05.06.2012

MOBILE SECURITY

Von: Silke Geiß

Sicher arbeiten in einer mobilen Welt

APPS SIND DAS EINLASSTOR FÜR MOBILE ANGREIFER

Über Apps verschaffen sich mobile Angreifer immer häufiger Zugang zum Firmennetzwerk. Ein effektives Applikationsmanagement ist für die Sicherheit Unternehmen daher unabdingbar. Was leisten hier Mobile-Device-Managemen Lösungen?

Sicher arbeiten in einer mobilen Welt – bei diesem Thema spielt der Umgang mit Applikationen eine große Rolle. Der Markt bietet mittlerweile eine unüberschaubare Fülle von Anwendungen – die Palette reicht vom einfachsten Werkzeug oder der Spaßanwendung bis hin zu Paketen mit umfangreichen

Funktionalitäten. Geräte wie das iPhone laden geradezu dazu ein, neben geschäftlichen Apps auch Spiele und andere private Applikationen herunterzuladen. Laut einer aktuellen Studie erlauben vier von zehn Unternehmen ihren Angestellten bisher noch die freie Internetnutzung und das Herunterladen von Anwendungssoftware mit Mobilgeräten. Fehlende Reglementierungen beim Download von Smartphone-Apps stellen jedoch ein großes Sicherheitsrisiko dar.

„Applikationen sind das Einlasstor für mobile Angreifer und Schadsoftware“, weiß Robert Himmelsbach, Experte für Mobile Device Management bei der MPC Mobilservice GmbH. „App-Trojaner zum Beispiel tarnen sich als harmlose Applikation und können den Benutzer mit Gebühren belasten, indem Sie teure SMS an Premiumrufnummern verschicken.“ Im Hintergrund greifen Apps zudem oftmals unbemerkt sensible Daten ab oder lesen auf dem Gerät automatisch gespeicherte Nutzerverhalten-Profile oder Positionsdaten aus. „Malware kann in Sekundenschnelle über die Netze übertragen werden und eine große Anzahl Smartphonenutzer lahmlegen“, stellt Himmelsbach fest. Schließen lässt sich dieses Sicherheitsloch nur, indem Unternehmen den Download privater Inhalte und Apps entweder verbieten – oder gezielt reglementieren.

Anbieter von Mobile-Device-Management(MDM)-Lösungen unterstützen die sichere Appnutzung im Unternehmensumfeld durch einen so genannten „Enterprise App Store“. In solchen firmeneigenen Stores bekommen Nutzer ausgewählte Unternehmens- oder Business-Applikationen angeboten, die dann über die Luftschnittstelle auf die Endgeräte installiert werden. „Nutzer können sich quasi selbst bedienen und die gewünschten Apps herunterladen“, erklärt Himmelsbach. Ob obligatorische Apps auch vorschriftsmäßig installiert werden, lässt sich dabei über ein zentrales Webportal nachverfolgen.

Generell ist es bei allen gängigen Systemen möglich, das so genannte „Software-Inventory“ der Geräte auszulesen und den Nutzer aktiv auf unerwünschte Downloads anzusprechen. Zu beachten ist jedoch, dass sich per MDM-Lösung das Herunterladen und / oder die Ausführung einzelner Apps aus den allgemeinen Anbieter-Stores bisher nicht bei jedem Betriebssystem unterbinden lassen. „Bei iOS, dem Betriebssystem für Apple-Geräte, kann man aber auch bestimmte Nutzungsfunktionen wie Filme oder anstößige Inhalte sperren“, so Himmelsbach. Zur Aufgabe eines IT-Verantwortlichen gehöre es jedoch nicht nur, den Umgang mit Apps in geregelte Bahnen zu lenken – sondern auch die Mitarbeiter selbst für die damit zusammenhängenden Sicherheitsrisiken zu sensibilisieren. Daneben sollten klare Regeln für den Umgang mit und die Nutzung von Applikationen aufgestellt und durchgesetzt werden. Nur so kann man nicht nur technisch sondern auch rechtlich den aktuellen Anforderungen im Bereich Mobile Device Management begegnen.

www.mpcservice.com

Bildquelle: © Thomas Max Müller / *pixelio.de*

« Home