Handreichung MDM – Mobile Device Management

Einsatzbereiche, Vorteile, Risiken

Einordnung Muster-IT-Konzept

Modul: Ausstattung Hard- und Software
Baustein: Muster Ausstattungskonzepte „Mobile Device Management“

Version: V. 1.0

Zweck

Die Handreichung MDM – Mobile Device Management – gibt einen Überblick über die Einsatzbereiche, Vorteile und Risiken von MDM-Systemen. Zudem werden Kriterien für die Auswahl eines passenden MDM-Systems vorgestellt.

Die Handreichung gibt Hinweise, wie ein Mobile Device Management in die schulische IT eingebunden werden kann. Dabei werden die Funktionalitäten und der Nutzen in der Administration der schulischen Endgeräte dargelegt. In einem anhängenden Glossar werden relevante Begriffe erläutert.

Anwendungsempfehlungen

- Entscheidungshilfe zur Nutzung und zum Einsatz eines Mobile Device Managements
- Grundlage für die Umsetzungsplanung eines Ausstattungskonzepts mit mobilen Endgräten mit Hilfe eines MDM-Werkzeugs

---

Das vorliegende Dokument im Muster-IT-Modul *IT-Ausstattung* wurde im Auftrag des Bundesministeriums der Finanzen (BMF), im Rahmen einer Ressortforschung, finanziert aus Mitteln des Deutschen Aufbau- und Resilienzplans (DARP), erstellt.

Finanziert von der Europäischen Union
NextGenerationEU

Haben Sie Feedback zu den Umsetzungshilfen für uns? Fehlt Ihnen in den Umsetzungshilfen noch etwas?
Haben Sie Anregungen zur Verbesserung? Wünschen Sie sich weitere Umsetzungshilfen?
Ihre Rückmeldungen sind für uns wichtig, da die Umsetzungshilfen kontinuierlich überarbeitet werden.
Wir freuen uns auf Ihre Rückmeldung.

Herausgeber: PD – Berater der öffentlichen Hand GmbH
Friedrichstr. 149
10117 Berlin
https://www.pd-g.de/

Kontakt: SchuleDigital@pd-g.de

Stand: 26.01.2024

1 Einordnung: Was ist ein Mobile Device Management?

Mobile-Device-Management (MDM) ist ein Begriff aus der Informationstechnologie und steht **für zentralisierte Verwaltung von mobilen Endgeräten**. MDM-Systeme zählen zu den Softwarelösungen und werden dediziert für die Verwaltung von Endgeräten genutzt. Teilweise bilden andere Software-Lösungen, wie ERP- und ITSM-Lösungen, Funktionen eines MDM ab. Häufig bieten Hersteller von mobil eingesetzter Hardware eigene Lösungen zur Verwaltung ihrer Geräteangebote an, was einerseits eine tiefer gehende technische Verwaltung ermöglicht, andererseits jedoch den Ausschluss hersteller-fremder Gerätetypen bedingt.

Neben MDM-Lösungen kommen in Organisationen auch breiter gefasste und sehr spezialisierte Ausprägungen des MDM zum Einsatz. Dazu zählen zum Beispiel EMM- (Enterprise Mobility Management) und MAM-Lösungen (Mobile Application Management) zum Einsatz. EMM-Lösungen verfolgen einen umfassenderen Ansatz, der MDM-Funktionalitäten einschließt, aber darüber hinausgeht. EMM umfasst MDM, MAM (Mobile Application Management) und andere Aspekte wie Mobile Content Management (MCM) und Mobile Identity Management. [1]

Neben dem **Geräte-Management mittels MDM** sind vor allem **MAM-Lösungen (Mobile Application Management)** gebräuchlich, die sich primär auf die Verwaltung und Sicherheit von Anwendungen auf mobilen Geräten fokussieren. Ein MAM unterstützt das mobile Anwendungsmanagement gemäß dem Lebenszyklus von (mobilen) Anwendungen, wie der Installation, Aktualisierung und dem Rückbau.

Die Kernfunktionen eines MDM sind in Abgrenzung zum EMM und MAM:

- **die Geräteverwaltung (auch als Asset-Management bezeichnet)**
- **das Gerätemanagement, was sich am Lebenszyklus eines Geräts von der Beschaffung, Einrichtung, Inbetriebnahme, Aufrechterhaltung im Betrieb bis hin zur Aussonderung orientiert**
- **das Sicherheitsmanagement des Geräts, was durch die Besonderheit des mobilen Einsatzes als besondere Anforderung anzusehen ist und**
- **das Multi-User-Management, wenn Geräte nicht nur von einer Anwenderin oder eines Anwenders genutzt wird und**
- **der Fernzugriff auf das mobile Endgerät.**

Teilweise enthalten die MDM-Lösungen auch Elemente des IT-Service Managements (ITSM), womit Störungen (Incidents) und Änderungsanträge (Service Request bzw. Changes) in der Lösung selbst und nicht durch eine Drittlösung prozessiert werden können.

Komplexere MDM-Lösungen bieten darüber hinaus ebenfalls ein Network Service Management an, was eine Konfiguration der Zugriffsmöglichkeiten für die mobilen Endgeräte inkludiert. Auch hinter Bezeichnungen bzw. angebotenen Lösungen wie UEM (Unified Endpoint Management), EMM (Enterprise Mobility Management) oder mit etwas spezieller Ausrichtung MAM (Mobile Application Management) verstecken sich im Kern MDM-Funktionalitäten.

Im Kern zählen zu den zu verwaltenden Geräteklassen folgende Gerätetypen:

[1] Vergleichen Sie dazu die Definitionen und Erklärungen in dem Glossar.

2 Entscheidungsfindung: Anforderungserhebung an ein MDM für die schulische IT

Der zunehmende Grad an Digitalisierung schlägt sich u.a. in dem Zuwachs an Endgeräten und komplexeren Netzwerken in den Schulen nieder. Eine angemessene Verwaltung dieses quantitativen Anstiegs ist notwendig, deshalb schauen verantwortliche Institutionen – meist IT-Abteilungen – wiederum auf geeignete Werkzeuge, um den Prozess der Geräte- und Netzwerkverwaltung bestmöglich zu automatisieren bzw. selbst zu digitalisieren.

Zunächst sollte die Frage beantwortet werden, ob es eines neuen Werkzeugs – im Weiteren einer MDM-Software bedarf – oder ob in bestehenden Lösungen durch einen vertretbaren Anpassungsaufwand (engl. Customizing) die klassischen Funktionen eines MDM abgebildet werden können. Wenn für die Entscheidungsfindung die oben aufgeführte Liste an Kernfunktionen nicht ausreicht, empfiehlt sich eine vertiefte Anforderungsanalyse.

Die detaillierte Analyse der Anforderungen erweist sich als förderlich für die Beschaffungsprozesse, weil sie der nachträglichen Verwendung in der Leistungsbeschreibung dienen kann. In der anschließenden Testphase gewinnt diese Analyse an Bedeutung, da sie eine unkomplizierte Ableitung von Testfällen aus den definierten Anforderungen ermöglicht.

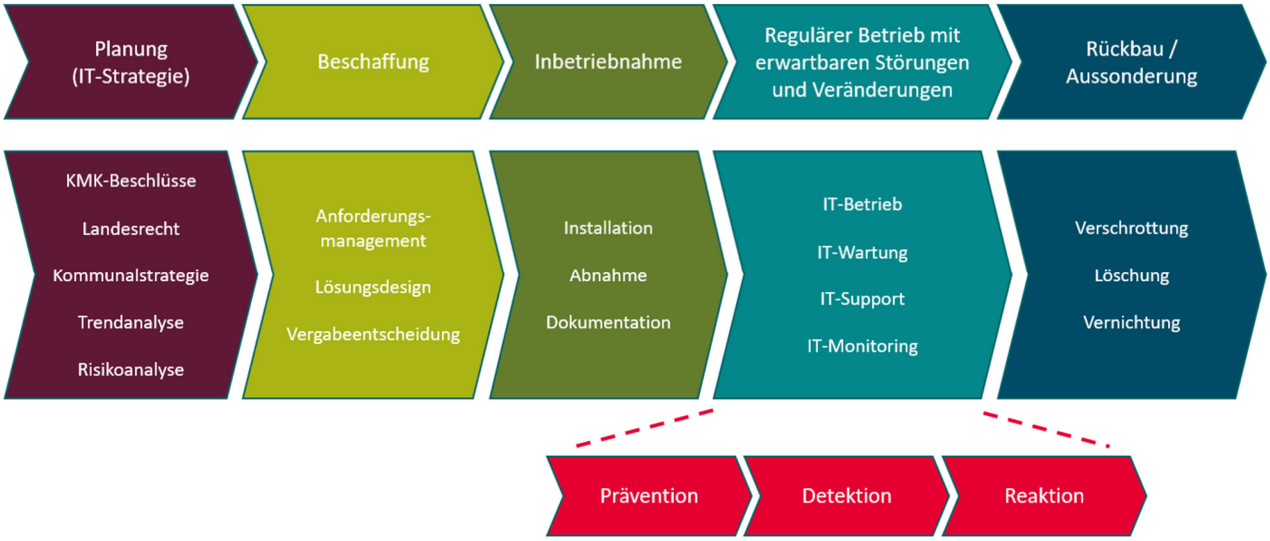
Zu klären ist die Frage, ob die Geräteverwaltung von schulisch genutzten Geräten und von Geräten für die Kernverwaltung getrennt zu erfolgen hat oder ob beide Anwendergruppen in ein und derselben MDM-Lösung mittels Mandantentrennung verwaltet werden sollen. Sobald technische Komponenten von beiden Anwendergruppen genutzt werden, zahlt sich ein gemeinsames MDM aus. Ein weiterer Pluspunkt sind die Kenntnisse und Fähigkeiten der IT-Mitarbeitenden, die bereits mit MDM versiert sind und bei einer gemeinsamen Nutzung des MDM bereichsübergreifend und gegenseitig den Betrieb des MDM sicherstellen können.

Für eine Trennung der MDM-Lösungen von schulischem und Kernverwaltungsbereich spricht die besondere Support-Struktur im schulischen- und vor allem pädagogischen Bereich durch die Einbindung der Lehrkräfte.

Die Funktionalität eines oder mehrerer MDM-Systeme orientiert sich am Lebenszyklus des mobilen Endgeräts, der folgend dargestellt wird.

2.1 Funktionsübersicht und Einsatzszenarien

Die Kernfunktionen eines MDM orientieren sich am Lebenszyklus der verwalteten Endgeräte.



Klassisches Lebenszyklusbild einer IT-Hardware-Komponente (Handreichung 2 – Informationssicherheit – Schule im IT-Betrieb)

Sind die ersten Phasen des Lebenszyklus eines Endgerätes durchlaufen, muss in der **Phase der Inbetriebnahme** eine dokumentierte Prozedur zur Ausgabe / Verteilung der Geräte an die Nutzenden geben. Im Rahmen dieser Prozedur wird das Gerät registriert, das zugrundeliegende Betriebssystem noch einmal aktualisiert, eingerichtet und ausgegeben. Im Zuge der Einrichtung werden insbesondere die für die Installation von Anwendungen und weiteren Services notwendigen Schritte der Anmeldung des Endgeräts am MDM umgesetzt.

Die Registrierung (in einer Asset- oder Inventardatenbank), die Aktualisierung und die Einrichtung zählen zum klassischen Funktionsumfang eines MDM. Durch einen vorausschauend geplanten Inventarisierungsprozess wird auch der ungewollte Nicht-Einsatz von Endgeräten minimiert. Ist die Inventar-/Asset-Datenbank mit dem MDM verbunden, lässt sich über Auswertungen aufzeigen, welche ausgegebenen Geräte noch gar nicht im Einsatz waren.

Ist das mobile Endgerät ausgegeben, steht das Bestreben eines störungsfreien Betriebs im Vordergrund. Um dieses besonders aus der Perspektive der IT-Sicherheit zu gewährleisten, erfolgen im Hintergrund regelmäßige Aktualisierungen des Betriebssystems und weiterer genutzter Softwarelösungen. Das MDM unterstützt bei der Steuerung dieser Aktualisierungen mit einem hohen Automatisierungsgrad.

Darüber hinaus ermöglichen **MDM-Lösungen die aktive Steuerung des Einsatzes des mobilen Endgeräts**. Vor allem bei einer Mehrfachnutzung von mobilen Endgeräten im Schulbetrieb erweisen sich viele Funktionen als hilfreich, wie zum Beispiel:

- **die Gesamtnutzungsdauer des Geräts,**
- **konkrete Nutzungszeitfenster mit festen Pausen,**
- **unterschiedliche Profile, wie z. B. ein „Unterrichts-Profil", ein „Pausen-Profil" und ein Heimarbeitsprofil,**
- **individuelle Konfigurationen,**
- **aktive Sperrung des Geräts durch die Administratoren oder berechtigte Dritte – bis hin zur Deaktivierung (=Unbrauchbarmachung) des gesamten Geräts, sodass eine Rückgabe forciert werden kann,**
- **Anwendungsverwaltung einschließlich Rechte- und Zugriffsmanagement,**
- **Internetfilter,**
- **Übertragung von Nachrichten auf das Gerät,**
- **Datensicherungen,**
- **Ortungsfunktion und**
- **Berichtswesen.**

Eine wesentliche **Kernfunktion zur Aufrechterhaltung eines sicheren Betriebs der mobilen Endgeräte ist das Policy Enforcement** (dt.: Das Arbeiten mit einem strengen, technischen Regelwerk), das der Stärkung bzw. Durchsetzung von Richtlinien – was ist mit dem Gerät erlaubt und was ist verboten - dient. Damit wird über technische Richtlinien eine **Rechte- und Rollenverwaltung** umgesetzt, die bezogen auf die zu verwaltenden Geräte Funktionen ermöglicht, wie etwa

- **Erkennen des Betriebssystems (Version, installierte Apps, manipulierte Daten, usw.)**
- **Erkennen, ob das Gerät mit einer nicht-legitimen Betriebsversion (auch als „jail-break" bezeichnet) betrieben wird**
- **Filtermanagement mit dem Ziel, nur vertrauenswürdigen Quellen (andere Geräte) zuzulassen**
- **Verwaltung von Einschränkungen zum Download von Anwendungen**
- **Verwaltung von Einschränkungen in benannten Stores (Marktplätze für mobile Endgeräte)**
- **Verwaltung des Datenvolumens**
- **Verwaltung von Containern, um zwischen Verwaltungs- und privaten Daten zu unterscheiden**
- **Erkennen von Regelbrüchen und Verstößen (u. a. Nutzung des Geräts in nicht zugelassenen Umgebungen, wie z. B. Roaming).**

Kommt es hingegen zu einer Störung am mobilen Gerät, können vorsorglich vor Wartungs- und Reparaturleistungen weitere Steuerungsaktivitäten mittels des MDM unternommen werden. Dazu zählen

- **die Löschung aller Daten**
- **das komplette Zurücksetzen des Geräts**
- **die Anfertigung von Back-ups und die Wiederherstellung der Daten**
- **die Ausfertigung von Auditprotokollen und**
- **die Remote-Sperre.**

Zu den Störungen zählen auch der Diebstahl und der Verlust des Geräts. Die Steuerungsoptionen während einer Störung des Geräts dienen primär dem Schutz vor dem Abfluss von auf dem mobilen Endgerät befindlichen Daten und andererseits die Wiederherstellung für einen zügigen Einsatz.

Um die Geräte mit dem Mobile-Device-Management zu verwalten, verfügt die Managementsoftware über eine Vielzahl administrativer Funktionen, die in einem zentralen Portal bereitgestellt werden. Dadurch wird der Bestand an mobilen Geräten verwaltet, die Bedienung der Geräte weitestgehend vereinheitlicht und die Sicherheit der Daten auf den mobilen Geräten gewährleistet.

Gerade bei den gegenwärtigen Zuwächsen an schulischen IT-Geräten bietet sich eine MDM-Lösung für die initiale Inventarisierung an. Aber auch im weiteren Einsatz, insbesondere, wenn mobile Geräte temporär Schülerinnen und Schülern zugewiesen werden, zahlen sich die administrativen Möglichkeiten eines MDM aus. Anderes kann der notwendige Überblick über den Bestand an ausgegebenen Geräten kaum gewährleistet werden.

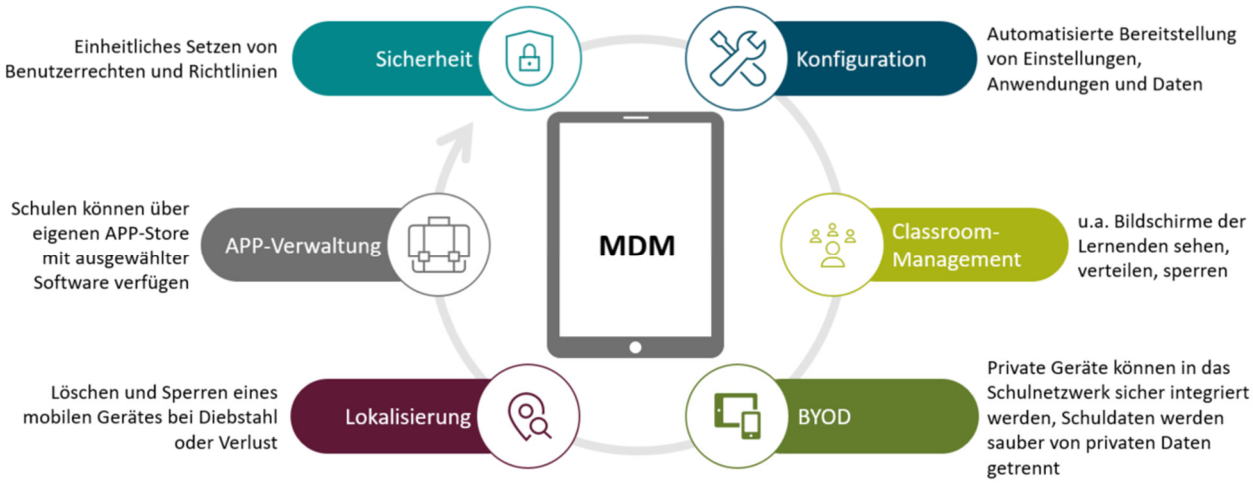
Bei der Aufrechterhaltung der IT-Sicherheit spielen MDM-Lösungen gleichfalls eine zentrale Rolle. Dadurch, dass der Einsatz eines mobilen Endgeräts geradezu vorsieht, dass sich das Gerät „bewegt“ und in diverse Netzwerke einloggen kann, stellt jedes unbekannte Netzwerk einen potenziellen Angriffsvektor dar. Ohne eine effektive MDM-Lösung würden mobile Geräte leichtes Ziel von Angriffen werden.

Zusammenfassend kann festgehalten werden, dass ein MDM grundsätzlich die Möglichkeit bietet, mobile Geräte schnell und einfach zu konfigurieren. Die einzelnen MDM-Lösungen divergieren in ihrem Ansatz, wobei die größte Einschränkung in der Unterstützung unterschiedlicher Gerätetypen und Betriebssysteme festzustellen ist. Je nach Implementation des MDM hilft die Software, signifikant Zeit und Kosten zu sparen.

Ein zusätzlicher Mehrwert kommt dem MDM zu, wenn Einrichtungen sich für das Konzept des „Bring-Your-Own-Device“ entscheiden. In diesem Fall unterstützt das MDM bei der Trennung von privatem und schulischen Bereich (u. a. durch Container oder Tresore) auf dem mobilen Endgerät.

Weitere Infos zu Ausstattungsoptionen können in dem Muster-Ausstattungskonzept nachgelesen werden.

Die folgende Grafik fasst wesentliche **Funktionsbausteine eines MDM** zusammen:



2.2 Vorteile und Risiken in der Nutzung einer MDM-Lösung

Der große Vorteil von Mobile-Device-Management-Lösungen ist die Möglichkeit, mobile Endgeräte wie Smartphones, Tablets, Laptops etc. trotz unterschiedlicher Betriebssysteme (iOS, Android, Windows, Chrome OS, macOS) konfigurieren zu können. Die Integration unterschiedlicher Betriebssysteme ist jedoch mit einem erhöhten Aufwand verbunden und muss von der MDM-Lösung auch unterstützt werden.

Für Schulen und Schulträger ergeben sich wie oben beschrieben viele Vorteile bei den Arbeitsabläufen, insbesondere durch den ortsunabhängigen Zugriff auf Daten und Geräte. Als weitere Vorteile gelten die Durchsetzung von Richtlinien für mobiles Arbeiten und Datenschutz, die Konfiguration von Netzwerkzugängen, die Bereitstellung und Verwaltung von Apps, die Möglichkeit des White- und Blacklistings („Welche Daten dürfen vom Gerät empfangen werden und welche nicht?“) sowie die Möglichkeiten zum Monitoring und zur Protokollierung.

Auf der anderen Seite sind mit dem Einsatz eines MDM aber auch Risiken und ein höherer Verwaltungsaufwand verbunden. So zählen die Kontrolle und Transparenz über die ordnungsgemäße Nutzung des MDM dazu. Der Einsatz des MDM muss datenschutzkonform erfolgen. Es muss sichergestellt werden, dass ein MDM-System nur erforderliche Daten sammelt und dass diese Daten geschützt sind. Dies gilt insbesondere dann, wenn ein Schulträger bzw. eine Schule seinen Mitarbeitenden und Lernenden die Nutzung privater Geräte erlaubt oder sogar vorschreibt.

Durch die zentrale Administration und Zuteilung von Funktionen und Rollen, kommt es zudem auch zu Einschränkungen in der Benutzerfreiheit, die bei zu strengem Reglement zu Frustration bei den Benutzenden führen kann, wenn die bereitgestellten und vielleicht in deren Besitz befindlichen Geräte nicht in gewohnter Art und Weise genutzt werden können. Dadurch kann die Produktivität beeinträchtigt werden.

Je mehr unterschiedliche mobile Geräte von den Mitarbeitenden und Lernenden genutzt werden, desto komplexer wird die Administration des Mobile-Device-Managements. Für eine optimale Verwaltung und Implementierung von MDM-Systemen ist häufig ein hohes Maß an administrativem Know-how notwendig. Andernfalls kann fehlendes Bedienvermögen ein Sicherheitsrisiko darstellen. Es sollte daher sichergestellt werden, dass Schulträger oder Schulen die erforderliche Zeit und Ressourcen sowie die erforderliche Fachkenntnis einplanen, um ein MDM-System zu betreiben.

2.3 Open Source versus Close Source (kommerziell)

Derzeit sind auf dem Markt MDM-Systeme in beiden Varianten verfügbar. Bei der Auswahl einer Open-Source-Variante müssen Schulpersonal und Administratoren zusätzlichen Zeit- und Ressourcenaufwand einplanen, da sie sich intensiver mit der Lösung auseinandersetzen müssen.

Kommerzielle MDM-Systeme befinden sich oft im höheren Preissegment und können zu einer Abhängigkeit vom jeweiligen Anbieter führen. Ein Wechsel zwischen MDM-Systemen gestaltet sich in der Regel schwierig und kostspielig, insbesondere wenn es darum geht, den bestehenden Datenbestand und die Konfiguration zu übertragen. Infolgedessen entstehen sowohl bei der Nutzung von Open-Source- als auch von kommerziellen MDM-Systemen Kosten, die in Abhängigkeit von der Anzahl der zu verwaltenden Geräte beträchtlich steigen können.

Beim Vergleich der beiden Varianten ist zu beachten, dass Open-Source-Systeme häufiger Ziel von Cyberangriffen sind. Die entstehenden Folgekosten im Falle eines erfolgreichen Angriffs könnten möglicherweise deutlich höher ausfallen als die Kosten für kommerzielle MDM-Systeme.

2.4 Betrieb eines Mobile Device Managements (MDM)

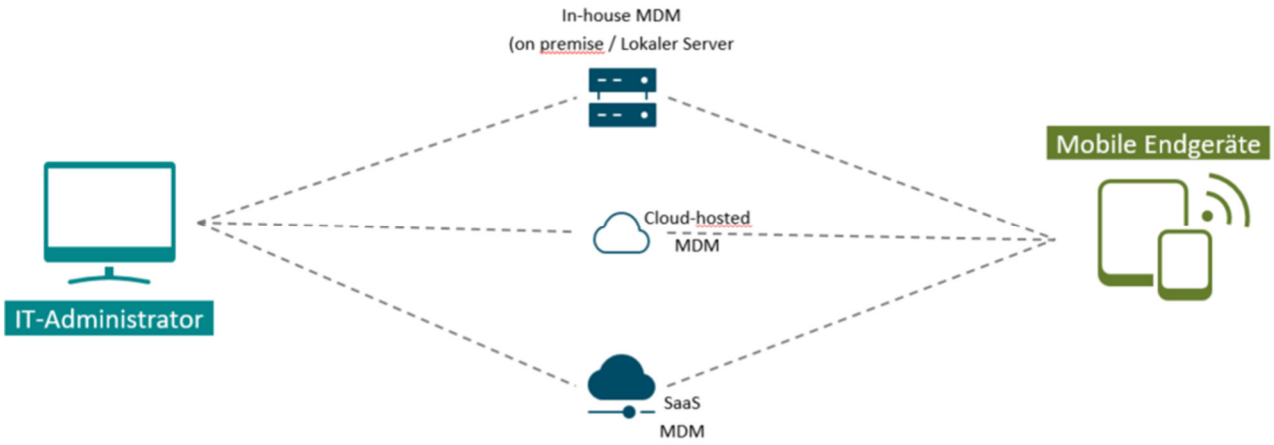
Wie für alle Anwendungen ergeben sich auch für das MDM mehrere Betriebsoptionen. Und wie für alle Anwendungen gilt auch für das MDM die Frage des „MAKE-or-BUY“.

Verfügt eine IT, und in dem Fall werden sowohl die Schul-IT als auch die städtische IT betrachtet, über Rechenzentrumskapazitäten, dann empfiehlt sich eine Installation von Ort. D.h., die MDM-Software wird bestenfalls redundant auf eigenen Servern mit einem eigenen Storage betrieben. Updates und Upgrades sind entweder durch die eigene IT oder einen beauftragten Dienstleister durchzuführen.

Stehen hingegen eigene Rechenzentrumskapazitäten nicht zur Verfügung, könnte alternativ der Bezug von Colocation-/Housing-Leistungen genutzt werden. Die eigenen Server- und Speichersysteme werden in ein Fremd-Rechenzentrum verbracht und dort wiederum durch die eigene IT oder einen beauftragten Dienstleister betrieben. Meist bieten Colocation/Hosting-Anbieter mehrere Brandabschnitte an, sodass gerade in einer Colocation ein redundantes Konzept einfach umgesetzt werden kann.

Wollen sich die Schul-IT-Abteilung oder der beauftragte Dienstleister gar nicht mehr mit Server- und Speichertechnik auseinandersetzen, bietet sich der „Software-as-a-Service-Ansatz“ (SaaS) an. In diesem Fall werden die MDM-Software und alle dafür notwendigen Komponenten durch einen Hosting-Dienstleister bereitgestellt. Die eigene IT oder ein beauftragter Dritter loggen sich auf dem System ein und können von diesem aus die Funktionen des MDM, angewendet auf die eigenen mobilen Endgeräte, nutzen.

Die folgende Grafik stellt alle drei Ansätze kurz gegenüber.



2.5 Anforderungen an die MDM-Software

Die MDM-Software gibt den Administrator:innen viele Befugnisse und Möglichkeiten zur Steuerung, die besonnen und bewusst genutzt werden sollte. Dazu gehört einerseits, dass die Administration über den Betrieb des Endgeräts entscheiden kann. Und andererseits ist das Augenmerk darauf zu richten, dass die Administration den Standort des Endgeräts, Zeitpunkt der Nutzung und welche Daten im Einsatz waren, nachvollziehen kann.

Das heißt, eine erste grundlegende Regelung zum Einsatz der MDM-Software ist gemeinschaftlich mit der Personalvertretung oder den Eltern, bei privat genutzten Endgeräten, zum Einsatz mobiler Endgeräte zu erarbeiten. Häufig wird diese Vereinbarung um eine Regelung zur zum mobilen Arbeiten oder dem außerschulischen Lernen ergänzt, sodass geregelt ist, wann und von wo ein mobiles Gerät sich erwartbar in ein Netzwerk einwählt.

Im schulischen Bereich ist zu klären, wer das MDM selbst und mittels des MDM die mobilen Endgeräte administriert. Erfahrungen zeigen, dass diese Aufgabe nicht den EDV-Koordinierenden, wie den Medienbeauftragten oder IT-Beauftragten in den Schulen überlassen werden sollte. Vielmehr kristallisiert sich der Aufgabenbereich einer Schul-IT heraus. Ob diese im kommunalen IT-Bereich verankert oder durch einen externen Dienstleister erbracht wird, ist je nach Fall zu entscheiden. Mit Blick auf die Zunahme von mobilen Endgeräten in den Kernverwaltungen sollten Schulträger, Schulleitung und kommunale IT in gemeinsamen Beratungen prüfen, ob der Einsatz einer MDM-Lösung für alle mobilen Endgeräte die beste Lösung ist.

In Anbetracht der Zunahme an Endgeräten und vor allem mobilen Endgeräten ist es zudem zwingend erforderlich, den Überblick über den Verbleib und den Einsatz der mobilen Endgeräte zu bewahren. Die Funktionalitäten eines MDM unterstützen die jeweiligen IT-Verantwortlichen bei der Planung und Umsetzung dieser Verwaltungsaufgabe. Mit der Zunahme an Endgeräten steigt auch der Verwaltungsaufwand. Folglich müssen sich Schulträger, Schulleitung und IT-Bereiche über weitere Stellen (VZÄ) abstimmen, die geschaffen und besetzt werden müssen, um die Geräteverwaltung und den Gerätesupport sicherzustellen.

Größtes Risiko beim Einsatz eines MDM ist ein erfolgreicher (Cyber-)Angriff auf das MDM. Gelingt dieser, übernehmen die Angreifer die Steuerung aller mobilen Endsysteme und können großen Schaden anrichten. Folglich sollte das MDM in einer geschützten Umgebung, mit einer MFA/2FA betrieben werden und redundant ausgelegt sein.

Ein weiteres Risiko ist die Fehlkonfiguration von mobilen Endgeräten. Daher empfiehlt sich bei größeren Änderungen ein Vier-Augen-Prinzip, bevor ein neues Profil verteilt wird.

Ein mobiles Endgerät kann nur verwaltet werden, wenn es sich an einem Netz anmeldet. Erfolgt dies über eine längere Dauer nicht, müssen organisatorische Regelungen greifen. Diese sollten bestenfalls mit Ausgabe des Geräts beschrieben und von den Empfangenden gegengezeichnet werden.

2.6 Datenschutz und Informationssicherheit

Der Datenschutz und die IT-Sicherheit sind zwei ganz wesentliche Aspekte, die vor und mit der Einführung eines MDM zu regeln sind. Im Kern geht es darum, dass auf mobilen Endgeräten vertrauliche und teils personenbezogenen Daten abgelegt sind. Das heißt, der Verlust oder der Einbruch in ein mobiles Endgerät kann dazu führen, dass diese Daten in die falschen Hände geraten.

Mit dem Datenschutz soll geregelt werden, wie und welche Daten während der Nutzung des mobilen Endgeräts verarbeitet werden und ob diese DSGVO-konform verläuft. Gerade bei der Einbindung von externen Dienstleistern, die das MDM für eine Schule / Schulträger betreiben, ist eine Auftragsverarbeitungsvereinbarung (AVV) zwingend erforderlich.

Mit der IT-Sicherheit soll geregelt und umgesetzt werden, dass Daten nicht unwissentlich vom mobilen Gerät abfließen.

2.7 Der Zero Trust-Ansatz mittels MDM

Zero Trust bedeutet, „vertraue Keinem, verifiziere alles“. Das heißt, mittels eines MDM werden die mobilen Endgeräte maximal abgesichert und erst nach Prüfung und Freigabe werden ausgewählte Funktionen freigeschaltet. Die Sicherheitsvorkehrungen beziehen sich auf jede Zugriffstransaktion und jeden Benutzenden. Einem gemeinsam genutzten, sicheren Netzwerk wird nicht mehr grundsätzlich vertraut. Angreifenden wird dadurch eine deutlich geringere Anzahl an Angriffsvektoren geboten.

Was im ersten Moment überzeugend erscheint, bringt auf der anderen Seite Herausforderungen mit sich. Die Einführung eines Zero-Trust-Ansatzes ist als Kulturwandel zu verstehen. IT-Sicherheit wird an die erste Stelle gesetzt und kann zu Einschränkungen der Benutzerfreundlichkeit führen. Und das Motto „vertraue keinem, verifiziere alles“ verlangt nach einem intensiven Ressourceneinsatz, der sich in hohen Anschaffungs-, Wartungs- und Betriebskosten widerspiegeln kann.

Kriterien zur Auswahl eines Anbieters: [2]

- Unterstützt das MDM möglichst viele Betriebssysteme?
- Ist die Benutzeroberfläche intuitiv und mehrsprachig verfügbar?
- Werden Klassenraum-Lösungen (Classroom Apps) der einzelnen Geräte-Hersteller unterstützt?
- Ist eine zentrale Inventarisierung von Geräten möglich?
- Ist eine Anbindung an vorhandene Verzeichnisdienste (Active Directory, LDAP, Open ID Connect, SAML, Azure Active Directory, Shibboleth etc.) möglich, oder ist ein Identitätsmanagement (IDM) im MDM bereits integriert?
- Ist der Funktionsumfang des MDM auf eine vereinheitlichte und komfortable Verwaltung von Geräten ausgelegt und werden zudem schulspezifische Anforderungen unterstützt?

[2] Vgl. hierzu: BfB-Leitfaden zur Beschaffung von Schülergeräten

3 Glossar

Assetmanagement	Beschreibt die Verwaltung von Endgeräten
AVV	Auftragsverarbeitungs-Vertrag, der die Datenverarbeitung im Sinne der Datenschutz-Grundverordnung regelt
Blacklisting	Liste mit Programmen, Webseiten etc., die auf den Endgeräten **nicht** geöffnet oder installiert werden können
Bring-Your-Own-Device	Ausstattungskonzept bei dem die Schülerinnen und Schüler ihre eigenen Geräte von zu Hause mit in die Schule bringen.
Colocation/ Housing	Prozess, bei dem ein Kunde einen eigenen Server in einem von ihm unabhängigen Rechenzentrum gegen eine Miete unterbringt
Container	Bei der Containerisierung werden spezifische Apps in eine Art Container verkapselt. So kann die IT Apps mit relevanten Unternehmensdaten in einen speziellen Bereich verschieben und komplett kontrollieren
Customizing	Anpassung von bereits bestehenden Software-Lösungen zur Einbindung neuer Funktionen
Enterprise Mobility Management	Umfasst die Verwaltung und Kontrolle von Endgeräten, mobilen Apps und Daten in Unternehmen. Es besteht aus verschiedenen Komponenten wie Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Content Management (MCM) und Mobile Identity and Access Management (MIAM).
EPP-Lösung	Eine Endpoint Protection Plattform (EPP) dient dazu die verschiedenen Endgeräte in einer Enterprise-IT-Umgebung wie PCs, Laptops, Tablets oder Smartphones vor diversen Gefahren zu schützen. Die Software besitzt Funktionen zum Schutz vor Viren, Malware, Spyware oder Phishing.
Get-Your-Own-Device	Ausstattungskonzept, bei dem Schülerinnen und Schüler bzw. deren Eltern ein konkretes Gerät bzw. einen Gerätetyp nach Vorgaben der Schule anschaffen, welches in einem MDM verwaltet wird.
Incidents	IT-Vorfall
IT (Informationstechnologie)	Oberbegriff für die Informations- und Datenverarbeitung auf Basis dafür bereitgestellter technischer Services und Funktionen.
ITSM-Lösung	Service-Management-Tool
MAM-Lösung	MAM-Lösungen (Mobile Application Management) konzentrieren sich primär auf die Verwaltung und Sicherheit von Anwendungen auf mobilen Geräten. Ein MAM unterstützt das mobile Anwendungsmanagement gemäß dem Lebenszyklus von (mobilen) Anwendungen, wie der Installation, Aktualisierung und dem Rückbau.
MFA/ 2FA	Mehrfaktorauthentifizierung
Mobile Content Management (MCM)	Mithilfe von Mobile Content Management Lösungen können Inhalte auf und Apps auf Endgeräten zur Verfügung gestellt werden.

Mobile Identity Management (MIM)	Das Mobile Identity Management regelt Identifizierung, Authentifizierung und Autorisierung einer oder mehrerer Personen für den Zugang zu Anwendungen, Systemen oder Netzen auf mobilen Endgeräten.
Monitoring	Beschreibt die (automatische) Überwachung von Prozessen in der IT-Infrastruktur
Multi-User-Management	Multi-User-Management bezeichnet die Verwaltung und Organisation von mehreren Benutzern innerhalb eines Systems, wobei Funktionen wie Authentifizierung, Berechtigungen und Ressourcenzuweisung eine zentrale Rolle spielen. Das Ziel besteht darin, einen strukturierten und sicheren Umgang mit mehreren gleichzeitigen Nutzern in einer gemeinsamen Umgebung zu gewährleisten.
Network Service Management	Network-Service-Management bezeichnet die Verwaltung und Organisation von Netzwerkdiensten, einschließlich der Überwachung, Konfiguration und Optimierung, um eine effiziente und sichere Netzwerkleistung zu gewährleisten.
Policy Enforcement	Durchsetzung von IT-Richtlinien
Protokollierung	Aufzeichnung von Prozessen in der IT-Infrastruktur
Roaming	Bezeichnet den Austausch von Daten in anderen Netzwerken als dem Heimnetzwerk
Services	Beschreibt alle Arten einer Dienstleistung. IT-Services beziehen sich auf Dienstleistungen, die mit der Anwendung von technischem und betriebswirtschaftlichem Fachwissen entwi ckelt wurden, um die Nutzung der Technologie für Unternehmen und Endbenutzer zu erleichtern. Auch ein Server kann einen Service als Dienst bereitstellen (z. B.: Emailserver, Dateiablageserver, Chatserver …)
Service Requests	Formale Anfrage eines Anwenders nach einer IT-Dienstleistung.
Storage	Beschreibt Speicherlösungen bestehend aus einem Speichermedium und notwendigen technischen Komponenten zur Sicherung von digitalen Daten
Unified Endpoint Management	Unified Endpoint Management bezieht sich auf die ganzheitliche Verwaltung und Steuerung von Endgeräten wie Computer, Mobilgeräten und anderen Endpunktgeräten über eine zentrale Plattform zur Optimierung von Sicherheit, Konformität und Effizienz.
Whitelisting	Liste mit Programmen, Webseiten etc., die auf den Endgeräten **ausschließlich** geöffnet oder installiert werden können.

Kontakt

PD – Berater der öffentlichen Hand GmbH
Friedrichstr. 149
10117 Berlin
pd-g.de/
pd-g.de/schul-it-navigator

Autorinnen und Autoren

Mathias Ragnow (PD)

Vivien Knies (PD)

Alexander Gutendorf (SONOXO.AI GmbH & Co. KG)