Mobile (Un-)Sicherheit im Unternehmen durch Smartphones

Smartphoneverlust mit Unternehmensdaten - was nun?

Mobiles Business heißt überall und immer Daten mobil vorzuhalten. Die Zahl mobiler Endgeräte wächst rasend schnell. Allein in Deutschland gab es 2011 bereits 11,5 Mio. Mobile Devices.

Die Unternehmen haben meist keine Regel (Policy) für die Handhabung der Smartphones, iPads usw., noch weniger sind die Prozesse - wie die Ausgabe eines mobilen Endgerätes an einen Mitarbeiter - standardisiert.

Eine wesentliche Herausforderung liegt zu einem in der Automatisierung der Ausgabe von Geräten an Mitarbeiter. Jedem Mitarbeiter sollen bestimmte Apps und Sicherheitsstandards (z. B. Verschlüsselung und Authentifizierung) zugeordnet werden. Dazu muss im Vorfeld ein Regelwerk im Unternehmen erstellt werden. Das Regelwerk (Policy) beinhaltet u.a. Kennwortlänge, Art und Gültigkeitsdauer, erlaubte Apps, Verwendung von iCloud, Trennung von privaten Daten und Unternehmensdaten usw.

Das Endgerät soll dem Nutzer ja noch maximalen Nutzen und Spaß in der Anwendung bieten. Trotzdem müssen die Geräte gegen Datenverlust und Datendiebstahl (Data Loss Prevention / Data Leakage Prevention) geschützt werden, auch oder gerade wenn die Mitarbeiter ihre privaten Endgeräte mit ins Unternehmen bringen (Bring Your Own Device - BYOD).

Der Hauptfokus liegt in der Sicherheit des täglichen Betriebes. Über Smartphones und Tablets wird ständig auf interne Daten im Unternehmen zugegriffen, was zu einer Sicherheitslücke zum Beispiel durch ungeprüfte Apps führen kann. Dazu kommt noch das Risiko des Verlusts von Unternehmensdaten, wenn das mobile Endgerät einmal verloren geht oder gestohlen wird.

Der Datenschutz beim "Einloggen" in das Firmennetz wird über sichere Applikationstunnel hergestellt. Über eine Whitelist werden nur Apps auf dem Gerät zugelassen, die erlaubt sind. Durch die Anbindung über das amagu MDM Portal ist das Smartphone oder z. B. ein iPad jederzeit remote kontrollierbar. Der Administrator kann sehen, welche Apps installiert sind und ob Regelverstöße vorliegen. Bei Verlust eines Gerätes oder bei einem Regelverstoß können beispielsweise unternehmenskritische Daten "over the air" gelöscht werden.

Eine umfassende Lösung bietet die amagu GmbH. Der Roll-Out an die Mitarbeiter ist über das Softwareportal der amagu GmbH in einem individuell erstellten Workflow inkl. Nutzervereinbarung standardisiert, so ist in wenigen Minuten ein Gerät einsatzbereit und die Policy des Unternehmens auf dem Gerät installiert. Eine individuelle, zeit- und kostenintensive Installation ist nicht mehr erforderlich.
Sicherheit für Unternehmensdaten und bei Verlust

Das Unternehmen sollte für die Definition der von ihm benötigten Anforderungen professionelle Beratung von MDM-Topspezialisten in Anspruch nehmen. In einem ersten Schritt werden die Unternehmensrichtlinien gemeinsam definiert und dann in der IT-Infrastruktur des Unternehmens abgebildet. Danach erfolgt die Einweisung der Administratoren. Über das amagu-Portal kann auch ein "Laie" innerhalb weniger Stunden das Management der mobilen Geräte im Unternehmen übernehmen. Im Normalfall benötigt amagu vom Entschluss des Kunden bis zur kompletten Implementierung der technischen Lösung nicht mehr als drei Werktage.
Kosten

Die Kosten werden in der Regel pro Gerät und Monat abgerechnet. Dazu kommt lediglich der Beratungsaufwand für die Integration, sowie die Einweisung für die Administratoren. Der Einsatz einer Mobile-Device-Management Lösung im Full Managed Service gegenüber einer Inhouselösung lohnt sich nachweislich ab ca. 20 Geräten.

Die Vorteile einer Portallösung? Der Vorteil beim Einsatz der Portallösung liegt darin, dass weder für aufwendige Hard- und Software-Infrastruktur, noch in die äußerst spezialisierte Ausbildung des Service-Personals investiert wird. Die Innovationszyklen der führenden MDM-Anbieter liegen derzeit unter 3 Monaten, das heißt der Endkunde einer Full Managed Lösung kann auch ohne extremen Änderungs- und Anpassungsaufwand immer auf aktuelle Technik zugreifen. Der hauseigene Administrator hat die Kontrolle und kann jederzeit die Smartphones über ein Onlineportal selbst verwalten. Und das immer auf aktueller Backend-Technologie mit vollem Support des Dienstleisters amagu. Das spart Zeit und Kosten und entresst die Situation enorm.

Weitere Information erhalten Sie bei
amagu GmbH Richard-Strauss-Strasse 71
81679 München
tel: +49 89 4522 16-30
www.amagu.de
  amagu Mobile Security email: presse@amagu.de

Pressekontakt

amagu GmbH

Herr Tom Zeller
Richard-Strauss-Str 71
81679 München

amagu.de
presse@amagu.de

Firmenkontakt

amagu GmbH

Herr Tom Zeller
Richard-Strauss-Str 71

81679 München

amagu.de
presse@amagu.de

Die amagu GmbH ist exklusiv auf die Beratung und Bereitstellung von Services zu Mobile Device Management spezialisiert. Amagu bietet seinen Kunden
?Wahlfreiheit
?Unabhängigkeit
?Sicherheit
?Flexibilität
?Wirtschaftlichkeit

amagu arbeitet seit dem Jahr 2001 an Mobile Device Lösungen und baut damit auf mehr als 20 Mannjahre Erfahrung.

Anlage: Bild