Umsetzungshinweise für die Einführung eines MDMs

- Apple-Geräte

Verwaltung mit dem Apple School Manager und einem nachgeordneten MDM

Zur korrekten Einrichtung einer zentralen Verwaltung werden mehrere Schritte benötigt:

  - Registrierung der Schule beim Apple School Manager
    Vorbereitend beantragt die Schule einen kostenlosen Zugang zum Apple School Manager. Pro Schule kann nur ein Zugang beantragt werden, die angegebenen Daten werden von Apple in der Regel telefonisch überprüft.
    Außer bei der Festlegung der Verantwortlichen an der Schule sollten bei der Registrierung keine personenbezogenen Daten (E-Mail-Adressen) verwendet werden.
  - Händler ID eintragen
    Zertifizierte Apple Partner besitzen eine Händler ID, die bei der Grundkonfiguration des School Manager Zugangs der Schule eingetragen werden muss. Anschließend kann der Händler bei ihm gekaufte Geräte im School Manager Account der Schule registrieren.
    Registrierte Geräte können einer MDM Lösung zugewiesen werden.
    Eine nachträgliche Registrierung von Geräten erfordert zusätzliche Schritte vom Administrator der Schule.
  - Herstellen der Verbindung zum MDM
    Die gewählte MDM-Lösung muss mit dem Apple School Manager verbunden werden. Dies geschieht durch wechselseitiges Erzeugen und Hochladen von Token bzw. Zertifikaten. Diese Zertifikate müssen nach einer gewissen Zeitspanne wieder erneuert werden.
  - Gerätekonfiguration

    Endgeräte werden nach der Aufnahme in die MDM-Lösung über zugewiesene Profile konfiguriert. iOS Updates und didaktische Funktionen stehen (je nach MDM-Lösung) zur Verfügung.

  - Zuweisen von Accounts
    Die Schule muss sich für ein Konzept mit oder ohne Anmeldung zur Verwendung der Endgeräte entscheiden (Mehrbenutzernutzung, Gerät an Benutzer zugeordnet, Geführte Zugänge, SCIM)
  - Zuweisen von Apps
    Apps für mobile Geräte können im Apple School Manager erworben werden. Die Schule kann dabei von erheblichen Rabatten für den Bildungsbereich profitieren (beim Erwerb größerer Stückzahlen).
    Apps können Geräten oder Benutzern zugewiesen werden und über die MDM-Lösung installiert und auch deinstalliert werden.

Datenschutzrechtlicher Hinweis für das „Geteilte IPad“:

  - Bei der Verwendung des "Geteiltes iPad"-Modus werden während der Benutzersession personenbezogene Daten erzeugt, welche gemeinsam mit erzeugten Inhalten, wie zum Beispiel Dokumenten oder Bildern, in der iCloud gespeichert werden.
  - Die Authentisierung am IPad erfolgt über eine zentral verwalteten Apple ID (Managed Apple IDs. Die Apple IDs müssen daher bei dieser Variante angemessen pseudonymisiert sein.

- Windows-Geräte

Für Windows-Geräte bietet sich vor allem Microsofts eigenes MDM „Endpoint Manager“ (ehemals „Intune“) an. Von anderen Anbietern sind (Stand: Ende 2021) keine vergleichbaren Lösungen verfügbar.

- Die Schule muss zunächst über einen „Microsoft-Tenant“ verfügen. So wird das Hauptkonto der Schule bezeichnet, in dem alle Geräte, Benutzer und Einstellungen verwaltet werden.
- Geräte können diesem Tenant über verschiedene Methoden hinzugefügt werden:
  - Registrierung neuer Geräte beim Kauf durch den Händler (empfohlen)
  - Hinzufügen vorhandener Geräte im Rahmen einer Neuinstallation von Windows (z.B. durch Anmelden mit einem „Geräteregistrierungsmanager“ oder durch Installation mit einem speziell dafür vorbereiteten USB-Stick)
  - Hinzufügen bereits in Verwendung befindlicher Geräte ohne Neuinstallation durch ein „Bereitstellungspaket“, das mit dem „Windows Configuration Designer“ erzeugt werden kann.

  Die letzten beiden Möglichkeiten sind mit zusätzlichem Aufwand seitens der Schule bzw. des IT-Dienstleisters verbunden.
- Nach erfolgreicher Aufnahme in die MDM-Lösung können die Geräte zentral verwaltet werden.

- ChromeOS-Geräte
  - Geräte mit dem Betriebssystem ChromeOS sind für das webbasierte Arbeiten ausgelegt und benötigen einen stabilen Zugriff auf das Internet.
  - Zentral verwaltet können die Geräte über die kostenlos nutzbare Google Admin Konsole werden. Hier können verwaltete Google Konten neben Gastsitzungen konfiguriert werden. Für registrierte Geräte ist eine einmalige Lizensierung notwendig. Diese Lizenzen sollten zusammen mit den Geräten gekauft werden.
  - Die Verwendung von Google Konten (zusammen mit Google Workspace for Education) ist ebenfalls möglich.
  - Die meisten Programme laufen als Web-Anwendungen, deren Daten werden standardmäßig in der Google-Cloud gespeichert.
- Android-Geräte
  - Aktuelle MDM-Lösungen für Android, welche separat erworben bzw. lizensiert werden müssen, nutzen meist Android Enterprise.
  - Es ist zu beachten, dass nur bestimmte Geräte bzw. Android-Versionen unterstützt werden. Eine Auswahl an Geräten und die dazu passende MDM-Lösung mit dem jeweiligen Funktionsumfang findet man z.B. hier.
  - Bei der Konfiguration eines Mehrbenutzermodus muss beachtet werden, dass nach der Abmeldung des Benutzers keine personenbezogenen Daten auf dem Gerät verbleiben dürfen.

HINWEIS:

Eine angemessene und geeignete Pseudonymisierung der verarbeiteten personenbezogenen Daten muss beachtet werden. Zudem ist dem Grundsatz der Datenminimierung Rechnung zu tragen.