M/4.3.6 Technisch-organisatorische Maßnahmen

Die hier vorgestellten technisch-organisatorischen Maßnahmen stellen nur eine Auswahl an Möglichkeiten dar, die bei der Integration mobiler Endgeräte ergriffen werden können. Der Restriktionsgrad der notwendigen technisch-organisatorischen Maßnahmen sollte sich direkt aus der Schutzbedarfsfeststellung ergeben. Sofern ein hoher beziehungsweise sehr hoher Schutzbedarf ermittelt worden ist, sind in der Regel effektivere Schutzmaßnahmen erforderlich.

Die Maßnahmen sind allgemein für Smartphones und Tablets beschrieben; konkrete Umsetzungsvorschläge sind in M/4.3.8 für Android und iOS dargestellt. Grundsätzlich kann es sich hierbei aber nur um Vorschläge handeln, die in jedem Fall differenziert für jede Gesundheitseinrichtung betrachtet werden müssen.

Verschlüsselung und Bildschirmsperre

Der Speicher des Smartphones/Tablets ist vor unbefugtem Zugriff zu schützen. Dies kann durch Verschlüsselung oder äquivalente Verfahren realisiert werden. Schützenswerte Informationen dürfen insbesondere nicht unverschlüsselt auf Speicherkarten abgelegt werden.

Sinnvollerweise wird hierfür die von iOS und Android zur Verfügung gestellte Verschlüsselung (AES-256) des gesamten Speicherbereichs genutzt. Da das Smartphone jedoch in der Regel eingeschaltet ist, muss auch in diesem Zustand der Zugriff auf die Gerätedaten gesichert werden. Der Zugriff auf das Smartphone sollte daher über eine von der SIM-Karte unabhängige PIN-Sperre gesteuert werden. Nach mehrfacher Fehleingabe sollten eine Rücksetzung des Gerätes in den Werkszustand und die Löschung aller Informationen erfolgen. Die Kennwortrichtlinie für die PIN sollte sich hierbei, abhängig vom Schutzbedarf, an den sonstigen Vorgaben im Unternehmen orientieren. Trivialkennwörter (bspw. 1111 oder abcd) und PINs, die nur aus Zahlen bestehen, sind ebenso wie Wischgesten zu vermeiden, da diese in der Öffentlichkeit aus mehreren Metern Entfernung mitgelesen werden können. Ausgehend von dem hohen Schutzbedarf sollte die PIN eine Mindestlänge von sechs Zeichen haben und alle 90 Tage gewechselt werden.

Ortung und Fernlöschung

Die Fernlösch- und -sperrfunktion, d. h. das Löschen aller Daten und die Deaktivierung des Gerätes, sollte aktiviert werden, um bei Diebstahl oder Verlust die Primär- und Sekundärwerte aktiv löschen zu können. Typischerweise können die gängigen MDM-Lösungen neben der Fernlöschung bzw. -sperrung das Smartphone auch orten. Es sollte im Rahmen der Richtlinie bzw. Betriebsvereinbarung genau definiert werden, unter welchen Umständen eine Ortung erfolgt (vgl. M/4.3.6 Richtlinien/Betriebsvereinbarungen). In der Regel bieten MDM-Lösungen hierfür eigene Benutzerrollen an bzw. die Ortung kann in der MDM-Lösung in speziellen Fällen über eine Rolle „Super-Administrator“ aktiviert werden.

Absicherung der Kommunikation

Um die Übertragung von Unternehmensdaten im Hinblick auf Integrität und Vertraulichkeit zu schützen, sollte die Kommunikation zwischen dem Unternehmensnetz und dem Smartphone ausschließlich verschlüsselt erfolgen.

Aufgrund des hohen Schutzbedarfs ist der Einsatz eines VPN (Virtual Private Network) empfehlenswert, wobei sich die Endgeräte über Gerätezertifikate authentisieren. iOS unterstützt seit Version 7 die Funktion „per app vpn". Dadurch wird ein vom Endgerät unabhängiges VPN für jede einzelne App und somit eine stärkere Trennung zwischen beruflich und privat genutzten Apps ermöglicht.

Reglementierung der App-Zugriffsberechtigungen

Sofern die eingesetzten Smartphones auch für private Zwecke genutzt werden können, muss die Installation von Apps reglementiert werden. Generell gilt, dass keine unautorisierte App auf Unternehmensdaten zugreifen darf. Sowohl iOS als auch Android sehen grundsätzlich keine wirksame Trennung zwischen privaten und geschäftlichen Daten vor, obwohl bestimmte Speicherbereiche (Fotos, E-Mails, Kontakte, Kalender, Speicherkarte) beide Arten von Daten enthalten können.

Abhängig von der konkreten Implementierung sind unterschiedliche Ansätze möglich:

- **Reglementierung von Apps:** Sowohl iOS als auch Android bieten die Möglichkeit, Apps den Zugriff auf bestimmte Datenquellen zu verweigern.
- **Blacklist:** Sofern eine differenzierte Zugriffsberechtigung nicht möglich ist, bieten gängige MDM-Lösungen die Möglichkeit, bestimmte Apps über eine Blacklist zu sperren. Beispielsweise könnten hierbei bekannte Apps, die das komplette Adressbuch auslesen und an die Server des Betreibers übersenden, gesperrt werden.
- **Whitelist/Enterprise-Market:** Sofern die Pflege einer Blacklist zu aufwendig ist bzw. der Schutzbedarf zu hoch ist, können über das MDM vorher definierte Apps freigegeben werden und lediglich diese dürfen und können installiert werden. Eine Steigerung hiervon ist der unternehmenseigene App-Store oder auch „Enterprise-Market", wobei hier auch Lizenzen verteilt werden.
- **Container-Apps:** Hierbei werden alle Unternehmensdaten in einer App gekapselt. Die App übernimmt sowohl die sichere Kommunikation zum Server als auch die lokale Verschlüsselung aller sensiblen Informationen.

- **Terminalserver:** Hierbei werden die eigentlichen Informationen nicht auf das Endgerät übermittelt, sondern verbleiben auf dem Server. Die Informationen werden lediglich angezeigt.

Aufgrund des hohen Schutzbedarfs sollte die Inter-App-Kommunikation generell unterbunden werden. Hierdurch wird beispielsweise verhindert, dass vertrauliche E-Mail-Anhänge bewusst oder versehentlich in Cloudspeicher übertragen werden, was einen Verlust der Vertraulichkeit bedeuten würde.

Eine Installation von Apps, die nicht aus dem offiziellen Apple App Store bzw. Google Play Store stammen, sollte in jedem Fall unterbunden werden.

Richtlinien/Betriebsvereinbarungen

Nicht alle Maßnahmen zur Vermeidung von sicherheitsrelevanten Vorfällen lassen sich technisch umsetzen, sodass mit dem Anwender folgende Nutzungsvereinbarung über einzuhaltende Mindeststandards getroffen werden muss:

- Die Sorgfalt im Umgang mit dem Smartphone ist unumgänglich, auch um Diebstahl entgegenzuwirken.
- Eine Umgehung von Sicherheitsmaßnahmen – dazu zählen insbesondere das sog. „Rooten“ oder „Jailbreaken“ – sollte untersagt werden.
- Passwörter für Zertifikate dürfen nicht im Passwortmanager abgelegt werden.
- Datensparsamkeit: Unternehmensdaten dürfen nur solange auf dem Gerät vorgehalten werden, wie es ihre Bearbeitung verlangt, und nur in den dafür vorgesehenen Bereichen und Containern verarbeitet werden.
- Das Smartphone darf nicht an Dritte (einschließlich Familie) weitergegeben werden.
- Der Verlust ist umgehend anzuzeigen.
- Der Verdacht auf Befall mit Schadprogrammen ist umgehend zu melden.
- Sofern eine Fernlöschung vorgesehen ist, muss der Benutzer vorher einwilligen. Dies gilt insbesondere, wenn die Löschung nicht auf die Unternehmensdaten beschränkt ist, sondern auch die privaten Daten des Mitarbeiters betreffen könnte.

- Sofern eine Ortung vorgesehen ist, sollte im Vorfeld sehr detailliert geregelt werden, unter welchen Voraussetzungen diese erfolgt. Insbesondere ist der Betriebsrat frühzeitig einzubinden, da mittels Ortung eine sehr differenzierte Mitarbeiterüberwachung möglich ist.
- Updates müssen – sofern dies technisch nicht umgesetzt ist – durch den Nutzer zeitnah installiert werden.

M/4.3.7 Exkurs: Mobile Device Management

Sofern möglich sollten alle Maßnahmen technisch erzwungen werden. Für die Verwaltung und das Ausrollen (Provisioning) ist ein Mobile Device Management (MDM) nicht zwingend erforderlich, aber äußerst hilfreich.

Um den unterschiedlichen Anforderungen gerecht zu werden, sollte der Einsatz unterschiedlicher MDM-Benutzerprofile erwogen werden. So können die Restriktionen für Benutzer mit geringeren Sicherheitsanforderungen gesenkt werden bzw. über stärkere Restriktionen können spezifische Defizite von Betriebssystemen kompensiert werden.

Allgemeine Vorgaben zur Konfiguration eines MDM

Prinzipiell arbeiten alle MDM-Lösungen nach dem gleichen Prinzip. Die Betriebssystemhersteller bieten Schnittstellen (Englisch: application programming interface oder auch API), die Dritthersteller ansprechen können. In der Regel werden die vorher definierten Konfigurationen in Profilen hinterlegt, die über den MDM-Server auf die Smartphones ausgerollt werden. Für bestimmte Funktionalitäten ist zusätzlich die Installation einer App des MDM-Herstellers notwendig. Aufgrund der Vielzahl an MDM-Lösungen am Markt können sich sowohl der Funktionsumfang als auch die Bezeichnung unterscheiden. Im Folgenden werden die gängigsten Bezeichnungen verwendet.

Typischerweise kann ein Smartphone im MDM seinem Status entsprechend in vier unterschiedliche Kategorien eingeteilt werden:

- **unmanaged:** Geräte, die nicht im MDM registriert und konfiguriert sind
- **managed:** im MDM registrierte Geräte mit entsprechend definierten Regeln
- **compliant:** bereits registrierte Geräte, die alle Vorgaben erfüllen