Datentrennung auf Apple-Geräten

Eine Trennung von Daten in einen privaten und geschäftlichen Bereich ist sinnvoll, wenn ein Gerät nicht nur zur Arbeit verwendet wird, sondern auch für private Zwecke genutzt werden darf. Unternehmen schaffen damit einen Benefit für ihre Mitarbeitenden, indem sie diese Doppelnutzung ermöglichen. Bei Apple gibt es zwei Varianten der geschäftlichen und privaten Nutzung: **BYOD (Bring your Own Device)** und die **Einrichtung eines privaten Bereichs** auf Apple-DEP-Geräten.

Funktionsweise

Grundsätzlich basiert die Trennung der Bereiche auf einer Trennung der Apple IDs. Neben der privaten Apple ID wird auch eine durch die Firma oder Bildungseinrichtung verwaltete Apple-ID auf dem Gerät installiert. Dadurch werden Daten und Apps getrennt und haben keinen Zugriff auf den jeweils anderen Bereich.

Allgemein unterscheidet Apple zwischen zwei Arten von Apps:

- Apps, die vom MDM installiert werden (**Managed Apps**), die vom IT-Admin verwaltet werden können. Diese sind mit der Apple ID des Unternehmens verknüpft.
- Apps, die vom User aus dem Store geladen werden (**Unmanaged Apps**), die nicht mit dem MDM verwaltet werden können. Diese sind mit der privaten Apple ID verknüpft.

Voraussetzungen:

- Apple-DEP-Account für firmeneigene Geräte
- MDM zur Verwaltung des geschäftlichen Bereichs

MOBIVISOR

BYOD mit Apple-Geräten

BYOD bedeutet, dass der Mitarbeitende ein eigenes Gerät für die Arbeit nutzt. Dieses sollte dennoch den Sicherheitsstandards des Unternehmens genügen, damit es nicht zu DSGVO-Verstößen kommt. Grundsätzlich können alle iOS, iPads und MacBooks zu BYOD-Geräten gemacht werden.

Einrichtung:

Die Geräte sind mit einer privaten Apple ID eingerichtet. Der Endnutzer lädt sich die MDM Client App (zum Beispiel MobiVisor MDM) aus dem App Store herunter und registriert sich.
Auf dem Gerät wird ein eigener Arbeitsbereich eingerichtet. Dieser ist jedoch nicht extra gekennzeichnet. Nachdem das MDM-Profil erfolgreich installiert wurde, kann der IT-Admin Apps über das MDM auf dem Gerät installieren. Diese gelten als “managed Apps”.

Funktionsweise:

- Managed Apps, sowie MDM Client App können jederzeit vom Endnutzer entfernt werden
- IT-Admin kann Managed Apps per MDM Richtlinien verwalten
- Im MDM können vom Endnutzer heruntergeladene Apps eingesehen, aber nicht verwaltet oder deinstalliert werden
- Apps können Managed oder Unmanaged sein, existieren jedoch niemals doppelt auf einem Gerät

Hinweise zum Datenschutz:

- Verhindern Sie per Richtlinie das Kopieren von Daten von Unmanaged zu Managed Apps
- Deaktivieren Sie den Zugriff der Unmanaged Apps auf Managed Contacts
- Verbieten Sie das Öffnen von Inhalten aus Managed Apps in Unmanaged Apps
- Apps die auf einer Blacklist sind, können vom Endnutzer trotzdem als Unmanaged App heruntergeladen werden

Einrichtung eines privaten Bereichs auf Apple-Geräten

Als Apple-DEP-Geräte werden alle unternehmenseigenen Geräte bezeichnet, die über den Apple Business Manager dem Unternehmen und einem MDM Server zugeordnet wurden.
Das Gerät wird mit der unternehmenseigenen Apple ID eingerichtet und das MDM-Profil kann nicht entfernt werden.

Einrichtung:

Um einen privaten Bereich auf dem unternehmenseigenen Apple Gerät einzurichten, muss per MDM-Richtlinie erlaubt werden, dass der Endnutzer zusätzlich eine private Apple ID hinzufügen kann. Der Endnutzer kann dann Unmanaged Apps installieren.

Funktionsweise:

- Apps können auf Blacklist gesetzt werden, und können dann auch nicht vom Nutzer installiert werden
- MDM-Profil sowie Managed Apps können nicht vom Nutzer entfernt werden
- Auch hier gilt: Apps sind entweder Managed oder Unmanaged.
    - Unmanaged Apps können durch eine Managed App ersetzt werden, wenn dieselbe App per MDM installiert wird

Hinweise zum Datenschutz:

- Setzen Sie unerwünschte Apps auf eine Blacklist
- Nutzen Sie die Richtlinien des MDM um Zugriffe und Rechte der Endnutzer*innen zu verwalten und die Geräte DSGVO-konform einzurichten
- Mithilfe von Passcode-Richtlinien erhöhen Sie die Sicherheit der Geräte

Sie wünschen noch mehr Information oder haben Fragen zur Einbindung von Apple-Geräten im MDM?
Besuchen Sie unseren YouTube Channel @iotiq
Kontaktieren Sie uns per Mail: mds@iotiq.de

MOBIVISOR