Abgrenzung und Modellierung

Erst einmal b**ei der Implementierung von MDM** müssen die Anforderungen des **Bausteines**

SYS 3.2.1 Allgemeine **Smartphones** und **Tablets** berücksichtigt werden.

Wie Smartphone, Tablets oder auch Phablets spezifisch gesichert werden wird **in** den **jeweiligen Bausteinen beschrieben**.

SYS 3.2.3 iOS

SYS 3.2.4 Android

Bei der Implementierung des **MDM** muss ein **Berechtigungskonzept** erstellt werden, **welches** im Baustein

ORP.4 Identitäts- und Berechtigungsmanagement genauer **beschrieben** wird.

Beim **Identitätsmanagement** geht es dort **um** die **Verwaltung der notwendigen Informationen** um einen IT-Komponenten **zweifelsfrei identifizieren und authentisieren** zu können.

Beim **Berechtigungsmanagement** geht es darum, den **Nutzern basierend auf** ihren **Rechten Zugang zu** gewissen **Ressourcen** zu ermöglichen oder zu verbieten.

Keine ausreichende Synchronisation mit dem MDM

Damit die definierten Regelungen auf den mobilen Endgeräten in Kraft treten, müssen sie regelmäßig synchronisiert werden.

Wenn ein Gerät über eine **längere Zeit nicht synchronisiert** wird, können **aktualisierte oder neue Regelungen nicht aufgespielt** werden

Wenn **bei Verlust** des Geräts **keine Verbindung** besteht, können die **Daten nicht aus der Ferne gelöscht** werden.

Fehlerhafte Administration des MDM

Innerhalb MDM-Lösungen können Regelungen voneinander abhängen oder nicht kompatibel mit anderen sein. Durch Fehler in der Administration können somit die **Vertraulichkeit, Verfügbarkeit** und **Integrität** der Daten **in Gefahr** sein.

Ungeeignetes Rechtemanagement im MDM

Wenn Benutzerkonten eine falsche Rolle zugewiesen wird, könnte es dazu führen, dass sie in **Daten einsehen können, für die sie befugt sind**. Es kann auch passieren, dass sie sich **mit den erlangten Rechten einen Cloud-Service auf ihr Gerät installieren**.

Dadurch können **schützenswerte Daten** aus der Institution **abfließen** oder es wird gegen die **Datenschutzbestimmungen verstoßen**.

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**.

Das Speichern dieser Daten **ohne Informierung an den Benutzenden verstößt gegen die DSGVO**

Im Falle eines Angriffs können diese **Daten an die Angreifer fallen**.

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

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 schriftlich fixiert und von dem oder der ISB** freigegeben werden

SYS.3.2.2.A2 Festlegung erlaubter mobiler Endgeräte

Es MUSS festgelegt werden, **welche mobilen Endgeräte und Betriebssysteme** in der Institution zugelassen sind.

Das **MDM MUSS so konfiguriert werden, dass nur mit freigegebenen Geräten auf Informationen** der Institution **zugegriffen** werden kann.

SYS.3.2.2.A3 Auswahl eines MDM-Produkts

Eine **MDM-Software** muss alle in der **MDM-Strategie festgelegten Anforderungen erfüllen**, **sämtliche technische und organisatorische Sicherheitsmaßnahmen umsetzen können** und alle zugelassenen mobilen Endgeräte unterstützen.

SYS.3.2.2.A4 Verteilung der Grundkonfiguration auf mobile Endgeräte

Alle mobilen Endgeräte MÜSSEN, **bevor sie eingesetzt** werden, **in das MDM integriert** werden **sich dabei im Werkszustand befinden**.

Bei **bereits genutzten Geräten** müssen **vorher alle Institutionsbezogenen Daten gelöscht** werden.

Ein **nicht konfiguriertes Gerät darf nicht auf Informationen der Institution zugreifen** können

SYS.3.2.2.A5 Installation des MDM-Clients

Wenn mobile **Geräte** an die Mitarbeiter übergeben werden, **müssen sie über den MDM-Client verfügen**

SYS.3.2.2.A20 Regelmäßige Überprüfung des MDM

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**.

Die zugeteilten **Berechtigungen für Benutzende und Administrierende** MÜSSEN regelmäßig daraufhin **überprüft werden, ob sie weiterhin angemessen** sind

SYS.3.2.2.A6 Protokollierung des Gerätestatus

Der **Lebenszyklus einschließlich der Konfigurationshistorie** eines mobilen Endgerätes SOLLTE **ausreichend protokolliert und zentral abrufbar sein**. **Bei Bedarf** sollte der **Aktuelle Status jederzeit ermittelt** werden können. (**Device Audit**)

SYS.3.2.2.A7 Installation von Apps

Apps sollten über das **MDM installiert, aktualisiert und gelöscht** werden.

Vom MDM installierte Apps sollten vom **Nutzer nicht gelöscht werden können**

Das **MDM sollte über eine Block-/Allow-Liste** für die Installation **von Apps verfügen**

SYS.3.2.2.A12 Absicherung der MDM-Betriebsumgebung

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.A22 Fernlöschung und Außerbetriebnahme von Endgeräten

Das MDM SOLLTE sicherstellen, dass sämtliche dienstliche Daten auf dem mobilen Endgerät aus der Ferne gelöscht werden können. Dies betrifft **auch externe Speicher** auf den Geräten. Diese Funktion SOLLTE vom MDM unterstützt werden.

Der **Prozess zur Außerbetriebnahme** des mobilen Endgerätes **SOLLTE sicherstellen**, dass **keine schutzbedürftigen Daten auf dem mobilen Endgerät** oder eingebundenen Speichermedien **verbleiben**.

SYS.3.2.2.A14 Benutzung externer Reputation-Services für Apps

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**, mit dessen Informationen **das MDM die Installation von manchen Apps einschränken kann**.

SYS.3.2.2.A17 Kontrolle der Nutzung von mobilen Endgeräten

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**

Jailbreaking oder Rooting bedeutet, dass man Einschränkungen entfernt oder umgeht, die absichtlich gesetzt wurden

SYS.3.2.2.A19 Einsatz von Geofencing

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**.

SYS.3.2.2.A23 Durchsetzung von Compliance-Anforderungen

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

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