Wie die MobileIron-Plattform die Mindeststandards des BSI* für Mobile Device Management erfüllt

Anleitung zur Einhaltung der Mindeststandards unter dem Einsatz von MobileIron

Die Mindeststandards des Bundesamts für die Sicherheit in der Informationstechnik (BSI) für Mobile Device Management sind für einen EMM-Hersteller wie MobileIron Herausforderung und Chance zugleich. Im Folgenden stellen wir Punkt für Punkt dar, dass und wie die MobileIron-Plattform die Mindeststandards erfüllt und demzufolge für alle Stellen des Bundes, der Länder und Kommunen in der Bundesrepublik Deutschland eine exzellente Wahl ist. Vor allem auch deshalb, weil die Plattform noch sehr viel mehr kann, als in den Mindeststandards gefordert wird.

MobileIron

Balanstraße 73, Building 8
81541 München
Deutschland
Tel.: +49 (0) 89 12503644-0
Fax: +49 (0)89 12503644-9
dach@mobileiron.com

*BSI Mindeststandards für MDM, Version 1.0 vom 11.05.2017

Einleitung

Moderne Endgeräte wie Smartphones, Tablets und Desktop Computer auf Basis von Windows 10 und macOS nehmen auch in der Bundesverwaltung und den Behörden der Länder und Kommunen einen zunehmend wichtiger werdenden Platz ein. Dabei werden auf diesen Geräten auch immer mehr sensible Informationen gespeichert und verarbeitet. Grund genug, dass sich das Bundesamt für die Sicherheit in der Informationstechnik (BSI) auch der Mobile-IT annimmt und entsprechende Mindeststandards für den Betrieb moderner Endgeräte bei den Behörden der Bundesrepublik Deutschland definiert. Dies hat das BSI mit den am 11. Mai 2017 in der Version 1.0 veröffentlichten „Mindeststandards des BSI für Mobile Device Management" getan. Das Amt erfüllt damit eine in § 8 Absatz 1, Satz 1 des BSI-Gesetzes festgelegte Aufgabe. Im Prinzip fließen solche Empfehlungen des BSI in entsprechende Verwaltungsvorschriften des Bundes, der Länder und Kommunen der Bundesrepublik Deutschland ein und haben für Hersteller entsprechender Hardware und Software zumindest insoweit bindende Wirkung, als diese mit öffentlichen Auftraggebern Geschäfte machen. Wenn wir im Folgenden die vollständige Kompatibilität der MobileIron-Plattform mit den Mindeststandards des BSI aufzeigen, heißt das nicht zuletzt, dass sich die Stellen des Bundes, der Länder und der Kommunen bei einem Einsatz der MobileIron-Plattform zur Sicherung ihrer mobilen Geräte und Services auf verlässlichem juristischen, organisatorischen und technischen Terrain bewegen.

In seiner Beschreibung der Sicherheitslage in einem Szenario mit mobilen und modernen Endgeräten weist das BSI darauf hin, dass aufgrund von „Art und Umfang der anfallenden Daten vielfältige Bedrohungen und Risiken entstehen können". Auch die Komplexität – verursacht durch eine Vielzahl von installierten Applikationen und zahlreichen Ökosystemen – beeinflusse ganz entscheidend die potenzielle Bedrohungslage. Dieser müsse auch mit technischen Hilfsmitteln begegnet werden.

Die Autoren des BSI-Papiers weisen deshalb darauf hin, dass in dem beschriebenen Szenario der Einsatz eines Mobile Device Management (MDM) Systems unabdingbar sei. Mit einem MDM-System könnten moderne Endgeräte in die IT-Infrastruktur einer Stelle des Bundes integriert und zentral verwaltet werden. Mit Blick auf die Sicherheit ist für die BSI-Autoren die „Kernfunktion des MDM-Systems die wirksame Durchsetzung definierter Sicherheitsrichtlinien und Konfigurationsparameter auf den mobilen Endgeräten". Der Mindeststandard definiere funktionale und nicht-funktionale Mindestsicherheitsanforderungen, die ein MDM-System zu erfüllen habe, wenn es in einer staatlichen Stelle des Bundes eingesetzt werden solle. Durch die Umsetzung sowohl technischer als auch organisatorischer Maßnahmen ermögliche der Mindeststandard ein Mindestsicherheitsniveau beim Einsatz eines MDM. Der Mindeststandard könne somit – so die Autoren weiter – „bereits im Rahmen eines Vergabeverfahrens herangezogen werden".

Die MobileIron-Plattform im Spiegel des BSI-Katalogs

Im Folgenden werden die in dem BSI-Papier aufgeführten Mindeststandards an ein MDM-System dargestellt und erörtert, wie diese durch den Einsatz der MobileIron-Plattform erfüllt werden können. Die Mindeststandards werden dabei kursiv dargestellt, die Beschreibung der MobileIron-Plattform als Unterpunkt in Normalschrift.

MDM.01: Nutzdaten

Anfallende Nutzdaten des MDM müssen innerhalb der IT-Infrastruktur des Betreibers verbleiben. Nutzdaten sind insbesondere Konfigurationsprotokolle, PINs, Schlüssel sowie Anwendernamen und andere persönliche Identitätsmerkmale (z. B. International Mobile Subscriber Identity (IMSI), Rufnummern).

- Die Nutzdaten, die über das durch SSL abgesicherte MDM-Protokoll übertragen werden, verbleiben in einer abgesicherten Datenbank und können nicht von Dritten abgerufen oder ausgelesen werden. Die MobileIron Appliance basiert auf einem gehärteten Linux (CentOS). Dieses wird bei jeder Aktualisierung einem Penetration-Test unterzogen.

MDM.02: Cloud-Dienste

Wird das MDM ganz oder auch nur teilweise von einem externen Cloud-Anbieter bezogen, sind zusätzlich die Anforderungen aus dem Mindeststandard des BSI zur "Nutzung externer Cloud-Dienste" [(1)] einzuhalten.

- Die MobileIron Produkte gibt es sowohl als On-Premise als auch als Cloud-Lösung. Die Cloud-Lösung kann entweder von MobileIron direkt oder aber von anderen Anbietern bezogen werden. Wird MobileIron über einen 3rd Party Provider bezogen, so muss dieser entsprechend den Anforderungen "Nutzung externer Cloud-Dienste" selbst dafür haften. Die MobileIron Cloud für den europäischen Raum wird in Frankfurt am Main, Deutschland, gehosted und betrieben und erfüllt somit die Anforderungen an den Datenschutz nach dem BDSG.

MDM.03: Mandantentrennung

Werden mehrere Mandanten auf einem MDM verwaltet, so muss eine wirksame Trennung der Mandanten sichergestellt sein.

- Durch die Funktion Spaces können Administratoren nur Konfigurationen/Geräte sehen, die zu ihrem Bereich gehören. Im Support-Portal gibt es ebenfalls Dokumente, welche die Spaces-Funktionalität und die Trennung von Mandanten im Detail beschreibt.

MDM.04: Kompromittierte mobile Endgeräte

Zum Schutz des MDM und der Konfiguration müssen kompromittierte verwaltete mobile Endgeräte (z.B. Jailbreak und Rooting) zeitnah erkannt und vom MDM sowie der Infrastruktur der Stelle des Bundes ausgeschlossen werden. Hierfür müssen die Schutzmaßnahmen sicherstellen, dass Sicherheitsvorfälle dem Administrator in geeigneter Weise angezeigt werden. Stellt das MDM hierfür keine wirksamen Schutzmaßnahmen bereit, sind zusätzliche technische und /oder organisatorische Maßnahmen zu ergreifen.

- Der im Rahmen des Registrierungsprozesses installierte Mobile@Work-Client (MDM Client) überprüft, ob das mobile Endgerät kompromittiert ist (Jailbreak oder Rooting). Wenn das der Fall ist, können entsprechende Korrekturmaßnahmen (Compliance Actions) getroffen werden, wie zum Beispiel „Alert / Block Access / Quarantine / Wipe". Beim Alert werden der Administrator oder eine dafür hinterlegte Gruppe alarmiert. Das betreffende Endgerät wird auf der MobileIron Konsole zudem rot hinterlegt dargestellt.

(1) Mindeststandards des BSI zur Nutzung externer Cloud-Dienste; Version 1.0 vom 24.04.2017;
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.pdf?__blob=publicationFile&v=7

MDM.05: Berechtigungsmanagement im MDM

Das MDM muss über ein Rechtemanagement verfügen, so dass das Berechtigungskonzept vollständig umgesetzt werden kann. Über das Rechtemanagement müssen Zugriffsrechte zuverlässig zugeordnet werden können, sodass Benutzergruppen und Administratoren nur über Berechtigungen verfügen, die für die Aufgabenerfüllung notwendig sind (Minimalprinzip).

- MobileIron bietet über die Integration in ein bestehendes Active Directory/LDAP die Übernahme bestehender Rollen und Rechte, die bereits in der jeweiligen Behörde gesetzt sind. Das Berechtigungskonzept kann darüber hinaus in der Administrationskonsole von MobileIron zusätzlich angepasst werden. Im Supportportal von MobileIron gibt es Dokumente, die verschiedene Berechtigungskonzepte beschreiben.

MDM.06: SIM-Karten

Das MDM muss die notwendigen Informationen bereithalten, um eine Sperrung der SIM-Karte veranlassen zu können.

- Die SIM-Karten Informationen: Subscriber Carrier Network Current Mobile Country Code, Current Mobile Network Code, Current Phone Number, Carrier Settings Version IMSI (Android), Subscriber Carrier Network Current Mobile Country Code, Current Mobile Network Code, Current Phone Number Carrier Settings Version, IMSI (Android) können durch die Lösung ausgelesen werden; dadurch vereinfacht sich die Sperrung der SIM-Karte beim jeweiligen Anbieter. Durch ein zusätzliches von MobileIron bereitgestelltes Tool (Assemble) können weitere SIM-Karten-Daten ausgelesen werden.

MDM.07: Verteilung von Applikationen

Eine zentrale Verteilung von Applikationen muss möglich sein. Diese muss den Anforderungen des geplanten Einsatzszenarios genügen (z. B. rollen- oder gruppenbasierte Verteilung). Die Deinstallation von Applikationen und das Verteilen von Updates müssen durch den Administrator auch aus der Ferne erzwingbar sein (z. B. Over-The-Air (OTA)). Werden Sicherheitsprobleme einer Applikation bekannt, so muss es möglich sein, diese Applikation zeitnah von allen mobilen Endgeräten zu deinstallieren. Dieser Vorgang muss durch das MDM erzwungen werden können, sobald eine Verbindung zwischen MDM und mobilem Endgerät besteht.

- MobileIron bietet über eine gruppenbasierte Verteilung (Labels), die anhand von LDAP-Gruppen oder Geräte-Variablen arbeitet, die Möglichkeit, Applikationen, Richtlinien und Einstellungen an das Gerät zu pushen. Diese können ebenso zeitgesteuert verteilt oder entfernt werden. Auch können die Apps auf Grund von Compliance-Verstößen wieder entzogen werden.

MDM.08: MDM-Client

Stellt das MDM einen MDM-Client auf den mobilen Endgeräten bereit, so sollte eine Deinstallation des MDM-Clients durch den Benutzer nicht möglich sein. Kann eine Deinstallation durch den Benutzer nicht unterbunden werden, so muss das MDM den Administrator darauf hinweisen (siehe hierzu auch Anforderung MDM.37).

- MobileIron bietet nach Best Practice einer großen Kundenbasis an, eine AppControlRule zu konfigurieren, die dann, wenn der MDM-Client sich nicht mehr auf dem Endgerät befindet, eine Meldung (Push-Notification, Email oder SMS) an den vorher festgelegten Administrator, zu senden. Darüber hinaus lassen sich auch noch weitere Maßnahmen einstellen, wie zum Beispiel die Sperrung der geschäftsrelevanten Applikationen.

MDM.09: Protokollierung

Der Lebenszyklus einschließlich Konfigurationshistorie eines mobilen Endgerätes muss ausreichend protokolliert und zentral abrufbar sein. Bei Bedarf muss der aktuelle Status der verwalteten Endgeräte durch den Administrator ermittelt werden können (Device Audit). Dies umfasst insbesondere die Abfrage von

- sicherheitstechnisch relevanten Konfigurationseinstellungen,
- installierten Zertifikaten,
- installierten Applikationen inkl. Versionsstand,
- Betriebssystemversion eines Endgeräts.

Das MDM muss alle sicherheitsrelevanten Ereignisse und Konfigurationsänderungen sowie Aktualisierungen der Betriebssysteme der mobilen Endgeräte protokollieren. Eine manuelle Erfassung und Protokollierung kann die vom MDM automatisch erhobenen Daten ergänzen. Die erhobenen Daten dürfen nicht von unbefugten Personen eingesehen oder verändert werden. Das Protokoll muss durch den Administrator zentral einsehbar sein.

- Die zentrale Konfigurationshistorie ist auf der Core gegeben (Detailansicht Device -> Detail Ansicht Configuration, Device->Logs -> Certificate Inventory Detail Ansicht Device-> Apps Detail Ansicht Device-> Device Details -> OS Version. Die zentrale Konsole bietet eine zentrale Konfigurationshistorie, die nur durch rollenberechtige User eingesehen werden kann. Durch das Öffnen der Geräte- Ansicht können unter der Detailansicht Device-Logs-> Certificate Inventories installierte Zertifikate angezeigt werden, des Weiteren können unter Device-> Apps Detail installierte Applikationen inkl. Versionsstand angezeigt werden sowie unter Device Details-> OS Version die Betriebssystemversion eines Endgerätes.

MDM.10: Konfigurationsprofile

Konfigurationsprofile (VPN-Verbindungen, WLAN-Einstellungen, usw.) dürfen nicht durch den Nutzer manuell verändert oder rückgängig gemacht werden können (siehe hierzu auch Anforderung MDM.37)

- Konfigurationen, die von der MobileIron-Plattform auf das Mobilgerät gepushed werden, sind nicht änderbar.

MDM.11: Sichere Erstinstallation

Für die Erstinstallation der mobilen Endgeräte muss das MDM eine sichere Schnittstelle bereitstellen.

- Die Erstinstallation/Enrollment Profil wird über eine Verbindung vom Endgerät zu dem Server über Port 443 ausgerollt. Der MobileIron Server ist zwingend über ein öffentliches Trusted SSL-Zertifikat abgesichert. Es wird über so genannte ACL-Richtlinien direkt auf dem zentralen Server (Core) die Sperrung von Port 8080 angeboten.

MDM.12: Kennwörter und Gerätecodes

Die Einrichtung und wirksame Durchsetzung komplexer Kennwörter und Gerätecodes auf den mobilen Endgeräten muss zentral konfigurierbar sein. Die Vorgabe, nach wie vielen Fehleingaben das Endgerät gesperrt oder gelöscht wird, muss zentral konfigurierbar sein. Ein Reset von Kennwörtern und Gerätecodes zum Entsperren des Endgeräts muss durch den Administrator auch aus der Ferne (z. B. OTA) möglich sein.

- Über die Sicherheitsrichtlinien können die Mindestvorgaben konfiguriert werden, z.B. Mindestpasswortlänge (hier empfiehlt MobileIron einen mindestens vier Stellen langen Code), Mindestanzahl komplexer Zeichen (hier empfiehlt MobileIron mindestens 1 Sonderzeichen), die maximal zulässige Anzahl von Fehlversuchen (MobileIron empfiehlt: nach zehn Fehleingaben soll das Endgerät auf

Werkseinstellungen zurückgesetzt werden). Die Sicherheitsrichtlinien werden unter Policy & Configuration -> Policy-> Security konfiguriert. Auf der Konsole unter Devices-> More Actions-> Unlock kann der Gerätecode aus der Ferne durch den Administrator zurückgesetzt werden (gilt sowohl für Android als auch iOS).

MDM.13: Fernlöschung (Remote-Wipe) und Außerbetriebnahme

Das MDM muss sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät einschließlich Zugangsdaten und Zertifikate auch aus der Ferne gelöscht werden können (Remote-Wipe bei bestehender Netzwerkverbindung). Werden in dem mobilen Endgerät externe Speicher genutzt, muss geprüft werden, ob diese bei einem Remote-Wipe ebenfalls gelöscht werden sollen und ob dies vom MDM unterstützt wird. Der Prozess zur Außerbetriebnahme des mobilen Endgerätes (Unenrollment) muss sicherstellen, dass keine sensitiven Daten auf dem mobilen Endgerät oder eingebundenen Speichermedien verbleiben. Dies gilt insbesondere dann, wenn das Unenrollment aus der Ferne ausgeführt wird.

- Die Fernlöschung ist für ein einzelnes oder für mehrere Geräte auf einmal anwendbar. Dabei wird das Gerät auf Werkseinstellungen zurückgesetzt und keine der Daten bleiben auf dem Gerät erhalten. Auszuführen unter Devices -> More Actions -> Wipe (Full Wipe). Sollten nur die MobileIron Applikationen und Daten gelöscht werden, kann ein Selective-Wipe diese vom Gerät entfernern; dabei wird das Gerät aus dem Management und auch aus der zentralen Konsole gelöscht. Auszuführen unter: Devices, More Actions -> Retire.

MDM.14: Automatische Sperre und Gerätesperrung (Remote-Lock)

Die Einrichtung und wirksame Durchsetzung einer automatischen Sperre des mobilen Endgerätes nach Zeitvorgabe muss zentral konfigurierbar sein. Eine Gerätesperrung muss durch den Administrator auch aus der Ferne möglich sein (Remote-Lock). Kann der Remote-Lock auf dem mobilen Endgerät nicht ausgeführt werden, muss dies vom MDM in geeigneter Weise angezeigt werden können.

- Für eine automische Sperre kann eine Zeitvorgabe eingestellt werden. Darüber hinaus kann eingegeben werden, wann der Gerätecode aktiviert wird. Ein Remote-Lock ist über den Punkt „Devices-More Actions- Remote Lock" ausführbar. Dabei kann der Administrator das Endgerät aus der Ferne sperren. Sollte dies nicht ausführbar sein, so kann dies in den Geräte-Logs ausgelesen werden.

MDM.15: Administration von Schnittstellen und Funktionen

Schnittstellen müssen zentral über das MDM administrierbar sein. Unter Schnittstellen sind insbesondere Bluetooth, Infrarot, WLAN, SMS, MMS, GPS, NFC, RFID und USB zu verstehen. Gleiches gilt für Funktionen wie z.B. Kameras, Mikrofone, Sprachsteuerungen und Ortungsdienste. Ein Koppeln oder Verbinden mit anderen Geräten (z. B. via Apple AirPlay oder AirDrop) zum Datenaustausch oder zur Datenweitergabe muss unterbunden werden können.

- Die Verwaltung bzw. Sperre von Schnittstellen kann über die MobileIron Lockdown Policy (Android) beziehungsweise die Restriction Policy (iOS) konfiguriert werden. Die SMS /MMS-Schnittstelle ist nur bei Android konfigurierbar (Samsung Safe). Die entsprechenden Einstellungen lauten: Lockdown Policy: Policy & Configs -> Policy -> Add new -> Lockdown & Restriction: Policy & Configs -> Add new -> Configuration-> iOS -> Restrictions

MDM.16: Verschlüsselung des Speichers

Die systemeigene Verschlüsselung des mobilen Endgerätes von nicht-flüchtigem Speicher muss vom MDM zuverlässig aktiviert und durchgesetzt werden können. Die Verschlüsselung muss auch schützenswerte Daten auf externen Speichermedien (z. B. SD-Karte) umfassen.

- Diese Verschlüsselung ist nur für Android-Geräte zu beachten und wird von MobileIron über eine Sicherheitsrichtlinie erzwungen. Konfiguriert werden muss hier unter Policy & Configs -> Policy -> Security der Punkt „Device Encryption". Hier muss "on" aktiviert werden. Dasselbe gilt auch bei der Verschlüsselung für die SD-Karte. Mit iOS 4 hat Apple eine zusätzliche Verschlüsselung namens Data Protection eingeführt, die bestimmte Daten zusätzlich mit dem gesetzten Code verschlüsselt. Dies verhindert, dass geschützte Daten ohne Kenntnis des Codes auch bei physischem Zugriff auf dem Gerät lesbar sind.

MDM.17: Zertifikate

Zertifikate zur Nutzung von Diensten (z. B. Email, ActiveSync, VPN, WLAN und Websites) auf dem mobilen Endgerät müssen zentral installiert, deinstalliert, aktualisiert und angezeigt werden können. Die Installation von nicht vertrauenswürdigen und nicht verifizierbaren (Root-) Zertifikaten durch den Benutzer muss verhindert werden können. Das MDM muss Mechanismen zur Überprüfung der Gültigkeit von Zertifikaten (z.B. OCSP) unterstützen. Die Ungültigkeit eines Zertifikates muss vom MDM in geeigneter Weise angezeigt werden.

- Zertifikate können durch die MobileIron-Plattform auf das Gerät gepushed werden und werden unter Device Details -> Logs-> Cerficate Inventory" angezeigt (Subject, Issuer, not before, not after, Serial Number, Version). Sollte ein Zertifikat ungültig sein, wird dies durch rote Schrift angezeigt. Ebenso bietet MobileIron die Möglichkeit seinen Core Server als Intermediate- oder eigenständige CA fungieren zu lassen.

MDM.18: Administrations- und Self-Service-Portale

Zur Gewährleistung der Authentizität der Teilnehmer sowie Vertraulichkeit und Integrität der übertragenen Inhalte ist sämtliche Kommunikation zwischen MDM und Administrations- und Self-Service-Portalen dem Schutzbedarf entsprechend abzusichern. Die Transportverschlüsselung muss die Sicherheitsanforderungen nach Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls (2) erfüllen. VPN-Verbindungen müssen den IT-Sicherheitsrichtlinien für VPN-Verbindungen der Stelle des Bundes entsprechen.

- MobileIron stellt eine sichere Kommunikation aller Verbindungen zwischen MDM und Administrations- und Self-Service-Portalen durch TLS1.2 mit PFS nach Standard des BSI für Einsatz des SSL/TLS-Protokoll §8Abs.1Satz1BSIG bereit.

MDM.19: Mobile Endgeräte

Die Kommunikation zwischen MDM und mobilem Endgerät muss über einen sicheren Kanal erfolgen. Hierfür muss die Stärke der Schlüssel (Schlüssellänge und -verfahren) den IT-Sicherheitsrichtlinien der Stelle des Bundes entsprechen. Liegt dem sicheren Kanal eine Transportverschlüsselung nach TLS zu Grunde, dann muss diese dem Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls (siehe 2) genügen. Wird eine VPN-Verbindung genutzt, muss diese den IT-Sicherheitsrichtlinien für VPN-Verbindungen der Stelle des Bundes entsprechen.

- Für die Kommunikation zwischen MDM und einem mobilen Endgerät wird das SSL Protokoll verwendet. Der SSL/TLS Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden nach §8 Abs.1 Satz 1 BSIG ist erfüllt.

(2) Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden vom 21.11.2014;
https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards/SSL-TLS-Protokoll/SSL-TLS-Protokoll_node.htm

MDM.20: Dokumentation des MDM

Das MDM sowie entsprechende Aktualisierungen müssen vollständig und nachvollziehbar dokumentiert sein. Die Dokumentation umfasst:

- *Unterstützte mobile Endgeräte mit Betriebssystemversionen,*
- *Angabe über Funktionalitäten, die nur auf bestimmte mobile Endgeräte oder Betriebssystemversionen anwendbar sind,*
- *Schutzeinrichtungen für personenbezogene Daten,*
- *Schutzeinrichtungen für die Verwaltung von kryptografischem Material (Zertifikate, Schlüssel, Kennwörter),*
- *Angaben über die Verwendung von sicheren Protokollen und dem Aufbau von sicheren Kanälen, VPN-Konfigurationen sowie die Anbindung des MDM an die IT-Infrastruktur des Betreibers,*
- *Angaben darüber, welche Dienste innerhalb und außerhalb der Infrastruktur des Betreibers das MDM nutzen oder nutzen kann (z. B. Active Directory, LDAP, Push-Notification),*
- *Angaben darüber, ob und wie die Kommunikation des MDM mit diesen Diensten gesichert werden kann (z. B. Verschlüsselung, Ports, VPN),*
- *mögliche Einschränkungen der Jailbreak oder Root Detection-Function, und*
- *Angaben über die unterstützten Mechanismen zur Verteilung von Applikationen und darüber wie freigegebene Applikationen identifiziert werden.*

- MobileIron bietet alle Dokumentationen auf Wunsch des Kunden zur Bereitstellung an; diese können durch einen Zugang in der MobileIron Community geladen werden (Feature Matrix; Gettings Started Guide; cryptography whitepaper und viele weitere Dokumente).

MDM.21: Support

Supportleistungen des Anbieters müssen den Anforderungen des jeweiligen Einsatzszenarios entsprechen. Dies gilt insbesondere für:

- *die Erstinstallation und Inbetriebnahme,*
- *Unterstützung ohne Fernzugriffsmöglichkeiten,*
- *Erreichbarkeits- und Reaktionszeiten.*

- MobileIron bietet die Erstinstallation durch einen von MobileIron zertifizierten Partner an oder durch einen Professional Service-Mitarbeiter von MobileIron. Es werden verschiedene SLAs angeboten. Details können direkt bei MobileIron unter dach@mobileiron.com angefragt werden.

MDM.22: Aktualisierungen des MDM

Der Anbieter muss den Prozess zur Bereitstellung von Aktualisierungen des MDM (Updates und Patches) darstellen und zusichern.

- MobileIron veröffentlicht im Jahr zwei „Major Updates“ und diverse “Feature Updates” und ist darauf bedacht, für neue Versionen der mobilen Betriebssysteme einen „Day Zero-Support“ anzubieten.

MDM.23: Datensicherungen des MDM

Es müssen wirksame Mechanismen für das Backup aller Daten und Einstellungen des MDM existieren, sodass diese im Bedarfsfall funktionsfähig wiederhergestellt werden können.

- MobileIron bietet einen eingebauten Backup Mechanismus an, der es erlaubt über verschiedene Dateizugriffs-Protokolle auf diversen Servertechnologien zu sichern und alle Daten wieder ordnungsgemäß herzustellen.

MDM.24: Fernzugriff auf das MDM

Fernzugriffe auf das MDM müssen auf einem kryptografisch abgesicherten Kanal erfolgen (vertraulich, integer, authentisch). Die Vorgaben der technischen Richtlinie TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen" [(3)] müssen beachtet werden. Liegt eine Transportverschlüsselung nach TLS zu Grunde, dann muss diese dem Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls (siehe 2) genügen.

- Die MobileIron-Plattform unterstützt die in (3) gelisteten kryptografischen Verfahren und Schlüssellängen.

MDM.25: Erstinstallation der mobilen Endgeräte

Alle mobilen Endgeräte sind in dem MDM zu verwalten. Vor Verteilung der Grundkonfiguration muss sich das mobile Endgerät im Werkszustand befinden. Nicht konfigurierte mobile Endgeräte dürfen keinen Zugriff auf die Infrastruktur der Stelle des Bundes haben.

- Das ist eine Kundenaufgabe. Hier müssen Einstellungen vorgenommen werden, sodass nur im MDM befindliche Systeme Zugriff auf interne Systeme wie z. B. Email erhalten dürfen. Es lassen sich auch durch s.g. ACL-Richtlinien oder in der Kundenfirewall Konfigurationen durchführen, die einen Rollout nur aus dem internen Netz oder von bestimmten Hosts durchgeführt werden können.

MDM.26: Verschlüsselung des Speichers

Die systemeigene Verschlüsselung des mobilen Endgerätes von nicht-flüchtigem Speicher muss aktiviert sein. Schützenswerte Daten auf externen Speichermedien (z. B. SD-Karten) sind zu verschlüsseln.

- Diese Verschlüsselung ist nur für Android-Geräte zu beachten und wird von MobileIron über eine Sicherheitsrichtlinie erzwungen. Konkret muss unter Policy & Configs -> Policy -> Security der Punkt Device Encryption auf "on" konfiguriert werden. Dies gilt ebenso für die Verschlüsselung der SD-Karte. Mit iOS 4 hat Apple eine zusätzliche Verschlüsselung namens Data Protection eingeführt, die bestimmte Daten zusätzlich mit dem gesetzten Code verschlüsselt. Dies verhindert, dass geschützte Daten ohne Kenntnis des Codes bei physischem Zugriff auf dem Gerät lesbar sind.

MDM.27: Monitoring und Diagnose

Falls Funktionen zur Übermittlung von Monitoring- und Diagnose-Informationen an Dritte vorhanden sind, sind diese zu deaktivieren.

- MobileIron übermittelt keine Monitoring- und Diagnose-informationen an Dritte. Es lässt sich dennoch jeglicher Traffic vom MobileIron System zu anderen Servern über s.g. ACL-Richtlienen reglementieren.

MDM.28: Kennwörter und Gerätecodes

Die mobilen Endgeräte müssen durch Kennwörter oder Gerätecodes geschützt sein. Die Stärke von Kennwörtern und Gerätecodes (minimale Länge, Beschaffenheit, Komplexität und Gültigkeitsdauer) muss der IT-Sicherheitsrichtlinie der Stelle des Bundes entsprechen. Dies gilt für Zugriffe auf das MDM (Server und Administrationsportale) und mobile Endgeräte gleichermaßen. Der Prozess zur Zurücksetzung eines Kennwortes oder Gerätecodes muss etabliert sein. Die Anzahl der maximal möglichen Fehlversuche für die Eingabe des Gerätecodes muss festgelegt und technisch umgesetzt werden. Die Anzahl der möglichen Fehlversuche darf 10 nicht überschreiten. Nach Überschreitung der Grenze müssen alle auf dem Gerät gespeicherten Daten automatisch gelöscht werden.

- Über die Sicherheitsrichtlinien können die Mindestvorgaben konfiguriert werden, z.B. Mindest-Passwortlänge (hier empfiehlt MobileIron einen mindestens vier Stellen langen Sicherheitscode), Mindestanzahl komplexer Zeichen (hier empfiehlt MobileIron mindestens

(3) Technische Richtlinie TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen", Version 2017-01 vom 08.02.2017;
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile

1 Sonderzeichen), maximal zulässige Anzahl von Fehlversuchen (MobileIron empfiehlt: nach zehn Fehleingaben soll das Endgerät auf Werkseinstellungen zurückgesetzt werden). Die Sicherheitsrichtlinien werden unter Policy & Configuration -> Policy -> Security konfiguriert. Auf der Konsole unter Devices -> More Actions -> Unlock kann der Administrator den Gerätecode aus der Ferne zurücksetzen (gilt sowohl für Android als auch für iOS).

MDM.29: Automatische Sperre und Gerätesperrung

Die automatische Sperre des mobilen Endgerätes muss genutzt und zentral vorgegeben werden. Die Gerätesperrung muss sich bereits nach einer angemessenen Phase von Inaktivität einschalten. Die Frist muss den Vorgaben der IT-Sicherheitsrichtlinien der Stelle des Bundes entsprechen, darf aber einen Zeitraum von 10 Minuten nicht überschreiten.

- Die Sicherheitseinstellung kann auf der zentralen Konsole über eine Sicherheitsrichtlinie gesetzt werden. Security Policy: Policy & Configs-> Policy -> Add new -> Security -> Max. inactivity timeout -> 10 Minutes.

MDM.30: Administration des MDM

Das MDM muss von geschulten Administratoren bedient werden.

- Diese Voraussetzung ist durch den Kunden zu verantworten. MobileIron bietet über seine Partner verschiedene Schulungen und Zertifizierungen zur Administration oder für den Support der Serversystem an. Eine entsprechende Liste gibt es auf Anfrage.

MDM.31: Sensibilisierung der Benutzer

Benutzer von mobilen Endgeräten müssen über Sinn und Zweck der Sicherheitsmaßnahmen sensibilisiert werden. Dies gilt insbesondere, wenn eine Veränderung der Konfigurationsprotokolle technisch nicht verhindert werden kann. In diesem Fall müssen die Benutzer entsprechend verpflichtet werden, diese nicht zu verändern.

- Das ist eine Kundenaufgabe. MobileIron Integrationspartner oder das MobileIron Professional Services Team können bei der Umsetzung unterstützen.

MDM.32: Dokumentation

Die Sicherheitsmechanismen und -einstellungen für mobile Endgeräte müssen festgelegt und nachvollziehbar beschrieben sein (z. B. PIN-Code-Verfahren, automatische Sperre, Regeln für die Deinstallation von Konfigurationsprotokollen).

- Eine Dokumentation kann entweder vom Kunden selbst oder einem der zertifizierten MobileIron Partner erstellt und bereitgestellt werden.

MDM.33: Regelmäßige Überprüfungen

Konfigurationsprotokolle und Sicherheitseinstellungen müssen regelmäßig überprüft werden. Hierbei sind insbesondere die Vorgaben dieses Mindeststandards sowie Vorgaben aus den eigenen IT-Sicherheitsrichtlinien der Stelle des Bundes zu berücksichtigen. Sollen neue Betriebssystemversionen der mobilen Endgeräte eingesetzt werden, ist vorab zu prüfen, ob die Konfigurationsprotokolle und Sicherheitseinstellungen weiterhin wirksam und ausreichend sind. Abweichungen müssen korrigiert werden. Die vom MDM erzeugten Protokolle müssen regelmäßig auf ungewöhnliche Einträge überprüft werden. Die zugeteilten Berechtigungen für Benutzer und Administratoren sind mindestens halbjährlich hinsichtlich ihrer Angemessenheit zu überprüfen (Minimalprinzip).

- MobileIron bietet „Zero Day Support" für die jeweils neuesten Betriebssystemversionen an. Es kann ebenso eine Dienstleistung durch einen Professional Service Mitarbeiter oder einen zertifizierten Partner beauftragt werden, welcher eine Einweisung in die neuen Features anbietet. Dabei werden die Einstellungen überprüft und die neuen Konfigurationsmöglichkeiten erklärt und anhand der Use-Cases des Endkunden umgesetzt.

MDM.34: Umgang mit Sicherheitsvorfällen

Für den Umgang mit Sicherheitsvorfällen muss ein angemessener Prozess etabliert sein. Dieser muss insbesondere folgende Szenarien abdecken:

- *Verlust eines mobilen Endgerätes,*
- *Verlust der Integrität des mobilen Endgerätes (z. B. durch Jailbreak oder Rooting) – kein Kontakt des mobilen Endgerätes zum MDM über einen längeren Zeitraum hinweg.*

In diesen Fällen muss der Zugang zur Infrastruktur der Stelle des Bundes wirksam verhindert werden.

- Diese liegen bei einem MDM/EMM in der Verantwortung des Kunden. MobileIron kann hier jedoch ebenso durch Einstellungen behilflich sein. Es müssen z.B. Compliance-Einstellungen auf der Konsole konfiguriert werden. Eine Einstellung wäre z.B: „Kein Kontakt der Mobile Devices seit x Tagen zum Server -> Quarantäne". Die (Iron)-Partner von MobileIron helfen darüber hinaus den Kunden bei der Erstellung eines Dokuments, welches die Risiken eines Sicherheitsvorfalls / Verlusts in Bezug auf die in Frage stehende Stelle des Bundes darstellt.

MDM.35: Aktualisierung der Betriebssysteme

Es müssen Arbeitsprozesse geplant, getestet und angemessen dokumentiert sein, damit sicherheitsrelevante Patches und Updates unverzüglich eingespielt werden können. Werden sicherheitskritische Aktualisierungen nicht innerhalb von vier Wochen nach der Veröffentlichung eingespielt, ist dies gesondert zu begründen und zu dokumentieren. MDMs und mobile Endgeräte für die keine sicherheitsrelevanten Aktualisierungen mehr bereitgestellt werden, sind aus dem Betrieb zu nehmen.

- MobileIron unterstützt neue Betriebssysteme vom ersten Tag an. Um davon zu profitieren, empfehlen wir den Kunden seine Infrastruktur mit der jeweils aktuellen EMM-Version auf dem neuesten Stand zu halten.

MDM.36: Konfigurationsprotokolle und MDM-Client

Kann eine unautorisierte Löschung von Konfigurationsprotokollen oder des MDM-Clients technisch nicht verhindert werden (z. B. durch Passwortschutz), sind organisatorische Maßnahmen (z. B. Belehrung und Sensibilisierung des Nutzers) zu ergreifen.

- Es müssen organisatorische Maßnahmen wie z. B. Vereinbarungen erstellt und verteilt werden. Die MobileIron-Partner das Team von MobileIron sind beratend gerne behilflich.

MDM.37: Endgerätenamen

Namen der mobilen Endgeräte dürfen keine Merkmale enthalten, die Rückschlüsse auf den Benutzer oder die Stelle des Bundes ermöglichen.\

- MobileIron schlägt aufgrund seiner Praxiserfahrung vor, die Gerätenamen durch einen generisch erstellten Namen und dann eine fortlaufende Nummer zu erstellen, beispielsweise MID001, MID002, MID003 usw. Zertifizierte MobileIron Partner können hier jedoch auch Konzepte erstellen und beratend unterstützen.

MDM.38: Bereitstellung von Applikationen

Es muss sichergestellt sein, dass ausschließlich sicherheitsgeprüfte Applikationen bereitgestellt werden. Dies kann durch einen definierten Freigabeprozess mit geeigneten Bewertungskriterien sichergestellt werden. Die Nutzung von vorinstallierten Applikationen und Online-Diensten, insbesondere von externen cloudbasierten Diensten, muss bewertet und im Bedarfsfall systemseitig verhindert werden.

- MobileIron bietet über seine Ökosystem-Partner Funktionen zur Bewertung von Risiken einer Applikation an (mediaTest digital, Appthority). Alle Ökosystem-Partner sind im Marketplace aufzufinden (http://marketplace.mobileiron.com)

MDM.39: Nutzung von Schnittstellen und Funktionen

Die Freischaltung von Schnittstellen und Funktionen ist zu regeln und auf das dienstlich notwendige Maß zu reduzieren.

- MobileIron bietet für das Betriebssystem iOS 10.3 alle von Apple bereit gestellten Restriktionen, die unter Policies & Configs -> Configurations -> iOS -> Restrictions einzustellen sind. Für das Betriebssystem Android lassen sich unter Policies & Configs -> Policies -> Lockdown Schnittstellen und Funktionen auf das notwendige Maß reduzieren.

MDM.40: Push-Nachrichten

Es müssen Regelungen für das Anzeigen von Push-Nachrichten auf dem Sperrbildschirm der mobilen Endgeräte getroffen werden. Diese sind insbesondere vom jeweiligen Schutzbedarf abhängig. Die Benutzer sind entsprechend zu sensibilisieren.

- MobileIron bietet das Versenden von Push-Nachrichten auf allen Plattformen an. Darüber hinaus werden betriebsrelevante Push-Nachrichten im Sperrbildschirm der Benutzer angezeigt. Die Administratoren können zusätzlich individuelle Push-Nachrichten erstellen und verschicken, um den Benutzern über diesen Weg eine Information zukommen zu lassen, z.B. dass sie ihr Betriebssystem auf den neuesten Stand aktualisieren sollen.

Fazit

Der Leser erkennt unschwer, dass die MobileIron-Plattform die Mindeststandards des BSI in Sachen Mobile Device Management in vollem Umfang erfüllt. Der Leser sollte dabei nicht aus dem Blick verlieren, dass die Enterprise Mobility Management (EMM) Plattform von MobileIron weit mehr umfasst als ein „MDM-System", bei dem es – wie der Name schon sagt, in erster Linie um die „mobilen Devices" geht und vieles (und Wichtiges) drumherum unter den Tisch fällt.
Freilich gehen die MDM-Mindeststandards des BSI in vielen Punkten über ein reines MDM, wie wir diesen Terminus verstehen, hinaus. Wie dem auch sei: Ein modernes EMM-System enthält jedenfalls neben dem reinen Gerätemanagement unter anderem ein ausgefeiltes App- und Content-Management, mit dem private und geschäftliche Anwendungen auf einem Gerät sicher getrennt werden können sowie der Zugriff auf sensible Inhalte geregelt werden kann. Dadurch werden Datenverluste und Datendiebstahl verhindert. Nicht zuletzt hat ein EMM-System wie das MobileIron einen umfassenden und ganzheitlichen Blick auf Benutzer, Apps und Gerät. Jeder dieser Komponenten muss vertraut werden können: der Benutzer muss entsprechende Rechte haben, die Apps müssen aus einer vertrauenswürdigen Quelle stammen und das Gerät muss in einem vertrauenswürdigen Zustand sein; die Richtlinien des Unternehmens müssen auf dem Gerät umgesetzt sein und das Betriebssystem darf nicht manipuliert sein. Die MobileIron-Plattform bietet all das und weist deshalb technologisch schon deutlich über den Anforderungskatalog des BSI hinaus.

Bei Fragen und Anregungen kontaktieren Sie uns gerne unter dach@mobileiron.com !