



# Sichere Smartphones für Unternehmen

Infos zum Autor



**René G. Eberhard**

Dipl. El.-Ing. HTL/  
Betriebswirtschafts-  
ingenieur FH NDS/  
Softwareingenieur FH  
NDS, CEO der Keyon  
AG, [www.keyon.ch](http://www.keyon.ch),  
[eberhard@keyon.ch](mailto:eberhard@keyon.ch)

Smartphones stellen aus Sicht Verwaltung, Betrieb und Sicherheit analoge Anforderungen wie Laptops oder PCs. Die Eigenschaften von iOS, Android und Windows Mobile 7 unterscheiden sich jedoch grundsätzlich vom Windows-Betriebssystem für Laptops und Desktop-PCs. Erschwerend kommt hinzu, dass der Benutzer erwartet, das Smartphone auch uneingeschränkt für private Zwecke nutzen zu können. Die IT-Abteilungen der Unternehmen sind gefordert, kosteneffiziente Lösungen anzubieten, welche nahtlos in die eigenen betrieblichen und sicherheitstechnischen Prozesse integriert werden können.



## Einsatzgebiete

Tablet PCs sind leistungsfähige Geräte, die heute in Unternehmen primär im Rahmen des «Personal Information Management, PIM» zur Synchronisation der E-Mail-, Kontakt- und Kalenderdaten verwendet werden. Im Zusammenhang mit Tablet PCs sind aufgrund des grösseren Bildschirms weitere Anwendungen wie beispielsweise der Zugriff auf webbasierte Applikationen im Intranet des Unternehmens oder das Bearbeiten von Office-Dokumenten möglich.

## Nichts Neues und dennoch alles anders

Die Anforderungen an Verwaltung, Betrieb und Sicherheit der Smartphones sind analog zu denjenigen der Laptops oder PCs. Das Unternehmen will die eigenen Richtlinien zur Applikations-, Daten- und Zugriffssicherheit durchsetzen sowie die Zuordnung eines spezifischen Endgeräts zum Mitarbeiter kennen. Die Herausforderung hierbei ist, dass die bisher verwendeten Konzepte, Prozesse und Applikationen, die im Zusammenhang mit Windows-Betriebssystemen im Einsatz sind, nicht einfach auf iOS, Android und Windows Mobile 7 übertragen werden können. Neue Aspekte wie beispielsweise die Over-The-Air (OTA) Verwaltung von Endgeräten, Richtlinien und Applikationen oder die Koexistenz von privaten und geschäftlichen Daten und Applikationen kommen hinzu.

## Bring Your Own Device

Viele Mitarbeiter nutzen privat leistungsstarke Smartphones, die auch geschäftlich eingesetzt werden könnten. Daher überlegen viele Unternehmen, ob sie solche Smartphones in ihre Infrastruktur integrieren wollen.

«Bring Your Own Device» bedeutet, dass ein Mitarbeiter sein privates Smartphone auch geschäftlich nutzt. Aus Sicht des Mitarbeiters ist dieser Ansatz gewinnbringend, da er nur ein Gerät auf sich tragen muss und sein meist modernes und leistungsstarkes Gerät privat und geschäftlich nutzen kann. Aus Sicht des Unternehmens ist dieser Ansatz gewinnbringend, da die einmaligen Beschaffungskosten für das Gerät wegfallen oder durch eine einmalige oder monatliche Pauschale abgegolten werden kön-

nen. Zudem muss das Unternehmen den kurzen Produktzyklen nicht nachgehen, um den Mitarbeitern das jeweils modernste Gerät bereitzustellen.

«Bring Your Own Device» kann für ein Unternehmen eine interessante Strategie sein, wenn alle damit verbundenen technischen, organisatorischen und rechtlichen Aspekte berücksichtigt werden. Diese sind beispielsweise:

- **Heterogene Endgeräte:** Technische und organisatorische Unterstützung der unterschiedlichen Plattformen und Betriebssysteme (Rollout, Support, etc.)
- **Eigentum:** Festlegen der Eigentumsverhältnisse, insbesondere den Rechten und Pflichten des Mitarbeiters im Falle von Verlust oder Missbrauch des Gerätes oder forensischen Untersuchungen in einem Schadensfall.
- **Nutzungsbestimmungen:** Festlegen der Rechte und Pflichten des Mitarbeiters im Umgang mit dem Gerät, den Applikationen und den Daten.
- **Verfügbarkeit:** Festlegen der Supportprozesse im Falle eines defekten oder verlorengegangenen Gerätes.
- **Steuern:** Festlegen der steuerlichen Relevanz einer allfällig pauschalen Teilvergütung eines Gerätes

## Anforderungen an Betrieb und Sicherheit

Aus Sicht eines Unternehmens müssen die folgenden Anforderungen im Zusammenhang mit Verwaltung, Betrieb und Sicherheit von Smartphones erfüllt sein:

- Sichere und authentische Übermittlung der Unternehmensdaten
- Schutz der Unternehmensdaten bei Verlust des Smartphones
- Zugriff auf Unternehmensdaten nur durch berechtigte Personen und Applikationen
- Zentrale Administration (Profile, Remote Wipe, etc.)
- Ausschliesslich verschlüsselter Backup der Unternehmensdaten
- Einfacher und sicherer Rollout
- Hohe Benutzerfreundlichkeit
- Keine (oder möglichst geringe) Einschränkung der privaten Anwendungen (Spassfaktor)

Zudem muss sichergestellt sein, dass private Apps keinen Zugriff auf Unternehmensdaten erhalten. Besonderes Augenmerk gilt hierbei der gezielten Weitergabe und Verwendung von Adress-, Kalender- oder E-Mail-Daten durch einzelne Apps. Die Weitergabe von solchen Daten kann sogar durch den Benutzer gewollt sein, um eine Applikation in einer Gemeinschaft (Community) einsetzen zu können. Aus Sicht eines Unternehmens 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 und private Zwecke nutzen kann.

## Trennung der Daten und Applikationen

Ein Lösungsansatz, der sich mehr und mehr durchzusetzen vermag, ist die konsequente Trennung von geschäftlichen und privaten Daten und Applikationen.

Ein Beispiel hierfür ist die Sicherheitslösung von Good Technology. Sie besteht aus eigenständigen Applikationen für den Zugriff auf E-Mail, Kontakte oder Kalendereinträge, die im gewohnten Look and Feel des jeweiligen Endgeräts genutzt werden können. Dies garantiert die sichere Übermittlung und Speicherung der Unternehmensdaten auf dem Smartphone und verhindert den Zugriff auf diese durch Drittapplikationen. Das Unternehmen kann, unabhängig von den jeweiligen Eigenschaften des Gerätes, seine jeweiligen Sicherheitsrichtlinien durchsetzen, während der Mitarbeiter keine Einschränkung in seiner privaten Nutzung des Geräts erfährt. Integriert wird die Lösung über eine serverseitige Komponente, welche die Daten über Push-Technologie sicher und authentisch mit den jeweiligen Geräten synchronisiert. Der Rollout erfolgt dezentral durch den kostenlosen Download der Applikation sowie der sicheren Aktivierung durch die Eingabe spezifischer Sicherheitsmerkmale. □

