security zone newsletter
PLATTFORM FÜR INFORMATIONSSICHERHEIT

Sichere Smartphones im Unternehmen

Moderne Smartphones bieten eine Vielzahl von Möglichkeiten, die privat und geschäftlich genutzt werden können. Die Koexistenz von privaten und geschäftlichen Daten und Applikationen birgt Gefahren, die oft unterschätzt werden. Die Lösung von Good Technology trennt private und geschäftliche Daten und Applikationen auf dem Smartphone und garantiert eine sichere Übermittlung der Daten über das Internet.

René G. Eberhard

CEO keyon AG

eberhard@keyon.ch
www.keyon.ch

Die konsequente Trennung von geschäftlichen und privaten Daten und Applikationen ist der sicherste Lösungsansatz.

Eigenschaften der Smartphones

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. Sie verfügen über leistungsfähige Betriebssysteme mit offenen Schnittstellen (API) und ermöglichen es, Programme von Drittherstellern zu installieren und zu nutzen.

Besonders interessant für Unternehmen sind Applikationen, die den Mitarbeitern erlauben, auf Unternehmensdaten zugreifen zu können. Am meisten verbreitet ist heute der Einsatz der Email-, 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 (Profile, remote Wipe, etc.)
- Einfacher und sicherer Rollout
- Hohe Benutzerfreundlichkeit

Besonderes Augenmerk gilt der Datensammlung durch verschiedene 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 Gemeinschaft einsetzen zu können. Aus Sicht eines Un-

ternehmens ist dies überaus problematisch.

Zielkonflikte und Lösungsansätze

Das Unternehmen möchte seine Daten bestmöglich schützen und die Erreichbarkeit und Flexibilität 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 Email (S/MIME)

Einführung einer internen Secure Email Lösung, um die Daten auf den Smartphones verschlüsselt abzuspeichern. Dieser Lösungsansatz ist aus den folgenden Gründen zu hinterfragen:

- Stellvertreterregelungen auf Postfächern entfällt
- Die Volltextsuche für Emails entfällt
- Der private Schlüssel für die Entschlüsselung der Emails ist ungenügend geschützt
- Daten sind gegenüber anderen Applikationen nicht geschützt
- Kalender und Kontakte sind weiterhin nicht verschlüsselt

Remote Terminal

Einführung einer Lösung, um Emails über Remote Terminal einzusehen und 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 Mausklick, verschieben von Fenstern, etc.)
- 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 speziell 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 Email, 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 auf die Daten durch Drittapplikationen.

Integriert wird die Lösung über eine serverseitige Komponente, welche die Daten über die Push-Technologie sicher und authentisch mit den jeweiligen Smartphones synchronisiert. Der Rollout erfolgt dezentral durch den kostenlosen Download der Applikation sowie der sicheren Aktivierung durch die Eingabe spezifischer Sicherheitsmerkmale.