Bundesamt
für Sicherheit in der
Informationstechnik

Mindeststandard des BSI für Mobile Device Management

nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 11.05.2017

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

Inhaltsverzeichnis

Vorwort

§ 8 Absatz 1 BSIG regelt die Befugnis des Bundesamtes für Sicherheit in der Informationstechnik (BSI), allgemeine Mindeststandards für die Sicherheit der Informationstechnik für Stellen des Bundes festzulegen. Mindeststandards können nach der Gesetzesbegründung etwa die IT-Grundschutz-Kataloge oder auch Prüfkriterien sein. Der Mindeststandard beschreibt die zu erfüllenden sicherheitstechnischen Anforderungen an eine Produkt- bzw. Dienstleistungskategorie oder Methoden, um einen angemessenen Mindestschutz gegen IT-Sicherheitsbedrohungen zu erreichen.

Mindeststandards sind Vorgaben des BSI für die Stellen des Bundes. Allerdings kann das Bundesministerium des Innern (BMI) im Benehmen mit dem IT-Rat die dort formulierten Anforderungen ganz oder teilweise als allgemeine Verwaltungsvorschrift erlassen und dadurch für die Stellen des Bundes mit Ausnahme der in § 8 Absatz 1 Satz 4 BSIG[1] genannten als verbindlich erklären.

Über die Stellen des Bundes hinaus sind Mindeststandards nach § 8 Absatz 1 BSIG auch in der öffentlichen Verwaltung der Länder und Kommunen für den Einsatz von Informationstechnik und zur Sicherung kritischer Infrastrukturen von grundsätzlicher Bedeutung. Ziele, Anforderungen und Empfehlungen von Mindeststandards können dazu genutzt werden, eigene Sicherheitsanforderungen anzupassen oder zu überprüfen, auch bei der Erstellung von Leistungsbeschreibungen im Rahmen eigener Vergabeverfahren. Anbieter von Informationstechnik und IT-Dienstleister können Mindeststandards dazu nutzen, ihre angebotenen Produkte sicherer zu machen.

1 Dies sind Bundesgerichte, der Bundestag, Bundesrat, Bundespräsident und Bundesrechnungshof.

1 Beschreibung

Mithilfe von Mobile Device Management (MDM) können mobile Endgeräte (Mobile Devices) in die IT-Infrastruktur einer Stelle des Bundes integriert und zentral verwaltet werden. Mit Blick auf die Sicherheit ist die Kernfunktion des MDM die wirksame Durchsetzung definierter Sicherheitsrichtlinien und Konfigurationsparameter auf den mobilen Endgeräten. Der Mindeststandard setzt mit seinen Vorgaben ein definiertes Sicherheitsniveau für den Einsatz solcher MDMs durch Stellen des Bundes.

Hinsichtlich seiner Umsetzung richtet sich der Mindeststandard an IT-Verantwortliche, IT-Sicherheitsbeauftragte (bzw. Informationssicherheitsbeauftragte) und IT-Fachkräfte sowie mit der Beschaffung beauftragte Stellen des Bundes. Anbieter von MDMs und andere Interessierte können diesen Mindeststandard zur Erhöhung der Informationssicherheit oder zum Abgleich ihrer Angebote heranziehen.

Der Einsatz eines MDM stellt nur einen Baustein des Gesamtkonzeptes des sicheren mobilen Arbeitens dar. Weitere Bausteine sind u. a. die Auswahl sicherheitsgeprüfter Applikationen oder der Einsatz von sicheren Lösungen für die PIM-Datenverarbeitung. Überschneidungen mit dem Mobile Application Management (MAM) und weiteren Bausteinen sind aufgrund der engen Verzahnung möglich.[2] Im Fokus des Mindeststandards stehen jedoch Sicherheitsanforderungen für MDMs.

Dieser Mindeststandard setzt dabei die IT-Grundschutz-Vorgehensweise des BSI zum Management der Informationssicherheit voraus.[3] Er gilt für alle Schutzbedarfskategorien.

Sicherheitsanforderungen dieses Mindeststandards sind in verschiedene Abschnitte thematisch gegliedert (siehe Kapitel 2). Vor der Beschaffung eines MDM ist zusätzlich zur Schutzbedarfsfeststellung aus dem IT-Grundschutz eine vorgelagerte Datenkategorisierung für die zukünftig mit dem MDM zu verarbeitenden Daten durchzuführen. Risiken für die Daten müssen zudem in einer Risikoanalyse betrachtet und bewertet werden. Im Rahmen der Datenkategorisierung und Risikoanalyse sind die zuständigen Datenschutz-, Geheimschutz- und IT-Sicherheitsbeauftragen angemessen zu beteiligen.

Mobile Endgeräte sind Smartphones, Phablets und Tablets, die mit einem für den mobilen Einsatz angepassten Betriebssystem ausgestattet sind (z. B. Android, iOS oder BlackBerryOS). Tragbare Computer mit Betriebssystemen für den Desktopbereich liegen außerhalb der Betrachtung.

2 Vgl. BSI (2016), S.17ff.
3 Vgl. BSI (2008), S.1ff.

2 Sicherheitsanforderungen

Nachfolgende Sicherheitsanforderungen adressieren das MDM selbst sowie dessen Betrieb. Diese sind von den Stellen des Bundes einzuhalten, um ein definiertes Sicherheitsniveau zu gewährleisten. Sie können jedoch bei Bedarf durch zusätzliche Anforderungen erweitert werden.

2.1 Funktionale Sicherheitsanforderungen an das MDM

Funktionale Sicherheitsanforderungen sind durch das MDM zu erfüllen.

2.1.1 Arbeitsweise des MDM

MDM.01: Nutzdaten

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

MDM.02: Cloud-Dienste

Wird das MDM ganz oder auch nur teilweise von einem externen Cloud-Anbieter bezogen, sind zusätzlich die Anforderungen aus dem Mindeststandard des BSI zur "Nutzung externer Cloud-Dienste"[4] einzuhalten.

MDM.03: Mandantentrennung

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

MDM.04: Kompromittierte mobile Endgeräte

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

MDM.05: Berechtigungsmanagement im MDM

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

MDM.06: SIM-Karten

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

2.1.2 Applikationsverwaltung

MDM.07: Verteilung von Applikationen

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

4 BSI (2017a), S. 1ff.

MDM.08: MDM-Client

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

2.1.3 Audit

MDM.09: Protokollierung

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

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

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

2.1.4 Sichere Konfiguration der mobilen Endgeräte

MDM.10: Konfigurationsprofile

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

MDM.11: Sichere Erstinstallation

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

MDM.12: Kennwörter und Gerätecodes

Die Einrichtung und wirksame Durchsetzung komplexer Kennwörter und Gerätecodes auf den mobilen Endgeräten muss zentral konfigurierbar sein. Die Vorgabe, nach wie vielen Fehleingaben das Endgerät gesperrt oder gelöscht wird, muss zentral konfigurierbar sein. Ein Reset von Kennwörtern und Gerätecodes zum Entsperren des Endgeräts muss durch den Administrator auch aus der Ferne (z. B. OTA) möglich sein.[5]

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

Das MDM muss sicherstellen, dass sämtliche Daten auf dem mobilen Endgerät, einschließlich Zugangsdaten und Zertifikate, auch aus der Ferne gelöscht werden können (Remote-Wipe bei bestehender Netzwerkverbindung). Werden in dem mobilen Endgerät externe Speicher genutzt, muss geprüft werden, ob diese bei einem Remote-Wipe ebenfalls gelöscht werden sollen und ob dies vom MDM unterstützt wird.

Der Prozess zur Außerbetriebnahme des mobilen Endgerätes (Unenrollment) muss sicherstellen, dass keine sensitiven Daten auf dem mobilen Endgerät oder eingebundenen Speichermedien verbleiben. Dies gilt insbesondere dann, wenn das Unenrollment aus der Ferne ausgeführt wird.

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

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

5 Komponenten außerhalb des Einflussbereichs des MDMs (z.B. Smartcards) sind hiermit nicht gemeint.

MDM.15: Administration von Schnittstellen und Funktionen

Schnittstellen müssen zentral über das MDM administrierbar sein. Unter Schnittstellen sind insbesondere Bluetooth, Infrarot, WLAN, SMS, MMS, GPS, NFC, RFID und USB zu verstehen.

Gleiches gilt für Funktionen wie z. B. Kameras, Mikrofone, Sprachsteuerungen und Ortungsdienste.

Ein Koppeln oder Verbinden mit anderen Geräten (z. B. via Apple AirPlay oder AirDrop) zum Datenaustausch oder zur Datenweitergabe muss unterbunden werden können.

MDM.16: Verschlüsselung des Speichers

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

MDM.17: Zertifikate

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

2.1.5 Vertrauenswürdige Kommunikation

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

Zur Gewährleistung der Authentizität der Teilnehmer sowie Vertraulichkeit und Integrität der übertragenen Inhalte ist sämtliche Kommunikation zwischen MDM und Administrations- und Self-Service-Portalen dem Schutzbedarf entsprechend abzusichern. Die Transportverschlüsselung muss die Sicherheitsanforderungen nach Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls[6] erfüllen. VPN-Verbindungen müssen den IT-Sicherheitsrichtlinien für VPN-Verbindungen der Stelle des Bundes entsprechen.

MDM.19: Mobile Endgeräte

Die Kommunikation zwischen MDM und mobilem Endgerät muss über einen sicheren Kanal erfolgen. Hierfür muss die Stärke der Schlüssel (Schlüssellänge und -verfahren) den IT-Sicherheitsrichtlinien der Stelle des Bundes entsprechen. Liegt dem sicheren Kanal eine Transportverschlüsselung nach TLS zu Grunde, dann muss diese dem Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls[7] genügen. Wird eine VPN-Verbindung genutzt, muss diese den IT-Sicherheitsrichtlinien für VPN-Verbindungen der Stelle des Bundes entsprechen.

2.2 Nicht-funktionale Sicherheitsanforderungen an das MDM

Nicht-funktionale Anforderungen sind durch den jeweiligen MDM-Anbieter zu erfüllen.

MDM.20: Dokumentation des MDM

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

- Unterstützte mobile Endgeräte mit Betriebssystemversionen,
- Angabe über Funktionalitäten, die nur auf bestimmte mobile Endgeräte oder Betriebssystemversionen anwendbar sind,
- Schutzeinrichtungen für personenbezogene Daten,

6 BSI (2015), S. 1ff.
7 BSI (2015), S. 1ff.

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

MDM.21: Support

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

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

MDM.22: Aktualisierungen des MDM

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

2.3 Sicherheitsanforderungen an den Betrieb

Die Wirksamkeit von Sicherheitsmechanismen hängt auch vom jeweiligen Betrieb ab. Der Betreiber hat daher nachfolgende technische und organisatorische Maßnahmen umzusetzen.

2.3.1 Technische Maßnahmen

MDM.23: Datensicherungen des MDM

Es müssen wirksame Mechanismen für das Backup aller Daten und Einstellungen des MDMs existieren, so dass dieser im Bedarfsfall funktionsfähig wiederhergestellt werden kann.

MDM.24: Fernzugriff auf das MDM

Fernzugriffe auf das MDM müssen auf einem kryptographisch abgesicherten Kanal erfolgen (vertraulich, integer, authentisch). Die Vorgaben der technischen Richtlinie TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“[8] müssen beachtet werden. Liegt eine Transportverschlüsselung nach TLS zu Grunde, dann muss diese dem Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls[9] genügen.

MDM.25: Erstinstallation der mobilen Endgeräte

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

8 BSI (2017), S.1ff.
9 BSI (2015), S. 1ff.

MDM.26: Verschlüsselung des Speichers

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

MDM.27: Monitoring und Diagnose

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

MDM.28: Kennwörter und Gerätecodes

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

MDM.29: Automatische Sperre und Gerätesperrung

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

2.3.2 Organisatorische Maßnahmen

MDM.30: Administration des MDM

Das MDM muss von geschulten Administratoren bedient werden.

MDM.31: Sensibilisierung der Benutzer

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

MDM.32: Dokumentation

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

MDM.33: Regelmäßige Überprüfungen

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

MDM.34: Umgang mit Sicherheitsvorfällen

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

- Verlust eines mobilen Endgerätes,
- Verlust der Integrität des mobilen Endgerätes (z. B. durch Jailbreak oder Rooting),

– kein Kontakt des mobilen Endgerätes zum MDM über einen längeren Zeitraum hinweg.

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

MDM.35: Aktualisierung der Betriebssysteme

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

MDM.36: Konfigurationsprofile und MDM-Client

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

MDM.37: Endgerätenamen

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

MDM.38: Bereitstellung von Applikationen

Es muss sichergestellt sein, dass ausschließlich sicherheitsgeprüfte Applikationen bereitgestellt werden. Dies kann durch einen definierten Freigabeprozess mit geeigneten Bewertungskriterien sichergestellt werden. Die Nutzung von vorinstallierten Applikationen und Online-Diensten, insbesondere von externen cloudbasierten Diensten[10] muss bewertet und im Bedarfsfall systemseitig verhindert werden.

MDM.39: Nutzung von Schnittstellen und Funktionen

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

MDM.40: Push-Nachrichten

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

10 BSI (2017a), S. 1ff.

Literaturverzeichnis

BSI (2008) Bundesamt für Sicherheit in der Informationstechnik, BSI-Standard 100-2 – IT-Grundschutz-Vorgehensweise, Version 2.0, Bonn 2008

BSI (2015) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI für den Einsatz des SSL/TLS-Protokolls durch Bundesbehörden vom 21.11.2014

BSI (2016) Bundesamt für Sicherheit in der Informationstechnik: Sicheres mobiles Arbeiten - Problemstellung, Technische Voraussetzungen und Lösungswege anhand der Anforderungen für mobile Endgeräte in der Bundesverwaltung, Stand Februar 2016, Bonn

BSI (2017) Bundesamt für Sicherheit in der Informationstechnik: Technische Richtlinie TR-02102-1 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, Version 2017-01 vom 08.02.2017

BSI (2017a) Bundesamt für Sicherheit in der Informationstechnik: Mindeststandard des BSI zur Nutzung von externen Cloud-Diensten nach § 8 Absatz 1 Satz 1 BSIG – Version 1.0 vom 24.04.2017

Stichwort- und Abkürzungsverzeichnis

BMI	Bundesministerium des Innern
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
DMZ	Demilitarisierte Zone
GPS	Global Positioning System
IMSI	International Mobile Subscriber Identity
IPsec	Internet Protocol Security
LDAP	Lightweight Directory Access Protocol
MAM	Mobile Application Management
MDM	Mobile Device Management
MMS	Multimedia Messaging Service
NFC	Near Field Communication
OCSP	Online Certificate Status Protocol
OTA	Over-The-Air
RFID	Radio-Frequency Identification
SIM	Subscriber Identity Module
SD-Karte	Sichere Digitale Speicherkarte
SMS	Short Message Service
SSL	Secure Sockets Layer
TLS	Transport Layer Security
PIN-Code	Persönliche Identifikationsnummer
PIM	Personal Information Manager
USB	Universal Serial Bus
VPN	Virtual Private Network
WLAN	Wireless Local Area Network