

# Sichere Smartphones für Unternehmen

Moderne Smartphones bieten eine Vielzahl von Möglichkeiten, die privat und geschäftlich genutzt werden können. Diese Eigenschaft birgt Gefahren, die unterschätzt werden. Die Lösung von Good Technology vollzieht eine konsequente Trennung und garantiert eine sichere Übermittlung der Daten über das Internet.

Moderne Smartphones (iOS, Android und Windows Mobile basierte Geräte) sind multifunktionale Geräte, die neben den üblichen Funktionen wie Telefonieren und SMS-Schreiben viele weitere Anwendungen ermöglichen. Besonders interessant für Unternehmen sind Applikationen, die den Mitarbeitern erlauben, auf Unternehmensdaten zuzugreifen zu können. Am meisten verbreitet ist heute der Einsatz der E-Mail-, Kontakte- und Kalender-Applikationen, die im Rahmen des «Personal Information Management, PIM» auf den Smartphones vorinstalliert sind.

## Anforderungen an die Sicherheit

Aus Sicht eines Unternehmens müssen die folgenden Anforderungen im Zusammenhang mit der Sicherheit der Unternehmensdaten auf Smartphones erfüllt sein:

- Sichere und authentische Übermittlung
- Schutz bei Verlust des Smartphones
- Zugriff nur durch berechtigte Personen und Applikationen
- Zentrale Administration
- Einfacher und sicherer Rollout
- Hohe Benutzerfreundlichkeit

Besonderes Augenmerk gilt der Datensammlung durch Apps im Zusammenhang mit dem berechtigten Zugriff auf Unternehmensdaten. Viele Apps leiten benutzerspezifische Informationen an den Hersteller weiter, ohne den Benutzer explizit darüber zu informieren. Die Weitergabe von Adressdaten kann sogar durch den Benutzer gewollt sein, um eine Applikation gewinnbringend in einer Commu-

nity einsetzen zu können. Aus Sicht eines Unternehmens ist dies problematisch.

## Zielkonflikte und Lösungsansätze

Das Unternehmen möchte seine Daten bestmöglich schützen und die Erreichbarkeit eines Mitarbeiters nicht einschränken.

Der Mitarbeiter möchte ein einzelnes, benutzerfreundliches Gerät, das er für geschäftliche aber auch private Zwecke nutzen kann. Diesem Zielkonflikt kann durch geeignete Massnahmen entgegnet werden. Im Folgenden sind stichwortartig die grundsätzlichen Lösungsansätze aufgeführt, die sich Unternehmen im Zusammenhang mit Mobile Security überlegen:

### Secure E-Mail (S/MIME)

Einführung einer internen Secure E-Mail-Lösung, um die Daten auf den Smart-

phones verschlüsselt abzuspeichern. Dieser Lösungsansatz ist aus den folgenden Gründen zu hinterfragen:

- Stellvertreterregelungen und Volltextsuche entfallen
- Der private Schlüssel für die Entschlüsselung der E-Mails ist ungenügend geschützt
- Daten sind gegenüber anderen Applikationen nicht geschützt
- Kalender und Kontakte sind weiterhin nicht verschlüsselt

### Remote Terminal

Einführung einer Lösung, um E-Mails über Remote Terminal zu verarbeiten. Dieser Lösungsansatz ist aus den folgenden Gründen zu hinterfragen:

- Keine Offline Fähigkeit
- Grosse Bandbreiten für die Übermittlung der Daten
- Ungewohnte Bedienung der Windows Applikationen auf den Smartphones (Rechter Mausclick, verschieben von Fenstern, usw.)
- Mechanismen für die authentische Kommunikation müssen etabliert werden (X.509 Zertifikate)

### Trennung der Daten und Applikationen

Die konsequente Trennung von geschäftlichen und privaten Daten und Applikationen ist der sicherste Lösungsansatz, der mit «Good for Enterprise» einfach und kosteneffizient umgesetzt werden kann.

### Good for Enterprise

Good for Enterprise ist eine umfassende Sicherheitslösung für Smartphones. Sie erlaubt die sichere Verarbeitung, Übermittlung und Speicherung von Unternehmensdaten und umfasst eine zentrale Konsole für die Over the Air-Verwaltung der Smartphones. Die Lösung besteht aus eigenständigen Applikationen für den Zugriff auf E-Mail, Kontakte oder Kalendereinträge, die im gewohnten «look and feel» bedient werden können. Dies garantiert die sichere Speicherung der Daten auf dem Smartphone und verhindert den Zugriff durch Drittapplikationen. Integriert wird die Lösung über eine serverseitige Komponente, welche die Daten über die Push-Technologie sicher mit den jeweiligen Smartphones synchronisiert. Der Rollout erfolgt dezentral durch den kostenlosen Download der Applikation sowie der sicheren Aktivierung durch die Eingabe spezifischer Sicherheitsmerkmale. ■

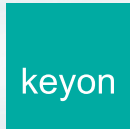


Keyon AG, 8645 Jona  
René G. Eberhard, CEO  
Telefon 055 220 64 00, Telefax 055 220 64 01  
eberhard@keyon.ch, www.keyon.ch



# Sichere Smartphones im Unternehmen

- ▶ Good trennt private und geschäftliche Daten und Applikationen auf Ihrem Smartphone
- ▶ Sichere Speicherung und Übermittlung aller Geschäftsdaten
- ▶ Zentrale Administration und Überwachung
- ▶ Unterstützt iPhone, iPad, Android und Windows Mobile



keyon AG  
Schlüsselstrasse 6  
8645 Jona  
Switzerland

Tel: +41 55 220 64 00  
Fax: +41 55 220 64 01

www.keyon.ch  
info@keyon.ch