Möglichkeiten des Mobile Device Management (MDM)

Sie können darauf vertrauen, dass Ihre Privatsphäre geschützt ist

Das folgende Dokument soll über grundsätzliche Möglichkeiten des Mobile Device Management des Gymnasiums „In der Wüste“ aufklären. Alle Nutzer, welche ein persönliches Gerät in das MDM einbinden lassen, stimmen der Fremdwartung der Geräte zu. **Das Gymnasium „In der Wüste“ übernimmt keine Haftung für Schäden am Gerät oder Datenverlust, der eventuell durch die Anwendung des MDM am Gerät hervorgerufen wird.** Vor der Einrichtung des MDM empfehlen wir die Erstellung eines Backups des Gerätes. Nach der Einbindung in das MDM können Anwender weiterhin eigenständig die besten Werkzeuge für ihre Arbeit auswählen und nutzen. Die Benutzerfreundlichkeit oder die Privatsphäre werden nicht beeinträchtigt.

Das Gymnasium „In der Wüste“ setzt auf benutzereigene Geräte

In Unternehmen wurden folgende Erfahrungen gemacht: Wenn Benutzerinnen und Benutzern gestattet wird, ihre Geräte mit ihren eigenen Apple-IDs zu personalisieren, übernehmen sie mehr Eigenverantwortung. Der Schlüssel für eine erfolgreiche mobile Strategie ist dann ein ausgewogenes Verhältnis zwischen Steuerung durch das Gymnasium „In der Wüste“ und Selbstbestimmung durch die Benutzerin/der Benutzer. Indem Benutzer/innen ihre iOS Geräte mit eigenen Apps und Inhalten personalisieren, übernehmen sie mehr Eigenverantwortung, was wiederum zu mehr Engagement und einer höheren Produktivität führt. Ermöglicht wird dies durch die Verwaltungsarchitektur von Apple: Sie bietet intelligente Möglichkeiten, um schuleigene Daten und Apps diskret zu verwalten und berufliche und private Daten nahtlos voneinander zu trennen. Zudem haben die Benutzer/innen auf diese Weise Kenntnis davon, wie ihre Geräte verwaltet werden.

Möglichst geringe Eingriffe

Durch die Nutzung der MDM-Lösung von IServ ist die Schule in der Lage, die nötigen Aspekte mit möglichst geringen Eingriffen zu verwalten– ohne dass Features gesperrt oder Funktionen deaktiviert werden müssen. Die Verwaltungsarchitektur von Apple ermöglicht eine fein abgestufte Kontrolle der Geräte und von der Schule bereitgestellter Apps. Vor allem aber haben die Eigentümer/innen der Geräte weiterhin keine Beeinträchtigung ihrer Privatsphäre.

Das Gymnasium „In der Wüste“ kann Apps zentral installieren

Mit MDM installierte Apps werden als „verwaltete Apps“ bezeichnet. Dabei kann es sich um kostenlose oder kostenpflichtige Apps aus dem App Store oder um eigene, interne Apps handeln. All diese Apps können drahtlos per MDM installiert werden. Kostenlose wie kostenpflichtige Apps als verwaltete Apps werden von der Schule gekauft und verteilt. Selbstverständlich entstehen den Eigentümern der Geräte ohne vorherige Einwilligung der Kostenübernahme keine Kosten bei verwalteten Apps.

Der MDM-Server kann verwaltete Apps und die zugehörigen Daten installieren, bei Bedarf entfernen oder angeben, ob die Apps gelöscht werden sollen, wenn das MDM-Profil entfernt wird. Darüber hinaus kann der MDM-Server das Sichern von Daten verwalteter Apps in iTunes und iCloud unterbinden.

Die Benutzer/innen werden benachrichtigt, wenn Apps zur Installation auf ihren Geräten bereitstehen.

Die Schule kann zu keinem Zeitpunkt auf private Daten zugreifen

Bei der verwalteten App-Konfiguration nutzt MDM die native iOS Verwaltungsarchitektur, um Apps während oder nach der Implementierung zu konfigurieren. Diese Architektur gestattet es Entwicklern, Konfigurationseinstellungen festzulegen, die angewandt werden sollen, wenn ihre App als verwaltete App installiert wird.

Wenn Geräte von den Benutzern/innen gekauft und eingerichtet werden, können die Geräte dennoch Zugriff auf Dienste im Schulgebäude wie das schuleigene WLAN erhalten. Die Benutzer/innen müssen sich für die Registrierung bei der MDM-Lösung des Gymnasiums „In der Wüste“ durch einen Admin von IServ anmelden lassen. Dafür muss der Admin sich einmalig mit seinen Daten persönlich auf dem Gerät bei auf der Plattform IServ einloggen und das Gerät dann freigeben. Dieser Vorgang dauert eine Minute.

Volle Kontrolle – für die Besitzer/innen der Geräte

Wenn sich Benutzer/innen auf einem iOS Gerät zum ersten Mal bei MDM registrieren, werden sie darüber informiert, auf welche Inhalte auf ihrem Gerät der MDM-Server zugreifen kann und welche Features er konfigurieren wird. Dies bietet den Benutzern/innen Transparenz im Hinblick auf die Frage, welche Aspekte verwaltet werden.

Es ist wichtig zu wissen, dass sie die Registrierung im MDM jederzeit rückgängig machen können, indem sie das Verwaltungsprofil vom Gerät entfernen, wenn sie diese Art der Verwaltung nicht wünschen. Dadurch werden alle per MDM installierten Schul-Accounts und -Apps entfernt.

Nachdem Benutzer/innen bei MDM angemeldet sind, sehen sie in den Einstellungen auf einen Blick, welche Apps und Accounts verwaltet werden und welche Einschränkungen implementiert wurden. Alle mit MDM installierten Einstellungen, Accounts und Inhalte des Unternehmens werden von iOS als „verwaltet“ gekennzeichnet.

Die Schule kann eigene Accounts, Einstellungen und Daten verwalten, welche per MDM bereitgestellt werden, doch auf die persönlichen Accounts der Benutzer/innen kann nicht zugegriffen werden.

Die folgenden Beispiele zeigen, welche Daten ein MDM-Server eines anderen Anbieters von einem persönlichen iOS Gerät abrufen kann und welche nicht.

Im MDM sichtbar:
- Gerätename
- Kapazität und freier Speicherplatz (nur bei Anschluss an den Apple Configurator 2, nicht über IServ)
- iOS Versionsnummer
- vom MDM installierte Apps
- Seriennummer
- Modellname und -nummer

Private Daten, die für MDM nicht sichtbar sind:
- Private und geschäftliche E-Mails, Kalender, Kontakte
- iMessages
- Safari Browserverlauf
- Protokolle von FaceTime
- Persönliche Erinnerungen und Notizen / gespeicherte Daten
- Häufigkeit der Nutzung von Apps
- Standort des Gerätes
- insgesamt installierte Apps
- Fotos u. a.

Mögliche Einschränkungen während des Schulbesuches:
- Das Betriebssystem iOS unterstützt die folgenden Einschränkungskategorien, die drahtlos konfiguriert werden können, um die Anforderungen der Schule etwa in Prüfungen ohne nachhaltige Beeinträchtigung der Benutzer/innen zu erfüllen:
- App-Installation
- App-Nutzung
- Classroom App
- Einschränkungen für Benutzer/innen und Benutzergruppen
- Safari
- Siri

Wenn ein Gerät verwaltet wird, kann eine Vielzahl von Verwaltungsaufgaben über einen MDM-Server ausgeführt werden, z. B. das automatische Ändern von Konfigurationseinstellungen ohne Benutzereingriff, die Durchführung eines iOS Updates auf mit einem Code gesperrten Gerät, das Sperren oder Löschen eines Geräts per Fernzugriff oder das Deaktivieren der Code-Sperre, sodass Benutzer vergessene Passwörter zurücksetzen können. Ein MDM-Server kann ein iOS Gerät auch anweisen, mit der AirPlay-Bildschirmsynchronisation an ein bestimmtes Ziel zu beginnen oder eine laufende AirPlay-Sitzung zu beenden.

Diese Kann-Optionen werden jedoch im Regelfall nicht durchgeführt. Der Zugriff auf Geräte dient ausschließlich der Kontrolle der Geräte in Unterrichts- oder Prüfungssituationen.

Zusammengefasst/kopiert aus:
https://www.apple.com/de/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf

https://support.apple.com/de-de/guide/deployment-reference-ios/welcome/web