Bundesamt
für Sicherheit in der
Informationstechnik

SYS.3.2.2 Mobile Device Management (MDM)

1. Beschreibung

1.1. Einleitung

Smartphones, Tablets und Phablets sind für viele Mitarbeitende ein nicht mehr wegzudenkender Teil ihrer Arbeit. Der IT-Betrieb muss jedoch immer mehr solcher Geräte in vielen unterschiedlichen Ausführungen bereitstellen und dabei gleichzeitig für eine angemessene Sicherheit sorgen. Hinzu kommt, dass mobile Endgeräte (Mobile Devices) besonderen Gefahren ausgesetzt sind und die Administration sich in grundlegenden Punkten von anderen IT-Systemen unterscheidet.

Deswegen ist ein Mobile Device Management (MDM) besonders in Institutionen mit einer größeren Anzahl von Smartphones, Tablets und Phablets unabdingbar für einen geregelten und sicheren Betrieb dieser Geräte. Mit einer entsprechenden Software für das MDM können die Endgeräte zentral verwaltet werden, es lassen sich Sicherheitsregeln durchsetzen und es können Notfallaktionen ausgelöst werden. Ein MDM gewährleistet somit auf allen Geräten einen gleichen oder zumindest vergleichbaren Sicherheitsstandard.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, aufzuzeigen, wie mit einem MDM mobile Endgeräte sicher von Institutionen genutzt werden können. Er gibt zudem Hinweise zum Betrieb eines MDM.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.3.2.2 *Mobile Device Management (MDM)* ist für den Informationsverbund einzusetzen, wenn mobile Endgeräte mit einem Mobile Device Management (MDM) verwaltet werden.

Mobile Endgeräte (Mobile Devices) im Sinne dieses Bausteins sind Smartphones, Tablets und Phablets, auf denen mobile Betriebssysteme wie Android oder iOS installiert sind. Die Sicherheitsanforderungen von Smartphones, Tablets, Notebooks und Tablets mit Desktop-Betriebssystemen werden in anderen Bausteinen der Schicht SYS *IT-Systeme* beschrieben. Die Anforderungen aus SYS.3.2.1 *Allgemeine Smartphones und Tablets* müssen ebenfalls berücksichtigt werden, wenn ein MDM verwendet wird. Wie die Smartphones, Tablets und Phablets spezifisch abgesichert werden, wird zusätzlich detailliert in den Bausteinen für die jeweiligen Betriebssysteme beschrieben, z. B. in SYS.3.2.3 *iOS (for Enterprise)* oder SYS.3.2.4 *Android*.

Für das MDM muss ein Berechtigungskonzept erstellt werden. Anforderungen dazu stellt der Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* auf. Eine der ureigensten Aufgaben eines MDM ist die Administration von mobilen Endgeräten. Sicherheitsanforderungen für Administrationen enthält der Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration*.

Nicht behandelt werden in diesem Baustein Aspekte von „Bring your own device“ (BYOD).

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.3.2.2 *Mobile Device Management (MDM)* von besonderer Bedeutung:

2.1. Keine ausreichende Synchronisation mit dem MDM

Damit das MDM die von den Zuständigen definierten Regelungen auf den mobilen Endgeräten durchsetzen kann, müssen die Geräte regelmäßig mit dem MDM synchronisiert werden. Wenn ein Gerät über einen längeren Zeitraum nicht mit dem MDM verbunden ist, können beispielsweise neue oder aktualisierte Regelungen nicht aufgespielt werden. Auch können, wenn zu einem verlorenen Gerät keine Verbindung besteht, die Daten nicht mehr aus der Ferne gelöscht werden.

2.2. Fehlerhafte Administration des MDM

MDM-Lösungen sind komplexe Anwendungen mit typischerweise mehreren Hundert unterschiedlichen Regeln. Nicht alle Regeln sind dabei miteinander kombinierbar und umgekehrt hängen viele Regeln voneinander ab. Durch Fehler bei der Administration können sowohl das MDM als auch die Endgeräte diversen Gefahren ausgesetzt sein, die sich direkt oder indirekt auf die Vertraulichkeit, Verfügbarkeit oder Integrität der Daten und Anwendungen auswirken.

2.3. Ungeeignetes Rechtemanagement im MDM

Das Rechtemanagement des MDM entscheidet, welche Benutzenden welche Einstellungen auf den mobilen Geräten vornehmen dürfen und wer auf welche Daten zugreifen darf. Wenn Benutzenden eine falsche Rolle zugeordnet wird, besteht die Gefahr, dass ihnen zu hohe Rechte eingeräumt werden. So könnten sie beispielsweise Daten unbefugt einsehen oder Einstellungen am Gerät verändern. Auch wäre es möglich, dass sie Apps installieren und benutzen, die in der Institution nicht zugelassen sind, beispielsweise zur Nutzung von Cloud-Speicherdiensten. Dadurch können schützenswerte Daten aus der Institution abfließen oder es wird gegen die gesetzlichen Datenschutzbestimmungen verstoßen.

2.4. Unberechtigte Erstellung von Bewegungsprofilen durch das MDM

Mit den meisten MDM-Produkten lässt sich ermitteln, wo sich ein Gerät gerade befindet, und es können standortabhängig Daten oder Apps freigegeben bzw. gesperrt werden (sogenanntes „Geofencing“). Dadurch entstehen detaillierte Bewegungsprofile der Geräte und somit auch der Benutzenden. Werden diese Daten erhoben, ohne die Benutzenden in geeigneter Weise darüber zu informieren, verstoßen die Verantwortlichen unter Umständen gegen datenschutzrechtliche Bestimmungen. Auch besteht die Gefahr, dass im Falle eines Angriffs diese Daten an Unbefugte gelangen. Ebenso kann Geofencing dazu missbraucht werden, um Mitarbeitende unzulässig zu kontrollieren.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.2.2 *Mobile Device Management (MDM)* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.3.2.2.A1 Festlegung einer Strategie für das Mobile Device Management (B)

Es MUSS eine Strategie erarbeitet werden, die festlegt, wie Mitarbeitende mobile Endgeräte benutzen dürfen und wie die Geräte in die IT-Strukturen der Institution integriert sind. Grundlage MUSS dabei der Schutzbedarf der zu verarbeitenden Informationen sein. Die Strategie MUSS mindestens folgende Aspekte abdecken:

- Darf das MDM als Cloud-Dienst betrieben werden?
- Soll das MDM durch die Institution selbst betrieben werden?
- Soll das MDM alle Apps bereitstellen oder dürfen die Benutzenden selber Apps installieren? Welche Restriktionen gibt die Institution bei bereitgestellten oder selbst installierten Apps vor?
- Soll das MDM in eine weitere Infrastruktur eingebunden werden?
- Welche Anforderungen bezüglich Supportleistungen und Reaktionszeiten sind an die anbietende Institution des MDM zu stellen?
- Welche Compliance-Anforderungen müssen durchgesetzt werden?
- Welche mobilen Geräte und welche Betriebssysteme muss das MDM unterstützen?
- Muss die MDM-Lösung mandantenfähig sein? Gewährleistet sie die notwendige Mandantentrennung?
- Müssen Cloud-Dienste eingebunden werden?
- Müssen Dokumentenmanagementsysteme eingebunden werden?
- Muss das MDM auch Peripheriegeräte einbinden und verwalten?
- Welches Betriebsmodell soll eingesetzt werden: private Endgeräte (Bring Your Own Device, BYOD), personalisierte Endgeräte (Eigentum der Institution) oder nicht personalisierte Endgeräte (Eigentum der Institution, gemeinsam genutzt)?

Die Strategie MUSS schriftlich fixiert und von dem oder der ISB freigegeben werden.

SYS.3.2.2.A2 Festlegung erlaubter mobiler Endgeräte (B)

Es MUSS festgelegt werden, welche mobilen Endgeräte und Betriebssysteme in der Institution zugelassen sind. Alle erlaubten Geräte und Betriebssysteme MÜSSEN den Anforderungen der MDM-Strategie genügen und die technischen Sicherheitsanforderungen der Institution vollständig erfüllen. Das MDM MUSS so konfiguriert werden, dass nur mit freigegebenen Geräten auf Informationen der Institution zugegriffen werden kann. Es DÜRFEN nur von der Institution zugelassene mobile Endgeräte beschafft werden.

SYS.3.2.2.A3 Auswahl eines MDM-Produkts (B)

Wenn eine geeignete MDM-Software beschafft werden soll, MUSS sichergestellt sein, dass sich mit ihr alle in der MDM-Strategie festgelegten Anforderungen erfüllen lassen. Auch MUSS sie sämtliche technischen und organisatorischen Sicherheitsmaßnahmen umsetzen können und alle zugelassenen mobilen Endgeräte unterstützen.

SYS.3.2.2.A4 Verteilung der Grundkonfiguration auf mobile Endgeräte (B)

Alle mobilen Endgeräte MÜSSEN, bevor sie eingesetzt werden, in das MDM integriert werden. Wenn die Geräte die Grundkonfiguration erhalten, MÜSSEN sie sich im Werkszustand befinden. Die Verbindung der mobilen Endgeräte zum MDM MUSS angemessen abgesichert werden. Bei bereits benutzten Geräten MÜSSEN vorher alle institutionsbezogenen Daten gelöscht werden. Ein nicht über MDM konfiguriertes Endgerät DARF NICHT auf Informationen der Institution zugreifen können.

SYS.3.2.2.A5 Installation des MDM-Clients (B)

Wenn mobile Endgeräte an Mitarbeitende übergeben werden, MUSS, wenn vom Betriebssystem nicht bereits bereitgestellt, darauf der MDM-Client installiert und konfiguriert sein.

SYS.3.2.2.A20 Regelmäßige Überprüfung des MDM (B)

Sicherheitseinstellungen MÜSSEN regelmäßig überprüft werden. Bei neuen Betriebssystemversionen der mobilen Endgeräte MUSS vorab geprüft werden, ob das MDM diese vollständig unterstützt und die Konfigurationsprofile und Sicherheitseinstellungen weiterhin wirksam und ausreichend sind. Abweichungen MÜSSEN korrigiert werden. Die zugeteilten Berechtigungen für Benutzende und Administrierende MÜSSEN regelmäßig daraufhin überprüft werden, ob sie weiterhin angemessen sind (Minimalprinzip).

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.3.2.2.A6 Protokollierung des Gerätestatus (S)

Der Lebenszyklus einschließlich der Konfigurationshistorie eines mobilen Endgerätes SOLLTE ausreichend protokolliert und zentral abrufbar sein. Bei Bedarf SOLLTE der aktuelle Status der verwalteten Endgeräte durch den IT-Betrieb ermittelt werden können (Device Audit).

SYS.3.2.2.A7 Installation von Apps (S)

Apps SOLLTEN gemäß den Anforderungen des geplanten Einsatzszenarios über das MDM installiert, deinstalliert und aktualisiert werden. Das MDM SOLLTE die Installation, Deinstallation und Aktualisierung erzwingen, sobald eine Verbindung zum mobilen Endgerät besteht. Über das MDM installierte Apps SOLLTEN NICHT durch Benutzende deinstalliert werden können. Das MDM SOLLTE eine Block- oder Allow-List für die Installation von Apps ermöglichen.

SYS.3.2.2.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.2.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.2.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.2.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.2.A12 Absicherung der MDM-Betriebsumgebung (S)

Das MDM selbst SOLLTE durch technische Maßnahmen abgesichert werden, um dem Schutzbedarf der hinterlegten oder verarbeiteten Informationen zu genügen. Das zugrundeliegende Betriebssystem SOLLTE gehärtet werden.

SYS.3.2.2.A21 Verwaltung von Zertifikaten (S)

Zertifikate zur Nutzung von Diensten auf dem mobilen Endgerät SOLLTEN zentral über das MDM installiert, deinstalliert und aktualisiert werden. Die Installation von nicht vertrauenswürdigen und nicht verifizierbaren (Root-) Zertifikaten durch Benutzende SOLLTE durch das MDM verhindert werden. Das MDM SOLLTE Mechanismen unterstützen, um die Gültigkeit von Zertifikaten zu überprüfen.

SYS.3.2.2.A22 Fernlöschung und Außerbetriebnahme von Endgeräten (S)

Das MDM SOLLTE sicherstellen, dass sämtliche dienstliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können (Remote Wipe bei bestehender Datenverbindung). Werden in dem mobilen Endgerät externe Speicher genutzt, SOLLTE geprüft werden, ob diese bei einem Remote Wipe ebenfalls gelöscht werden sollen. Diese Funktion SOLLTE vom MDM unterstützt werden.

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

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.3.2.2.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.2.A14 Benutzung externer Reputation-Services für Apps (H)

Wenn die Administrierenden einer Institution die erlaubten Apps nicht selbst auswählen können und die Benutzenden selbstständig Apps auf ihren Geräten installieren dürfen, SOLLTE ein sogenannter Reputation-Service eingesetzt werden. Das MDM SOLLTE dann mithilfe dieser Informationen aus dem Reputation-Service die Installation von Apps zumindest einschränken.

SYS.3.2.2.A15 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.2.A16 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.2.A17 Kontrolle der Nutzung von mobilen Endgeräten (H)

Es SOLLTEN angemessene Kriterien definiert werden, aufgrund derer die Geräte zu überwachen sind, ohne gegen gesetzliche oder interne Regelungen zu verstoßen. Insbesondere SOLLTEN sogenannte Jailbreaks oder sogenanntes Routen erkannt werden.

SYS.3.2.2.A18 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.3.2.2.A19 Einsatz von Geofencing (H)

Durch die Hinterlegung einer Geofencing-Richtlinie SOLLTE sichergestellt werden, dass Geräte mit schutzbedürftigen Informationen nicht außerhalb eines zuvor festgelegten geografischen Bereichs verwendet werden können. Wird der geografische Bereich verlassen, SOLLTEN entsprechend klassifizierte Informationen oder das Gerät vollständig gelöscht werden. Bevor das Gerät selektiv oder vollständig gelöscht wird, SOLLTEN die zuständigen Administrierenden und das Sicherheitsmanagement sowie die Benutzenden informiert werden. Erst mit einer angemessenen zeitlichen Verzögerung SOLLTE das Gerät selektiv oder vollständig gelöscht werden. Die Bereiche, an denen diese zusätzlichen Sicherheitsmaßnahmen nötig sind, SOLLTEN identifiziert werden. Anschließend SOLLTEN die Sicherheitsmaßnahmen unter Beachtung gesetzlicher und interner Regelungen umgesetzt werden.

SYS.3.2.2.A23 Durchsetzung von Compliance-Anforderungen (H)

Verstöße gegen die Regelungen der Institution oder sogar eine Manipulation des Betriebssystems SOLLTEN mit einer geeigneten Lösung erkannt werden. Die folgenden Aktionen SOLLTEN bei Verdacht auf Verstoß gegen Regelungen oder Manipulation des Betriebssystems ausgeführt werden. Hierzu SOLLTEN entsprechende Funktionen bereitgestellt werden:

1. selbstständiges Versenden von Warnhinweisen,
2. selbstständiges Sperren des Geräts,
3. Löschen der vertraulichen Informationen der Institution,
4. Löschen des kompletten Geräts,
5. Verhindern des Zugangs zu Unternehmens-Apps sowie
6. Verhindern des Zugangs zu den Systemen und Informationen der Institution.

Bei Verdacht auf einen Verstoß oder eine Manipulation SOLLTE ein Alarm an die zuständigen Administrierenden und das Sicherheitsmanagement in der Institution gesandt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI hat in den „BSI-Veröffentlichungen zur Cyber-Sicherheit“ das Dokument BSI-CS 052: „Mobile Device Management“ veröffentlicht.

Das BSI hat einen Mindeststandard zum Thema MDM veröffentlicht: „Mindeststandard des BSI für Mobile Device Management nach § 8 Absatz 1 Satz 1 BSIG - Version 1.0 vom 11.05.2017“. Die Mindeststandards sind von den in § 8 Abs. 1 Satz 1 BSIG genannten Stellen der Bundesverwaltung umzusetzen.

Das National Institute of Standards and Technology (NIST) stellt das Dokument „Guidelines for Managing the Security of Mobile Devices in the Enterprise: NIST Special Publication 800-124“, Revision 1, Juni 2013 zur Verfügung.