MDM.2.6.03: Sicheres Enrollment der mobilen Endgeräte

a) Für das Enrollment der mobilen Endgeräte MUSS das MDMS eine sichere Schnittstelle bereitstellen. Zusätzlich zu MDM.2.6.02[33] gilt während des Enrollments:

Der MDM-Server MUSS durch den MDM-Client authentifiziert werden. Die Kommunikation zwischen mobilen Endgeräten und MDM-Server MUSS kryptographisch abgesichert werden. Nach erfolgreichem Enrollment gilt MDM.2.5.03.

b) Alle mobilen Endgeräte, die Zugriff auf sensible IT-Infrastrukturen oder Daten der Einrichtung haben, SOLLTEN per MDM verwaltet werden. Die Einrichtung MUSS die zu verwaltenden mobilen Endgeräte so schnell wie möglich in das MDMS integrieren und nach den Richtlinien der Einrichtung konfigurieren und verwalten. Vor dem Enrollment MÜSSEN sich die mobilen Endgeräte im Werkszustand befinden.[34]

MDM.2.6.04: Konfigurationsprofile

a) Das MDMS MUSS Konfigurationsprofile (VPN-Verbindungen, WLAN-Einstellungen, usw.) an das mobile Endgerät übermitteln können. Das MDMS MUSS den Installationsstatus von Konfigurationsprofilen pro Gerät anzeigen können. Das MDMS MUSS verhindern können (z. B. durch Passwortschutz), dass Konfigurationsprofile durch den Benutzer manuell verändert oder rückgängig gemacht werden.

b) Kann eine unautorisierte Löschung von Konfigurationsprofilen – wie in (a) gefordert – technisch nicht verhindert werden, ~~z. B.~~MÜSSEN organisatorische Maßnahmen (z. B. Belehrung und Sensibilisierung des Benutzers, vgl. MDM.2.8.04) ergriffen werden.

MDM.2.6.05: MDM-Client

a) Stellt das MDMS einen MDM-Client als Applikation auf den mobilen Endgeräten bereit, SOLLTE das MDMS eine Deinstallation des MDM-Clients durch den Benutzer verhindern können (z. B. durch Passwortschutz).

b) Kann eine unautorisierte Löschung des MDM-Clients – wie in (a) gefordert – technisch nicht verhindert werden, MÜSSEN organisatorische Maßnahmen ergriffen werden – insbesondere die Sensibilisierung des Benutzers (vgl. MDM.2.8.04).

MDM.2.6.06: Administration von Schnittstellen, Diensten und Funktionen

a) Kommunikationsdienste wie SMS und MMS sowie Funktionen wie Kameras, Mikrofone, digitale Assistenten (z. B. Siri) und Sprachsteuerungen MÜSSEN zentral und so granular, wie das Betriebssystem ermöglicht, über das MDMS administrierbar sein.

Gleiches gilt für Schnittstellen-Funktionen. Unter Schnittstellen sind insbesondere Bluetooth, WLAN, GPS und USB, sofern vorhanden, zu verstehen. Das Betriebssystem der verwalteten Geräte kann weitere Schnittstellen bereitstellen; die zugehörigen Funktionen SOLLTEN durch das MDMS ebenfalls administrierbar sein.[35]

Ein Koppeln oder Verbinden mit anderen Geräten (z. B. via Apple AirDrop oder die Anbindung eines Monitors via USB) zum Datenaustausch oder zur Datenweitergabe MUSS unterbunden werden können.

[33] Zudem sind für das Enrollment insbesondere die folgenden Anforderungen aus diesem Mindeststandard zu beachten: MDM.2.2.04: Zugangscodes und –mittel, MDM.2.2.09: Cloud-Dienste beim Betrieb des MDMS und MDM.2.5.06: Zwischen MDM-Server und externen Diensten.

[34] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.2.A4 Verteilung der Grundkonfiguration auf mobile Endgeräte und SYS.3.2.2.A5 Installation des MDM Clients

[35] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.1.A16 Deaktivierung nicht benutzter Kommunikationsschnittstellen

b) Die Freischaltung der in (a) genannten Schnittstellen-Funktionen, Dienste und Funktionen MUSS geregelt und per MDMS auf das dienstlich notwendige Maß reduziert werden. Digitale Assistenten SOLLTEN per MDMS deaktiviert werden.[36]

MDM.2.6.07: Monitoring und Diagnose

a) Funktionen zur betriebssystemeigenen Übermittlung von Monitoring- und Diagnose-Informationen MÜSSEN zentral über das MDMS deaktiviert werden können.

b) Die Einrichtung MUSS die in (a) genannten Funktionen per MDMS deaktivieren.

MDM.2.6.08: Entwicklermodus

a) Das MDMS SOLLTE den Entwicklermodus des mobilen Betriebssystems deaktivieren können.

b) Die Einrichtung SOLLTE den Entwicklermodus per MDMS deaktivieren.

MDM.2.6.09: Konfiguration von Netzwerkparametern

Netzwerkparameter auf den mobilen Endgeräten (DNS, Gateways, DHCP, etc.) SOLLTEN über das MDMS konfigurierbar sein.

MDM.2.6.10: Verschlüsselung des Speichers

a) Das MDMS MUSS die systemeigene Verschlüsselung des mobilen Endgerätes von nichtflüchtigem Speicher aktivieren können.

b) Das MDMS MUSS auch die Verschlüsselung von schützenswerten Daten auf externen Speichermedien (z. B. SD-Karte) aktivieren können.

c) Die Einrichtung MUSS die in (a) genannte Verschlüsselung von nichtflüchtigem Speicher per MDMS aktivieren. Zudem SOLLTE sie die in (b) genannte Verschlüsselung schützenswerter Daten auf externen Speichermedien (z. B. SD-Karten) – mit Ausnahme von Smartcards – aktivieren.[37]

MDM.2.6.11: Zertifikate

a) Das MDMS MUSS auf den mobilen Endgeräten Zertifikate installieren, aktualisieren und anzeigen können, für die das Betriebssystem dies ermöglicht (z. B. Email, ActiveSync, VPN, WLAN und Websites). Die Installation von nicht verifizierbaren Zertifikaten durch den Benutzer MUSS verhindert werden können. Das MDMS muss in der Lage sein, Informationen zum Widerruf von Zertifikaten (z. B. CRLs) an die Endgeräte zu senden. Der Status eines Zertifikates (gültig/ungültig) MUSS vom MDMS in geeigneter Weise angezeigt werden. Das MDMS MUSS den sicheren Transfer (z. B. PKCS#12 verschlüsselt) von Zertifikaten unterstützen.[38]

b) Es MUSS ein Prozess für das Lebenszyklusmanagement der Zertifikate (z. B. Erneuerung, Widerruf) vorhanden sein. Die Einrichtung MUSS insbesondere vorinstallierte Zertifikate auf mobilen Endgeräten auf ihre Vertrauenswürdigkeit hin prüfen und Zertifikate nicht vertrauenswürdiger Aussteller deinstallieren oder widerrufen. Dies KANN per MDMS erfolgen.

MDM.2.6.12: Compliance-Verstöße und kompromittierte mobile Endgeräte

a) Zum Schutz des MDMS und der Konfiguration der Endgeräte MÜSSEN Verstöße gegen Compliance-Richtlinien (z. B. eine nicht erlaubte Betriebssystemversion) erfasst werden können. Zusätzlich KANN das MDMS die Möglichkeit bieten, Indikatoren für die Kompromittierung von mobilen Endgeräten (z. B. Jailbreak und Rooting) zu erfassen.

Treten Auffälligkeiten auf, SOLLTE das MDMS die folgenden Aktionen ausführen können:

[36] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.1.A3 Sichere Grundkonfiguration für mobile Endgeräte und SYS.3.2.1.A16 Deaktivierung nicht benutzter Kommunikationsschnittstellen.
[37] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.1.A11 Verschlüsselung des Speichers
[38] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.2.A21 Verwaltung von Zertifikaten

1. selbstständiges Versenden von Warnhinweisen,

2. selbstständiges Sperren des Geräts,

3. Löschen der vertraulichen Informationen der Einrichtung, insbesondere bei persönlicher Mitnutzung des Gerätes,

4. Zurücksetzen des Geräts auf den Werkszustand,

5. Verhindern des Zugangs zu dienstlichen Applikationen,

6. Verhindern des Zugangs zu den Systemen und Informationen der Einrichtung sowie

7. Verhindern des Zugangs zum MDMS.[39]

b) Die Einrichtung MUSS Compliance-Richtlinien definieren und die Konformität der mobilen Endgeräte mit diesen Richtlinien regelmäßig prüfen. Diese Prüfung KANN über die in (a) genannte Funktion des MDMS erfolgen.

MDM.2.6.13: Automatische Bildschirmsperrung

a) Die Konfiguration und wirksame Durchsetzung einer automatischen Bildschirmsperre des mobilen Endgerätes nach Zeitvorgabe MUSS über das MDMS zentral konfigurierbar sein.

b) Die in (a) beschriebene Funktion des MDMS MUSS im Betrieb genutzt und zentral vorgegeben werden. Die Zeitspanne bis zur Gerätesperrung bei Inaktivität MUSS in Abhängigkeit zum angestrebten Schutzniveau stehen und angemessen kurz sein.[40]

MDM.2.6.14: Sperrbildschirm

a) Das MDMS MUSS den Zugang zu dienstlichen Informationen im Sperrzustand der mobilen Endgeräte konfigurieren können. Dies betrifft auch die Anzeige von Push-Nachrichten, insbesondere deren Inhalt, auf dem Sperrbildschirm.

b) Die Einrichtung MUSS das Anzeigen von vertraulichen Informationen auf dem Sperrbildschirm mithilfe des MDMS verhindern.[41]

MDM.2.6.15: Ferngesteuerte Gerätesperrung (Remote-Lock)

Eine Gerätesperrung MUSS durch den Administrator auch aus der Ferne über das MDMS möglich sein (Remote-Lock). Kann der Remote-Lock auf den mobilen Endgeräten nicht ausgeführt werden, MUSS dies vom MDMS in geeigneter Weise angezeigt werden können.

MDM.2.6.16: Fernlöschung (Remote-Wipe)

a) Das MDMS MUSS die Möglichkeit bereitstellen, auch aus der Ferne einen Befehl an verwaltete Geräte zu senden, um sämtliche dienstliche Daten auf mobilen Endgeräten – einschließlich Zugangsdaten und Zertifikaten – zu löschen (Remote-Wipe bei bestehender Netzwerkverbindung).

b) Werden in mobilen Endgeräten externe Speicher genutzt, MUSS geprüft werden, ob die darauf befindlichen Daten – sofern vom MDM und von der Plattform unterstützt – gelöscht werden sollen.[42]

MDM.2.6.17: Gerätecodes

a) Die Konfiguration und wirksame Durchsetzung von (auch biometrischen) Gerätecodes, Gerätecode-Richtlinien sowie der Gerätecode-Lebensdauer auf den mobilen Endgeräten MUSS zentral über das MDMS konfigurierbar sein. Gleiches gilt für die Vorgabe, nach wie vielen Fehleingaben Endgeräte gesperrt oder

[39] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.2.A23 Durchsetzung von Compliance-Anforderungen
[40] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.1.A4 Verwendung eines Zugriffsschutzes
[41] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.1.A4 Verwendung eines Zugriffsschutzes
[42] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.2.A22 Fernlöschung und Außerbetriebnahme von Endgeräten

gelöscht werden. Ein Reset von Gerätecodes zum Entsperren der Endgeräte MUSS durch den Administrator auch aus der Ferne (z. B. OTA) über das MDMS möglich sein (vgl. MDM.2.5.03).[43]

b) Die mobilen Endgeräte MÜSSEN durch Gerätecodes geschützt sein. Diese müssen die Anforderungen aus MDM.2.2.04 (b) erfüllen.[44]

MDM.2.6.18: Name der mobilen Endgeräte

Der Name der mobilen Endgeräte DARF KEINE Merkmale enthalten, die Rückschlüsse auf den Benutzer oder die Einrichtung ermöglichen.[45] Wählen die Benutzer den Namen der Endgeräte, MÜSSEN sie entsprechend sensibilisiert werden (vgl. MDM.2.8.04).

2.7 Applikationsverwaltung

MDM.2.7.01: Verteilung von Applikationen

a) Eine zentrale Verteilung von Applikationen über das MDMS MUSS möglich sein. Diese MUSS den Anforderungen des geplanten Einsatzszenarios genügen (z. B. rollen- oder gruppenbasierte Verteilung). Die Deinstallation oder Deaktivierung von Applikationen sowie das Verteilen oder Zurückhalten von Updates (auch für System- und vorinstallierte Applikationen) MÜSSEN durch den Administrator auch aus der Ferne erzwingbar sein (z. B. OTA). Dieser Vorgang MUSS durch das MDMS erzwungen werden können, sobald eine Verbindung zwischen MDMS und mobilen Endgeräten besteht.[46]

b) Die Einrichtung MUSS dienstliche Applikationen zentral über das MDMS verwalten und aufbringen. Sicherheitskritische Updates MÜSSEN zeitnah eingespielt werden. Dürfen die Mitarbeiter dienstliche Geräte auch privat nutzen, ~~MUSS~~ SOLLTE ~~geprüft werden, ob der Schutzbedarf der dienstlichen Applikationen es erfordert, dass~~ persönlicher und dienstlicher Bereich separiert werden.

MDM.2.7.02: Bereitstellung von Applikationen

a) Die Einrichtung MUSS sicherstellen, dass ausschließlich vertrauenswürdige Applikationen Zugriff auf sensible IT-Infrastrukturen und Daten der Einrichtung erhalten.

b) Die Einrichtung SOLLTE sicherstellen, dass ausschließlich vertrauenswürdige Applikationen auf den mobilen Endgeräten installiert werden. Dies KANN durch Whitelisting oder Blacklisting erreicht werden.[47] Die Einrichtung SOLLTE unterbinden, dass Applikationen aus nicht vertrauenswürdigen Quellen installiert werden. Ist dies technisch nicht möglich, SOLLTEN die Benutzer hierfür sensibilisiert werden (vgl. MDM.2.8.04: Sensibilisierung der Benutzer).

c) Die Einrichtung SOLLTE bewerten, ob Apps, die sich ohne Installation öffnen lassen (Instant Apps), genutzt werden dürfen. Falls dies nicht erlaubt wird, MÜSSEN entsprechende technische oder organisatorische Maßnahmen ergriffen werden.

MDM.2.7.03: Vorinstallierte Applikationen und Online-Dienste

Die Einrichtung MUSS die Nutzung von vorinstallierten Applikationen und Online-Diensten, insbesondere von externen cloudbasierten Diensten[48], bewerten und im Bedarfsfall per MDMS verhindern oder einschränken. Wird diese Maßnahme nicht technisch durch das Betriebssystem unterstützt, MÜSSEN die

[43] Komponenten außerhalb des Einflussbereichs des MDMS (z. B. Smartcards) sind hiermit nicht gemeint.
[44] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.1.A4 Verwendung eines Zugriffsschutzes
[45] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.1.A12 Verwendung nicht personalisierter Gerätenamen
[46] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.2.A7 Installation von Apps
[47] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.1.A8 Installation von Apps und SYS.3.2.1.A30 Einschränkung der App-Installation mittels Whitelist
[48] vgl. BSI (2021), Mindeststandard des BSI zur Nutzung von externen Cloud-Diensten nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0, S. 1ff.

Benutzer instruiert werden, die entsprechenden Applikationen und Online-Dienste nicht oder nur eingeschränkt zu nutzen (vgl. MDM.2.8.04).[49]

2.8 Betriebsprozesse

MDM.2.8.01: Administration des MDMS

Das MDMS MUSS von Personal (vgl. MDM.2.2.06) bedient werden, das in der sicheren Administration von MDM-Systemen geschult ist.

MDM.2.8.02: Datensicherungen des MDMS

Es MÜSSEN wirksame Mechanismen für das Backup aller Daten und Einstellungen des MDMS existieren, so dass dieses im Bedarfsfall funktionsfähig wiederhergestellt werden kann.

MDM.2.8.03: Umgang mit Sicherheitsvorfällen

Für den Umgang mit Sicherheitsvorfällen MUSS ein angemessener Prozess etabliert sein. Dieser MUSS mindestens eine sofortige Meldung des Vorfalls an eine definierte Stelle, eine Untersuchung der Konsequenzen sowie die Einleitung geeigneter Gegenmaßnahmen beinhalten. Benutzer MÜSSEN dafür sensibilisiert werden, wie sie mit Sicherheitsvorfällen umgehen – insbesondere, dass sie bei Verlust oder Diebstahl eines Geräts sofort die definierte Stelle informieren (vgl. auch MDM.2.8.04).[50]

Insbesondere MUSS der Prozess folgende Szenarien abdecken:

– Verlust mobiler Endgeräte,

– Verdacht des Verlusts der Integrität mobiler Endgeräte (z. B. durch Manipulation durch Dritte) (vgl. MDM.2.6.12),

– kein Kontakt der mobilen Endgeräte zum MDMS über einen längeren Zeitraum hinweg.

In diesen Fällen MUSS der Zugang zu sensiblen IT-Infrastrukturen der Einrichtung wirksam verhindert werden.

MDM.2.8.04: Sensibilisierung der Benutzer

Benutzer von mobilen Endgeräten MÜSSEN für die MDM-Sicherheitsmaßnahmen sensibilisiert werden. Eine Sensibilisierung der Benutzer KANN notwendig sein, um folgende Anforderungen zu erfüllen:

- MDM.2.2.01: Einschränkungen durch Endgeräte oder Betriebsmodell
- MDM.2.2.04: Zugangscodes und -mittel
- MDM.2.6.04: Konfigurationsprofile
- MDM.2.6.05: MDM-Client
- MDM.2.6.18: Name der mobilen Endgeräte
- MDM.2.7.02: Bereitstellung von Applikationen
- MDM.2.7.03: Vorinstallierte Applikationen und Online-Dienste
- MDM.2.8.03: Umgang mit Sicherheitsvorfällen
- MDM.2.6.17: Gerätecodes

MDM.2.8.05: Regelmäßige Überprüfungen

Konfigurationsprofile und Sicherheitseinstellungen MÜSSEN regelmäßig überprüft werden. Die vom MDMS erzeugten Protokolle MÜSSEN regelmäßig auf ungewöhnliche Einträge überprüft werden. Hierbei sind Vorgaben aus der IT-Sicherheitsrichtlinie der Einrichtung zu berücksichtigen. Die zugeteilten

[49] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.1.A2 Festlegung einer Strategie für die Cloud-Nutzung

[50] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.1.A7 Verhaltensregeln bei Sicherheitsvorfällen

Berechtigungen für Benutzer und Personal MÜSSEN mindestens halbjährlich hinsichtlich ihrer Angemessenheit überprüft werden (Minimalprinzip).[51]

MDM.2.8.06: Aktualisierung der Betriebssysteme von MDMS und mobilen Endgeräten

Sollen neue Betriebssystemversionen der mobilen Endgeräte eingesetzt werden, MUSS die Einrichtung vorab prüfen, ob die Konfigurationsprofile und Sicherheitseinstellungen weiterhin wirksam und ausreichend sind. Abweichungen MÜSSEN korrigiert werden. Es MÜSSEN Arbeitsprozesse geplant, getestet und angemessen dokumentiert sein, damit sicherheitsrelevante Patches und Updates für die Betriebssysteme des MDMS und der mobilen Endgeräte unverzüglich eingespielt oder bei bekannten Problemen – sofern vom mobilen Betriebssystem unterstützt – vorerst zurückgehalten werden können.

Werden sicherheitskritische Aktualisierungen nicht innerhalb von 42 Tagen nach der Veröffentlichung eingespielt, MUSS dies gesondert begründet und dokumentiert werden. Bei begründeter Verzögerung von Updatebereitstellung aufgrund personeller Abwesenheit ist darauf zu achten, dass Updates innerhalb eines Zeitraums von 90 Tagen erfolgen MÜSSEN.

MDM.2.8.07: Außerbetriebnahme

Die Einrichtung MUSS MDMS und mobile Endgeräte, für die keine sicherheitsrelevanten Aktualisierungen mehr bereitgestellt werden, außer Betrieb nehmen.[52]

Der Prozess zur Außerbetriebnahme mobiler Endgeräte (Unenrollment) MUSS sicherstellen, dass keine sensitiven Daten auf den mobilen Endgeräten oder eingebundenen Speichermedien verbleiben. Dies gilt insbesondere dann, wenn das Unenrollment aus der Ferne ausgeführt wird (vgl. MDM.2.6.16)).[53]

[51] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.2.A20 Regelmäßige Überprüfung des MDM
[52] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.1.A5 Updates von Betriebssystem und Apps
[53] vgl. IT-Grundschutz-Kompendium, (BSI 2021), SYS.3.2.2.A22 Fernlöschung und Außerbetriebnahme von Endgeräten

Anhang

Zuordnung der Sicherheitsanforderungen zur zuständigen Stelle

Die in Kapitel 2 genannten Sicherheitsanforderungen sind durch die in folgender Tabelle definierte Stelle umzusetzen. Die Einrichtung hat die Umsetzung durch die zuständige Stelle in geeigneter Form sicherzustellen.

Anforderung	MDMS	MDMS-Anbieter	Einrichtung	MDMS-Betreiber[54]
MDM.2.1.01: Strategie für das Mobile Device Management			x	
MDM.2.1.02: Erlaubte mobile Endgeräte			x	
MDM.2.2.01 (a): Einschränkungen durch Endgeräte oder Betriebsmodell	x		x	
MDM.2.2.01 (b): Einschränkungen durch Endgeräte oder Betriebsmodell			x	
MDM.2.2.02: Integration des MDM-Clients	x			
MDM.2.2.03: Nutzdaten	x			
MDM.2.2.04 (a): Zugangscodes -mittel	x			
MDM.2.2.04 (b): Zugangscodes -mittel			x	
MDM.2.2.05: Mandantentrennung	x			
MDM.2.2.06 (a): Berechtigungsmanagement im MDMS	x			
MDM.2.2.06 (b): Berechtigungsmanagement im MDMS			x	
MDM.2.2.07: Absicherung der MDMS-Betriebsumgebung				x
MDM.2.2.08: Sicherheitsanforderungen an den Betrieb im Rechenzentrum				x
MDM.2.2.09: Cloud-Dienste beim Betrieb des MDMS				x
MDM.2.2.10: Mobile Zugänge zu Netzen des Bundes				x
MDM.2.3.01 (a): Protokollierung von Gerätedaten	x			
MDM.2.3.01 (b): Protokollierung von Gerätedaten			x	
MDM.2.3.02 (a): Protokollierung von MDMS-Daten	x			
MDM.2.3.02 (b): Protokollierung von MDMS-Daten			x	
MDM.2.4.01: Dokumentation des MDMS		x		
MDM.2.4.02: Support		x		
MDM.2.4.03: Aktualisierungen des MDMS		x		
MDM.2.5.01: Abgesicherter Kanal				

[54] Wenn die Einrichtung das MDMS selbst betreibt, muss sie die in dieser Spalte genannten Anforderungen selbst umsetzen.

Anforderung	MDMS	MDMS-Anbieter	Einrichtung	MDMS-Betreiber[54]
MDM.2.5.02: Separation des MDMS	x			
MDM.2.5.03: Kommunikation zwischen MDM-Server und MDM-Client	x			
MDM.2.5.04: Kommunikation zwischen MDM-Server sowie Administrations- und Self-Service-Komponenten	x			
MDM.2.5.05 (a): Kommunikation zwischen MDM-Server und sensiblen Infrastrukturen der Einrichtung	x		x	
MDM.2.5.05 (b): Kommunikation zwischen MDM-Server und sensiblen Infrastrukturen der Einrichtung			x	
MDM.2.5.06: Kommunikation zwischen MDM-Server und externen Diensten	x			
MDM.2.6.01: Dokumentation für mobile Endgeräte			x	
MDM.2.6.02: Zusätzliche Dienste zur Verwaltung der mobilen Endgeräte			x	
MDM.2.6.03 (a): Sicheres Enrollment der mobilen Endgeräte	x			
MDM.2.6.03 (b): Sicheres Enrollment der mobilen Endgeräte			x	
MDM.2.6.04 (a): Konfigurationsprofile	x			
MDM.2.6.04 (b): Konfigurationsprofile			x	
MDM.2.6.05 (a): MDM-Client	x			
MDM.2.6.05 (b): MDM-Client			x	
MDM.2.6.06 (a): Administration von Schnittstellen, Diensten und Funktionen	x			
MDM.2.6.06 (b): Administration von Schnittstellen, Diensten und Funktionen			x	
MDM.2.6.07 (a): Monitoring und Diagnose	x			
MDM.2.6.07 (b): Monitoring und Diagnose			x	
MDM.2.6.08 (a): Entwicklermodus	x			
MDM.2.6.08 (b): Entwicklermodus			x	
MDM.2.6.09: Konfiguration von Netzwerkparametern	x			
MDM.2.6.10 (a): Verschlüsselung des Speichers	x			
MDM.2.6.10 (b): Verschlüsselung des Speichers	x			
MDM.2.6.10 (c): Verschlüsselung des Speichers			x	
MDM.2.6.11 (a): Zertifikate	x			
MDM.2.6.11 (b): Zertifikate			x	

Anforderung	MDMS	MDMS-Anbieter	Einrichtung	MDMS-Betreiber[54]
MDM.2.6.12 (a): Compliance-Verstöße und kompromittierte mobile Endgeräte	x			
MDM.2.6.12 (b): Compliance-Verstöße und kompromittierte mobile Endgeräte			x	
MDM.2.6.13 (a): Automatische Bildschirmsperrung	x			
MDM.2.6.13 (b): Automatische Bildschirmsperrung			x	
MDM.2.6.14 (a): Sperrbildschirm	x			
MDM.2.6.14 (b): Sperrbildschirm			x	
MDM.2.6.15: Ferngesteuerte Gerätesperrung (Remote-Lock)	x			
MDM.2.6.16 (a): Fernlöschung (Remote-Wipe)	x			
MDM.2.6.16 (b): Fernlöschung (Remote-Wipe)			x	
MDM.2.6.17 (a): Gerätecodes	x			
MDM.2.6.17 (b): Gerätecodes			x	
MDM.2.6.18: Name der mobilen Endgeräte			x	
MDM.2.7.01 (a): Verteilung von Applikationen	x			
MDM.2.7.01 (b): Verteilung von Applikationen			x	
MDM.2.7.02 (a): Bereitstellung von Applikationen			x	
MDM.2.7.02 (b): Bereitstellung von Applikationen			x	
MDM.2.7.02 (c): Bereitstellung von Applikationen			x	
MDM.2.7.03: Vorinstallierte Applikationen und Online-Dienste			x	
MDM.2.8.01: Administration des MDMS			x	
MDM.2.8.02: Datensicherungen des MDMS			x	
MDM.2.8.03: Umgang mit Sicherheitsvorfällen			x	
MDM.2.8.04: Sensibilisierung der Benutzer			x	
MDM.2.8.05: Regelmäßige Überprüfungen			x	
MDM.2.8.06: Aktualisierung der Betriebssysteme von MDMS und mobilen Endgeräten			x	
MDM.2.8.07: Außerbetriebnahme			x	

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (BSI). 2021. BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. 2021.

—. 2017. BSI-Standard 200-2 – IT-Grundschutz-Methodik, Version 1.0.

—. 2021. IT-Grundschutz-Kompendium, Edition 2021.

—. 2018. Mindeststandard des BSI zur Anwendung des HV-Benchmark kompakt 4.0 nach § 8 Absatz 1 Satz 1 BSIG – Version 1.1 vom 19.06.2018.

—. 2021. Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 07.07.2021.

—. 2021. Mindeststandard des BSI zur Nutzung der ressortübergreifenden Kommunikationsnetze des Bundes („Nutzerpflichten NdB“). nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0a vom 25.02.2021.

—. 2021. Mindeststandard des BSI zur Verwendung von Transport Layer Security nach § 8 Absatz 1 Satz 1 BSIG – Version 2.2 vom 03.05.2021.

Bundesministerium des Innern, für Bau und Heimat (BMI). 2017. Umsetzungsplan Bund 2017 - Leitlinie für die Informationssicherheit in der Bundesverwaltung. Berlin : s.n., 2017.

Deutsches Institut für Normung e.V. (DIN). 2018. DIN 820-2:2018-09: Normungsarbeit - Teil 2: Gestaltung von Dokumenten. Berlin: Beuth Verlag GmbH, 2018.

Internet Engineering Task Force (IETF). 1997. RFC 2119: Key words for use in RFCs to Indicate Requirement Levels. 1997. https://tools.ietf.org/html/rfc2119.

Abkürzungsverzeichnis

APIs	Application Programming Interfaces
BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
DHCP	Dynamic Host Configuration Protocol
DIN	Deutsches Institut für Normung e.V.
DNS	Domain-Name-System
FAQ	Frequently Asked Questions
IETF	Internet Engineering Task Force
ISB	Informationssicherheitsbeauftragte
IT-SiBe	IT-Sicherheitsbeauftragte
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Management
MDMS	Mobile Device Management System
MST	Mindeststandard
NCD	Nutzung externer Cloud-Dienste
NdB	Netze des Bundes
OTA	Over-the-air
RFC	Request for Comments
RZ	Rechenzentren
TR	Technische Richtlinie
UP	Umsetzungsplan
VPN	Virtual Private Network

Konsultationsverfahren Mindeststandard für Mobile Device Management (v1.04) - BSI Stellungname zu Ihren Rückmeldungen

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
2.1.01	Die Einrichtung MUSS eine Strategie für das Mobile Device Management gemäß der Basis-Anforderung SYS.3.2.2.A17 des IT-Grundschutz-Kompendiums erstellen. Zusätzlich zu den in SYS.3.2.2.A1 definierten Aspekten MUSS die Strategie folgende Fragestellungen abdecken: • Wie soll das MDMS in das Netzwerk der Einrichtung eingebunden werden (vgl. auch MDM.2.2.10)? • Welche Maßnahmen zur Absicherung des MDMS und des internen Netzes der Einrichtung sollen getroffen werden?	AA	Es fehlt hier oder im referenzierten Dokument auf den Verweis nach der Art der eingesetzten Lösung: Wie können VS-NfD Lösungen und NON-VS-NfD Lösungen ggf. gleichzeitig eingesetzt werden?	**BSI:** Der Mindeststandard definiert ein verbindliches Mindestniveau für die Informationssicherheit des Bundes. Die Anforderungen gelten also für alle Lösungen gleichermaßen - unabhängig davon, welchem Geheimhaltungsgrad sie entsprechen. Eine Unterscheidung nach VS-NfD- und Non-VS-NfD-Lösungen wäre daher gegenstandslos.	
2.1.02	Allgemein	AA	Hier sollten auch die Beschaffungswege/-prozesse Berücksichtigung finden, da gerade auch die Sicherheitsmechanismen der VS-NfD Lösungen ggf. auf diese aufbauen.	**BSI**: Wir haben eine Mindestanforderung für die Beschaffung ergänzt. Der Mindeststandard macht jedoch keine Vorgaben auf VS-NfD-Niveau, dies geschieht über die Einsatz- und Betriebsbedingungen der VS-NfD-Lösungen.	
MDM.2.2.04	Die Anzahl der maximal möglichen Fehlversuche für	AA	Zusätzlich sollte die Zeitspanne zwischen einer Falscheingabe und	**BSI:** Diese Zeitspanne ist allein bei iOS schon nicht per MDM	

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
	die Eingabe des Zugangscodes MUSS festgelegt und technisch umgesetzt werden. Nach Überschreitung der Grenze MUSS der Zugang des Benutzers gesperrt werden.		dem nächsten Versuch konfigurierbar sein.	konfigurierbar. Daher ginge eine solche Anforderung über die praktischen Möglichkeiten hinaus.	
MDM.2.2.06	b) Die Einrichtung MUSS über ein Berechtigungskonzept für das MDMS verfügen. Benutzergruppen und Personal DÜRFEN NUR über Berechtigungen verfügen, die für die Aufgabenerfüllung notwendig sind (Minimalprinzip).20 Die Zugriffsrechte für das Personal MÜSSEN mindestens in die in (a) genannten Rollen unterteilt werden.	AA	Die Einrichtung muss über ein übergreifendes Berechtigungskonzept verfügen in dem das MDMs mit abgedeckt ist.	**BSI:** Das ist zu empfehlen, eine solche Empfehlung ginge aber über den Rahmen des Mindeststandards MDM hinaus. Die jetzige Formulierung lässt es aber durchaus zu, dass das "Berechtigungskonzept für das MDMS" nur ein Teil eines übergreifenden Konzepts ist.	
MDM.2.3.01	– installierten Zertifikaten,	AA	Und Schlüsselmitteln/ -lesegeräten?	**BSI:** Falls damit zum Beispiel ein Smartcard-Reader und eine Smartcard gemeint sind, kann das MDMS nicht auf deren Status zugreifen, da diese geräteextern sind.	
MDM.2.3.01	– installierten Applikationen inkl. Versionsstand.	AA	Änderungsvorschlag: – installierten Applikationen inkl. Versionsstand und Zugriffsberechtigungen,. – Konfigurations- und Installationshistorie .	**BSI:** Die Konfigurations- und Installationshistorie ist bereits mit der jetzigen Formulierung abgedeckt: Sie wird im MDMS geloggt, siehe letzter Satz von MDM.2.3.01a). MDMS sind leider nicht in der Lage, die Zugriffsberechtigungen	

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
			Nicht nur der Stand zu einem bestimmten Zeitpunkt, auch der Verlauf über die Zeit (Logs) müssen abrufbar sein. Um dem bspw. Dem Vorgehen „Applikation installieren, nutzen, deinstallieren“ gewahr zu werden. Ähnlich für Konfigurationseinstellungen. Nur so kann bspw. eine Einbindung in ein SIEM erfolgreich sein. GGF. ist hier auch etwas zum Log-Standard zu definieren, wenigstens, dass die Einrichtung diesen festlegen und dieser auf offenen Standards beruhen sollte.	von Apps beim Endgerät abzufragen. Die Anforderung an das MDMS, beim Logging offene Standards zu nutzen, adressiert vor allem ein betriebliches Problem und gehört daher nicht in diesen Mindeststandard. Zudem könnte im Einzelfall auch eine proprietäre Schnittstelle aus Sicherheitssicht von Vorteil sein, daher wollen wir sie hier nicht ausschließen.	
MDM.2.3.01	b) Die Einrichtung MUSS das MDMS so konfigurieren, dass nur Personal mit den Rollen Administrator und Auditor (vgl. MDM.2.2.06) die erhobenen Gerätedaten eingesehen kann.	AA	einsehen statt eingesehen	**BSI:** Geändert.	b) Die Einrichtung MUSS das MDMS so konfigurieren, dass nur IT-Betriebspersonal mit den Rollen Administrator und Auditor (vgl. MDM.2.2.06) die erhobenen Gerätedaten einsehen kann. Die Einrichtung MUSS durch technische oder organisatorische Maßnahmen (z. B. die Berechtigungen der Rollen Auditor und Administrator entsprechend einschränken) sicherstellen, dass die Daten nicht manipuliert werden können.
MDM.2.3.02	Allgemein	AA	Das MDMS SOLLTE die Möglichkeit bieten, Protokolldaten über einen abgesicherten Kanal zu übertragen (Push).	**BSI:** Es ist unklar, ob hier gemeint ist, dass Protokolldaten vom mobilen Endgerät zum MDMS über einen abgesicherten Kanal übertragen werden sollen, oder von MDMS an ein zweites System (z.B. ein SIEM). In beiden Fällen jedoch ist diese Möglichkeit dank Kapitel 2.5 gegeben.	
MDM.2.4.01	Allgemein	AA	Sollte sich an Standardprozessen wie z.B. ITIL orientieren.	**BSI:** Da wir hier als Inhalt der Dokumentation vor allem	

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
				technische Informationen abfragen, werden eher keine Prozesse beschrieben.	
MDM.2.4.01	– Angaben über die grundlegende Architektur des MDMS,	AA	Oder der lösungsbezogenen Infrastruktur?	**BSI:** Dies ist eine Anforderung, die sich nur auf das MDM-System bezieht und an dessen Hersteller richtet. Dieser kann über die lösungsbezogene Infrastruktur (z.B. die Komponenten für die iOS-Systemlösung im Netz des Betreibers) keine Aussage treffen.	
MDM.2.4.02	Allgemein	AA	Sollte sich an Standardprozessen wie z.B. ITIL orientieren.	**BSI**: Text entsprechend angepasst.	Supportleistungen des Anbieters MÜSSEN den Anforderungen des jeweiligen Einsatzszenarios entsprechen. Dabei MÜSSEN zumindest betrachtet werden: • Support rund um das Enrollment, • Support bei der Wartung des MDMS (besonders bzgl. MDMS-Updates) sowie der Wartung der zugehörigen Komponenten, • Support auch ohne Fernzugriffsmöglichkeiten, • Erreichbarkeits- und Reaktionszeiten, • Incident Management. Die Support-Prozesse SOLLTEN sich an Standardprozessen (z. B. ITIL) orientieren.
MDM.2.4.02	Supportleistungen des Anbieters MÜSSEN den Anforderungen des jeweiligen Einsatzszenarios entsprechen. Dies gilt insbesondere für:	AA	Wartung des MDMs inklusive zugehörigen Komponenten und der Infrastruktur	**BSI:** Wir haben den Punkt "MDMS-Updates" entsprechend erweitert, allerdings ohne Bezug auf die "Infrastruktur", da diese nicht zum Geltungsbereich des MDM-Mindeststandards gehört.	Supportleistungen des Anbieters MÜSSEN den Anforderungen des jeweiligen Einsatzszenarios entsprechen. Dabei MÜSSEN zumindest betrachtet werden:

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
					• Support rund um das Enrollment, • Support bei der Wartung des MDMS (besonders bzgl. MDMS-Updates) sowie der Wartung der zugehörigen Komponenten, • Support auch ohne Fernzugriffsmöglichkeiten, • Erreichbarkeits- und Reaktionszeiten, • Incident Management. Die Support-Prozesse SOLLTEN sich an Standardprozessen (z. B. ITIL) orientieren.
2.5	Allgemein	AA	Wie soll eine Absicherung des MDMS zu Mailserver (für Mailversand durch MDMS) erfolgen, bspw. TLS/SSL?	**BSI:** Auch diese Kommunikation sollte über einen abgesicherten Kanal nach MDM.2.5.01 erfolgen, also z.B. Mutual TLS gemäß Mindeststandard "Verwendung von Transport Layer Security". Dies ist über "MDM.2.5.05: Kommunikation zwischen MDM-Server und sensiblen Infrastrukturen der Einrichtung" abgedeckt. Wir haben dort Mailserver als Beispiel ergänzt.	MDM.2.5.05 Soll das MDMS an Infrastrukturen der Einrichtung (z. B. Verzeichnisdienste oder Mailserver) angebunden werden, sind folgende Anforderungen zu erfüllen: 1. a) Die Verbindung zwischen MDMS und den Infrastrukturen der Einrichtung MUSS über einen *Abgesicherten Kanal* (vgl. MDM.2.5.01) erfolgen. 2. b) Die Einrichtung MUSS bewerten, ob ihre sensiblen Infrastrukturen durch weitere Maßnahmen geschützt werden müssen (z. B. wenn ein Zonenmodell verwendet wird).
2.6	Allgemein	AA	Zusätzlich sollte eine Anforderung zu aktuell gültigem Schutz vor Malware und dessen Überprüfung aufgenommen werden.	**BSI:** Solche Funktionen sind nicht Teil von Mobile Device Management an sich, sondern fallen eher allgemein unter den	

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
				Oberbegriff Sicherheit mobiler Endgeräte und können auch unabhängig von einem MDM-System umgesetzt werden. Daher möchten wir sie hier nicht aufnehmen.	
MDM.2.6.03	Allgemein	AA	Beschaffungsweg der Endgeräte wird nicht erwähnt obwohl sichere mobile Lösungen im VS-NfD Bereich auf Sicherheitsmechanismen der Hersteller vertrauen, bspw. DEP	**BSI**: Wir haben eine Mindestanforderung für die Beschaffung in MDM.2.1.02 ergänzt. Der Mindeststandard macht jedoch keine Vorgaben auf VS-NfD-Niveau, dies geschieht über die Einsatz- und Betriebsbedingungen der VS-NfD-Lösungen.	MDM.2.1.02 Es MUSS festgelegt werden, welche mobilen Endgeräte und Betriebssysteme in der Einrichtung erlaubt sind. Bereits bei der Auswahl zu beschaffender mobiler Endgeräte MUSS die Einrichtung darauf achten, dass der Hersteller über den geplanten Nutzungszeitraum Sicherheitsaktualisierungen für die Geräte bereitstellt. Die Einrichtung MUSS die mobilen Endgeräte über eine *vertrauenswürdige* Quelle beschaffen.
MDM.2.6.03	a) Für das Enrollment der mobilen Endgeräte MUSS das MDMS eine sichere Schnittstelle bereitstellen. Zusätzlich zu MDM.2.6.0233 gilt während des Enrollments:	AA	Dienstliche vs. Private Endgeräte: Grundsätzlich fehlen der Ausschluss bzw. die Separierung zu privaten Geräten und deren möglichen Zugriff auf dienstliche Infrastrukturen und Informationen.	**BSI:** Der MDM-Mindeststandard schließt BYOD-Szenarien weder explizit aus, noch werden sie empfohlen. Die Separierung von privaten Apps ist mit MDM.2.7.01 abgedeckt.	
MDM.2.6.03	b) Alle mobilen Endgeräte, die Zugriff auf sensible IT-Infrastrukturen oder Daten der Einrichtung haben, SOLLTEN per MDM verwaltet werden. Die Einrichtung MUSS die zu verwaltenden mobilen Endgeräte so schnell wie möglich in das MDMS integrieren und nach den	AA	Private Endgeräte via MDMS zu verwalten? Gemischte Nutzung möglich?	**BSI:** Der MDM-Mindeststandard schließt BYOD-Szenarien weder explizit aus, noch werden sie empfohlen. Die Separierung von privaten Apps ist mit MDM.2.7.01 abgedeckt.	

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
	Richtlinien der Einrichtung konfigurieren und verwalten.				
MDM.2.6.03	Vor dem Enrollment MÜSSEN sich die mobilen Endgeräte im Werkszustand befinden.	AA	1.) Wie definiert sich Werkszustand? Ein iPhone 11 bspw. wird ab Werk mit iOS 13 ausgeliefert und kann auf iOS 15 geupdatet werden. Zählt nach Reset des Gerätes iOS 15 als Werkszustand? Enrollment erfolgt beim Kunden mit iOS 15 und ist unserer Meinung nach nicht mehr 2.) Wenn Geräte mittels DEP bestellt werden sind diese für das AA Werkszustand. Wird kurzfristig ein Gerät bei einem anderen Händler ohne DEP gekauft, ist dies auch Werkszustand. Wird das Gerät nun manuell dem DEP zugeführt, hat sich der Werkszustand geändert. Wie muss damit umgegangen werden?	**BSI:** 1) Wir haben den Text entsprechend geändert. 2) Bei iOS beinhaltet ein Enrollment immer automatisch - außer bei User Enrollment - ein Reset. Daher ist die Anforderung erfüllt.	Vor dem Enrollment SOLLTEN sich die mobilen Endgeräte im Werkszustand befinden oder zurückgesetzt werden.
MDM.2.6.05	a) Stellt das MDMS einen MDM-Client als Applikation auf den mobilen Endgeräten bereit, SOLLTE das MDMS eine Deinstallation des MDM-Clients durch den Benutzer verhindern können (z. B. durch Passwortschutz).	AA	Deinstallation des MDM-Client sollte durch MDM-Server automatisiert erkannt und gemeldet werden.	**BSI:** Dies ist über "MDM.2.3.01 Protokollierung von Gerätedaten" abgedeckt. Im Zuge der Diskussionen ist außerdem MDM.2.6.05 zur Löschung der MDM-Client-App ganz weggefallen, da eine Löschung durch den Benutzer bei Erfüllung von "MDM.2.2.02: Integration einer MDM-Client-App" ohnehin technisch nicht möglich ist.	entfallen
MDM.2.6.05	b) Kann eine unautorisierte Löschung des MDM-Clients – wie in (a) gefordert – technisch nicht verhindert werden, MÜSSEN	AA	Die Löschung des MDM-Client ist zwingend zu protokollieren. Das Protokoll muss enthalten: Datum+ Uhrzeit (Timestamp in UTC), Gerätekennung und Nutzerkennung	**BSI**: Dies ist über "MDM.2.3.01 Protokollierung von Gerätedaten" abgedeckt. Wir haben die Anforderung MDM.2.3.01 zudem noch um Zeitstempel etc. ergänzt.	entfallen

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
	organisatorische Maßnahmen ergriffen werden – insbesondere die Sensibilisierung des Benutzers (vgl. MDM.2.8.04).		die die Löschung veranlasst hat, sofern technisch möglich.		
MDM.2.6.06	a) Kommunikationsdienste wie SMS und MMS sowie Funktionen wie Kameras, Mikrofone, digitale Assistenten (z. B. Siri) und Sprachsteuerungen MÜSSEN zentral und so granular, wie das Betriebssystem ermöglicht, über das MDMS administrierbar sein.	AA	Ggf. umformulieren: alle Ressourcen und externen Dienste	**BSI:** Wir möchten hier um der Verständlichkeit Willen bei der konkreteren Formulierung bleiben. Die Formulierung über "wie" deckt nicht genannte Funktionen ausreichend mit ab.	
MDM.2.6.06	Gleiches gilt für Schnittstellen-Funktionen. Unter Schnittstellen sind insbesondere Bluetooth, WLAN, GPS und USB, sofern vorhanden, zu verstehen. Das Betriebssystem der verwalteten Geräte kann weitere Schnittstellen bereitstellen; die zugehörigen Funktionen SOLLTEN durch das MDMS ebenfalls administrierbar sein.	AA	NFC, Lightning	**BSI:** NFC und Lightning aufgenommen.	Gleiches gilt für Schnittstellen-Funktionen. Unter Schnittstellen sind insbesondere Bluetooth, WLAN, GPS, NFC und USB bzw. Lightning, sofern vorhanden, zu verstehen. Das Betriebssystem der verwalteten Geräte kann weitere Schnittstellen bereitstellen; die zugehörigen Funktionen SOLLTEN durch das MDMS ebenfalls administrierbar sein.
MDM.2.6.06	Ein Koppeln oder Verbinden mit anderen Geräten (z. B. via Apple AirDrop oder die Anbindung eines Monitors via USB) zum Datenaustausch oder zur Datenweitergabe MUSS	AA	…ist zu unterbinden, wenn nicht verhindert werden kann, das VS-NfD Daten übertragen werden können	**BSI:** Der Mindeststandard gilt für Lösungen jeglicher Einstufung und macht daher keine Vorgaben für VS-NfD. Für VS-NfD müssen die entsprechenden SecOps beachtet werden.	

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
	unterbunden werden können.				
MDM.2.6.08	Allgemein	AA	Wie sieht es mit Beta Tests aus? Sollte für den betrieblichen Einsatz reguliert werden.	**BSI:** Wir haben eine neue Anforderung zu Beta-Tests von Apps und mobilen Betriebssystemen aufgenommen.	**MDM.2.6.06: Betatests** Nutzt die Einrichtung auf gewissen mobilen Endgeräten Betaversionen von Applikationen oder Betriebssystemen, MÜSSEN diese Endgeräte im MDMS separat verwaltet werden.
MDM.2.6.11	a) Das MDMS MUSS auf den mobilen Endgeräten Zertifikate installieren, aktualisieren und anzeigen können, für die das Betriebssystem dies ermöglicht (z. B. Email, ActiveSync, VPN, WLAN und Websites). Die Installation von nicht verifizierbaren Zertifikaten durch den Benutzer MUSS verhindert werden können. Das MDMS muss in der Lage sein, Informationen zum Widerruf von Zertifikaten (z. B. CRLs) an die Endgeräte zu senden. Der Status eines Zertifikates (gültig/ungültig) MUSS vom MDMS in geeigneter Weise angezeigt werden. Das MDMS MUSS den sicheren Transfer (z. B. PKCS#12 verschlüsselt) von Zertifikaten unterstützen	AA	zu: Das MDMS **MUSS** in der Lage sein, Informationen zum Widerruf von Zertifikaten (z. B. CRLs) an die Endgeräte zu senden. Hierbei handelt es sich um einen für die gesamte Infrastruktur kritischen Prozess. Die Zeitspanne zur Aktualität der Revocation Lists MUSS festgelegt sein, um ein residuales Risiko für die Organisation akzeptierbar zu machen. Vorschlag: als Vorgabe min. alle 24h die CRLs aktualisieren oder On-Line Protokolle wie OCSP Multistapling (RFC6961, bitte nicht „normales“ OCSP) zur Zertifikatsvalidierung nutzen.	**BSI:** "MUSS" nun großgeschrieben. Wir haben einen entsprechenden Satz ergänzt.	**MDM.2.6.12: Zertifikate** a) Das MDMS MUSS auf den mobilen Endgeräten Zertifikate installieren, aktualisieren und anzeigen können, für die das Betriebssystem dies ermöglicht (z. B. E-Mail, ActiveSync, VPN, WLAN oder Websites). Die Installation von nicht verifizierbaren Zertifikaten durch den Benutzenden MUSS verhindert werden können. Das MDMS MUSS in der Lage sein, Informationen zum Widerruf von Zertifikaten (z. B. Certificate Revocation Lists (CRLs)) an die Endgeräte zu senden. Der Status eines Zertifikates (gültig/ungültig) MUSS vom MDMS in geeigneter Weise angezeigt werden. Das MDMS MUSS den sicheren Transfer (z. B. PKCS#12 verschlüsselt) von Zertifikaten unterstützen.
MDM.2.6.12	Allgemein	AA	Verstöße gegen die Compliance-Regeln oder vom MDMS als kompromittiert identifizierte Endgeräte	**BSI:** Wir haben die Compliance-Verstöße in MDM2.3.01 ergänzt, die Kompromittierungsindikatoren	**MDM.2.3.01: Protokollierung von Gerätedaten**

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
			müssen vollständig protokolliert werden. Für die Auditierung sind Gerätekennung, Art des Verstoßes / IoC, Datum + Uhrzeit (Timestamp) und Nutzerkennung erforderlich.	nicht, da ihre Erfassung in MDM2.6.13a) bewusst nur eine KANN-Anforderung ist.	1. a) Der aktuelle Status der verwalteten Endgeräte MUSS über das MDMS ermittelt werden können. Dies MUSS mindestens Folgendes umfassen: • installierte Zertifikate, • Konfigurationseinstellungen, • Betriebssystemversion / Patch-Level von Endgeräten, • installierten Applikationen inkl. Versionsstand, • Compliance-Verstößen. Das MDMS MUSS Änderungen an diesen Gerätemerkmalen, deren Verursacher, einen Zeitstempel und die Gerätekennung protokollieren und zentral zum Abruf bereitstellen.
MDM.2.7.01	Allgemein	AA	Wie deckt sich das mit VS-NfD und selbstsignierten Apps?	**BSI:** Auch selbst signierte Apps wie SecurePIM lassen sich per MDMS verteilen.	
MDM.2.7.02	Allgemein	AA	1) Zusätzlich sollte gesteuert werden können, in welchen Verzeichnissen Applikationen voneinander getrennt installiert werden. Weiterhin sollten Zugriffsberechtigungen von Applikationen überwacht und gesteuert werden sowie das Ausführen im Hintergrund unterbunden werden können. 2) Das MDMS SOLLTE die Möglichkeit bieten, für die bereitgestellten Applikationen Datenschutz- &	**BSI:** 1.1 In welchen Verzeichnissen Applikationen installiert werden, kann nicht per MDMS gesteuert werden. 1.2. MDMS sind leider nicht in der Lage, die Zugriffsberechtigungen von Apps beim Endgerät abzufragen. 1.3 Das Unterbinden einer App-Ausführung im Hintergrund ist bei iOS nicht nötig, da das Betriebssystem selbst ausreichende Maßnahmen	

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
			Geräteberechtigungseinstellungen zentral und Systemweit vorzugeben.	ergreift. Bei Android werden wie bei iOS die Hintergrundprozesse hinsichtlich des Ressourcen-Verbrauchs bewertet und bei Bedarf automatisch beendet. Ein vollständiges Unterbinden von Hintergrundprozessen ist grundsätzlich zwar möglich, aber für die Benutzung aus unserer Sicht wenig sinnvoll. 2. Siehe Antwort 1.2.	
2.8	Allgemein	AA	HA Setup, Notfallkonzept, Georedundanz?	**BSI:** Der Mindeststandard definiert ja nur ein Mindestniveau der Sicherheit, also zum Beispiel für eine kleine Behörde, die mobile Endgeräte rein für offene Telefonie nutzt. Hier wären Hochverfügbarkeit, Notfallkonzept und Georedudanz zu hohe Anforderungen.	
MDM.2.8.03	MDM.2.8.03: Umgang mit Sicherheitsvorfällen	AA	Beschaffung von Endgeräten im Ausland?	**BSI**: Wir haben eine Mindestanforderung für die Beschaffung in MDM.2.1.02 ergänzt.	**MDM.2.1.02: Erlaubte mobile Endgeräte** Es MUSS festgelegt werden, welche mobilen Endgeräte und Betriebssysteme in der Einrichtung erlaubt sind. Bereits bei der Auswahl zu beschaffender mobiler Endgeräte MUSS die Einrichtung darauf achten, dass der Hersteller über den geplanten Nutzungszeitraum Sicherheitsaktualisierungen für die Geräte bereitstellt. Die Einrichtung MUSS die mobilen Endgeräte über eine *vertrauenswürdige* Quelle beschaffen.
MDM.2.8.03	Für den Umgang mit Sicherheitsvorfällen MUSS	AA	Diese Anforderung wird als manueller Prozess, angestoßen durch den	**BSI:** Es ist durchaus so gemeint, dass diese Meldung je nach	Für den Umgang mit Sicherheitsvorfällen MUSS ein angemessener Prozess

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
	ein angemessener Prozess etabliert sein. Dieser MUSS mindestens eine sofortige Meldung des Vorfalls an eine definierte Stelle, eine Untersuchung der Konsequenzen sowie die Einleitung geeigneter Gegenmaßnahmen beinhalten. Benutzer MÜSSEN dafür sensibilisiert werden, wie sie mit Sicherheitsvorfällen umgehen – insbesondere, dass sie bei Verlust oder Diebstahl eines Geräts sofort die definierte Stelle informieren (vgl. auch MDM.2.8.04).50 Insbesondere MUSS der Prozess folgende Szenarien abdecken: – Verlust mobiler Endgeräte, – Verdacht des Verlusts der Integrität mobiler Endgeräte (z. B. durch Manipulation durch Dritte) (vgl. MDM.2.6.12), – kein Kontakt der mobilen Endgeräte zum MDMS über einen längeren Zeitraum hinweg. In diesen Fällen MUSS der Zugang zu sensiblen IT-Infrastrukturen der Einrichtung wirksam verhindert werden.		Endnutzer, verstanden. Es sollte um eine automatisierte Komponente ergänzt werden.	Vorfallsart auch automatisch passieren kann, z.B. eine Nachricht vom MDMS an den User und/oder Admin bei einem Compliance-Verstoß des Endgeräts. Wir haben entsprechend ergänzt.	etabliert sein. Dieser MUSS mindestens eine sofortige (automatisierte oder manuelle) Meldung des Vorfalls an eine definierte Stelle, eine Untersuchung der Konsequenzen sowie die Einleitung geeigneter Gegenmaßnahmen beinhalten. Benutzende MÜSSEN dafür sensibilisiert werden, wie sie mit Sicherheitsvorfällen umgehen – insbesondere, dass sie bei Verlust oder Diebstahl eines Geräts sofort die definierte Stelle informieren (vgl. auch MDM.2.8.05). Insbesondere MUSS der Prozess folgende Szenarien abdecken: • Verlust mobiler Endgeräte, • Verdacht des Verlusts der Integrität mobiler Endgeräte (z. B. durch Manipulation durch Dritte) (vgl. MDM.2.6.13), • kein Kontakt der mobilen Endgeräte zum MDMS über einen längeren Zeitraum hinweg. In diesen Fällen MUSS der Zugang zu IT-Infrastrukturen der Einrichtung wirksam verhindert werden.

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
MDM.2.8.06	Werden sicherheitskritische Aktualisierungen nicht innerhalb von 42 Tagen nach der Veröffentlichung eingespielt, MUSS dies gesondert begründet und dokumentiert werden. Bei begründeter Verzögerung von Updatebereitstellung aufgrund personeller Abwesenheit ist darauf zu achten, dass Updates innerhalb eines Zeitraums von 90 Tagen erfolgen MÜSSEN.	AA	Wie definieren sich Tage (Werktage vs. Kalendertage) Im AA werden ca. 4.500 mobile Endgeräte weltweit eingesetzt. Tests von neuen Betriebssystemversionen dauern mind. 10 Werktage. 42 Tage für die Aktualisierung von 4.500 Endgeräten sind in der Praxis unzureichend und können mit den bestehen Lösungen (VS-NfD: iOS Systemlösung und SS4SK) nicht realisiert werden.	**BSI:** Auch aufgrund anderer Rückmeldungen haben wir nun eine flexiblere Formulierung gewählt.	**MDM.2.8.07: Aktualisierung der Betriebssysteme von MDMS und mobilen Endgeräten** Sollen neue Betriebssystemversionen der mobilen Endgeräte eingesetzt werden, MUSS die Einrichtung vorab prüfen, ob die Konfigurationsprofile und Sicherheitseinstellungen weiterhin wirksam und ausreichend sind. Abweichungen MÜSSEN korrigiert werden. Es MÜSSEN Arbeitsprozesse geplant, getestet und angemessen dokumentiert sein, damit sicherheitsrelevante Patches und Updates für die Betriebssysteme des MDMS und der mobilen Endgeräte unverzüglich eingespielt oder bei bekannten Problemen – sofern vom mobilen Betriebssystem unterstützt – vorerst zurückgehalten werden können. Die Einrichtung MUSS eine möglichst kurze Frist definieren, bis zu der sicherheitskritische Aktualisierungen[1] eingespielt werden müssen. [1] Als sicherheitskritisch anzusehen sind insbesondere Aktualisierungen, welche die Gefahr eines ungewollten Abflusses dienstlicher Daten, einer Manipulation sensibler Daten oder eines Ausfalls verringern.

Konsultationsverfahren Mindeststandard für Mobile Device Management (v1.04) - BSI Stellungname zu Ihren Rückmeldungen

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
Allgemein		BeschA	Unserer Einschätzung nach sollte grundsätzlich geprüft werden, ob es zielführend ist (Minimierung doppelter Datenhaltung), Schnittstellen zu anderen Systemen bereitzustellen. Beispielsweise wären hier Telekommunikationsmanagementsysteme zu nennen, die bei der Tarifoptimierung und der Abrechnung unterstützen.	**BSI:** Schnittstellen zu externen Diensten sind über MDM.2.5.06 abgedeckt. Wir haben die entsprechende Anforderung so verallgemeinert, dass nicht nur sicherheitsrelevante Dienste darunter fallen. Damit sind Schnittstellen des MDM-Servers zu anderen Systemen wie z.B. Telekommunikationsmanagementsysteme n aus Sicherheitssicht abgedeckt.	
Zu Version 1.0: MDM.06: SIM-Karten	Das MDM muss die notwendigen Informationen bereithalten, um eine Sperrung der SIM-Karte veranlassen zu können.	BeschA	Die Anforderung soll in der neuen Version entfallen. Sofern die erforderlichen Daten unter MDM.01: Nutzdaten zu finden sind, sollte das passen. Falls nicht wäre zu prüfen, inwieweit die Anforderung erhalten bleibt.	**BSI:** Die Sperrung der SIM oder eSIM (im Gegensatz zum Endgerät) wird nicht vom MDMS selbst durchgeführt, sondern durch den Mobilfunkanbieter. Daher haben wir die Anforderung wieder integriert, aber als Anforderung an die Einrichtung.	
MDM.2.2.04	Zudem SOLLTE Zwei-Faktor-Authentifizierung genutzt werden. Für das Zurücksetzen von Passwörtern SOLLTE ein angemessenes sicheres Verfahren definiert und umgesetzt werden. Der Zugriff auf Application Programming Interfaces (APIs) SOLLTE durch einen Authentifizierungsmechanismus (z. B. Access Tokens) geschützt sein.	BeschA	Hier sollte geprüft werden, inwieweit in dem folgenden Passus statt SOLL ein MUSS zielführend ist:„Zudem MUSS eine Zwei-Faktor-Authentifizierung genutzt werden. Für das Zurücksetzen von Passwörtern MUSS ein angemessenes sicheres Verfahren definiert und umgesetzt werden. Der Zugriff auf Application Programming Interfaces (APIs) MUSS durch einen Authentifizierungsmechanismus (z. B. Access Tokens) geschützt sein.“	**BSI:** Der IT-Grundschutz beinhaltet die Zwei-Faktor-Authentifizierung sowie ein sicheres Verfahren für das Zurücksetzen von Passwörtern nur als Standardanforderung ("SOLLTE"). Wie im Vorwort erläutert, geht das Sicherheitsniveau des Grundschutzes über das der Mindeststandards hinaus. Hier wird daher das Modalverb aus dem Grundschutz übernommen. In Bezug auf APIs haben wir das "MUSS" übernommen.	Zudem SOLLTE Zwei-Faktor-Authentifizierung genutzt werden. Für das Zurücksetzen von Passwörtern SOLLTE ein angemessenes sicheres Verfahren definiert und umgesetzt werden. Der Zugriff auf APIs MUSS durch einen Authentifizierungsmechanismus (z. B. Access Tokens) geschützt sein.

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
MDM.2.6.02	Wird ein zusätzlicher Dienst genutzt, der die Funktionalität des genutzten MDMS erweitert (z. B. ein Service für OTA-Betriebssystemupdates oder zum automatisierten Enrollment aus der Ferne, vgl. MDM.2.6.03), MUSS ein vertrauenswürdiger Anbieter hierfür gewählt werden.	BeschA	Falls „vertrauenswürdiger Anbieter“ nicht definiert ist, sollte der Begriff konkretisiert/erläutert werden. Ergänzend wurde von einem Beschaffungsreferat der Hinweis gegeben, dass in den dortigen Verfahren bzw. Verträgen MDM bisher nur als Teil einer sicheren Lösung enthalten sind (RV für SecurePIM und SecuVOICE MobileIron-Lizenzen).	**BSI:** Was "vertrauenswürdig" bedeutet, ist in Kapitel 1.1 definiert. Danke für den Hinweis. Bei der Nutzung zusätzlicher Diensten zur Verwaltung der mobilen Endgeräte im Rahmen der sicheren mobilen Lösungen sind die SecOps zu beachten. Wir sehen hier keinen Widerspruch zu MDM.2.6.02. Der Mindeststandard gilt zudem auch für MDM-Systeme, die für andere Lösungen als eine sichere mobile Lösung genutzt werden.	Wird ein Dienst genutzt, der die Funktionalität des genutzten MDMS erweitert (z. B. ein Service für Over-the-air(OTA)-Betriebssystemupdates oder zum automatisierten Enrollment aus der Ferne, vgl. MDM.2.6.03), MUSS ein *vertrauenswürdiger* Anbieter hierfür gewählt werden. 1.1 Was der Begriff *vertrauenswürdig* in diesem Mindeststandard bedeutet, hängt vom jeweiligen Einsatzszenario des MDMS ab (zum Beispiel vom Schutzbedarf der mobil verarbeiteten Daten) und ist von der Einrichtung bewusst zu evaluieren und zu entscheiden.

Konsultationsverfahren Mindeststandard für Mobile Device Management (v1.04) - BSI Stellungname zu Ihren Rückmeldungen

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
MDM.2.5.04	Sämtliche Kommunikation zwischen MDM-Server und Administrations- und Self-Service-Komponenten, sofern solche genutzt werden sollen, MUSS über einen Abgesicherten Kanal (vgl. MDM.2.5.01) erfolgen.	BMF	An anderen Stellen des Dokuments ist von "MDM-Server und MDM-Client" die Rede. Bei der zitierten Textstelle ist unklar, ob mit "Administrations- und Self-Service-Komponente" ebenfalls der MDM-Client gemeint ist. Änderungsvorschlag: Sollten "MDM-Client" und "Administrations- und Self-Service-Komponente" analog verwendbar sein, sollte vereinheitlichte Begriffe genutzt werden. Sollte es sich um unterschiedliche Komponenten handeln, sollten deren Abgrenzung/Definition klargestellt werden.	**BSI:** Nein, "MDM-Client" und "Administrations- und Self-Service-Komponenten" sind nicht synonym. MDM-Client ist in Kapitel 1.1 definiert: als eine Komponenten auf dem mobilen Endgerät, die eine Applikation oder Teil des Betriebssystems (z.B. die von iOS bereitgestellte MDM-Schnittstelle) sein kann. Administrations- und Self-Service-Komponenten meinen hier Verwaltungsschnittstellen zum MDM-Server, z.B. Webbrowser, Anwendungssoftware (s. MDM.2.5.02) oder ein Self-Service-Portal für den Endnutzer. Wir haben eine Definition zu letzteren in 1.1 ergänzt.	

Konsultationsverfahren Mindeststandard für Mobile Device Management (v1.04) - BSI Stellungname zu Ihren Rückmeldungen

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
MDM.2.8.07	Die Einrichtung MUSS MDMS und mobile Endgeräte, für die keine sicherheitsrelevanten Aktualisierungen mehr bereitgestellt werden, außer Betrieb nehmen.	BWI	Hier wäre die konkrete Vorgabe einer Karenzzeit wünschenswert.	**BSI:** Wir haben eine Formulierung für einen möglichst kurzen Zeitraum ergänzt, die zugleich genügend Spielraum für Szenarien mit verschiedenen Schutzbedarfen bietet.	**MDM.2.8.09: Außerbetriebnahme** Die Einrichtung MUSS MDMS und mobile Endgeräte, für die keine sicherheitsrelevanten Aktualisierungen mehr bereitgestellt werden, außer Betrieb nehmen. Die Einrichtung MUSS eine möglichst kurze Frist für die Außerbetriebnahme definieren.

Konsultationsverfahren Mindeststandard für Mobile Device Management (v1.04) - BSI Stellungname zu Ihren Rückmeldungen

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
MDM.2.2.03	Bei Speicherung besonders schützenswerter Nutzdaten wie Zugangscodes oder Schlüssel auf dem MDM-Server MUSS das MDMS diese verschlüsseln und vor Kompromittierung und Abgreifen schützen. Dabei MÜSSEN die Vorgaben der technischen Richtlinie TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“10 beachtet werden.	ZITiS	...und DEM Abgreifen schützen...	**BSI:** Danke für den Hinweis, wir haben den Text entsprechend geändert.	Bei Speicherung besonders schützenswerter Nutzdaten wie Zugangscodes oder Schlüssel auf dem MDM-Server MUSS das MDMS diese verschlüsseln und vor einer Kompromittierung sowie einem Abgreifen schützen. Dabei MÜSSEN die Vorgaben der technischen Richtlinie TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ beachtet werden.
MDM.2.3.01	b) Die Einrichtung MUSS das MDMS so konfigurieren, dass nur Personal mit den Rollen Administrator und Auditor (vgl. MDM.2.2.06) die erhobenen Gerätedaten eingesehen kann.	ZITiS	einsehen statt eingesehen	**BSI:** Geändert.	b) Die Einrichtung MUSS das MDMS so konfigurieren, dass nur IT-Betriebspersonal mit den Rollen Administrator und Auditor (vgl. MDM.2.2.06) die erhobenen Gerätedaten einsehen kann. Die Einrichtung MUSS durch technische oder organisatorische Maßnahmen (z. B. die Berechtigungen der Rollen Auditor und Administrator entsprechend einschränken) sicherstellen, dass die Daten nicht manipuliert werden können.
MDM.2.5.02	Der Server des MDMS MUSS für die Kommunikation mit den Endgeräten sowie für die Interaktion mit Administrationskomponenten (z. B. Webbrowser, Anwendungssoftware) zwei logisch oder physisch getrennte Komponenten mit separaten Interfaces bereitstellen.	ZITiS	Ergänzung: Kommunikation mit den Endgeräten (*vgl. MDM.2.5.03*) Ergänzung: (z. B. Webbrowser, Anwendungssoftware) (*vgl. MDM.2.5.04*)	**BSI:** Verweise ergänzt. Separate Interfaces für externe Dienste und sensible Infrastrukturen zu ergänzen, ist eine gute Idee, aber leider eine zu tiefgreifende Änderung an dieser Stelle des Entwicklungsprozesses. Wir haben dies als Verbesserungswunsch für die	Der Server des MDMS MUSS eine eigene Komponente für die Kommunikation mit den Endgeräten (vgl. MDM.2.5.03) sowie eine eigene Komponente für die Interaktion mit Administrations- und Self-Service-Komponenten (vgl. MDM.2.5.04) bereitstellen. Diese beiden Komponenten MÜSSEN logisch oder

Kapitel / Anforderung	Bezug (Version 1.04)	Stelle	Ihre Kommentare	Stellungnahme BSI	Überarbeitung (Version 2.0)
			Meiner Ansicht nach sollte auch bei den Anforderungen MDM.2.5.05 und 2.5.06 eine logische Trennung mit separatem Interface erforderlich sein.	nächste Mindeststandard-Version notiert.	physisch voneinander getrennt sein und über einen *Abgesicherten Kanal* (vgl. MDM.2.5.01) miteinander kommunizieren.
MDM.2.6.04	b) Kann eine unautorisierte Löschung von Konfigurationsprofilen – wie in (a) gefordert – technisch nicht verhindert werden, z. B.MÜSSEN organisatorische Maßnahmen (z. B. Belehrung und Sensibilisierung des Benutzers, vgl. MDM.2.8.04) ergriffen werden.	ZITiS	z.B. vor MÜSSEN streichen	**BSI:** Entsprechend geändert.	b) Kann eine unautorisierte Löschung von Konfigurationsprofilen – wie in (a) gefordert – technisch nicht verhindert werden, MÜSSEN organisatorische Maßnahmen (z. B. Belehrung und Sensibilisierung des Benutzenden, vgl. MDM.2.8.05) ergriffen werden.
MDM.2.6.17	Ein Reset von Gerätecodes zum Entsperren der Endgeräte MUSS durch den Administrator auch aus der Ferne (z. B. OTA) über das MDMS möglich sein.	ZITiS	Ergänzung: ...MDMS möglich sein (*vgl. MDM.2.5.03*).	**BSI**: Der Verweis auf den sicheren Kanal zwischen MDM-Client und MDM-Server ist hier nicht zwingend nötig, daher um der Lesbarkeit Willen weggelassen.	**MDM.2.6.18: Gerätecodes** a) Die Konfiguration und wirksame Durchsetzung von (auch biometrischen) Gerätecodes, Gerätecode-Richtlinien sowie, falls anwendbar, der Gerätecode-Lebensdauer auf den mobilen Endgeräten MUSS zentral über das MDMS konfigurierbar sein. Gleiches gilt für die Vorgabe, nach wie vielen Fehleingaben Endgeräte gesperrt oder gelöscht werden. Ein Zurücksetzen von Gerätecodes zum Entsperren der Endgeräte MUSS durch den Administrator auch aus der Ferne (z. B. OTA) über das MDMS möglich sein.
MDM.2.7.01	Dürfen die Mitarbeiter dienstliche Geräte auch privat nutzen, MUSS geprüft werden, ob der Schutzbedarf der dienstlichen Applikationen es erfordert, dass persönlicher und dienstlicher Bereich separiert werden.	ZITiS	Dürfen die Mitarbeiter dienstliche Geräte auch privat nutzen, SOLLTE persönlicher und dienstlicher Bereich separiert werden.	**BSI:** Übernommen.	Dürfen die Mitarbeiter dienstliche Geräte auch privat nutzen, SOLLTEN persönlicher und dienstlicher Bereich separiert werden.

Von:	GP Geschaeftszimmer_BL
An:	BSI VL Abteilungsleiter; GP Fachbereich BL 1; GP Fachbereich BL 2; GP Fachbereich BL 3; BSI VL ReferatsleiterBL
Cc:	GP Stab 3 - Strategie und Leitungsunterstuetzung; GP Geschaeftszimmer_BL
Betreff:	[n.A.z.K.] [MST MDM] Mindeststandards nach § 8 BSIG Abs.1 BSIG Mobile Device Management
Datum:	Donnerstag, 8. September 2022 14:53:37
Anlagen:	20220908-Mindeststandards nach § 8 BSIG Abs.1 BSIG Mobile Device Management.pdf Mindeststandard_Mobile_Device_Management_v2.0.pdf Referenztabelle_Mindeststandard_Mobile_Device_Management-v2.0_IT-Grundschutz_2022.xls

Liebe Kolleginnen und Kollegen,

nachfolgende E-Mail n.A.z.K.

Vielen Dank und viele Grüße
Im Auftrag

[redacted]

Geschäftszimmer BL
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582-[redacted]
Mobil: +[redacted]
E-Mail: geschaeftszimmer-bl@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Von: GP Geschaeftszimmer_BL <geschaeftszimmer-bl@bsi.bund.de>
Gesendet: Donnerstag, 8. September 2022 14:52
An: BK <poststelle@bk.bund.de>; AA <poststelle@auswaertiges-amt.de>; BMI <poststelle@bmi.bund.de>; BMF <poststelle@bmf.bund.de>; 'poststelle@bmjv.bund.de' <poststelle@bmjv.bund.de>; BMVg <poststelle@bmvg.bund.de>; BMWi <info@bmwi.bund.de>; BMAS <poststelle@bmas.bund.de>; 'poststelle@bmel.bund.de' <poststelle@bmel.bund.de>; BMFSFJ <poststelle@bmfsfj.bund.de>; 'poststelle@bmg.bund.de' <poststelle@bmg.bund.de>; 'poststelle@bmvi.bund.de' <poststelle@bmvi.bund.de>; Maileingang BMU <Poststelle@bmu.bund.de>; [redacted]@bmbf.bund.de; 'poststelle@bmz.bund.de' <poststelle@bmz.bund.de>; [redacted]@bmwsb.bund.de; 'bverfg@bundesverfassungsgericht.de' <BVerfG@bundesverfassungsgericht.de>; 'poststelle@bpra.bund.de' <poststelle@bpra.bund.de>; 'bundesrat@bundesrat.de' <bundesrat@bundesrat.de>; 'Poststelle@brh.bund.de' <poststelle@brh.bund.de>; [redacted]@bundestag.de' [redacted]@bundestag.de>; 'Poststelle@bkm.bund.de' <poststelle@bkm.bund.de>; 'Poststelle@bfdi.bund.de' <poststelle@bfdi.bund.de>; [redacted]@itzbund.de' [redacted]@itzbund.de>; GP AG-InfoSic <[redacted]@bsi.bund.de>
Cc: GP Geschaeftszimmer_BL <geschaeftszimmer-bl@bsi.bund.de>

Betreff: [MST MDM] Mindeststandards nach § 8 BSIG Abs.1 BSIG Mobile Device Management

Sehr geehrte Damen und Herren,

anbei übersende ich Ihnen das Anschreiben sowie den Mindeststandard des BSI für Mobile Device Management Version 2.0 nach § 8 Absatz 1 Satz 1 BSIG. Die Referenztabelle zum Mindeststandard ist der E-Mail ebenfalls beigefügt.

Mit freundlichen Grüßen
Im Auftrag

[redacted]

_____

Geschäftszimmer BL
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 185 - 189
53175 Bonn
Telefon: +49 (0)228 99 9582[redacted]
Mobil: [redacted]
E-Mail: geschaeftszimmer-bl@bsi.bund.de
Internet: www.bsi.bund.de

#DeutschlandDigitalSicherBSI

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Dienststellen der obersten Bundesbehörden

ITZ Bund (ISB)

Landes-CISOs über Geschäftsstelle der AG InfoSic

Geschäftsstelle BLK

- per E-Mail -

[redacted]
Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189
53175 Bonn
Postanschrift:
Postfach 20 03 63
53133 Bonn
Tel. +49 228 99 9582 [redacted]
Fax +49 228 99 10 9582 [redacted]
mindeststandards@bsi.bund.de
www.bsi.bund.de
De-Mail-Adresse:
poststelle@bsi-bund.de-mail.de

Betreff: Mindeststandard des BSI gem. § 8 Abs. 1 BSIG
hier: Mobile Device Management

Bezug: Mein Schreiben BL 35 – 750-00-07 vom 05.01.2022
RESSORTKONSULTATION
Geschäftszeichen: BL 35 – 750-00-07
Datum: 08.09.2022

Anlage: -1- Mindeststandard des BSI für Mobile Device Management Version 2.0
-2- IT-Grundschutz-Referenztabelle zum Mindeststandard

Sehr geehrte Damen und Herren,

mithilfe von Systemen für Mobile Device Management (MDM) können mobile Endgeräte in die IT-Infrastruktur einer Stelle des Bundes integriert und zentral verwaltet werden. Um auch in der Bundesverwaltung einen sicheren Einsatz von MDM zu ermöglichen, hat das BSI bereits 2017 den Mindeststandard für Mobile Device Management veröffentlicht. Seitdem konnten insbesondere durch technologische Entwicklungen und damit verbundenen Erkenntnisse weitere Konkretisierungen und Änderungsbedarfe identifiziert werden. Auf diese Entwicklung reagiert das BSI mit der Veröffentlichung des aktualisierten Mindeststandards für Mobile Device Management Version 2.0, den ich Ihnen als Anlage 1 übersende.

Zusätzlich zum Mindeststandard übersende ich Ihnen in Anlage 2 ebenfalls die IT-Grundschutz-Referenztabelle. Sie enthält eine Übersicht über die Mindeststandard-Anforderungen sowie die dort referenzierten IT-Grundschutz-Anforderungen in bearbeitbarem Format und soll Ihnen als Arbeitshilfe dienen.

Eine Änderungsübersicht finden Sie zeitnah auf der BSI-Webseite unter:
https://www.bsi.bund.de/mindeststandards.

Für die zahlreichen und konstruktiven Rückmeldungen aus dem vorgelagerten Konsultationsverfahren (siehe Bezugsschreiben) möchte ich mich auf diesem Wege ganz herzlich bei Ihnen bedanken.

Ich möchte Sie bitten, diesen Mindeststandard in Ihrem Bereich entsprechend bekannt zu geben. Rückfragen und Anregungen nehme ich über das zentrale Postfach mindeststandards@bsi.bund.de gerne entgegen.

Mit freundlichen Grüßen
Im Auftrag

Samsel

Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Mindeststandard des BSI für Mobile Device Management

nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 05.09.2022

Änderungshistorie

Version	*Datum*	*Beschreibung*
1.0	11.05.2017	Erstveröffentlichung
2.0	05.09.2022	Major Release – umfassende Überarbeitung

Tabelle 1: Versionsgeschichte des Mindeststandards für Mobile Device Management. Eine ausführliche Änderungsübersicht zum Mindeststandard erhalten Sie unter: https://www.bsi.bund.de/dok/453264

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-6262
E-Mail: mindeststandards@bsi.bund.de
Internet: https://www.bsi.bund.de

Vorwort

Die erfolgreiche Digitalisierung der Bundesverwaltung gelingt nur gemeinsam.

Risiken für die Cyber- und Informationssicherheit sind nicht zuletzt aufgrund der zunehmenden Komplexität und Vernetzung von IT-Systemen allgegenwärtig. Dadurch betreffen potenzielle Schwachstellen und Cyber-Angriffe in der Regel nicht nur einzelne Stellen.

Umso wichtiger ist die Vorgabe verbindlicher Sicherheitsanforderungen an die Informationstechnik des Bundes. So kann ein einheitliches Mindestsicherheitsniveau mit effektiven Maßnahmen zur Abwehr von Cyber-Angriffen innerhalb der heterogenen Behördenlandschaft etabliert werden

Dazu legt das Bundesamt für Sicherheit in der Informationstechnik (BSI) Mindeststandards (MST) für die Sicherheit der Informationstechnik des Bundes[1] fest. Dies erfolgt auf der Grundlage des § 8 Absatz 1 BSIG im Benehmen mit den Ressorts. Als gesetzliche Vorgabe definieren Mindeststandards somit ein verbindliches Mindestniveau für die Informationssicherheit.

Bereits 2017 hat das Bundeskabinett mit dem Umsetzungsplan Bund 2017 (UP Bund 2017) eine Leitlinie für Informationssicherheit in der Bundesverwaltung in Kraft gesetzt. Damit wurde die Beachtung der Mindeststandards für den Bereich der Stellen des Bundes verbindlich. Durch das IT-Sicherheitsgesetz 2.0 wurde die Einhaltung der Mindeststandards des BSI auch gesetzlich geregelt. Die Umsetzungspflicht der Mindeststandards ergibt sich aus dem dadurch neu gefassten § 8 BSIG.

Die Mindeststandards richten sich primär an IT-Verantwortliche, IT-Sicherheitsbeauftragte (IT-SiBe), Informationssicherheitsbeauftragte (ISB), IT-Betriebspersonal und Beschaffungsstellen. Die Gesamtverantwortung für die Informationssicherheit und damit auch für die Einhaltung der Mindeststandards trägt gemäß UP Bund 2017 die jeweilige Hausleitung.

IT-Systeme sind in der Regel komplex und in ihren individuellen Anwendungsbereichen durch die unterschiedlichsten (zusätzlichen) Rahmenbedingungen und Anforderungen gekennzeichnet. Daher können sich in der Praxis regelmäßig höhere Anforderungen an die Informationssicherheit ergeben, als sie in den Mindeststandards beschrieben werden. Aufbauend auf dem Mindestsicherheitsniveau sind diese individuellen Anforderungen in der Planung, der Etablierung und im Betrieb der IT-Systeme zusätzlich zu berücksichtigen, um dem jeweiligen Bedarf an Informationssicherheit zu genügen. Die Vorgehensweise dazu beschreiben die IT-Grundschutz-Standards des BSI.

Zur Sicherstellung der Effektivität und Effizienz in der Erstellung und Betreuung von Mindeststandards arbeitet das BSI nach einer standardisierten Vorgehensweise. Zur Qualitätssicherung durchläuft jeder Mindeststandard mehrere Prüfzyklen einschließlich des Konsultationsverfahrens mit der Bundesverwaltung.[2] Über die Beteiligung bei der Erarbeitung von Mindeststandards hinaus kann sich jede Einrichtung[3] auch bei der Erschließung fachlicher Themenfelder für neue Mindeststandards einbringen oder im Hinblick auf Änderungsbedarf für bestehende Mindeststandards Kontakt mit dem BSI aufnehmen. Einhergehend mit der Erarbeitung von Mindeststandards berät das BSI die Einrichtungen auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards.

[1] Die von den Mindeststandards adressierten Stellen werden in § 8 Absatz 1 BSI-Gesetz (BSIG) definiert (siehe https://www.gesetze-im-internet.de/bsig_2009/__8.html). Zur besseren Lesbarkeit wird im weiteren Verlauf für alle dort genannten Stellen der Begriff „Einrichtung“ verwendet.

[2] Siehe FAQ zu den MST: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/FAQ_MST/faq_mst_node.html

[3] Siehe Fußnote 1

Als die Cyber-Sicherheitsbehörde des Bundes gestalten wir mit Ihnen gemeinsam die präventive Informationssicherheit für die Bundesverwaltung. Informationssicherheit ist die Voraussetzung einer erfolgreichen und nachhaltigen Digitalisierung.

Ich wünsche Ihnen gutes Gelingen bei der Umsetzung der Mindeststandards.

Arne Schönbohm

Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Inhalt

1 Beschreibung

1.1 Einleitung und Abgrenzung

Unter den Begriff *Mobile Device Management (MDM)* im Sinne dieses Mindeststandards fallen alle technischen und organisatorischen Maßnahmen für die zentralisierte Verwaltung mobiler Endgeräte, die Teil der IT-Infrastruktur einer Einrichtung sind. Eine der Kernfunktionen des MDM ist die Konfiguration der mobilen Endgeräte mit dem Ziel, Daten und Infrastrukturen der Einrichtung abzusichern.

MDM ist eine Teilkomponente von *Enterprise Mobility Management*. Unter *Enterprise Mobility Management* fallen zusätzlich Funktionen wie *Mobile Content Management* sowie erweiterte Verwaltungsfunktionen für mobile Applikationen. Diese zusätzlichen Funktionen von *Enterprise Mobility Management* sind nicht Inhalt dieses Mindeststandards.

Unter dem Begriff *Mobile Endgeräte* versteht dieser Mindeststandard Smartphones und Tablets mit einem Betriebssystem (z. B. Android oder iOS), das für den mobilen Einsatz angepasst ist. Das bedeutet insbesondere eine Optimierung auf Touch-Bedienung und geringe Ressourcen. Die Verwaltung von Geräten mit Betriebssystemen für den Desktopbereich liegt außerhalb der Betrachtung dieses Mindeststandards, da solche Geräte derzeit sehr eng mit zusätzlichen Diensten (z. B. Active Directory) verknüpft und über diese verwaltet werden.

Als *Mobile Device Management System (MDMS)* wird eine technische Lösung bezeichnet, mit der mobile Endgeräte zentral verwaltet werden können. Ein MDMS besteht aus einem MDM-Server und einem MDM-Client auf den mobilen Endgeräten. Ein *MDM-Client* kann eine Applikation oder Teil des Betriebssystems (z. B. die von iOS bereitgestellte MDM-Schnittstelle) sein. Der *MDM-Server* ist eine zentrale Software, welche Daten, Anwendungen, Updates sowie Konfigurationskommandos und Einstellungen an den MDM-Client verteilt.

Administrationskomponenten sind zum Beispiel Webbrowser und Anwendungssoftware, mit Hilfe derer das IT-Betriebspersonal den MDM-Server konfiguriert und verwaltet. *Self-Service-Komponenten* wie ein Online-Portal erlauben den Benutzenden der mobilen Endgeräte, gewisse MDMS-Funktionen selbst zu initiieren, z. B. das Zurücksetzen ihres Endgeräts, wenn es gestohlen wurde.

Was der Begriff *vertrauenswürdig* in diesem Mindeststandard bedeutet, hängt vom jeweiligen Einsatzszenario des MDMS ab (zum Beispiel vom Schutzbedarf der mobil verarbeiteten Daten) und ist von der Einrichtung bewusst zu evaluieren und zu entscheiden.

Der Begriff *regelmäßig* in einer Anforderung wird von der Einrichtung jeweils durch eine Zeitspanne konkretisiert, welche dem Schutzbedarf des Einsatzszenarios entspricht.

Dieser Mindeststandard behandelt keine spezifischen Anforderungen für *Bring Your Own Device* (BYOD).

Die Erfüllung der Sicherheitsanforderungen muss in jeweils geeigneter Form sichergestellt werden. Dabei können üblicherweise nicht alle Sicherheitsanforderungen allein durch die Einrichtung umgesetzt werden. Im Anhang wird daher die Zuordnung der Sicherheitsanforderungen zur jeweils zuständigen Stelle dargestellt. Auch die Erfüllung der Sicherheitsanforderungen durch externe Stellen muss durch die Einrichtung sichergestellt werden. Dazu können beispielsweise Vertragsregelungen oder auch Selbstauskünfte Dritter herangezogen werden.

1.2 Modalverben

In Anlehnung an den IT-Grundschutz[4] werden die Sicherheitsanforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert. Darüber hinaus wird das Modalverb KANN für ausgewählte Prüfaspekte verwendet. Die hier genutzte Definition basiert auf RFC 2119[5] und DIN 820-2: 2018[6].

MUSS / DARF NUR

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

DARF NICHT / DARF KEIN

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann im Rahmen einer Risikoanalyse nicht akzeptiert werden.

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Die Begründung muss dokumentiert und bei einem Audit auf ihre Stichhaltigkeit geprüft werden können.

SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Die Begründung muss dokumentiert und bei einem Audit auf ihre Stichhaltigkeit geprüft werden können.

KANN

bedeutet, dass die Umsetzung oder Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.

[4] Vgl. BSI-Standard 200-2 (Bundesamt für Sicherheit in der Informationstechnik, 2017), S. 18
[5] Vgl. Key words for use in RFCs (Internet Engineering Task Force (IETF), 1997)
[6] Vgl. DIN-820-2: Gestaltung von Dokumenten (Deutsches Institut für Normung e.V. (DIN), 2018)

2 Sicherheitsanforderungen

Nachfolgende Sicherheitsanforderungen adressieren die technische Funktionalität des MDM-Systems, dessen Betrieb sowie Prozesse für die Verwaltung mobiler Endgeräte.

2.1 Strategie

MDM.2.1.01: Strategie für das Mobile Device Management

Die Einrichtung MUSS eine Strategie für das Mobile Device Management gemäß der Basis-Anforderung SYS.3.2.2.A1[7] des IT-Grundschutz-Kompendiums erstellen. Zusätzlich zu den in SYS.3.2.2.A1 definierten Aspekten MUSS die Strategie folgende Fragestellungen abdecken:

- Wie soll das MDMS in das Netzwerk der Einrichtung eingebunden werden (vgl. auch MDM.2.2.10)?
- Welche Maßnahmen zur Absicherung des MDMS und des internen Netzes der Einrichtung sollen getroffen werden?

MDM.2.1.02: Erlaubte mobile Endgeräte

Es MUSS festgelegt werden, welche mobilen Endgeräte und Betriebssysteme in der Einrichtung erlaubt sind.[8] Bereits bei der Auswahl zu beschaffender mobiler Endgeräte MUSS die Einrichtung darauf achten, dass der Hersteller über den geplanten Nutzungszeitraum Sicherheitsaktualisierungen für die Geräte bereitstellt.[9]

Die Einrichtung MUSS die mobilen Endgeräte über eine *vertrauenswürdige* Quelle beschaffen.

2.2 Arbeitsweise des MDMS

MDM.2.2.01: Einschränkungen durch Endgeräte oder Betriebsmodell

a) Das MDMS und die Einrichtung MÜSSEN nur diejenigen Anforderungen in Kapitel 2.6 und 2.7 dieses Mindeststandards erfüllen, die von den zu verwaltenden mobilen Endgeräten im ausgewählten Betriebsmodell technisch unterstützt werden.

b) Im Fall einer eingeschränkten oder fehlenden Unterstützung, die durch das gewählte Betriebsmodell entsteht (z. B. Remote Wipe bei BYOD), MUSS die Einrichtung das entsprechende Risiko adressieren, indem sie die Benutzenden in die Pflicht nimmt (vgl. MDM.2.8.05) oder andere organisatorische Maßnahmen ergreift.

MDM.2.2.02: Integration einer MDM-Client-App

Ein MDM-Client, der als Applikation bereitgestellt wird, MUSS auf die Betriebssystem-Einstellungen über die vom Betriebssystem bereitgestellten Application Programming Interfaces (APIs) zugreifen und darüber die in diesem Mindeststandard beschriebenen Parameter setzen können, sodass diese in das Betriebssystem übernommen werden.

MDM.2.2.03: Nutzdaten

Anfallende Nutzdaten des MDMS MÜSSEN in einer gesicherten Umgebung gespeichert werden (vgl. auch MDM.2.2.08 und MDM.2.2.09). Nutzdaten sind insbesondere Konfigurationsprofile sowie Benutzernamen

[7] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.2.A1 Festlegung einer Strategie für das Mobile Device Management

[8] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.2.A2 Festlegung erlaubter mobiler Endgeräte

[9] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A5 Updates von Betriebssystem und Apps

und andere persönliche Identitätsmerkmale (z. B. International Mobile Subscriber Identity (IMSI), Rufnummern).

Bei Speicherung besonders schützenswerter Nutzdaten wie Zugangscodes oder Schlüssel auf dem MDM-Server MUSS das MDMS diese verschlüsseln und vor einer Kompromittierung sowie einem Abgreifen schützen. Dabei MÜSSEN die Vorgaben der technischen Richtlinie TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“[10] beachtet werden.

MDM.2.2.04: Zugangscodes und -mittel

a) Zugriffe auf den MDM-Server sowie Administrations- und Self-Service-Portale MÜSSEN durch eine Nutzerauthentifizierung geschützt sein. Zudem SOLLTE Zwei-Faktor-Authentifizierung genutzt werden.[11] Für das Zurücksetzen von Passwörtern SOLLTE ein angemessenes sicheres Verfahren definiert und umgesetzt werden.[12] Der Zugriff auf APIs MUSS durch einen Authentifizierungsmechanismus (z. B. Access Tokens) geschützt sein.

b) Die Einrichtung MUSS die Stärke von Zugangscodes und -mitteln[13] dem angestrebten Schutzbedarf entsprechend festlegen.[14] Sofern anwendbar, umfasst dies folgende Aspekte: minimale Länge, ggf. Beschaffenheit im Falle biometrischer Zugangscodes, Komplexität und Gültigkeitsdauer der Zugangscodes. Für Passwörter gilt zudem die Basis-Anforderung ORP.4.A22 des IT-Grundschutz-Kompendiums.[15]

- Der Prozess zur Zurücksetzung eines Zugangscodes oder -mittels SOLLTE etabliert sein.[16]
- Die Anzahl der maximal möglichen Fehlversuche für die Eingabe des Zugangscodes MUSS festgelegt und technisch umgesetzt werden. Nach Überschreitung der Grenze MUSS der Zugang des Benutzenden gesperrt werden.[17] Der Prozess zur Entsperrung eines Benutzerzugangs SOLLTE etabliert sein.
- Werden Passwörter genutzt, SOLLTE vermieden werden, dass bei einem Passwortwechsel Passwörter genutzt werden, die erst vor Kurzem verwendet wurden. Die Anzahl der Passwörter, nach der sich ein Passwort wiederholen darf, SOLLTE festgelegt werden.[18]
- Erlaubt die Einrichtung biometrische Zugangscodes und ermöglicht die genutzte Technik Biometrie, SOLLTEN die Benutzenden für die Fälschbarkeit biometrischer Merkmale sensibilisiert werden (vgl. MDM.2.8.05).[19]

MDM.2.2.05: Mandantentrennung

Werden mehrere Mandanten[20] auf einem MDMS verwaltet, so MUSS eine wirksame Trennung der Mandanten sichergestellt sein.

---

[10] TR-02102-1 (Bundesamt für Sicherheit in der Informationstechnik, 2022)
[11] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), ORP.4.A10 Schutz von Benutzerkennungen mit weitreichenden Berechtigungen
[12] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), ORP.4.A11 Zurücksetzen von Passwörtern
[13] Zugangscodes und -mittel sind z. B. Passwörter, Chipkarte oder biometrische Merkmale.
[14] Um die Stärke von Zugangscodes und -mitteln festzulegen, können gängige Regelwerke wie die der OWASP zurate gezogen werden.
[15] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), ORP.4.A22 Regelung zur Passwortqualität
[16] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), ORP.4.A11 Zurücksetzen von Passwörtern
[17] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), ORP.4.A13 Geeignete Auswahl von Authentisierungsmechanismen
[18] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), ORP.4.A23 Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme
[19] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A18 Verwendung biometrischer Authentisierung
[20] Mandanten können zum Beispiel unterschiedliche juristische Personen, Interessengemeinschaften oder Gruppen mit unterschiedlichem Schutzbedarf sein.

MDM.2.2.06: Berechtigungsmanagement im MDMS

a) Das MDMS MUSS über ein Rechtemanagement verfügen, so dass das Berechtigungskonzept der Einrichtung vollständig umgesetzt werden kann.

Für die Administration des MDMS SOLLTE das MDMS mindestens die folgenden Rollen unterscheiden können:

- Die Rolle *Administrator* ist berechtigt, den Lebenszyklus mobiler Endgeräte zu verwalten (z. B. Enrollment und Außerbetriebnahme) sowie im MDMS registrierte Endgeräte für die Dauer ihrer Nutzung zu verwalten (z. B. Betriebssystemupdates).
- Die Rolle *Auditor* ist zu Audits inklusive des Zugriffs auf alle Protokolldaten berechtigt.

b) Die Einrichtung MUSS über ein Berechtigungskonzept für das MDMS verfügen. Benutzende der mobilen Endgeräte und IT-Betriebspersonal DÜRFEN NUR über Berechtigungen verfügen, die für die Aufgabenerfüllung notwendig sind (Minimalprinzip).[21] Die Zugriffsrechte für das IT-Betriebspersonal MÜSSEN mindestens in die in (a) genannten Rollen unterteilt werden. Eine Person SOLLTE nur eine Rolle innehaben.

MDM.2.2.07: Absicherung der MDMS-Betriebsumgebung

Die MDMS-Betriebsumgebung SOLLTE die Standard-Anforderung SYS.3.2.2.A12 des IT-Grundschutz-Kompendiums erfüllen.[22] Im Fall einer Fernzugriffsmöglichkeit KANN diese gemäß Baustein OPS.1.2.5[23] abgesichert werden.

MDM.2.2.08: Sicherheitsanforderungen an den Betrieb im Rechenzentrum

Für die Rechenzentren (RZ), aus denen das MDMS oder Teile davon erbracht werden, MÜSSEN – zusätzlich zu dem vorliegenden Mindeststandard – die Anforderungen des „Mindeststandard des BSI zur Anwendung des HV-Benchmark kompakt“[24] eingehalten werden. Je nach Szenario gilt zudem MDM.2.2.09.

MDM.2.2.09: Cloud-Dienste beim Betrieb des MDMS

Wird das MDMS oder werden das MDMS ergänzende Dienste (vgl. MDM.2.6.02) ganz oder auch nur teilweise von einem externen Cloud-Anbieter bezogen, MÜSSEN die Anforderungen des „Mindeststandard des BSI zur Nutzung externer Cloud-Dienste“[25] eingehalten werden.

MDM.2.2.10: Mobile Zugänge zu Netzen des Bundes

Wird das MDMS im Rahmen einer mobilen Lösung mit den Netzen des Bundes genutzt, MÜSSEN die Anforderungen des „Mindeststandard des BSI zur Nutzung der ressortübergreifenden Kommunikationsnetze des Bundes“[26] eingehalten werden.

[21] IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), ORP.4.A2. Einrichtung, Änderung und Entzug von Berechtigungen
[22] IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.2.A12 Absicherung der MDM-Betriebsumgebung
[23] IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), OPS.1.2.5 Fernwartung
[24] Mindeststandard des BSI zur Anwendung des HV-Benchmark kompakt 4.0 nach § 8 Absatz 1 Satz 1 BSIG – Version 1.1 (Bundesamt für Sicherheit in der Informationstechnik, 2018)
[25] Mindeststandard des BSI zur Nutzung externer Cloud-Diensten nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 (Bundesamt für Sicherheit in der Informationstechnik, 2021)
[26] Mindeststandard des BSI zur Nutzung der ressortübergreifenden Kommunikationsnetze des Bundes nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0a (Bundesamt für Sicherheit in der Informationstechnik, 2021)

2.3 Audit

MDM.2.3.01: Protokollierung von Gerätedaten

a) Der aktuelle Status der verwalteten Endgeräte MUSS über das MDMS ermittelt werden können.[27] Dies MUSS mindestens Folgendes umfassen:

- installierte Zertifikate,
- Konfigurationseinstellungen,
- Betriebssystemversion / Patch-Level von Endgeräten,
- installierten Applikationen inkl. Versionsstand,
- Compliance-Verstößen.

Das MDMS MUSS Änderungen an diesen Gerätemerkmalen, deren Verursacher, einen Zeitstempel und die Gerätekennung protokollieren und zentral zum Abruf bereitstellen.[28]

b) Die Einrichtung MUSS das MDMS so konfigurieren, dass nur IT-Betriebspersonal mit den Rollen Administrator und Auditor (vgl. MDM.2.2.06) die erhobenen Gerätedaten einsehen kann. Die Einrichtung MUSS durch technische oder organisatorische Maßnahmen (z. B. die Berechtigungen der Rollen Auditor und Administrator entsprechend einschränken) sicherstellen, dass die Daten nicht manipuliert werden können.

MDM.2.3.02: Protokollierung von MDMS-Daten

a) Das MDMS MUSS die Möglichkeit bereitstellen, alle sicherheitsrelevanten Aktionen, die das MDMS selbst betreffen, (z. B. die Zuordnung von Rollen zu Personen) mitsamt der Identität des Verursachers zu protokollieren.[29]

b) Die Einrichtung MUSS das MDMS so konfigurieren, dass die Einsicht der Protokolle auf Auditoren begrenzt ist. Die Einrichtung MUSS durch technische oder organisatorische Maßnahmen sicherstellen, dass die Protokolle nicht manipuliert werden können.

2.4 Services des MDMS-Anbietenden

MDM.2.4.01: Dokumentation des MDMS

Das MDMS sowie entsprechende Aktualisierungen MÜSSEN vollständig und nachvollziehbar dokumentiert sein. Bei Änderungen am MDMS MUSS die Dokumentation zeitnah angepasst werden. Die Dokumentation MUSS enthalten:

- Angaben über die grundlegende Architektur des MDMS,
- Angaben über unterstützte mobile Endgeräte mit Betriebssystemversionen,
- Angaben über Funktionalitäten, die nur auf bestimmte mobile Endgeräte oder Betriebssystemversionen anwendbar sind,
- Sicherheitsmaßnahmen für personenbezogene Daten,
- Sicherheitsmaßnahmen für die Verwaltung von kryptografischem Material (wie Zertifikate, Schlüssel und Passwörter),

[27] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.2.A6 Protokollierung des Gerätestatus

[28] Bei der Erfassung, Speicherung und Verarbeitung personenbezogener Daten sind zusätzlich Datenschutzvorgaben zu beachten. Diese sind jedoch nicht Teil dieses Mindeststandards und daher separat zu betrachten (vgl. zum Beispiel IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), CON.2 Datenschutz).

[29] Bei der Erfassung, Speicherung und Verarbeitung personenbezogener Daten sind zusätzlich Datenschutzvorgaben zu beachten. Diese sind jedoch nicht Teil dieses Mindeststandards und daher separat zu betrachten (vgl. zum Beispiel IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), CON.2 Datenschutz).

- Angaben über die Verwendung sicherer Protokolle und den Aufbau *Abgesicherter Kanäle* (vgl. MDM.2.5.01), Konfigurationen für Virtual Private Networks (VPN) sowie die Anbindung des MDMS an die IT-Infrastruktur des Betreibers,
- Angaben darüber, welche Dienste innerhalb und außerhalb der IT-Infrastruktur des Betreibers das MDMS nutzt oder nutzen kann (z. B. Active Directory, Lightweight Directory Access Protocol (LDAP), Push-Notification),
- Angaben darüber, ob und wie die Kommunikation des MDMS mit diesen Diensten gesichert werden kann (z. B. Verschlüsselung, Ports oder VPN),
- Angaben über die unterstützten Mechanismen zur Verteilung von Applikationen und darüber, wie freigegebene Applikationen identifiziert werden,
- Angaben zum Identitäts- und Berechtigungsmanagement.

MDM.2.4.02: Support

Supportleistungen des Anbieters MÜSSEN den Anforderungen des jeweiligen Einsatzszenarios entsprechen. Dabei MÜSSEN zumindest betrachtet werden:

- Support rund um das Enrollment,
- Support bei der Wartung des MDMS (besonders bzgl. MDMS-Updates) sowie der Wartung der zugehörigen Komponenten,
- Support auch ohne Fernzugriffsmöglichkeiten,
- Erreichbarkeits- und Reaktionszeiten,
- Incident Management.

Die Support-Prozesse SOLLTEN sich an Standardprozessen (z. B. ITIL) orientieren.

MDM.2.4.03: Aktualisierungen des MDMS

Der MDMS-Anbieter MUSS den Prozess zur Bereitstellung von Aktualisierungen des MDMS (Updates und Patches) darstellen und zusichern. Wird der Support des MDMS eingestellt, MUSS der Anbieter unverzüglich nach Kenntnisnahme hierüber informieren.

2.5 Vertrauenswürdige Kommunikation

MDM.2.5.01: Abgesicherter Kanal

Zur Etablierung eines *Abgesicherten Kanals*, wie er in diesem Mindeststandard verwendet wird, sind die folgenden Anforderungen zu erfüllen:

- Der Kanal MUSS kryptographisch abgesichert sein. Die Vorgaben der technischen Richtlinie TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“[30] MÜSSEN beachtet werden. Der *Abgesicherte Kanal* MUSS beidseitige Authentifizierung sicherstellen.
- Liegt eine Transportverschlüsselung nach TLS zu Grunde, MÜSSEN die Anforderungen des „Mindeststandard des BSI zur Verwendung von Transport Layer Security“[31] eingehalten werden. Wird eine VPN-Verbindung genutzt, MUSS diese den IT-Sicherheitsrichtlinien für VPN-Verbindungen der Einrichtung entsprechen.

MDM.2.5.02: Separation des MDMS

Der Server des MDMS MUSS eine eigene Komponente für die Kommunikation mit den Endgeräten (vgl. MDM.2.5.03) sowie eine eigene Komponente für die Interaktion mit Administrations- und Self-Service-Komponenten (vgl. MDM.2.5.04) bereitstellen. Diese beiden Komponenten MÜSSEN logisch oder physisch

[30] TR-02102-1 (Bundesamt für Sicherheit in der Informationstechnik, 2022)
[31] Mindeststandard des BSI zur Verwendung von Transport Layer Security nach § 8 Absatz 1 Satz 1 BSIG – Version 2.3 (Bundesamt für Sicherheit in der Informationstechnik, 2022)

voneinander getrennt sein und über einen *Abgesicherten Kanal* (vgl. MDM.2.5.01) miteinander kommunizieren.

MDM.2.5.03: Kommunikation zwischen MDM-Server und MDM-Client

Die Kommunikation zwischen MDM-Server und MDM-Client MUSS über einen *Abgesicherten Kanal* (vgl. MDM.2.5.01) erfolgen, solange der MDM-Client beim MDM-Server registriert ist(vgl. MDM.2.6.03: Sicheres Enrollment der mobilen Endgeräte).[32]

MDM.2.5.04: Kommunikation zwischen MDM-Server sowie Administrations- und Self-Service-Komponenten

Sämtliche Kommunikation zwischen MDM-Server und Administrations- und Self-Service-Komponenten, sofern solche genutzt werden sollen, MUSS über einen *Abgesicherten Kanal* (vgl. MDM.2.5.01) erfolgen.

MDM.2.5.05: Kommunikation zwischen MDM-Server und Infrastrukturen der Einrichtung

Soll das MDMS an Infrastrukturen der Einrichtung (z. B. Verzeichnisdienste oder Mailserver) angebunden werden, sind folgende Anforderungen zu erfüllen:

a) Die Verbindung zwischen MDMS und den Infrastrukturen der Einrichtung MUSS über einen *Abgesicherten Kanal* (vgl. MDM.2.5.01) erfolgen.

b) Die Einrichtung MUSS bewerten, ob ihre sensiblen Infrastrukturen durch weitere Maßnahmen geschützt werden müssen (z. B. wenn ein Zonenmodell verwendet wird).

MDM.2.5.06: Kommunikation zwischen MDM-Server und externen Diensten

Die Kommunikation zwischen MDM-Server und externen Diensten (z. B. Update-Server für das MDMS) MUSS über einen *Abgesicherten Kanal* (vgl. MDM.2.5.01) erfolgen.

2.6 Sichere Konfiguration der mobilen Endgeräte

MDM.2.6.01: Dokumentation für mobile Endgeräte

Die Sicherheitsmechanismen und -einstellungen für mobile Endgeräte MÜSSEN festgelegt und nachvollziehbar beschrieben sein (z. B. PIN-Code-Verfahren, automatische Sperre oder Regeln für die Deinstallation von Konfigurationsprofilen).[33]

MDM.2.6.02: Zusätzliche Dienste zur Verwaltung der mobilen Endgeräte

Wird ein Dienst genutzt, der die Funktionalität des genutzten MDMS erweitert (z. B. ein Service für Over-the-air(OTA)-Betriebssystemupdates oder zum automatisierten Enrollment aus der Ferne, vgl. MDM.2.6.03), MUSS ein *vertrauenswürdiger* Anbieter hierfür gewählt werden.

Bei Nutzung des Dienstes MUSS die Einrichtung einen angemessenen Authentifizierungsmechanismus sicherstellen. Dies beinhaltet die Sicherstellung, dass nur berechtigte Geräte oder Benutzende den Dienst nutzen können. Hierfür KANN die Geräteregistrierung beispielsweise durch einen Administrator der Einrichtung erfolgen oder eine Authentisierung des Benutzenden (z. B. über ein dem Benutzenden bekanntes Passwort) stattfinden. Wenn die Administrationsschnittstelle des Dienstes aus dem Internet erreichbar ist, SOLLTE Zwei-Faktor-Authentifizierung genutzt werden. Die Kommunikation zwischen dem Dienst und den mobilen Endgeräten MUSS entsprechend dem Schutzbedarf kryptographisch abgesichert sein.

Der Dienst KANN auch aus der Ferne (OTA) erfolgen.

[32] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.2.A4 Verteilung der Grundkonfiguration auf mobile Endgeräte

[33] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A3 Sichere Grundkonfiguration für mobile Geräte

MDM.2.6.03: Sicheres Enrollment der mobilen Endgeräte

a) Für das Enrollment der mobilen Endgeräte MUSS das MDMS eine sichere Schnittstelle bereitstellen. Zusätzlich zu MDM.2.6.02[34] gilt während des Enrollments:

Der MDM-Server MUSS durch den MDM-Client authentifiziert werden. Die Kommunikation zwischen mobilen Endgeräten und MDM-Server MUSS kryptographisch abgesichert werden. Nach erfolgreichem Enrollment gilt MDM.2.5.03.

b) Alle mobilen Endgeräte, die Zugriff auf IT-Infrastrukturen oder Daten der Einrichtung haben, SOLLTEN per MDM verwaltet werden. Die Einrichtung MUSS die zu verwaltenden mobilen Endgeräte so schnell wie möglich in das MDMS integrieren und nach den Richtlinien der Einrichtung konfigurieren und verwalten. Vor dem Enrollment SOLLTEN sich die mobilen Endgeräte im Werkszustand befinden oder zurückgesetzt werden.[35]

MDM.2.6.04: Konfigurationsprofile

a) Das MDMS MUSS Konfigurationsprofile (z. B. VPN-Verbindungen, WLAN-Einstellungen) an die mobilen Endgeräte übermitteln können. Das MDMS MUSS den Installationsstatus von Konfigurationsprofilen pro Gerät anzeigen können. Das MDMS MUSS verhindern können (z. B. durch Passwortschutz), dass Konfigurationsprofile durch den Benutzenden manuell verändert oder rückgängig gemacht werden.

b) Kann eine unautorisierte Löschung von Konfigurationsprofilen – wie in (a) gefordert – technisch nicht verhindert werden, MÜSSEN organisatorische Maßnahmen (z. B. Belehrung und Sensibilisierung des Benutzenden, vgl. MDM.2.8.05) ergriffen werden.

MDM.2.6.05: Entfernen des Endgeräts aus der Verwaltung

Das MDMS SOLLTE verhindern können, dass der Benutzende die provisionierte Verbindung des mobilen Endgeräts zum MDM-Server trennt (z. B. durch Löschen der MDM-Client-App).

MDM.2.6.06: Betatests

Nutzt die Einrichtung auf gewissen mobilen Endgeräten Betaversionen von Applikationen oder Betriebssystemen, MÜSSEN diese Endgeräte im MDMS separat verwaltet werden.

MDM.2.6.07: Administration von Schnittstellen, Diensten und Funktionen

a) Kommunikationsdienste wie SMS und MMS sowie Funktionen wie Kameras, Mikrofone, digitale Assistenten (z. B. Siri) und Sprachsteuerungen MÜSSEN zentral und so granular, wie das Betriebssystem es ermöglicht, über das MDMS administrierbar sein.

Gleiches gilt für Schnittstellen-Funktionen. Unter Schnittstellen sind insbesondere Bluetooth, WLAN, GPS, NFC und USB bzw. Lightning, sofern vorhanden, zu verstehen. Das Betriebssystem der verwalteten Geräte kann weitere Schnittstellen bereitstellen; die zugehörigen Funktionen SOLLTEN durch das MDMS ebenfalls administrierbar sein.[36]

Ein Koppeln oder Verbinden mit anderen Geräten (z. B. via Apple AirDrop oder die Anbindung eines Monitors an die mobilen Endgeräte via USB) zum Datenaustausch oder zur Datenweitergabe MUSS unterbunden werden können.

[34] Zudem sind für das Enrollment insbesondere die folgenden Anforderungen aus diesem Mindeststandard zu beachten: MDM.2.2.04: Zugangscodes und –mittel, MDM.2.2.09: Cloud-Dienste beim Betrieb des MDMS und MDM.2.5.06: Kommunikation zwischen MDM-Server und externen Diensten.

[35] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.2.A4 Verteilung der Grundkonfiguration auf mobile Endgeräte und SYS.3.2.2.A5 Installation des MDM Clients

[36] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A16 Deaktivierung nicht benutzter Kommunikationsschnittstellen

b) Die Freischaltung der in (a) genannten Schnittstellen-Funktionen, Dienste und Funktionen MUSS geregelt und per MDMS auf das dienstlich notwendige Maß reduziert werden. Digitale Assistenten SOLLTEN per MDMS deaktiviert werden.[37]

MDM.2.6.08: Monitoring und Diagnose

a) Funktionen zur betriebssystemeigenen Übermittlung von Monitoring- und Diagnose-Informationen MÜSSEN zentral über das MDMS deaktiviert werden können.

b) Die Einrichtung MUSS die in (a) genannten Funktionen per MDMS deaktivieren.

MDM.2.6.09: Entwicklermodus

a) Das MDMS MUSS den Entwicklermodus des mobilen Betriebssystems deaktivieren können.

b) Die Einrichtung SOLLTE den Entwicklermodus per MDMS deaktivieren.

MDM.2.6.10: Konfiguration von Netzwerkparametern

Netzwerkparameter auf den mobilen Endgeräten (Domain-Name-System (DNS), Gateways, Dynamic Host Configuration Protocol (DHCP)) SOLLTEN über das MDMS konfigurierbar sein.

MDM.2.6.11: Verschlüsselung des Speichers

a) Das MDMS MUSS die systemeigene Verschlüsselung des mobilen Endgerätes von nichtflüchtigem Speicher aktivieren können.

b) Das MDMS MUSS auch die Verschlüsselung von Daten auf externen Speichermedien (z. B. SD-Karte) aktivieren können.

c) Die Einrichtung MUSS die in (a) genannte Verschlüsselung von nichtflüchtigem Speicher per MDMS aktivieren. Zudem SOLLTE sie die in (b) genannte Verschlüsselung von Daten auf externen Speichermedien (z. B. SD-Karten) – mit Ausnahme von Smartcards – aktivieren.[38]

MDM.2.6.12: Zertifikate

a) Das MDMS MUSS auf den mobilen Endgeräten Zertifikate installieren, aktualisieren und anzeigen können, für die das Betriebssystem dies ermöglicht (z. B. E-Mail, ActiveSync, VPN, WLAN oder Websites). Die Installation von nicht verifizierbaren Zertifikaten durch den Benutzenden MUSS verhindert werden können. Das MDMS MUSS in der Lage sein, Informationen zum Widerruf von Zertifikaten (z. B. Certificate Revocation Lists (CRLs)) an die Endgeräte zu senden. Der Status eines Zertifikates (gültig/ungültig) MUSS vom MDMS in geeigneter Weise angezeigt werden. Das MDMS MUSS den sicheren Transfer (z. B. PKCS#12 verschlüsselt) von Zertifikaten unterstützen.[39]

b) Es MUSS ein Prozess für das Lebenszyklusmanagement der Zertifikate (z. B. Erneuerung oder Widerruf) vorhanden sein. Falls die Einrichtung kein Online-Protokoll wie Online Certificate Status Protocol (OCSP) Multistapling nutzt, SOLLTE sie sicherstellen, dass die CRLs *regelmäßig* - mindestens einmal pro Werktag - per MDMS an die mobilen Endgeräte übertragen werden, sofern das Endgerät erreichbar ist. Die Einrichtung MUSS insbesondere vorinstallierte Zertifikate auf mobilen Endgeräten auf ihre *Vertrauenswürdigkeit* hin prüfen und Zertifikate nicht *vertrauenswürdiger* Aussteller deinstallieren oder widerrufen.

[37] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A3 Sichere Grundkonfiguration für mobile Endgeräte und SYS.3.2.1.A16 Deaktivierung nicht benutzter Kommunikationsschnittstellen.

[38] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A11 Verschlüsselung des Speichers

[39] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.2.A21 Verwaltung von Zertifikaten

MDM.2.6.13: Compliance-Verstöße und kompromittierte mobile Endgeräte

a) Zum Schutz des MDMS und der Konfiguration der Endgeräte MÜSSEN Verstöße gegen Compliance-Richtlinien (u.a. eine nicht erlaubte Betriebssystemversion oder fehlender Kontakt zum MDM-Client über einen längeren Zeitraum) erfasst werden können (vgl. auch MDM.2.3.01). Zusätzlich KANN das MDMS die Möglichkeit bieten, Indikatoren für die Kompromittierung mobiler Endgeräte (z. B. Jailbreak und Rooting) zu erfassen.

Treten Auffälligkeiten auf, SOLLTE das MDMS die folgenden Aktionen ausführen können:

1. selbstständiges Versenden von Warnhinweisen an eine zuvor definierte Stelle,
2. selbstständiges Sperren des Gerätes,
3. Löschen der vertraulichen Informationen der Einrichtung, insbesondere bei persönlicher Mitnutzung des Gerätes,
4. Zurücksetzen des Gerätes auf den Werkszustand,
5. Verhindern des Zugangs zu dienstlichen Applikationen,
6. Verhindern des Zugangs zu den Systemen und Informationen der Einrichtung sowie
7. Verhindern des Zugangs zum MDMS.[40]

b) Die Einrichtung MUSS Compliance-Richtlinien definieren und die Konformität der mobilen Endgeräte mit diesen Richtlinien *regelmäßig* prüfen. Diese Prüfung KANN über die in (a) genannte Funktion des MDMS erfolgen.

MDM.2.6.14: Automatische Bildschirmsperrung

a) Die Konfiguration und wirksame Durchsetzung einer automatischen Bildschirmsperre des mobilen Endgerätes nach Zeitvorgabe MUSS über das MDMS zentral einstellbar sein.

b) Die in (a) beschriebene Funktion des MDMS MUSS im Betrieb genutzt und zentral vorgegeben werden. Die Zeitspanne bis zur Gerätesperrung bei Inaktivität MUSS in Abhängigkeit zum angestrebten Schutzniveau stehen und angemessen kurz sein.[41]

MDM.2.6.15: Sperrbildschirm

a) Das MDMS MUSS den Zugang zu dienstlichen Informationen im Sperrzustand der mobilen Endgeräte konfigurieren können. Dies betrifft auch die Anzeige von Push-Nachrichten, insbesondere deren Inhalt, auf dem Sperrbildschirm.

b) Die Einrichtung MUSS das Anzeigen vertraulicher Informationen auf dem Sperrbildschirm mithilfe des MDMS verhindern.[42]

MDM.2.6.16: Ferngesteuerte Gerätesperrung (Remote-Lock)

Eine Gerätesperrung MUSS durch den Administrator auch aus der Ferne über das MDMS möglich sein (Remote-Lock). Kann der Remote-Lock auf den mobilen Endgeräten nicht ausgeführt werden, MUSS dies vom MDMS in geeigneter Weise angezeigt werden können.

MDM.2.6.17: Fernlöschung (Remote-Wipe)

a) Das MDMS MUSS die Möglichkeit bereitstellen, auch aus der Ferne einen Befehl an verwaltete Geräte zu senden, um sämtliche dienstliche Daten auf mobilen Endgeräten – einschließlich Zugangsdaten und Zertifikaten – zu löschen (Remote-Wipe bei bestehender Netzwerkverbindung).

[40] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.2.A23 Durchsetzung von Compliance-Anforderungen

[41] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A4 Verwendung eines Zugriffsschutzes

[42] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A4 Verwendung eines Zugriffsschutzes

b) Werden in mobilen Endgeräten externe Speicher genutzt, MÜSSEN die darauf befindlichen Daten im Fall einer Fernlöschung – sofern vom MDMS und von der mobilen Plattform unterstützt – gelöscht werden.[43]

MDM.2.6.18: Gerätecodes

a) Die Konfiguration und wirksame Durchsetzung von (auch biometrischen) Gerätecodes, Gerätecode-Richtlinien sowie, falls anwendbar, der Gerätecode-Lebensdauer auf den mobilen Endgeräten MUSS zentral über das MDMS konfigurierbar sein. Gleiches gilt für die Vorgabe, nach wie vielen Fehleingaben Endgeräte gesperrt oder gelöscht werden. Ein Zurücksetzen von Gerätecodes zum Entsperren der Endgeräte MUSS durch den Administrator auch aus der Ferne (z. B. OTA) über das MDMS möglich sein.[44]

b) Die mobilen Endgeräte MÜSSEN durch Gerätecodes geschützt sein. Diese MÜSSEN die Anforderungen aus MDM.2.2.04 (b) erfüllen.[45]

MDM.2.6.19: Name der mobilen Endgeräte

Der Name der mobilen Endgeräte DARF KEINE Merkmale enthalten, die Rückschlüsse auf den Benutzenden oder die Einrichtung ermöglichen.[46] Wählen die Benutzenden den Namen der Endgeräte, MÜSSEN sie entsprechend sensibilisiert werden (vgl. MDM.2.8.05).

2.7 Applikationsverwaltung

MDM.2.7.01: Verteilung von Applikationen

a) Eine zentrale Verteilung von Applikationen über das MDMS MUSS möglich sein. Diese MUSS den Anforderungen des geplanten Einsatzszenarios genügen (z. B. gruppenbasierte Verteilung bei Verwaltung von Android- und iOS-Geräten über dasselbe MDMS). Die Deinstallation oder Deaktivierung von Applikationen sowie das Verteilen oder Zurückhalten von Updates (auch für System- und vorinstallierte Applikationen) MÜSSEN durch den Administrator auch aus der Ferne erzwingbar sein (z. B. OTA). Dieser Vorgang MUSS durch das MDMS erzwungen werden können, sobald eine Verbindung zwischen MDMS und mobilen Endgeräten besteht.[47]

b) Die Einrichtung MUSS dienstliche Applikationen zentral über das MDMS verwalten und aufbringen. Die Einrichtung MUSS eine möglichst kurze Frist definieren, bis zu der sicherheitskritische Updates eingespielt werden müssen. Dürfen die Mitarbeiter dienstliche Geräte auch privat nutzen, SOLLTEN persönlicher und dienstlicher Bereich separiert werden.

MDM.2.7.02: Bereitstellung von Applikationen

a) Die Einrichtung MUSS sicherstellen, dass ausschließlich *vertrauenswürdige* Applikationen Zugriff auf IT-Infrastrukturen und Daten der Einrichtung erhalten.

b) Die Einrichtung SOLLTE sicherstellen, dass ausschließlich *vertrauenswürdige* Applikationen auf den mobilen Endgeräten installiert werden. Dies KANN mithilfe einer Liste erlaubter Anwendungen oder einer Liste verbotener Anwendungen erreicht werden.[48]
Die Einrichtung SOLLTE unterbinden, dass Applikationen aus nicht *vertrauenswürdigen* Quellen installiert

[43] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.2.A22 Fernlöschung und Außerbetriebnahme von Endgeräten
[44] Komponenten außerhalb des Einflussbereichs des MDMS (z. B. Smartcards) sind hiermit nicht gemeint.
[45] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A4 Verwendung eines Zugriffsschutzes
[46] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A12 Verwendung nicht personalisierter Gerätenamen
[47] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.2.A7 Installation von Apps
[48] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A8 Installation von Apps und SYS.3.2.1.A30 Einschränkung der App-Installation mittels Whitelist

werden. Ist dies technisch nicht möglich, SOLLTEN die Benutzenden hierfür sensibilisiert werden (vgl. MDM.2.8.05: Sensibilisierung der Benutzenden).

c) Die Einrichtung SOLLTE bewerten, ob Apps, die sich ohne Installation öffnen lassen (Instant Apps), genutzt werden dürfen. Falls dies nicht erlaubt wird, MÜSSEN entsprechende technische oder organisatorische Maßnahmen ergriffen werden.

MDM.2.7.03: Vorinstallierte Applikationen und Online-Dienste

Die Einrichtung MUSS die Nutzung vorinstallierter Applikationen und Online-Dienste, insbesondere externer cloudbasierter Dienste[49], bewerten und im Bedarfsfall per MDMS verhindern oder einschränken. Wird diese Maßnahme nicht technisch durch das Betriebssystem unterstützt, MÜSSEN die Benutzenden instruiert werden, die entsprechenden Applikationen und Online-Dienste nicht oder nur eingeschränkt zu nutzen (vgl. MDM.2.8.05).[50]

2.8 Betriebsprozesse

MDM.2.8.01: Administration des MDMS

Das MDMS MUSS von IT-Betriebspersonal (vgl. MDM.2.2.06) bedient werden, das in der sicheren Administration von MDM-Systemen geschult ist.

MDM.2.8.02: Datensicherungen des MDMS

Es MÜSSEN wirksame Mechanismen für das Backup aller Daten und Einstellungen des MDMS existieren, so dass dieses im Bedarfsfall funktionsfähig wiederhergestellt werden kann.

MDM.2.8.03: Umgang mit Sicherheitsvorfällen

Für den Umgang mit Sicherheitsvorfällen MUSS ein angemessener Prozess etabliert sein. Dieser MUSS mindestens eine sofortige (automatisierte oder manuelle) Meldung des Vorfalls an eine definierte Stelle, eine Untersuchung der Konsequenzen sowie die Einleitung geeigneter Gegenmaßnahmen beinhalten. Benutzende MÜSSEN dafür sensibilisiert werden, wie sie mit Sicherheitsvorfällen umgehen – insbesondere, dass sie bei Verlust oder Diebstahl eines Geräts sofort die definierte Stelle informieren (vgl. auch MDM.2.8.05).[51]

Insbesondere MUSS der Prozess folgende Szenarien abdecken:

- Verlust mobiler Endgeräte,
- Verdacht des Verlusts der Integrität mobiler Endgeräte (z. B. durch Manipulation durch Dritte) (vgl. MDM.2.6.13),
- kein Kontakt der mobilen Endgeräte zum MDMS über einen längeren Zeitraum hinweg.

In diesen Fällen MUSS der Zugang zu IT-Infrastrukturen der Einrichtung wirksam verhindert werden.

MDM.2.8.04: Sperrung von SIM

Die Einrichtung MUSS die notwendigen Informationen (z. B. die IMEI) bereithalten, um eine Sperrung der SIM-Karte oder des eSIM-Profils veranlassen zu können.

MDM.2.8.05: Sensibilisierung der Benutzenden

Benutzende mobiler Endgeräte MÜSSEN für die MDM-Sicherheitsmaßnahmen sensibilisiert werden. Eine Sensibilisierung der Benutzenden KANN notwendig sein, um folgende Anforderungen zu erfüllen:

[49] Mindeststandard des BSI zur Nutzung externer Cloud-Diensten nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 (Bundesamt für Sicherheit in der Informationstechnik, 2021)

[50] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A2 Festlegung einer Strategie für die Cloud-Nutzung

[51] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A7 Verhaltensregeln bei Sicherheitsvorfällen

- *MDM.2.2.01: Einschränkungen durch Endgeräte oder Betriebsmodell*
- *MDM.2.2.04: Zugangscodes und -mittel*
- *MDM.2.6.04: Konfigurationsprofile*
- *MDM.2.6.18: Gerätecodes*
- *MDM.2.6.19: Name der mobilen Endgeräte*
- *MDM.2.7.02: Bereitstellung von Applikationen*
- *MDM.2.7.03: Vorinstallierte Applikationen und Online-Dienste*
- *MDM.2.8.03: Umgang mit Sicherheitsvorfällen*

MDM.2.8.06: Regelmäßige Überprüfungen

Konfigurationsprofile und Sicherheitseinstellungen MÜSSEN *regelmäßig* überprüft werden. Die vom MDMS erzeugten Protokolle MÜSSEN *regelmäßig* auf ungewöhnliche Einträge überprüft werden. Hierbei MÜSSEN Vorgaben aus der IT-Sicherheitsrichtlinie der Einrichtung berücksichtigt werden. Die zugeteilten Berechtigungen für Benutzende der mobilen Endgeräte und IT-Betriebspersonal MÜSSEN mindestens halbjährlich hinsichtlich ihrer Angemessenheit überprüft werden (Minimalprinzip).[52]

MDM.2.8.07: Aktualisierung der Betriebssysteme von MDMS und mobilen Endgeräten

Sollen neue Betriebssystemversionen der mobilen Endgeräte eingesetzt werden, MUSS die Einrichtung vorab prüfen, ob die Konfigurationsprofile und Sicherheitseinstellungen weiterhin wirksam und ausreichend sind. Abweichungen MÜSSEN korrigiert werden. Es MÜSSEN Arbeitsprozesse geplant, getestet und angemessen dokumentiert sein, damit sicherheitsrelevante Patches und Updates für die Betriebssysteme des MDMS und der mobilen Endgeräte unverzüglich eingespielt oder bei bekannten Problemen – sofern vom mobilen Betriebssystem unterstützt – vorerst zurückgehalten werden können.

Die Einrichtung MUSS eine möglichst kurze Frist definieren, bis zu der sicherheitskritische Aktualisierungen[53] eingespielt werden müssen.

MDM.2.8.08: Benutzerwechsel

Sollen verwaltete mobile Endgeräte an einen anderen Benutzenden übergeben werden, MÜSSEN zuvor alle dienstlichen Daten und Zugänge von den Endgeräten, SIM-Karten und externen Speichermedien, die ebenfalls den Benutzenden wechseln, gelöscht werden. Zudem SOLLTEN die Endgeräte zurückgesetzt werden; dabei KÖNNEN auch eSIM-Profile gelöscht werden.

MDM.2.8.09: Außerbetriebnahme

Die Einrichtung MUSS MDMS und mobile Endgeräte, für die keine sicherheitsrelevanten Aktualisierungen mehr bereitgestellt werden, außer Betrieb nehmen.[54] Die Einrichtung MUSS eine möglichst kurze Frist für die Außerbetriebnahme definieren.

Der Prozess zur Außerbetriebnahme mobiler Endgeräte MUSS sicherstellen, dass keine dienstlichen Daten auf den mobilen Endgeräten, SIM-Karten oder eingebundenen Speichermedien verbleiben; dies SOLLTE ein Zurücksetzen des Endgeräts beinhalten. eSIM-Profile MÜSSEN gelöscht werden.[55,56]

[52] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.2.A20 Regelmäßige Überprüfung des MDM

[53] Als sicherheitskritisch anzusehen sind insbesondere Aktualisierungen, welche die Gefahr eines ungewollten Abflusses dienstlicher Daten, einer Manipulation sensibler Daten oder eines Ausfalls verringern.

[54] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.1.A5 Updates von Betriebssystem und Apps

[55] Vgl. IT-Grundschutz-Kompendium (Bundesamt für Sicherheit in der Informationstechnik, 2022), SYS.3.2.2.A22 Fernlöschung und Außerbetriebnahme von Endgeräten

[56] Hinweis: Als Zusatzmaßnahme kann die Einrichtung Zertifikate für dienstliche Zugänge, die auf dem Endgerät gespeichert waren, sperren.

Anhang

Zuordnung der Sicherheitsanforderungen zur zuständigen Stelle

Die in Kapitel 2 genannten Sicherheitsanforderungen sind durch die in folgender Tabelle definierte zuständige Stelle umzusetzen. Die Einrichtung hat die Umsetzung durch die zuständige Stelle in geeigneter Form sicherzustellen.

Ist in der folgenden Tabelle eine Anforderung für das MDMS vorgemerkt, so richtet sie sich an das technische Produkt MDMS.

Anforderungen, die für die Spalte MDMS-Anbieter gekennzeichnet sind, sind durch den Hersteller bzw. Anbieter des MDMS-Produktes umzusetzen.

MDMS-Betreiber betreiben ein MDMS für eine Einrichtung. Betreibt die Einrichtung das MDMS selbst, muss sie die in der entsprechenden Spalte genannten Anforderungen selbst umsetzen.

Anforderung	*MDMS*	*MDMS-Anbieter*	*Einrichtung*	*MDMS-Betreiber*
MDM.2.1.01: Strategie für das Mobile Device Management			x	
MDM.2.1.02: Erlaubte mobile Endgeräte			x	
MDM.2.2.01 (a): Einschränkungen durch Endgeräte oder Betriebsmodell	x		x	
MDM.2.2.01 (b): Einschränkungen durch Endgeräte oder Betriebsmodell			x	
MDM.2.2.02: Integration einer MDM-Client-App	x			
MDM.2.2.03: Nutzdaten	x			
MDM.2.2.04 (a): Zugangscodes -mittel	x			
MDM.2.2.04 (b): Zugangscodes -mittel			x	
MDM.2.2.05: Mandantentrennung	x			
MDM.2.2.06 (a): Berechtigungsmanagement im MDMS	x			
MDM.2.2.06 (b): Berechtigungsmanagement im MDMS			x	
MDM.2.2.07: Absicherung der MDMS-Betriebsumgebung				x
MDM.2.2.08: Sicherheitsanforderungen an den Betrieb im Rechenzentrum				x
MDM.2.2.09: Cloud-Dienste beim Betrieb des MDMS				x
MDM.2.2.10: Mobile Zugänge zu Netzen des Bundes				x
MDM.2.3.01 (a): Protokollierung von Gerätedaten	x			
MDM.2.3.01 (b): Protokollierung von Gerätedaten			x	
MDM.2.3.02 (a): Protokollierung von MDMS-Daten	x			
MDM.2.3.02 (b): Protokollierung von MDMS-Daten			x	
MDM.2.4.01: Dokumentation des MDMS		x		

Anforderung	*MDMS*	*MDMS-Anbieter*	*Einrichtung*	*MDMS-Betreiber*
MDM.2.4.02: Support		x		
MDM.2.4.03: Aktualisierungen des MDMS		x		
MDM.2.5.01: Abgesicherter Kanal				
MDM.2.5.02: Separation des MDMS	x			
MDM.2.5.03: Kommunikation zwischen MDM-Server und MDM-Client	x			
MDM.2.5.04: Kommunikation zwischen MDM-Server sowie Administrations- und Self-Service-Komponenten	x			
MDM.2.5.05 (a): Kommunikation zwischen MDM-Server und Infrastrukturen der Einrichtung	x		x	
MDM.2.5.05 (b): Kommunikation zwischen MDM-Server und Infrastrukturen der Einrichtung			x	
MDM.2.5.06: Kommunikation zwischen MDM-Server und externen Diensten	x			
MDM.2.6.01: Dokumentation für mobile Endgeräte			x	
MDM.2.6.02: Zusätzliche Dienste zur Verwaltung der mobilen Endgeräte			x	
MDM.2.6.03 (a): Sicheres Enrollment der mobilen Endgeräte	x			
MDM.2.6.03 (b): Sicheres Enrollment der mobilen Endgeräte			x	
MDM.2.6.04 (a): Konfigurationsprofile	x			
MDM.2.6.04 (b): Konfigurationsprofile			x	
MDM.2.6.05: Entfernen des Endgeräts aus der Verwaltung	x			
MDM.2.6.06: Betatests			x	
MDM.2.6.07 (a): Administration von Schnittstellen, Diensten und Funktionen	x			
MDM.2.6.07 (b): Administration von Schnittstellen, Diensten und Funktionen			x	
MDM.2.6.08 (a): Monitoring und Diagnose	x			
MDM.2.6.08 (b): Monitoring und Diagnose			x	
MDM.2.6.09 (a): Entwicklermodus	x			
MDM.2.6.09 (b): Entwicklermodus			x	
MDM.2.6.10: Konfiguration von Netzwerkparametern	x			
MDM.2.6.11 (a): Verschlüsselung des Speichers	x			
MDM.2.6.11 (b): Verschlüsselung des Speichers	x			
MDM.2.6.11 (c): Verschlüsselung des Speichers			x	
MDM.2.6.12 (a): Zertifikate	x			

Anforderung	*MDMS*	*MDMS-Anbieter*	*Einrichtung*	*MDMS-Betreiber*
MDM.2.6.12 (b): Zertifikate			x	
MDM.2.6.13 (a): Compliance-Verstöße und kompromittierte mobile Endgeräte	x			
MDM.2.6.13 (b): Compliance-Verstöße und kompromittierte mobile Endgeräte			x	
MDM.2.6.14 (a): Automatische Bildschirmsperrung	x			
MDM.2.6.14 (b): Automatische Bildschirmsperrung			x	
MDM.2.6.15 (a): Sperrbildschirm	x			
MDM.2.6.15 (b): Sperrbildschirm			x	
MDM.2.6.16: Ferngesteuerte Gerätesperrung (Remote-Lock)	x			
MDM.2.6.17 (a): Fernlöschung (Remote-Wipe)	x			
MDM.2.6.17 (b): Fernlöschung (Remote-Wipe)			x	
MDM.2.6.18 (a): Gerätecodes	x			
MDM.2.6.18 (b): Gerätecodes			x	
MDM.2.6.19: Name der mobilen Endgeräte			x	
MDM.2.7.01 (a): Verteilung von Applikationen	x			
MDM.2.7.01 (b): Verteilung von Applikationen			x	
MDM.2.7.02 (a): Bereitstellung von Applikationen			x	
MDM.2.7.02 (b): Bereitstellung von Applikationen			x	
MDM.2.7.02 (c): Bereitstellung von Applikationen			x	
MDM.2.7.03: Vorinstallierte Applikationen und Online-Dienste			x	
MDM.2.8.01: Administration des MDMS			x	
MDM.2.8.02: Datensicherungen des MDMS			x	
MDM.2.8.03: Umgang mit Sicherheitsvorfällen			x	
MDM.2.8.04: Sperrung von SIM			x	
MDM.2.8.05: Sensibilisierung der Benutzenden			x	
MDM.2.8.06: Regelmäßige Überprüfungen			x	
MDM.2.8.07: Aktualisierung der Betriebssysteme von MDMS und mobilen Endgeräten			x	
MDM.2.8.08: Benutzerwechsel			x	
MDM.2.8.09: Außerbetriebnahme			x	

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik. 2022. BSI IT-Grundschutz-Kompendium, Edition 2022. [Online] 2022. [Zitat vom: 03. Mai 2022.] https://www.bsi.bund.de/dok/989376.

—. 2017. BSI Standard 200-2, IT-Grundschutz-Methodik. [Online] 2017. [Zitat vom: 03. Mai 2022.] https://www.bsi.bund.de/dok/128640.

—. 2018. Mindeststandard des BSI zur Anwendung des HV-Benchmark kompakt 4.0 nach § 8 Absatz 1 Satz 1 BSIG – Version 1.1 vom 19.06.2018. [Online] 2018. [Zitat vom: 03. Mai 2022.] https://www.bsi.bund.de/dok/397148.

—. 2021. Mindeststandard des BSI zur Nutzung externer Cloud-Dienste nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0 vom 07.07.2021.s. [Online] 2021. [Zitat vom: 03. Mai 2022.] https://www.bsi.bund.de/dok/452272.

—. 2021. Mindeststandard des BSI zur Nutzung der ressortübergreifenden Kommunikationsnetze des Bundes („Nutzerpflichten NdB“). nach § 8 Absatz 1 Satz 1 BSIG – Version 2.0a vom 25.02.2021.

—.2022. BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen. 2022. [Online] 2022. [Zitat vom: 03. Mai 2022.] https://www.bsi.bund.de/dok/433400.

—. 2022. Mindeststandards – Antworten auf häufig gestellte Fragen zu den Mindeststandards. [Online] 2022. [Zitat vom: 03. Mai 2022.] https://www.bsi.bund.de/dok/11916758.

—. 2022. Mindeststandard des BSI zur Verwendung von Transport Layer Security nach § 8 Absatz 1 Satz 1 BSIG – Version 2.3 vom 15.03.2022. [Online] 2022. [Zitat vom: 03. Mai 2022.] https://www.bsi.bund.de/dok/1024420.

Bundesministerium des Innern und für Heimat. 2017. Umsetzungsplan Bund 2017. [Online] 2017. [Zitat vom: 03. Mai 2022.] https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/up-bund-2017.html.

Deutsches Institut für Normung e.V. (DIN). 2018. *DIN 820-2:2018-09: Normungsarbeit – Teil 2: Gestaltung von Dokumenten.* Berlin : Beuth Verlag GmbH, 2018.

Internet Engineering Task Force (IETF). 1997. RFC 2119: Key words for use in RFCs to Indicate Requirement Levels. [Online] 1997. [Zitat vom: 03. Mai 2022] https://tools.ietf.org/html/rfc2119.

Abkürzungsverzeichnis

APIs	Application Programming Interfaces
BMI	Bundesministerium des Innern, für Bau und Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
CRL	Certificate Revocation List
DHCP	Dynamic Host Configuration Protocol
DIN	Deutsches Institut für Normung e.V.
DNS	Domain-Name-System
FAQ	Frequently Asked Questions
IETF	Internet Engineering Task Force
ISB	Informationssicherheitsbeauftragte
IT-SiBe	IT-Sicherheitsbeauftragte
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Management
MDMS	Mobile Device Management System
MST	Mindeststandard
NdB	Netze des Bundes
OCSP	Online Certificate Status Protocol
OTA	Over-the-air
RFC	Request for Comments
RZ	Rechenzentren
TR	Technische Richtlinie
UP	Umsetzungsplan
VPN	Virtual Private Network

Nr.	Bezeichnung	Absatz	S cherheitsanforderung (MST-MDM V2.0)	IT-Grundschutz-K 2022
MDM.2.1.01	St ateg e fü das Mob le Dev ce Management		D e E n chtung MUSS e ne St ateg e fü das Mob le Dev ce Management gemäß de Bas s-Anfo de ung SYS.3.2.2.A1 des IT-G undschutz-Kompend ums e stellen. Zusätzl ch zu den n SYS.3.2.2.A1 def n e ten Aspekten MUSS d e St ateg e folgende	SYS.3.2 2.A1
MDM.2.1.02	E laubte mob le Endge äte		Es MUSS festgelegt we den, welche mob len Endge äte und Bet ebssysteme n de E n chtung e laubt s nd. Be e ts be de Auswahl zu beschaffende mob le Endge äte MUSS d e E n chtung da auf achten, dass de He stelle übe den geplanten	SYS.3.2 2.A2
MDM.2.1.02	E laubte mob le Endge äte		Es MUSS festgelegt we den, welche mob len Endge äte und Bet ebssysteme n de E n chtung e laubt s nd. Be e ts be de Auswahl zu beschaffende mob le Endge äte MUSS d e E n chtung da auf achten, dass de He stelle übe den geplanten	SYS.3.2 1.A5
MDM.2.2.01	E nsch ränkungen du ch Endge äte ode B r t l	a)	Das MDMS und d e E n chtung MÜSSEN nu d ejen gen Anfo de ungen n Kap tel 2.6 und 2.7 d eses M ndeststanda ds e füllen, d e von den zu ve waltenden mob len Endge äten m ausgewählten Bet ebsmodell techn sch unte stützt we den.	
MDM.2.2.01	E nsch ränkungen du ch Endge äte ode Bet ebsmode l	b)	Im Fall e ne e ngesch änkten ode fehlenden Unte stützung, d e du ch das gewäh te Bet ebsmodell entsteht (z. B. Remote W pe be BYOD), MUSS d e E n chtung das entsp echende R s ko ad ess e en, ndem s e d e Benutzenden n d e Pfl cht n mmt (vgl.	
MDM.2.2.02	Integ at on e ne MDM-Cl ent-App		E n MDM-Cl ent, de als Appl kat on be e tgestellt w d, MUSS auf d e Bet ebssystem-E nstellungen übe d e vom Bet ebssystem be e tgestel ten APIs zug e ten und da übe d e n d esem M ndeststanda d besch ebenen Pa amete setzen	
MDM.2.2.03	Nutzdaten		Anfa lende Nutzdaten des MDMS MÜSSEN n e ne ges che ten Umgebung gespe che t we den (vgl. auch MDM.2.2.08 und MDM.2.2.09). Nutzdaten s nd nsbesonde e Konf gu at onsp of le sow e Benutze namen und ande e pe sönl che	
MDM.2.2.04	Zugangscodes und -m ttel	a)	Zug ffe auf den MDM-Se ve sow e Adm n st at ons- und Se f-Se v ce Po tale MÜSSEN du ch e ne Nutze authent f z e ung geschützt se n. Zudem SOLLTE Zwe -Fakto -Authent f z e ung genutzt we den. Fü das Zu ücksetzen von Passwö te n SOLLTE e n	ORP 4.A10
MDM.2.2.04	Zugangscodes und -m ttel	a)	Zug ffe auf den MDM-Se ve sow e Adm n st at ons- und Se f-Se v ce Po tale MÜSSEN du ch e ne Nutze authent f z e ung geschützt se n. Zudem SOLLTE Zwe -Fakto -Authent f z e ung genutzt we den. Fü das Zu ücksetzen von Passwö te n SOLLTE e n	ORP 4.A11
MDM.2.2.04	Zugangscodes und -m ttel	b)	D e E n chtung MUSS d e Stä ke von Zugangscodes und -m ttel n dem angest ebten Schutzbeda f entsp echend festlegen. Sofe n anwendba , umfasst d es folgende Aspekte m n male Länge, ggf. Beschaffenhe t m Fa le b omet sche Zugangscodes,	ORP 4.A22
MDM.2.2.04	Zugangscodes und -m ttel	b)	D e E n chtung MUSS d e Stä ke von Zugangscodes und -m ttel n dem angest ebten Schutzbeda f entsp echend festlegen. Sofe n anwendba , umfasst d es folgende Aspekte m n male Länge, ggf. Beschaffenhe t m Fa le b omet sche Zugangscodes,	ORP 4.A11
MDM.2.2.04	Zugangscodes und -m ttel	b)	D e E n chtung MUSS d e Stä ke von Zugangscodes und -m ttel n dem angest ebten Schutzbeda f entsp echend festlegen. Sofe n anwendba , umfasst d es folgende Aspekte m n male Länge, ggf. Beschaffenhe t m Fa le b omet sche Zugangscodes,	ORP 4.A13
MDM.2.2.04	Zugangscodes und -m ttel	b)	D e E n chtung MUSS d e Stä ke von Zugangscodes und -m ttel n dem angest ebten Schutzbeda f entsp echend festlegen. Sofe n anwendba , umfasst d es folgende Aspekte m n male Länge, ggf. Beschaffenhe t m Fa le b omet sche Zugangscodes,	ORP 4.A23
MDM.2.2.04	Zugangscodes und -m ttel	b)	D e E n chtung MUSS d e Stä ke von Zugangscodes und -m ttel n dem angest ebten Schutzbeda f entsp echend festlegen. Sofe n anwendba , umfasst d es folgende Aspekte m n male Länge, ggf. Beschaffenhe t m Fa le b omet sche Zugangscodes,	SYS.3.2 1.A18
MDM.2.2.05	Mandantent ennung		We den meh e e Mandanten auf e nem MDMS ve waltet, so MUSS e ne w ksame T ennung de Mandanten s che geste lt se n.	
MDM.2.2.06	Be echt gungsmanagement m MDMS	a)	Das MDMS MUSS übe e n Rechtemanagement ve fügen, so dass das Be echt gungskonzept de E n chtung vollständ g umgesetzt we den kann.	
MDM.2.2.06	Be echt gungsmanagement m MDMS	b)	D e E n chtung MUSS übe e n Be echt gungskonzept fü das MDMS ve fügen. Benutzende de mob len Endge äte und IT-Bet ebspe sonal DÜRFEN NUR übe Be echt gungen ve fügen, d e fü d e Aufgabene füllung notwend g s nd (M n malp nz p).	ORP 4.A2
MDM.2.2.07	Abs che ung de MDMS-Bet ebsumgebung		D e MDMS-Bet ebsumgebung SOLLTE d e Standa d-Anfo de ung SYS.3.2.2 A12 des IT-G undschutz-Kompend ums e füllen. Im Fall e ne Fe nzug ffsmögl chke t KANN d ese gemäß Bauste n OPS.1.2 5 abges che t we den.	SYS.3.2 2.A12
MDM.2.2.07	Abs che ung de MDMS-Bet ebsumgebung		D e MDMS-Bet ebsumgebung SOLLTE d e Standa d-Anfo de ung SYS.3.2 2 A12 des IT-G undschutz-Kompend ums e füllen. Im Fall e ne Fe nzug ffsmögl chke t KANN d ese gemäß Bauste n OPS.1.2 5 abges che t we den.	OPS.1.2.5
MDM.2.2.08	S che he tsanfo de ungen an den Bet eb m B h t		Fü d e Rechenzent en (RZ), aus denen das MDMS ode Te le davon e b acht we den, MÜSSEN – zusätzl ch zu dem vo l egenden M ndeststanda d – d e Anfo de ungen des „M ndeststanda d des BSI zu Anwendung des HV-Benchma k kompakt" e ngehalten	
MDM.2.2.09	Cloud-D enste be m Bet eb des MDMS		W d das MDMS ode we den das MDMS e gänzende D enste (vgl. MDM.2 6 02) ganz ode auch nu te lwe se von e nem exte nen Cloud-Anb ete bezogen, MÜSSEN d e Anfo de ungen des „M ndeststanda d des BSI zu Nutzung exte ne Cloud-	
MDM.2.2.10	Mob le Zugänge zu Netzen des Bundes		W d das MDMS m Rahmen e ne mob len Lösung m t den Netzen des Bundes genutzt, MÜSSEN d e Anfo de ungen des „M ndeststanda d des BSI zu Nutzung de esso tübe g e fenden Kommun kat onsnetze des Bundes" e ngehalten we den.	
MDM.2.3.01	P otokoll e ung von Ge ätedaten	a)	De aktue le Status de ve wa teten Endge äte MUSS übe das MDMS e m tteilt we den können. D es MUSS m ndestens Folgendes umfassen	SYS.3.2 2.A6
MDM.2.3.01	P otokoll e ung von Ge ätedaten	a)	De aktue le Status de ve wa teten Endge äte MUSS übe das MDMS e m tteilt we den können. D es MUSS m ndestens Folgendes umfassen	CON.2
MDM.2.3.01	P otokoll e ung von Ge ätedaten	b)	D e E n chtung MUSS das MDMS so konf gu e en, dass nu IT-Bet ebspe sonal m t den Rollen Adm n st ato und Aud to (vgl. MDM.2.2.06) d e e hobenen Ge ätedaten e nsehen kann. D e E n chtung MUSS du ch techn sche ode o gan sato sche	
MDM.2.3.02	P otokoll e ung von MDMS-Daten	a)	Das MDMS MUSS d e Mögl chke t be e tstellen, alle s che he ts elevanten Akt onen, d e das MDMS selbst bet effen, (z. B. d e Zuo dnung von Ro len zu Pe sonen) m tsamt de Identi tät des Ve u sache s zu p otoko l e en.	CON.2
MDM.2.3.02	P otokoll e ung von MDMS-Daten	b)	D e E n chtung MUSS das MDMS so konf gu e en, dass d e E ns cht de P otokolle auf Aud to en beg enzt st. D e E n chtung MUSS du ch techn sche ode o gan sato sche Maßnahmen s che stellen, dass d e P otokolle n cht man pul e t we den können.	
MDM.2.4.01	Dokumentat on des MDMS		Das MDMS sow e entsp echende Aktual s e ungen MÜSSEN vollständ g und nachvo lz ehba dokument e t se n. Be Ände ungen am MDMS MUSS d e Dokumentat on ze tnah angepasst we den. D e Dokumentat on MUSS enthalten	
MDM.2.4.02	Suppo t		Suppo tle stungen des Anb ete s MÜSSEN den Anfo de ungen des ewe l gen E nsatzsena os entsp echen. Dabe MÜSSEN zum ndest bet achtet we den	
MDM.2.4.03	Aktual s e ungen des MDMS		De MDMS-Anb ete MUSS den P ozess zu Be e tstellung von Aktual s e ungen des MDMS (Updates und Patches) da ste len und aus che n. W d de Suppo t des MDMS e ngestel t, MUSS de Anb ete unve zügl ch nach Kenntn snahme h e übe nfo m e en.	
MDM.2.5.01	Abges che te Kanal		Zu Etabl e ung e nes Abges che ten Kanals, w e e n d esem M ndeststanda d ve wendet w d, s nd d e folgenden Anfo de ungen zu e fü len	
MDM.2.5.02	Sepa at on des MDMS		De Se ve des MDMS MUSS e n e gene Komponente fü d e Kommun kat on m t den Endge äten (vgl. MDM.2.5 03) sow e n e e gene Komponente fü d e Inte akt on m t Adm n st at ons- und Self-Se v ce-Komponenten (vgl. MDM.2.5.04) be e tstellen.	
MDM.2.5.03	Kommun kat on zw schen MDM-Se ve und MDM-Cl t		D e Kommun kat on zw schen MDM-Se ve und MDM-Cl ent MÜSS übe e nen Abges che ten Kanal (vgl. MDM 2.5.01) e folgen, solange de MDM-Cl ent be m MDM-Se ve eg st e t st (vgl. MDM.2.6.03 S che es En ollment de mob len Endge äte).	SYS.3.2 2.A4
MDM.2.5.04	Kommun kat on zw schen MDM-Se ve sow e t t C H-S		Sämtl che Kommun kat on zw schen MDM-Se ve und Adm n st at ons- und Self-Se v ce-Komponenten, sofe n solche genutzt we den sollen, MUSS übe e nen Abges che ten Kanal (vgl. MDM.2.5.01) e folgen.	
MDM.2.5.05	Kommun kat on zw schen MDM-Se ve und Inf ast uktu en de E n chtung		Soll das MDMS an Inf ast uktu en de E n chtung (z. B. Ve ze chn sd enste ode Ma lse ve) angebunden we den, s nd folgende Anfo de ungen zu e fü len	
MDM.2.5.05	Kommun kat on zw schen MDM-Se ve und I f t t E ht	a)	D e Ve b ndung zw schen MDMS und den Inf ast uktu en de E n chtung MUSS übe e nen Abges che ten Kanal (vgl. MDM.2.5.01) e folgen.	
MDM.2.5.05	Kommun kat on zw schen MDM-Se ve und Inf ast uktu en de E n chtung	b)	D e E n chtung MUSS bewe ten, ob h e sens blen Inf ast uktu en du ch we te e Maßnahmen geschützt we den müssen (z. B. wenn e n Zonenmodell ve wendet w d).	
MDM.2.5.06	Kommun kat on zw schen MDM-Se ve und exte t n t		D e Kommun kat on zw schen MDM-Se ve und exte nen D ensten (z. B. Update Se ve fü das MDMS) MUSS übe e nen Abges che ten Kanal (vgl. MDM.2.5.01) e folgen.	
MDM.2.6.01	Dokumentat on fü mob le Endge äte		D e S che he tunnelchan smen und -e nstellungen fü mob le Endge äte MÜSSEN festgelegt und nachvollz ehba besch eben se n (z. B. PIN-Code-Ve fah en, automat sche Spe e ode Regeln fü d e De nstallat on von Konf gu at onsp of len).	SYS.3.2 1.A3
MDM.2.6.02	Zusätzl che D enste zu Ve wa tung de I F t		W d e n D enst genutzt, de d e Funkt onal tät des genutzten MDMS e we te t (z. B. e n Se v ce fü Ove rthe-a OTA)-Bet ebssystemupdates ode zum automat s e ten En ollment aus de Fe ne, vgl. MDM.2.6.03), MUSS e n ve t auenswü d ge	
MDM.2.6.03	S che es En ollment de mob len Endge äte	a)	Fü das En o lment de mob len Endge äte MUSS das MDMS e n s che e Schn tstelle be e tstellen. Zusätzl ch zu MDM.2.6 02 g lt wäh end des En o lments	
MDM.2.6.03	S che es En ollment de mob len Endge äte	b)	A le mob len Endge äte, d e Zug ff auf IT-Inf ast uktu en ode Daten de E n chtung haben, SOLLTEN pe MDM ve waltet we den. D e E n chtung MUSS d e zu ve waltenden mob len Endge äte so schnell w e mögl ch n das MDMS nteg e en und	SYS.3.2 2.A4
MDM.2.6.03	S che es En ollment de mob len Endge äte	b)	A le mob len Endge äte, d e Zug ff auf IT-Inf ast uktu en ode Daten de E n chtung haben, SOLLTEN pe MDM ve waltet we den. D e E n chtung MUSS d e zu ve waltenden mob len Endge äte so schnell w e mögl ch n das MDMS nteg e en und	SYS.3.2 2.A5
MDM.2.6.04	Konf gu at onsp of le	a)	Das MDMS MUSS Konf gu at onsp of le (z. B. VPN-Ve b ndungen, WLAN E nste lungen) an d e mob len Endge äte übe m tteln können. Das MDMS MUSS den Insta lat onsstatus von Konf gu at onsp of len p o Ge ät anze gen können. Das MDMS MUSS	
MDM.2.6.04	Konf gu at onsp of le	b)	Kann e ne unauto s e te Löschung von Konf gu at onsp of len – w e n (a) gefo de t – techn sch n cht ve h nde t we den, MÜSSEN o gan sato sche Maßnahmen (z. B. Beleh ung und Sens b l s e ung des Benutzenden vgl. MDM.2.8.05) e g fen	
MDM.2.6.05	Entfe nen des Endge äts aus de Ve waltung		Das MDMS SOLLTE ve h nde n können, dass de Benutzende d e p ov s on e te Ve b ndung des mob len Endge äts zum MDM-Se ve t ennt (z. B. du ch Löschen de MDM-Cl ent-App).	
MDM.2.6.06	Betatests		Nutzt d e E n chtung auf gew ssen mob len Endge äten Betave s onen von Appl kat onen ode Bet ebssystemen, MÜSSEN d ese Endge äte m MDMS sepa at ve waltet we den.	
MDM.2.6.07	Adm n st at on von Schn ttstellen, D ensten und Funkt onen	a)	Kommun kat onsd enste w e SMS und MMS sow e Funkt onen w e Kame as, M k ofone, d g tale Ass stenten (z. B. S) und Sp achsteue ungen MÜSSEN zent al und so g amu la , w e das Bet ebssystem es e mögl cht, übe das MDMS adm n st e ba	SYS.3.2 1.A16
MDM.2.6.07	Adm n st at on von Schn ttstellen, D ensten F t	b)	D e F e schaltung de n (a) genannten Schn ttstellen-Funkt onen, D enste und Funkt onen MUSS ge egelt und pe MDMS auf das d enstl ch notwend ge MaßeduZ e t we den. D g tale Ass stenten SOLLTEN pe MDMS deakt v e t we den.	SYS.3.2 1.A3
MDM.2.6.07	Adm n st at on von Schn ttstellen, D ensten F t	b)	D e F e schaltung de n (a) genannten Schn ttstellen-Funkt onen, D enste und Funkt onen MUSS ge egelt und pe MDMS auf das d enstl ch notwend ge MaßeduZ e t we den. D g tale Ass stenten SOLLTEN pe MDMS deakt v e t we den.	SYS.3.2 1.A16
MDM.2.6.08	Mon to ng und D agnose	a)	Funkt onen zu bet ebssysteme genen Übe m ttlung von Mon to ng- und D agnose-Info rmat onen MÜSSEN zent al übe das MDMS deakt v e t we den können.	
MDM.2.6.08	Mon to ng und D agnose	b)	D e E n chtung MUSS d e n (a) genannten Funkt onen pe MDMS deakt v e en.	
MDM.2.6.09	Entw ckle modus	a)	Das MDMS MUSS den Entw ckle modus des mob len Bet ebssystems deakt v e en können.	
MDM.2.6.09	Entw ckle modus	b)	D e E n chtung SOLLTE den Entw ckle modus pe MDMS deakt v e en.	
MDM.2.6.10	Konf gu at on von Netzwe kpa amete n		Netzwe kpa amete auf den mob len Endge äten DNS, Gateways, DHCP) SOLLTEN übe das MDMS konf gu e ba se n.	
MDM.2.6.11	Ve schlüsselung des Spe che s	a)	Das MDMS MUSS d e systeme gene Ve schlüsselung des mob len Endge äte s von n chtflüch gem Spe che akt v e en können.	
MDM.2.6.11	Ve schlüsselung des Spe che s	b)	Das MDMS MUSS auch d e Ve schlüsselung von Daten auf exte nen Spe che med en (z. B. SD-Ka te) akt v e en können.	
MDM.2.6.11	Ve schlüsselung des Spe che s	c)	D e E n chtung MUSS d e n (a) genannte Ve schlüsselung von n chtflücht gem Spe che pe MDMS akt v e en. Zudem SOLLTE s e d e n (b) genannte Ve schlüsselung von Daten auf exte nen Spe che med en (z. B. SD-Ka ten) – m t Ausnahme von Sma tca ds –	SYS.3.2 1.A11
MDM.2.6.12	Ze t f kate	a)	Das MDMS MUSS auf den mob len Endge äten Ze t f kate nstall e en, aktual s e en und anae gen können, fü d e das Bet ebssystem d es e mögl cht (z. B. E Ma l, Act veSync, VPN, WLAN ode Webs tes). D e Installat on von n cht ve f z e ba en	SYS.3.2 2.A21
MDM.2.6.12	Ze t f kate	b)	Es MUSS e n P ozess fü das Lebenszyklusmanagement de Ze t f kate (z. B. E neue ung ode W de uf) vo handen se n. Falls d e E n chtung ke n Onl ne-P otokoll w e DCSP Mu t stapl ng nutzt, SOLLTE s e s che stellen, dass d e CRLs egelmäß g -m ndestens	
MDM.2.6.13	Compl ance-Ve stöße und komp om tt e te n E t	a)	Zum Schutz des MDMS und de Konf gu at on de Endge äte MÜSSEN Ve stöße gegen Compl ance-R chtl n en (u.a. e ne n cht e laubte Bet ebssystemve s on ode fehlende Kontakt zum MDM-Cl ent übe e nen länge en Ze t aum) e fasst we den können	
MDM.2.6.13	Compl ance-Ve stöße und komp om tt e te mob le Endge äte	b)	D e E n chtung MUSS Compl ance-R chtl n en def n e en und d e Konfo m tät de mob len Endge äte m t d esen R chtl n en egelmäß g p üfen. D ese P üfung KANN übe d e n (a) genannte Funkt on des MDMS e folgen.	
MDM.2.6.14	Automat sche B ldsch mspe ung	a)	D e Konf gu at on und w ksame Du chsetzung e ne automat schen B ldsch mspe e des mob len Endge äte s nach Ze tvo gabe MUSS übe das MDMS zent al e nstellba se n.	
MDM.2.6.14	Automat sche B ldsch mspe ung	b)	D e n (a) besch ebene Funkt on des MDMS MUSS m Bet eb genutzt und zent al vo gegeben we den. D e Ze tspanne b s zu Ge ätespe ung be Inakt v tät MUSS n Abhäng gke t zum angest ebten Schutzn veau stehen und angemessen ku z se n.	SYS.3.2 1.A4
MDM.2.6.15	Spe b ldsch m	a)	Das MDMS MUSS den Zugang zu d enstl chen Info rmat onen m Spe zustand de mob len Endge äte konf gu e en können. D es bet f t auch d e Anze ge von Push-Nach chten, nsbesonde e de en Inhalt, auf dem Spe b ldsch m.	
MDM.2.6.15	Spe b ldsch m	b)	D e E n chtung MUSS das Anze gen ve t aul che Info rmat onen auf dem Spe b ldsch m m th fe des MDMS ve h nde n.	SYS.3.2 1.A4
MDM.2.6.16	Fe ngesteue te Ge ätespe ung (Remote-L)		E ne Ge ätespe ung MUSS du ch den Adm n st ato auch aus de Fe ne übe das MDMS mögl ch se n (Remote-Lock). Kann de Remote-Lock auf den mob len Endge äten n cht ausgeführ t we den, MUSS d es vom MDMS n gee gnete We se angeze gt	
MDM.2.6.17	Fe nlöschung (Remote-W pe)	a)	Das MDMS MUSS d e Mögl chke t be e tstellen, auch aus de Fe ne e nen Befehl an ve wa tete Ge ät zu senden, um sämtl che d enstl che Daten auf mob len Endge äten n cht ausgeführ t we den, MUSS d es vom MDMS n gee gnete We se angeze gt	
MDM.2.6.17	Fe nlöschung (Remote-W pe)	b)	We den n mob len Endge äten exte ne Spe che genutzt, MÜSSEN d e da auf bef ndl chen Daten m Fa l e ne Fe nlöschung – sofe n vom MDMS und von de mob len Pla tfo m unte stützt – gelöscht we den.	SYS.3.2 2.A22
MDM.2.6.18	Ge ätecodes	a)	D e Konf gu at on und w ksame Du chsetzung von (auch b omet rischen) Ge ätecodes, Ge ätecode-R chtl n en sow e, fa ls anwendba , de Ge ätecode-Lebensdaue auf den mob len Endge äten MUSS zent al übe das MDMS konf gu e ba se n.	
MDM.2.6.18	Ge ätecodes	b)	D e mob len Endge äte MÜSSEN du ch Ge ätecodes geschützt se n. D ese MÜSSEN d e Anfo de ungen aus MDM.2.2.04 (b) e füllen.	SYS.3.2 1.A4
MDM.2.6.19	Name de mob len Endge äte		De Name de mob len Endge äte DARF KEINE Me kmale enthalten, d e Rückschlüsse auf den Benutzenden ode d e E n chtung e mögl chen. Wählen d e Benutzenden den Namen de Endge äte, MÜSSEN s e entsp echend sens b l s e t we den (vgl.	
MDM.2.7.01	Ve te lung von Appl kat onen	a)	E ne zent ale Ve te lung von Appl kat onen übe das MDMS MUSS mögl ch se n. D ese MUSS den Anfo de ungen des geplanten E nsatzszena os genügen (z. B. g uppenbas e te Ve te lung be. Ve wa tung von And o d- und OS-Ge äten übe dasselbe MDMS)	SYS.3.2 2.A7
MDM.2.7.01	Ve te lung von Appl kat onen	b)	D e E n chtung MUSS d enstl che Appl kat onen zent al übe das MDMS ve walten und aufb ngen. D e E n chtung MUSS e ne mögl chst ku ze F st def n e en, b s zu de s che he tsk t sche Updates e ngesp elt we den müssen. Dü fen d e M ta be te	
MDM.2.7.02	Be e tstellung von Appl kat onen	a)	D e E n chtung MUSS s che ste len, dass ausschl eßl ch ve t auenswü d ge Appl kat onen Zug f auf IT Inf ast uktu en und Daten de E n chtung e halten.	
MDM.2.7.02	Be e tstellung von Appl kat onen	b)	D e E n chtung SOLLTE s che stellen, dass ausschl eßl ch ve t auenswü d ge Appl kat onen auf den mob len Endge äten nstall e t we den. D es KANN m th fe e ne L ste e laubte Anwendungen ode e ne L ste ve botene Anwendungen e e cht	SYS.3.2 1.A8
MDM.2.7.02	Be e tstellung von Appl kat onen	b)	D e E n chtung SOLLTE s che stellen, dass ausschl eßl ch ve t auenswü d ge Appl kat onen auf den mob len Endge äten nstall e t we den. D es KANN m th fe e ne L ste e laubte Anwendungen ode e ne L ste ve botene Anwendungen e e cht	SYS.3.2 1.A30
MDM.2.7.02	Be e tstellung von Appl kat onen	c)	D e E n chtung SOLLTE bewe ten, ob Apps, d e s ch ohne Installat on öffnen lassen (instant Apps), genutzt we den dü fen. Falls d es n cht e laubt w d, MÜSSEN entsp echende techn sche ode o gan sato sche Maßnahmen e g ffen we den.	
MDM.2.7.03	Vo nstall e te Appl kat onen und Onl ne-n t	a)	D e E n chtung MUSS d e Nutzung vo nstall e te Appl kat onen und Onl ne-D enste, nsbesonde e exte ne cloudbas e te D enste, bewe ten und m Beda fsfall pe MDMS ve h nde n ode e nsch änken. W d d ese Maßnahme n cht techn sch du ch	SYS.3.2 1.A2
MDM.2.8.01	Adm n st at on des MDMS		Das MDMS MUSS von IT-Bet ebspe sonal (vgl. MDM.2.2 06) bed ent we den, das n de s che en Adm n st at on von MDM-Systemen geschult st	
MDM.2.8.02	Datens che ungen des MDMS		Es MÜSSEN w ksame Mechan smen fü das Backup a le Daten und E nstellungen des MDMS ex st e en, so dass d eses m Beda fsfall funkt onsfäh g w ede he gestellt we den kann.	
MDM.2.8.03	Umgang m t S che he tsvo fä len		Fü den Umgang m t S che he tsvo fä len MUSS e n angemessene P ozess etabl e t se n. D ese MUSS m ndestens e ne sofo t ge (automat s e te ode manuelle) Meldung des Vo falls an e ne def n e te Ste le, z ne Unte suchung de Konsequenzen sow e d e	SYS.3.2 1.A7
MDM.2.8.04	Spe ung von SIM		D e E n chtung MUSS d e notwend gen Info rmat onen (z. B. d e IMEI) be e thalten, um e ne Spe ung de SIM-Ka te ode des eSIM-P of le sve anlassen zu können.	
MDM.2.8.05	Sens b l s e ung de Benutzenden		Benutzende mob le Endge äte MÜSSEN fü d e MDM-S che he tsmaßnahmen sens b l s e t we den. E ne Sens b l s e ung de Benutzenden KANN notwend g se n, um folgende Anfo de ungen zu e füllen	
MDM.2.8.06	Regelmäß ge Übe p üfungen		Konf gu at onsp of le und S che he tse nstellungen MÜSSEN egelmäß g übe p üft we den. D e vom MDMS e zeugten P otokolle MÜSSEN egelmäß g auf ungewöhnl che E nt ägе übe p üft we den. H e be MÜSSEN Vo gaben aus de IT-S che he ts chtl n e	SYS.3.2 2.A20
MDM.2.8.07	Aktual s e ung de Bet ebssysteme von MDMS I F t		Sollen neue Bet ebssysteme s onen de mob len Endge äte e ngesetzt we den, MUSS d e E n chtung vo ab p üfen, ob d e Konf gu at onsp of le und S che he tse nstellungen we te h n w ksam und aus e chend s nd. Abwe chungen MÜSSEN ko g e t	
MDM.2.8.08	Benutze wechsel		Sollen ve waltete mob le Endge äte an e nen ande en Benutzenden übe geben we den, MÜSSEN zuvo alle d enstl chen Daten und Zugänge von den Endge äten, SIM Ka ten und exte nen Spe che med en, d e ebenfalls den Benutzenden wechseln, gelöscht	
MDM.2.8.09	Auße bet ebnahme		D e E n chtung MUSS MDMS und mob le Endge äte, fü d e ke ne s che he ts elevanten Aktual s e ungen meh be e tgestel t we den, außer Bet eb nehmen. D e E n chtung MUSS e ne mögl chst ku ze F st fü d e Außer bet ebnahme def n e en.	SYS.3.2 1.A5
MDM.2.8.09	Auße bet ebnahme		D e E n chtung MUSS MDMS und mob le Endge äte, fü d e ke ne s che he ts elevanten Aktual s e ungen meh be e tgestel t we den, außer Bet eb nehmen. D e E n chtung MUSS e ne mögl chst ku ze F st fü d e Außer bet ebnahme def n e en.	SYS.3.2 2.A22