimierung geschäftlich genutzter mobiler Anwendungen berät und unterstützt: „Die Vielzahl der Sicherheitsrichtlinien des BlackBerry-Servers können individuell an die Bedürfnisse des Kunden angepasst werden. Die Verwaltung der verschiedensten Blackberrys erfolgt über eine Software und erleichtert die Administration erheblich. Es können zum Beispiel Geräte- und Softwaresperren hinterlegt oder aber die Nutzung von bestimmter Software verboten werden. Auch die Remote-Löschung bei Diebstahl oder Verlust ist möglich.“

Doch mittlerweile existiert in den meisten Unternehmen eine heterogene Struktur unterschiedlichster Mobilfunkgeräte und Anwendungen. Die am häufigsten genutzten Betriebssysteme sind aktuell Android, IOS und Windows-Mobile. „Das bedeutet für uns, dass wir unsere Beratungsstrategie nicht mehr nur auf BlackBerry-Geräte und die Aufsetzung des Servers fokussieren, sondern die gesamte heterogene Endgerätestruktur eines Unternehmens in unserem Mobile-Device-Management berücksichtigen müssen. Neben dem Sicherheitsaspekt stehen dabei vor allem wirtschaftliche Fragestellungen im Vordergrund“, erklärt Friederike Homburg. Je komplexer, vielfältiger und unübersichtlicher die Endgerätestruktur einer Firma wird, desto größer werden natürlich auch die Herausforderungen und Problematiken und damit der Beratungsbedarf eines Administrators, IT-Verantwortlichen oder Geschäftsführers.

 **Detlev Spierling**
freier Journalist in Oberseel

Nach einer kürzlich veröffentlichten Studie der Technischen Universität Wien spionieren rund die Hälfte aller untersuchten I-Phone-Apps persönliche Daten der Nutzer ohne deren Wissen aus. Selbst, wenn es wie bei Apple eine „Code-Sperre“ gibt, die I-Phones vor Zugriffen schützen soll, ist diese meist leicht auszuhebeln. Mit Unterstützung eines professionellen Dienstleisters können Unternehmen dieses wachsende Sicherheitsrisiko eindämmen sowie durch die Optimierung und Konsolidierung ihrer Mobilfunkverträge und -Tarife auch noch Geld sparen.

Während 2009 weltweit gerade einmal 1,4 Milliarden Smartphone-Anwendungen – so genannte Apps – aus dem Internet heruntergeladen wurden, soll sich dieser Wert nach Angaben der Strategieberatung Booz & Company binnen fünf Jahren auf 18,7 Milliarden Anwendungen vervielfachen. Diese Zahl verdeutlicht die stark wachsende Bedeutung der Apps auch im mobilen Unternehmensalltag. Doch viele dieser praktischen Minianwendungen haben auch gravierende Nachteile. Darauf hat kürzlich eine Gruppe von Informatikern aus Österreich, Frankreich und den USA hingewiesen, die im Rahmen einer Studie der TU Wien gut 1400 Apps für I-Phones untersucht haben. Das erschreckende Ergebnis: über die Hälfte aller I-Phone-Apps

Höhere mobile Sicherheit zu geringeren Kosten

Welche Leistungen kann ein Kunde unter dem Schlagwort Mobile-Device-Management von einem qualifizierten Dienstleister im Einzelnen erwarten?

„Der Kunde sollte darauf achten, ob der Anbieter mit Hilfe einer speziellen Software die verschiedenen Betriebssysteme auf den unterschiedlichsten mobilen Endgeräten verwalten kann. Dabei werden die individuellen Anforderungen des Kunden hinterlegt und die Geräte dementsprechend konfiguriert – angefangen von den VPN-Einwahldaten bis hin zur Nutzung von Unternehmenssoftware oder von verschiedenen Applikationen.“

Wichtig ist auch, dass dieser Anforderungskatalog, der die Grundlage des Mobile-Device-Managements bildet, in einem Workshop mit dem Kunden gemeinsam erarbeitet wird. Das MDM sollte außerdem die Administration der ‚Standard-Funktionalitäten‘ auf den verschiedensten Endgeräte-Typen wie die Unternehmens-Mail, Kalender-Funktion, Schnittstelle zu ERP-Systemen oder Instant-Messaging beinhalten.“

Welche Aspekte und Faktoren sollten bei dem wichtigen Thema Mobile-Security im Vordergrund stehen?

„Um die Privat- und Firmendaten auf geschäftlich genutzten mobilen Endgeräten so gut wie möglich zu sichern und zu schützen sollten die Remote-Geräte-Kontrolle – inklusive der Konfiguration, Sperre und gegebenen-

falls Löschung sowie der Passwort-Schutz von Geräten im Vordergrund stehen.“

Dabei muss natürlich auch die Einhaltung von Betriebsvereinbarungen beachtet werden, die explizit definieren, wie der Mitarbeiter sein mobiles Endgerät nutzen darf. Also, darf er überhaupt bestimmte Apps downloaden und installieren oder die Kamera benutzen, darf er auf dem Gerät firmeninterne oder private Daten verwalten, nutzen oder speichern? Das sind wesentliche Sicherheitsfaktoren, die in das Mobile-Device-Management-Konzept einfließen müssen, um danach eine für den Kunden optimale Lösung umsetzen zu können. Außerdem sollte der Dienstleister seinen Kunden bei Bedarf auch bestimmte Verschlüsselungslösungen zum Schutz der Daten auf mobilen Endgeräten empfehlen können.“

Bis zu wie viel Prozent ihrer Mobilfunkkosten können Unternehmen denn durch die Optimierung und Konsolidierung ihrer Mobilfunkverträge und -Tarife maximal sparen?

Die Ersparnis ist von verschiedenen Faktoren abhängig (von der Kartenanzahl, von vorhandenen Rahmenverträgen und von dem individuellen Telefonieverhalten, etc.), aber in der Regel können durch ein professionelles Mobile-Device-Management Ersparnisse von 10 bis 20 Prozent erzielt werden.

Wir bei Consense beispielsweise arbeiten

funkschau INTERVIEW



Friederike Homburg

Teamleiterin Mobilfunk von Consense

mit einem eigenen Analyse-Tool, in das die Rechnungsdaten elektronisch eingespielt und dann mit allen am Markt aktuell verfügbaren Konditionen automatisch verglichen werden. Dabei werden auch verschiedene Tarifprofile hinterlegt und dem Kunden vorgestellt.“