

# Mobile Device Management

## Sicherheit und Mobilität im Einklang



Wie sicher sind die mobilen Endgeräte, mit denen Ihre Mitarbeiter auf die Geschäftsdaten und -systeme zugreifen? Was passiert, wenn sie verloren gehen oder gestohlen werden? Können Sie gewährleisten, dass kein Zugriff auf geschützte Firmendaten möglich ist? Mit unserem Mobile Device Management haben Sie Ihre mobilen Geräte fest im Griff!

### Verwaltung mobiler Geräte

Auf Smartphones und Tablets befinden sich immer mehr Firmendaten. Oft sind die Daten auf den mobilen Geräten nur mangelhaft geschützt.

Die am häufigsten auftretenden Schwachstellen sind

- ▶ Mangelnde Kontrolle
- ▶ Gefahr von Datenverlusten oder Datendiebstahl
- ▶ Gefahr vor Ausspionieren der Daten
- ▶ Steigende Kosten
- ▶ Fehlende Prozesse und Firmenrichtlinien
- ▶ Nicht genügend Informationen zur Nutzung
- ▶ Wildwuchs an Geräten

Wie gut Sie die mobilen Geräte im Griff haben, können Sie an Hand der folgenden Fragen sehr gut klären

- ➔ Wie sicher sind die mobilen Endgeräte, mit denen Ihre Mitarbeiter auf die Geschäftssysteme zugreifen?
- ➔ Was passiert, wenn sie verloren gehen oder gestohlen werden?
- ➔ Können Sie gewährleisten, dass kein Zugriff auf geschützte Firmendaten möglich ist?
- ➔ Dürfen die Mitarbeiter ihre privaten Geräte verwenden?
- ➔ Wie wird der Datenzugriff geregelt?
- ➔ Schränken Sie die verfügbaren Geräte ein oder lassen Sie den Mitarbeitern freie Wahl?

Mit unserem Mobile Device Management – kurz MDM – bieten wir Ihnen eine zuverlässig und einfach zu administrierende Lösung zur Verwaltung Ihrer mobilen Geräte, deren Sicherheit und Überwachung.

Unsere Lösung ist mehr als nur ein Mobile Device Management!

### Mobile Device Management

Für eine konsequente Umsetzung von Sicherheits- und Firmenrichtlinien auf mobilen Geräten ist ein MDM unerlässlich. Bringen Sie mit unserer Lösung Sicherheit und Mobilität in Einklang:

- ☑ Windows Phone, iOS und Adroid (inkl. Samsung Safe und KNOX)
- ☑ Managen und steuern Sie die Geräte einfach und komfortable
- ☑ Konfigurieren Sie Geräte Richtlinien und verteilen Sie diese drahtlos
- ☑ Setzen Sie eingebaute Sicherheitsfunktionen wie Passwörter und Geräteverschlüsselung mit Ihren Richtlinien ein
- ☑ Erstellen Sie gruppenbasierte IT-Sicherheitsrichtlinien
- ☑ Sperren Sie bei Verlust oder Diebstahl das Gerät vollständig.
- ☑ Löschung per Funkbefehl und Standortbestimmung.
- ☑ Trennung von privaten und Unternehmensdaten
- ☑ Einbindung privater (Bring-Your-Own-Device) Geräte
- ☑ Profile können ein Passwort, Restriktionen, WLAN, VPN, eMail, Anwendungen und mehr enthalten (je nach Betriebssystem unterschiedlich)
- ☑ Die Verwaltung erfolgt zentral über eine zentrale Webplattform



© ileezhun - fotolia.com

## Mobile Application Management

Smartphones laden geradezu dazu ein, Apps und Spiele herunterzuladen und Content zu nutzen, dies kann zu Sicherheitskonflikten führen und den Schutz der Unternehmensdaten gefährden.

Nicht jede App ist ungefährlich! Über Apps können sensible Daten abgegriffen und Daten ausgelesen, Gebühren verursacht, Malware ins Firmennetzwerk eingeschleust werden und schlicht „Zeitdiebe“ sein.

Mit dem Mobile Application Management erreichen Sie

- Eine sichere Verteilung von öffentlichen Apps und Unternehmens-Apps an einzelne Nutzer oder Gruppen
- Blacklisting von Apps, die gefährlich o. Zeitvergeudung sind.
- Management eines App-Verzeichnisses
- Compliance-Berichterstattung



© Melpomene - fotolia.com

## Anti-Malware u. WebFilterung

Für Android Geräte empfiehlt sich dringend eine zusätzliche Schutzsoftware gegen Malware. Sie haben optional die Möglichkeit Secure Anywhere von Webroot einzusetzen.

Im Hintergrund werden Apps und Dateien auf Viren, Spyware und Trojaner gescannt. Automatische Updates bieten bestmöglichen Schutz auch gegen die neuesten Sicherheitsrisiken.

- Optional und nur für Android Geräte (Powered by Webroot)
- Automatisches Scannen aller neu installierten Apps auf Malware
- Schützt den Anwender vor dem Zugriff aus bösartige Websites und blockiert Internetseiten nach Kategorien.
- Quarantäne für infizierte Geräte
- 0,50 € / Monat netto je Gerät

## Mobile Content Management

Ihre mobilen Mitarbeiter müssen schnell, einfach und sicher auf aktuelle Daten zugreifen können. In unserem MDM ist die passende Lösung integriert, aktuelle Informationen unverzüglich an die mobilen Geräte zu verteilen.

- Stellen Sie selektierte Dokumente zur Verfügung (z.B. Word-, Excel-, Powerpoint-, PDF-Dokumente)
- Verteilen Sie selbst erstellte Nachrichten, Grafiken, Videos oder Links
- Verschlüsselung aller Dateien sichert Dokumente und Daten
- Zugriffsfähiger Content wird im zentralen Repository gespeichert.

## Mobile eMail Management

Ideal für eine simple und automatische Einrichtung der eMail Accounts:

- Verteilung von eMail Einstellungen
- Steuerung des Zugriffs auf eMails über sichere eMail Gateways, basierend auf Gerätemerkmalen
- Unterstützt optional eMail Container wie Nitrodesk Touchdown (für Android)
- Selektive Löschung aller Unternehmens eMails, wenn ein Mitarbeiter das Unternehmen verlässt.
- Für Android Geräte empfehlen wir Nitrodesk Touchdown. Die Option kostet 0,50 € / Monat netto je Gerät

## Konfiguration & Rollout

Konfiguration, Inventarisierung und Rollout erfolgen zentral über das WebPortal, in dem ausführliche Anleitungen hinterlegt sind... und gibt es Fragen, steht Ihnen unser Support zur Seite.

Optional nutzen Sie den Brauner Telecom Managed Service: Erstkonfiguration, inklusive Benutzergruppen und Policies nach Ihren Vorgaben sowie Rollout übernehmen wir für Sie. Planen Sie neue Hardware einzusetzen, sind wir auf Wunsch bei der Beschaffung und Auswahl der Hardware behilflich. Für Erstkonfiguration und Rollout berechnen wir Ihnen für das 1. Gerät einmalig 29,99 € netto und für jedes weitere 9,99 € netto.

## Monitoring

Über das zentrale WebPortal lassen sich alle Geräte rund um die Uhr überwachen und steuern. Sie erhalten einen schnellen Überblick über sämtliche Geräte und Aktivitäten. Zusätzliche Reports bieten Ihnen aussagekräftige Fakten zu einzelnen Geräten.

## Backend-Integration

Die Integration von Directory-Services (Active Directory / LDAP) ermöglicht rollenbasierte Gruppen, die der vorhandenen Unternehmensstruktur nachgebildet sind.



© sdecorret - fotolia.com

## Tarif

-  24 Monate Mindestvertragslaufzeit
-  Je Gerät 3,65 € / Monat netto

So erreichen Sie uns:

**Brauner Telecom**

 0800 220 50 220

 support@brauner-telecom.de

www.brauner-telecom.de