



Firmendaten auf iPhone und iPad – wie steht's mit der Sicherheit

iPhone und iPad haben in der Unternehmenskommunikation eine starke Präsenz erreicht. Nach anfänglichen Sicherheitsbedenken gelten sie heute als sicher und lösen in vielen Bereichen Blackberrys als mobile Kommunikatoren ab. Ausgerüstet mit Gerätemanagement-Software sind sie vor Diebstahl und Fremdzugriff geschützt. Doch die Frage ist, ob die Firmendaten auf den iOS-Geräten wirklich sicher geschützt sind und kein Unbefugter Zugriff hat.

Apple verkaufte 2010 in der Schweiz laut dem Weissbuch von Robert Weiss 889 000 iPhones und iPads. Ein Grossteil dieser iOS-basierten Geräte werden in Unternehmen eingesetzt und in Firmenlösungen eingebunden. Vorwiegend werden E-Mail, Kalender und Kontakte zum Beispiel mittels Exchange Active Sync in die nativen Applikationen der Geräte synchronisiert. So sind die Mitarbeiter immer auf dem Laufenden und mobil. Eine Gerätemanagement-Software (MDM-Lösung) verwaltet die Geräte, die über ein Passwort vor Fremdzugriff geschützt sind. iPhones und iPads mit einem Jailbreak, die Nutzungseinschränkungen von Apple sind ausgeschaltet, werden über die MDM-Software von der Nutzung ausgeschlossen. Eine sichere Lösung – meint der Nutzer.

Infos zum Autor



Martin Ottiger
CEO, Comdirect AG

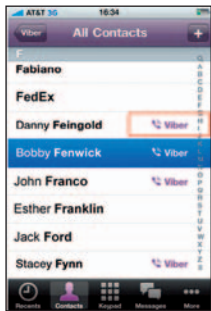
Apple erlaubt den Zugriff auf Kalender und Kontakte

So weit, so gut, doch sind E-Mail, Kalender und Kontakte wirklich sicher und vor Fremdnutzung und Diebstahl geschützt? Apple ist ja bekannt, sogar berechtigt für die Abschottung des iPhones und seiner anderen Geräte, die auf dem mobilen Betriebssystem iOS laufen. Die Nutzer sollen sich ausschliesslich im Apple-eigenen Ökosystem bewegen. Aber Apple erlaubt mittels integrierter Schnittstellen jeder Applikation im Appstore den Zugriff auf Kalender und Kontakte – eine gefährliche Hintertür. Diese Daten sind trotz installierter MDM-Software völlig ungeschützt.

Zu Programmen oder Apps, die diese Hintertür nutzen, gehören zum Beispiel Viber, Whatsapp oder Go-



walla. Viber ist eine Applikation, die das freie Telefonieren zwischen Geräten ermöglicht, die diese Applikation installiert haben. Beim Starten der Applikation werden sämtliche Kontakte auf einen Server von Viber in die Cloud übertragen. Der Anwender sieht das Resultat umgehend im Adressbuch: Kontakte, die Viber ebenfalls installiert haben, sind mit einem zusätzlichen Symbol markiert – der Anwender sieht sofort, mit wem er in Zukunft gratis telefonieren kann.



So toll und komfortabel dieser Dienst für den Anwender ist, so gefährlich kann er für das Unternehmen werden, wird doch auf diese Weise die Sicherheit der Gerätemanagement-Lösung umgangen. Das Unternehmen hat keinen Einfluss darauf, wie diese Daten sonst noch verwendet werden. Dazu Viber in ihren FAQs: «Anstelle der Suche nach Viber-Kontakten erledigt Viber die ganze Arbeit! Viber verwendet das Adressbuch auf dem Gerät und verknüpft die Kontakte automatisch.»



Dasselbe gilt im weiteren Sinne auch für den Kalender – stehen doch Kalendereinträge beliebigen anderen Anwendungen aus dem Appstore zur Verfügung. Aber auch Cyberkriminelle können auf das iPhone zugreifen. Laut dem Schweizer Softwareingenieur Nicholas Seriot bietet auch ein iPhone ohne Jailbreak keinen 100-prozentigen Schutz vor Datenklau. Der Programmierer wies an einer Tagung in Genf darauf hin, dass es nicht unmöglich ist, auch im Appstore Software anzubieten, die verschiedene private Informationen der Nutzer auslesen kann. Seriot stellte zum Beweis eine App (Spyphone), basierend auf den Standard-APIs von Apple, vor, mit der man das Adressbuch, den Keyboard-Cache, den Browser-Verlauf und GPS-Daten abfragen kann. Grundsätzlich sei das iPhone allerdings vergleichsweise sicher, da auch die strengen Auswahlverfahren des Appstores die schlimmsten Schädlinge entlarven. Dass dem so ist, zeigt auch der US-Sicherheitsforscher Phil Purviance in einem auf Youtube veröffentlichten «Proof of Concept»-Video am Beispiel von Skype. Es braucht, um die Kontakte zu stehlen, eine Applikation, die die Apple-Prüfung besteht, vordergründig einen sehr guten Nutzen hat, kostenlos ist, im Hintergrund aber unbemerkt die Daten abzieht und auf einen Server im Internet übermittelt.

Die Applikation hat freien Zugriff auf die Kalender- und Kontaktdaten in den nativen Applikationen, aber keinen Zugriff auf die Applikationen in der Sandbox.

tisch, gehören die Geräte doch vielfach den Benutzern. Da Apple nur ein «Alles oder nichts»-Prinzip zulässt, kann den Benutzern das Laden von Apps aus dem Appstore verunmöglicht werden – eine solche Einschränkung würde vom iPhone-Besitzer und Mitarbeiter sicher nicht akzeptiert.

Gewisse Gerätemanagement-Lösungen unterstützen die Verwendung von Black- und Whitelists. Mit dem Nachteil aber, dass neu installierte Anwendungen erst nach einer gewissen Zeit erkannt werden – wenn sich das iOS-Gerät das nächste Mal mit dem Gerätemanagement-Server verbindet. In dieser Zeit sind gewisse Daten bereits wegkopiert. Zudem ist der Aufwand für die Pflege dieser Black- und Whitelists bei der Anzahl vorhandener Apps immens.

Sandbox anstelle nativer Anwendungen

Mit Sandbox oder Container wird eine geschützte Umgebung innerhalb des Betriebssystems bezeichnet, die keine oder nur ein Set von genau definierten Daten nach draussen lässt. Innerhalb der Sandbox laufen zum Beispiel die Unternehmensanwendungen wie E-Mail, Kontakte, Kalender und Aufgaben. Es gibt für Drittanwendungen keine Möglichkeit, auf die Daten dieser Anwendungen direkt zuzugreifen. Selbstverständlich kann der Administrator der Sandbox zulassen, dass bestimmte Daten für andere, persönliche Apps sichtbar sind. Die kann wegen der Bedienerfreundlichkeit notwendig sein. So sind sich die Benutzer gewöhnt, den Namen des Anrufers zusammen mit seinem Bild auf dem Display zu sehen, wenn das iPhone klingelt. Ist die Sandbox komplett abgeschottet, ist dies mit den Firmkontakten jedoch nicht möglich. Der Administrator kann aber Telefonnummer und Name sichtbar machen und der Name des Firmkontakts erscheint auf dem Display. Der Vorteil gegenüber nativen Applikationen ist, dass festgelegt werden kann, welche Felder sichtbar sein dürfen. In besonders sensiblen Umgebungen kann selbst das Copy/Paste zwischen den Apps in der Sandbox und den anderen Apps unterbunden werden.

Mit Sandbox auf der sicheren Seite

Unternehmen, die iOS-Geräte für die Kommunikation einsetzen oder unterstützen, müssen sich bewusst sein, dass mit den üblichen Gerätemanagement-Lösungen die Unternehmensdaten nicht geschützt sind. Sie müssen Lösungen anwenden, die auf dem Sandbox-Ansatz beruhen, ansonsten wissen sie nie, was mit ihren Daten passiert.

Als zusätzlichen Nutzen wird mit der Sandbox das Prinzip der Trennung von geschäftlicher und privater Nutzung sauber umgesetzt. Die Mitarbeiter können über die Nutzung ihrer Geräte frei verfügen, die Geschäftsdaten bleiben geschützt in der Sandbox und werden separat verwaltet.

Firmendaten können auch im iPhone geschützt werden

Doch es gibt Möglichkeiten, die Sicherheit und den Zugriff auf die Kontaktdaten bei den iOS-Geräten zu erhöhen oder diese ganz abzuschotten. Dazu gehören einerseits die Verwendung von White- und Blacklists, andererseits sogenannte Sandboxes oder Container.

Werden sogenannte White- und Blacklists angewendet, entscheidet das Unternehmen, welche Apps der Mitarbeiter anwenden darf. Nicht ganz unproblema-

