Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Mobile Device Management

Der Wandel des Arbeitsumfelds vom stationären zum mobilen Arbeitsplatz hat zur Folge, dass auch die Arbeitsgeräte mobil sein müssen. Der Zugriff auf Unternehmensdaten ist praktisch von jedem Ort aus notwendig und mittlerweile auch möglich. „Mobile Daten" sind kein neues Phänomen, sondern schon seit Langem im täglichen Einsatz. Mit dem Laptop wurden Unternehmensdaten erstmals flächendeckend mobil. Die Geräte wurden zunächst offline betrieben, das heißt, die Daten wurden im Unternehmen aufgespielt und konnten unterwegs verwendet werden. Erst mit Anschluss an das Intranet des Unternehmens wurden aus diesen mobilen Daten synchronisierte mobile Daten. Hier hat sich ein enormer Wandel vollzogen: Jederzeit und an jedem Ort liegen jetzt aktuelle Dokumente und Zahlen vor, E-Mails erreichen den Benutzer zeitnah und Termine werden online mit Kollegen und Geschäftspartnern organisiert. Mobile Endgeräte sind aus der heutigen Arbeitswelt nicht mehr wegzudenken.

Smartphones und Tablet-Computer mit den Betriebssystemen *iOS* von Apple, *Android* von Google oder *Windows Phone* von Microsoft sind mit modernen, einfachen Bedienkonzepten eher für den Consumer-Markt gedacht und weniger für den geschäftlichen Einsatz. Damit unterscheiden sie sich grundlegend von anderen Konzepten mobiler Endgeräte, wie beispielsweise *Blackberry*, das speziell für den Unternehmenseinsatz konzipiert wurde. Trotzdem sind Geräte mit iOS und Android in der Geschäftswelt angekommen und verdrängen zunehmend etablierte Lösungen. Sie müssen in die Geschäftsprozesse integriert, beziehungsweise die Geschäftsprozesse müssen an sie angepasst werden. IT-Abteilungen stehen vor der Herausforderung, den Zugang der Geräte zur IT-Infrastruktur zu ermöglichen, diese Geräte zentral zu verwalten und gleichzeitig das Sicherheitsniveau des Unternehmens aufrechtzuerhalten. Als Möglichkeit zur Lösung dieser Aufgabe werden Mobile Device Management-Lösungen (im Folgenden *MDM-Lösungen*) angeboten.

Dieses Dokument soll Hinweise und Empfehlungen für die Auswahl und den Einsatz von MDM-Lösungen geben. Es ist in vielen Bereichen plattformübergreifend geschrieben, die genannten Beispiele zielen allerdings speziell auf die verbreiteten mobilen Betriebssysteme Android und iOS ab.

Die Empfehlungen sollen aber nicht die hinlänglich bekannten Konfigurationsempfehlungen für MDM-Lösungen wiederholen, zumal die Menüs der Verwaltungskonsolen in der Regel die Möglichkeiten der Plattform-Konfigurationen ausschöpfen und soweit selbsterklärend sind. Vielmehr sollen die zentralen Gesichtspunkte betrachtet werden, auf die bei der Auswahl und dem Betrieb einer MDM-Lösung geachtet werden sollte. Gleichwohl werden zur Veranschaulichung am Ende dieses Dokuments einige exemplarische Empfehlungen für die Konfiguration von iOS- und Android-basierten Smartphones und Tablets gegeben.

Die Empfehlungen sind bewusst kurz gehalten und erheben keinen Anspruch auf Vollständigkeit. Sie sollen in regelmäßigen Abständen aktualisiert und erweitert werden. Anregungen sind daher sehr willkommen.

Wandel hin zur Unsicherheit

Die Hardware und Systemsoftware der klassischen Mobilgeräte Laptop und Notebook sind sehr ähnlich bis identisch zu stationären Computern. Auch sie arbeiten hauptsächlich mit Windows, Mac OS X oder Linux als Betriebssystem. Damit gibt es praktisch keinen großen Unterschied bei der Verwendung dieser mobilen Geräte. Sind sie einmal über einen sicheren Kanal mit dem Intranet des Unternehmens verbunden, kann man wie gewohnt damit arbeiten. E-Mail, Kontakte, Kalender und Zugang zu Netzdiensten sind vorhanden, zentrale Administration, Patch- und Backup-Management werden transparent durchgeführt. Wichtig ist auch die Tatsache, dass die Absicherung der Geräte durch Sicherheitssoftware wie beim Desktop-Computer funktioniert und dass Sicherheitsrichtlinien wie gewohnt durchgesetzt werden können.

Anders sieht es bei der Klasse der Handheld-Computer – Smartphone und Tablet – aus. Diese sind bezüglich Ausstattung und Leistungsvermögen durchaus in der Lage, Geschäftsprozesse zu verarbeiten; Hardware, Systemsoftware und Bedienungskonzept unterscheiden sich aber meist grundlegend von den „klassischen" mobilen Endgeräten Laptop und Notebook.

Problematisch ist dabei die Vielfalt der Plattformen von Smartphones und Tablet-Computer mit ihren systembedingten Eigenschaften, die jeweils einzeln berücksichtigt werden müssen. Hinzu kommen noch Unterschiede innerhalb der Betriebssysteme. Das Betriebssystem Android – als mittlerweile führendes mobiles Betriebssystem (Stand 2012) – wird von den Smartphone-Herstellern speziell an die von ihnen entwickelten Geräte angepasst. Dabei werden auch grundlegende Funktionalitäten verändert wie beispielsweise die Bedienoberfläche. Das Patch-Management liegt vollständig in den Händen dieser OEM-Hersteller. Verzögerungen bei der Auslieferung von neuen Betriebssystem-Versionen sind unabdingbar, wenn man bedenkt, dass eine neue Version von Android zunächst von Google herausgegeben wird, dann vom Hardware-Hersteller an die einzelnen Geräte angepasst werden muss und schließlich vom Provider nochmals verändert wird (etwa zur Anpassung an den Zugangspunkt, über den Datenvolumen abgerechnet werden). Hinzu kommen noch Zeiten für Zertifizierung und Abnahme. Verzögerungen von bis zu einem halben Jahr sind keine Seltenheit. Oft kommen neue Geräte schneller auf den Markt, als vorhandene aktualisiert werden.

„Bring Your Own Device" (BYOD), also die (zusätzlich) dienstliche Verwendung privater Smartphones, stellt IT-Abteilungen vor immer neue Herausforderungen. Nicht die IT-Abteilung wählt die Geräte aus, sondern der Benutzer. Dies geht sogar soweit, dass Nutzer plattformbedingte Einschränkungen in Kauf nehmen, nur um mit bestimmten Geräten arbeiten zu können.

Auch der Einsatzort birgt ein erhöhtes Risiko. Zwar werden auch Laptops in unsicheren Umgebungen eingesetzt, bei Smartphones ist dies aber wesentlich leichter. Sie müssen nicht gebootet werden, sondern sind nach dem Einschalten sofort betriebsbereit. Die geometrischen Abmessungen erlauben den Gebrauch an fast jedem Ort. Vielfach stehen dem Benutzer freie, kostenlose Zugänge in nicht kontrollierbare WLANs zur Verfügung. Kommen die Geräte einmal abhanden, das heißt gehen sie verloren oder werden gestohlen, besteht für den Administrator nur die Möglichkeit, das Gerät aus der Ferne zu sperren und/oder zu löschen (wenn das Gerät noch erreichbar ist). Diebe, die an den gespeicherten Daten interessiert sind, werden daher diesen letzten Fernzugriff verhindern.

Für die Fernverwaltung muss die weitgehend gekapselte Infrastruktur des Unternehmens weiter aufgeweicht werden. Das heißt, teilweise ist es notwendig, Verwaltungs- und Kommunikationsserver in die DMZ zu stellen, damit eine Verbindung zwischen dem Intranet und den mobilen Endgeräten möglich wird.

Mobile Device Management in Unternehmen

Die Absicherung der Kommunikation, die Verarbeitung der Daten auf dem Gerät, die sichere Speicherung der Daten auf dem Gerät, die Trennung von dienstlicher und privater Nutzung sowie der Schutz der Geräte vor Schadsoftware sind Anforderungen, die von IT-Abteilungen im Desktop-/Laptop-Bereich sicher beherrscht werden. In Bezug auf mobile Endgeräte fehlt aber vielfach die Umsetzung von Lösungsmöglichkeiten, bzw. müssen Lösungsmöglichkeiten von Betriebssystem-Hersteller und Drittanbietern erst noch geschaffen werden. Diesen Anforderungen kann durch den Einsatz von Mobile Device Management – primär

im Hinblick auf zentrale Fernverwaltung – begegnet werden. Einige Lösungen bieten über die Verwaltung hinaus zusätzliche Funktionalitäten für die Absicherung geschäftlicher Daten auf dem mobilen Endgerät an.

MDM-Lösungen bauen im Wesentlichen auf den vier Säulen *Hardwareunterstützung*, *Softwareunterstützung*, *Kommunikation und deren Absicherung* sowie *Datensicherheit auf den mobilen Endgeräten* auf.

Die Hardwareunterstützung beinhaltet neben der generellen Unterstützung verschiedener Plattformen auch die Integration einer MDM-Lösung in die jeweilige Plattform, sodass der Betrieb des mobilen Endgerätes durch die Lösung nicht nachteilig beeinflusst wird, beispielsweise bezüglich der Batterielaufzeit. Zur Softwareunterstützung gehören unter anderem die Einbindung von neuen mobilen Endgeräten in die Verwaltung, die Verteilung von Konfigurationsprofilen, wie auch die Unterstützung der IT-Infrastruktur eines Unternehmens. Der Schutz der Daten auf den Kommunikationswegen durch die Verwendung von Verschlüsselung auf definierten Zugangspunkten spielt eine zentrale Rolle. Gleiches gilt auf den mobilen Endgeräten in Bezug auf sichere Konfiguration, Verschlüsselung, Benutzereinschränkungen usw. aber auch für die sichere Entfernung aus der Verwaltung.

Vorbereitungen zur Auswahl einer MDM-Lösung

Bevor die Entscheidung für eine bestimmte MDM-Lösung getroffen wird, muss grundsätzlich festgelegt werden, was diese Lösung leisten soll. Welche Plattformen sollen unterstützt werden? Welche Unternehmensdaten sollen auf dem mobilen Endgerät verarbeitet werden? Müssen neben den üblichen PIM-Daten (Kalender, Kontakten, Aufgaben und Notizen) und E-Mails auch Unternehmensdokumente verarbeitet werden? Wie werden diese Daten abgesichert bzw. von anderen auf dem mobilen Endgerät bearbeiteten (privaten) Daten separiert? Hat das Unternehmen eigene Apps, die verwaltet werden müssen und wird dazu ein eigener App-Store benötigt? Wird die Verwendung privater Smartphones für dienstliche Belange erlaubt?

Wenn man diese Fragen beantwortet hat und dazu einen entsprechenden Testplan vorbereitet hat, sollte man sich eine Vorauswahl von MDM-Lösungen ansehen. Vertrauen Sie nicht den Marketing-Abteilungen der Anbieter. Auch das Studium der Produktdokumentation allein reicht nicht aus. Teststellungen und eine intensive Beschäftigung mit dem Thema sind notwendig, um die Tauglichkeit der beworbenen Funktionalitäten auch wirklich in der Praxis bewerten zu können. Lassen Sie sich Referenzprojekte zeigen und profitieren Sie von den Erfahrungen dieser Unternehmen.

Bauarten

MDM-Server werden als reine Software-Lizenz oder als Appliance für den Einsatz im Unternehmen angeboten. Sie bestehen entweder aus einem einzelnen Server oder aus mehreren Komponenten und stehen – in Firewalls eingebettet – in der DMZ. Dort bilden sie das Bindeglied zwischen der IT-Infrastruktur des Unternehmens und den mobilen Endgeräten. Zudem enthalten sie die Verwaltungs-Konsole für die Konfiguration, Monitoring, Logging, Backup der mobilen Endgeräte usw. und können auch einen eigenen App-Store enthalten.

Daneben bieten einige Anbieter vollwertige MDM-Lösungen auf eigenen Servern als Clouddienst an. Vorteilhaft ist diese Lösung vor allem bei kleinen Installationen mit wenigen mobilen Endgeräten. Über einen solchen Clouddienst kann man eine MDM-Lösung auch ohne viel Aufwand ausgiebig testen, vorausgesetzt, sie erfüllt alle Anforderungen, die in einer eigenen Installation benötigt werden.

Wer die Installation einer eigenen MDM-Lösung scheut und sich bewusst für einen Clouddienst entscheidet, muss sich darüber im Klaren sein, dass sämtliche mobilen Daten – Geschäftsdaten, wie auch personenbezogene Daten – auf einem Fremdserver gehostet werden. Weitere Informationen dazu siehe Kapitel „Datenschutz“.

"Sicherheit"

Eine der wichtigsten Fragen im Bereich Mobile Device Management ist die nach der Absicherung der Geschäftsdaten auf dem mobilen Endgerät. Sowohl iOS- als auch Android-basierte Geräte wurden ursprünglich für den Consumer-Markt konzipiert, müssen jetzt aber in die geschäftlichen/dienstlichen Prozesse eingebunden werden. iOS wie Android bieten durchaus die Möglichkeiten zur Bearbeitung dienstlicher Belange (PIM-Daten, E-Mail usw.), haben darüber hinaus aber auch Funktionalitäten, die eher für den Privatgebrauch gedacht sind, beispielsweise die Integration von Twitter oder Facebook beziehungsweise YouTube oder Google+ in das Betriebssystem. Es gibt Hunderttausende Apps in den App-Stores, mit denen die Funktionalitäten eines Gerätes in jede denkbare Richtung erweitert werden können.

Sicherheitsbegriffe werden in den Produktbeschreibungen von MDM-Lösungen leider häufig verallgemeinert, was bedeutet, dass beworbene Sicherheitseigenschaften oft nur auf eine Teilmenge der unterstützten Geräte einer Plattform anwendbar sind. So gibt es beispielsweise Lösungen, die spezielle Programmierschnittstellen (APIs) bestimmter Hersteller/OEMs nutzen, um Android-basierte Smartphones zu verwalten und abzusichern. Dass dieser Mechanismus nicht für Geräte anderer Hersteller gilt und zudem nur für bestimmte Geräte eines Herstellers nutzbar ist, wird in der Produktpräsentation nicht genannt. Ebenso muss man sich darüber im Klaren sein, dass die Unterstützung unterschiedlicher Plattformen sowie deren Verwaltung in einer gemeinsamen Konsole nicht bedeutet, dass Konfigurationen und Richtlinien auf allen Plattformen in gleicher Weise umgesetzt werden. So gibt es beispielsweise systembedingte Unterschiede zwischen iOS und Android bei der Bereitstellung von Apps in einem eigenen App-Store (siehe dazu Kapitel „App-Management“).

Grundsätzlich muss man zwischen der Absicherung der Datenflüsse einerseits und der Absicherung der Daten auf dem Smartphone selbst unterscheiden („data in motion“ vs. „data at rest“).

Die Absicherung der Kommunikationswege haben MDM-Lösungen in der Regel sicher im Griff, auch wenn sie dazu auf Fremddienste angewiesen sind (siehe Kapitel „Fremddienste“). Beispiele sind die Verwendung von sicheren Protokollen und Zertifikaten, VPN-Konfigurationen, WLAN-Einstellungen sowie die Anbindung der MDM-Server an die IT-Infrastruktur des Unternehmens.

Für die Absicherung der Daten auf dem Smartphone können in der Regel nur die von der Smartphone-Plattform zur Verfügung gestellten Konfigurationsmöglichkeiten verwendet werden, wie Verschlüsselung, Kennworteinstellungen, Benutzereinschränkungen usw. Die Gefährdung der Unternehmensdaten durch fremde Apps, die beispielsweise auf Kontaktdaten zugreifen, wird von MDM-Lösungen nur dann berücksichtigt, wenn die Plattform entsprechende Schutzmechanismen zur Verfügung stellt. Eine saubere Abtrennung der dienstlichen Verwendung des Smartphones vom Privatgebrauch ist so ohne Weiteres nicht leistbar.

Durch das Sandbox-Prinzip, sowohl von Android als auch iOS, werden Apps und ihre Daten vor dem Zugriff durch andere Apps geschützt. Aufbauend auf dieser Grundsicherung haben einige Anbieter ihre MDM-Lösung um einen „App-Container“ erweitert, innerhalb dessen die geschäftlichen Belange bearbeitet werden (siehe Kapitel „Contentmanagement auf dem Smartphone“).

Datenschutz

Flankierend zu der Absicherung der Datenkommunikation zwischen mobilem Endgerät und MDM-Server sollte sich ein Unternehmen auch über die Auswirkungen des Einsatzes einer solchen Lösung auf den Datenschutz im Klaren sein. Die meisten Anbieter von MDM-Lösungen stammen nicht aus Deutschland oder der Europäischen Union und betreiben ihre Server außerhalb dieser Zone (etwa in den USA). Das heißt, dass diese Firmen nicht deutschem oder europäischem Datenschutzrecht unterliegen, sondern entweder gar keinem oder einem von Europa nicht anerkannten Datenschutzrecht. Aus diesem Grund hat die Europäische Union mit den USA das sogenannte „Safe Harbor“-Abkommen geschlossen, das die Übermittlung personenbezogener Daten an Server in die USA zumindest rechtlich regelt (Safe Harbor).

Außerdem wird an dieser Stelle speziell auf §11 des Bundesdatenschutzgesetzes (BDSG) „Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag“ hingewiesen. Dieser besagt, dass bei der Bearbeitung personenbezogener Daten durch andere Stellen (beispielsweise bei Nutzung einer Cloud-Lösung für MDM), der Auftraggeber nach wie vor für die Einhaltung des BDSG verantwortlich ist (Bundesdatenschutzgesetz).

Contentmanagement auf dem Smartphone

Eine weitere Herausforderung für eine MDM-Lösung besteht darin, die geschäftlichen Prozesse auf dem Gerät so zu separieren, dass sie nicht durch die sonstige (vor allem private) Verwendung beeinflusst oder gefährdet werden.

Die meisten MDM-Lösungen bieten dazu keine eigenen Mechanismen an. Zur Bearbeitung der dienstlichen Belange werden die nativen Apps verwendet. Das heißt, das Smartphone wird so genutzt, wie von der Betriebssystem-Plattform vorgesehen. Es findet also keine komplette Trennung zwischen dienstlicher und sonstiger Nutzung statt.

Daneben gibt es die sogenannte *Containerlösung*. Es handelt sich dabei um eine normale Smartphone-App, in der die dienstlichen Belange bearbeitet werden. Sie enthält sämtliche PIM-Daten, E-Mails und Dokumente sowie auch die für die Bearbeitung dieser Daten notwendigen Programmfunktionen, das heißt E-Mail-Client, Kalender, Kontaktverwaltung usw. Weiterhin muss auch ein Browser vorhanden sein, da nur über ihn auf Unternehmens-Server zugegriffen werden darf. Außerhalb dieser App kann das Gerät normal verwendet werden. Diese Art der dienstlichen Verwendung führt beim Benutzer häufig zu Akzeptanz-Problemen, kann man das Smartphone im dienstlichen Bereich doch nicht nach den Möglichkeiten nutzen, die im Privatbereich zur Verfügung stehen. Dennoch bietet diese Lösung eine grundsätzliche Trennung der dienstlichen und privaten Nutzung.

Ein weiterer Lösungsansatz zur Bearbeitung dienstlicher Belange auf dem mobilen Endgerät ist eine Terminalserver-Sitzung, bei der die Verarbeitung und Speicherung der Daten auf dem Terminalserver verbleibt. Das Mobilgerät wird nur für die Darstellung und Eingabe verwendet, das heißt, von/zum Mobilgerät werden nur Texteingaben, Bildschirminhalte und Eingabe-Gesten übertragen. Entsprechende Lösungen gibt es sowohl für das iPad als auch für Android-Smartphones/Tablets. Nachteilig können sich Engpässe bei der Datenübertragung auswirken, insbesondere dann, wenn die Datenverbindung des Smartphones über ein Mobilfunknetz hergestellt wird. Außerdem wird auf dem Smartphone/Tablet-Display oft ein Windows-Desktop dargestellt, der nicht für die Darstellung und Bedienung auf einem Touchscreen-Smartphone/Tablet optimiert ist. Hier gilt: Lassen Sie sich vor der Einführung einer solchen Lösung Referenzprojekte zeigen und testen Sie ausgiebig.

Bei Android gibt es außerdem verschiedene neue Ansätze, durch Virtualisierung zwei Betriebssysteme gleichzeitig auf einem Smartphone zu betreiben. Ein Lösungsansatz enthält zwei vollständige Android-Versionen, die gleichzeitig gestartet werden und zwischen denen man während des Betriebs wechseln kann. Ein anderer Lösungsansatz betreibt ein zweites Betriebssystem als App innerhalb des nativen Betriebssystems. Erfahrungswerte aus einem breiten praktischen Einsatz liegen jedoch noch nicht vor.

Doch die Entwicklung der mobilen Plattformen schreitet voran. So steht in Version 4.2 von Android eine Mehr-Benutzer-Verwaltung für Tablets zur Verfügung, die eine bessere Trennung verschiedener Benutzer oder Einsatzszenarien ermöglicht. Eine Neuerung in Version 6 von iOS ist beispielsweise die Möglichkeit zur Einrichtung eines globalen HTTP-Proxies, sodass die IT-Abteilung den Internetverkehr über einen kontrollierten Kanal leiten könnte.

Fremddienste

Die Datenverbindung zwischen dem mobilen Endgerät und dem MDM-Server wird entweder über einen Mobilfunk-Provider (via GPRS, EDGE, UMTS, HSDPA, LTE) oder über eine WLAN-Verbindung hergestellt. Die zugewiesene IP-Adresse ist nicht vorhersehbar beziehungsweise nicht erreichbar, sodass das Gerät nicht

von einem MDM-Server kontaktiert werden kann. Der Verbindungsaufbau zum Server muss demnach vom Smartphone aus erfolgen.

Mit dem sogenannten *Apple Push Notification Service* (APNS) beziehungsweise dem *Google Cloud Messaging* (GCM) bieten die Hersteller Dienste an, über die iOS- beziehungsweise Android-Geräte trotzdem kontaktiert werden können. Diese Dienste sind in das Betriebssystem integriert und können nicht abgeschaltet werden. Will ein MDM-Server eine Kommunikation mit einem Client aufbauen, sendet er eine Nachricht mit dem Kommunikationswunsch über APNS beziehungsweise GCM an das Smartphone, damit dieses eine Verbindung zu seinem MDM-Server aufbaut. Ohne diese Dienste müsste das Smartphone periodische Anfragen beim Server stellen, um seinen Status abzufragen.

Es gibt eine ganze Reihe von Apps, die Push Notifications empfangen können, bei iOS beispielsweise Erinnerungen, Kalender, Passbook, „Freunde finden“ usw. Es sollte geprüft werden, für welche Apps Push Notifications wirklich notwendig sind und bei welchen Anwendungen dieser Dienst deaktiviert werden kann.

Diebstahlschutz

Unter „Diebstahlschutz“ versteht man im Kontext von Mobile Device Management nicht den Schutz vor dem Abhandenkommen des Gerätes. Gemeint sind die Maßnahmen, die die IT-Abteilung oder der Besitzer nach Verlust oder Diebstahl einleiten können, um die auf dem Gerät befindlichen Daten vor Missbrauch zu schützen. Wird der Administrator über den Verlust informiert, kann er von der MDM-Konsole aus entsprechende Kommandos, wie etwa „Remote Lock“, absenden. Manche MDM-Lösungen besitzen auch ein Web-Portal, über das der Benutzer selbst solche Kommandos abgeben kann.

„Remote Lock“ sperrt das Gerät, eine weitere Verwendung ist nur mit dem Passcode möglich. „Remote Wipe“ löscht die Datenbestände auf dem Smartphone entweder vollständig oder selektiv. Neben den Unternehmensdaten müssen auch die Konfigurationsprofile, beispielsweise Zugangsdaten und Zertifikate, gelöscht werden. Bei der Verwendung einer SD-Karte zur Speicherung von Unternehmensdaten muss weiterhin darauf geachtet werden, dass diese in den Löschvorgang mit einbezogen wird. Dies sollte in jedem Fall getestet werden.

Weitere Möglichkeiten im Bereich „Diebstahlschutz“ sind:

- Löschen nach einer bestimmten Anzahl von fehlerhaften Passcodeeingaben
- Lokalisieren des Geräts mit übermittelten GPS-Koordinaten
- Tonausgabe zum Wiederauffinden

Weitere Informationen finden Sie im Kapitel „Notfallmaßnahmen / Notfallübungen“.

Eine besondere Situation besteht dann, wenn das Smartphone neben der dienstlichen Verwendung auch privat genutzt wird. Wenn eine MDM-Lösung bei dem Löschvorgang nicht zwischen dienstlichen und privaten Daten unterscheiden kann. Wird ein Gerät beispielsweise in den Auslieferungszustand zurückgesetzt, gehen auch alle privaten Daten verloren. Dies sollte in einer Dienstvereinbarung geregelt sein, da der Mitarbeiter ansonsten vor der jeweiligen Löschung seiner privaten Daten im Ernstfall erst um seine Zustimmung gebeten werden muss.

Bring Your Own Device (BYOD)

Bei der dienstlichen Nutzung von Privatgeräten bestehen rechtliche Konflikte bezüglich des Software-Lizenzrechts (dienstliche Nutzung privater Lizenzen und umgekehrt) sowie bezüglich Notfallmaßnahmen (Löschung des gesamten Datenbestands), Datenschutz und -sicherheit usw.

Außerdem ist der Eigentümer nicht mehr Herr über sein Gerät, da es von der IT-Abteilung fernverwaltet wird. Dies kann zu Akzeptanz-Problemen führen, insbesondere, weil die IT-Abteilung die gewählten Konfigurationen auf den Smartphones durchsetzen muss, was zwangsläufig zu Benutzereinschränkungen führt.

Im Android-Umfeld kommt die mittlerweile unüberschaubare Vielfalt von Geräten von verschiedensten Herstellern hinzu. Die Leistungsfähigkeit dieser Smartphones variiert sehr stark vom einfachen Einsteigergerät bis zum „Alleskönner“ aus dem High-End-Segment. Fast täglich erscheinen neue Modelle auf dem Markt. Eine IT-Abteilung ist nicht in der Lage, jedes einzelne Gerät hinsichtlich seiner Qualifikation für den Einsatz im Unternehmensumfeld zu prüfen. Dazu kommt bei Smartphones auf Android-Basis noch die bekannte Update-Problematik. Geräte, die nicht zeitnah oder gar nicht mehr mit Systemaktualisierungen versorgt werden (egal ob Privatgerät oder Dienstgerät), sollten nicht für dienstliche Belange eingesetzt werden.

Aus diesen Gründen ist das Konzept „Bring Your Own Device“ für den Unternehmenseinsatz grundsätzlich abzulehnen. Wird eine gleichzeitige Nutzung von dienstlichen und privaten Belangen auf diesen Geräten dennoch erlaubt, ist eine Dienstvereinbarung unter frühzeitiger Beteiligung der Personalvertretung notwendig.

Anmerkung: Dem Konzept „Bring Your Own Device“ steht ein anderes Konzept „Private Use Of Corporate Equipment“ (PUOCE) gegenüber. Das Unternehmen könnte Smartphones beschaffen, die alle plattformbedingten Forderungen erfüllen, die von der MDM-Lösung vollständig unterstützt werden und in gewissem Maße privat genutzt werden dürfen. Die oben genannten rechtlichen Bedenken bleiben aber auch hier bestehen.

Jailbreak / Root-Erkennung

Das Sandbox-Prinzip von iOS wie auch von Android basiert auf einer Rechtestruktur des Betriebssystems, die den Zugriff von Apps auf andere Apps und auf Systemressourcen limitiert und dafür sorgt, dass sie nur in ihrem lokalen Bereich Daten manipulieren können. Durch den sogenannten „Jailbreak“ bei iOS-basierten Geräten beziehungsweise dem „Rooten“ bei Android-basierten Geräten wird dieses Rechtekonzept außer Kraft gesetzt, sodass Apps Root-Rechte erhalten. Ein Trojaner auf einem manipulierten Gerät kann volle Kontrolle über das Smartphone erlangen und so sämtliche Daten – dienstliche, wie private – abgreifen. Apple hatte ab Version 4.0 von iOS eine Jailbreak-Erkennung in das Betriebssystem eingebaut. Die entsprechende Programmschnittstelle (API) konnte von MDM-Lösungen verwendet werden, um manipulierte Geräte zu erkennen. In Version 4.2 entschied sich Apple jedoch gegen dieses Konzept und baute die Schnittstelle wieder aus. Seitdem müssen MDM-Anbieter wieder eigene Jailbreak-Mechanismen verwenden, entsprechendes gilt für Android.

Eine MDM-Lösung braucht in jedem Fall eine effektive Jailbreak/Root-Erkennung, die von der IT-Abteilung getestet werden muss. Nur so lassen sich manipulierte Geräte, von denen ein hohes Risiko für das Unternehmen ausgeht, erkennen. Die IT-Abteilung muss daher auch entsprechende Geräte zum Test vorhalten.

Leider sind jedoch die Möglichkeiten von Techniken zur Jailbreak/Root-Erkennung begrenzt, da sie auf Software-Abfragen basieren und solche Funktionen durch geschickte Gegenmaßnahmen getäuscht werden können.

App-Management

Jeder kennt die App-Stores für Smartphones, aus denen Hunderttausende von Apps – kostenlose wie kostenpflichtige – heruntergeladen und installiert werden können. Für iOS-basierte Geräte ist dies der Apple „App Store“, Apps für Android-basierte Geräte werden im offiziellen Google Store „Google Play“, aber auch in vielen anderen Stores (z. B. Amazon App-Store) angeboten. Installationspakete für Android (apk-Dateien) sind aber nicht an einen Store gebunden. Im Prinzip kann man sie von jedem beliebigen Ort laden und installieren.

Viele MDM-Lösungen bieten einen „eigenen“ App-Store für Unternehmens-Apps und/oder ausgewählte öffentliche Apps als Web-Portal an. Neben der „Grundbetankung“ mit Apps im Auslieferungszustand hat ein Unternehmen damit die Möglichkeit, den Mitarbeitern eine Auswahl von erlaubten (und möglichst geprüften) Apps zur Verfügung zu stellen.

Die Ausprägungen der App-Stores sind unterschiedlich, vom einfachen Bereitstellen von öffentlichen Apps, über spezielle Unternehmens-Apps, bis hin zu einem umfassenden App-Management (Verteilung, Kontrolle, Überwachung). Bei Letzteren können angebotene Apps für Android (und teilweise iOS) über sogenannte „Wrapping"-Mechanismen mit zusätzlichen Kontrollfunktionen „umhüllt" werden. Dies ermöglicht der MDM-Lösung anschließend die Kontrolle von Funktionalitäten oder Berechtigungen.

Die regelmäßige Kontrolle der installierten Apps auf dem Smartphone des Mitarbeiters ist notwendig, um einer missbräuchlichen Verwendung des mobilen Endgerätes entgegenzuwirken. Einige MDM-Lösungen bieten dazu Inventarisierungs-Funktionalitäten an.

Gruppen-/Benutzerverwaltung, Mandantenfähigkeit

Als Mandantenfähigkeit einer Verwaltungssoftware wird häufig die Möglichkeit bezeichnet, verschiedene Unternehmen zu verwalten, also beispielsweise verschiedene Kunden eines IT-Dienstleister. Dies ist nicht falsch, aber nur ein Teilaspekt dieses Themas. Bei der Verwaltung mobiler Endgeräte steht die IT-Abteilung vor dem gleichen Problem wie auch bei der Verwaltung von Desktop-Computern. Bei größeren Unternehmen müssen verschiedene Niederlassungen, Abteilungen und Gruppen (beispielsweise Entwicklung, Vertrieb, Verwaltung) über eine Konsole unterschiedlich konfiguriert werden können. Möglicherweise existieren verschiedene Teilnetze in der IT-Infrastruktur, die gesondert berücksichtigt werden müssen. Die IT-Infrastruktur muss also auch in der Verwaltungskonsole der MDM-Lösung abbildbar sein.

MDM-Lösungen müssen in jedem Fall eine Gruppen- und Benutzerverwaltung für verschiedene Endgerätrollen beinhalten. Darüber hinaus können sie auch mandantenfähig (im oben genannten Sinne) sein. Werden über eine MDM-Lösung in einer größeren Umgebung verschiedene „Mandanten" verwaltet, so ist zu klären, wer die Verwaltung übernimmt. Sinnvoll ist ein Haupt-Administrator, der die grundlegenden Einstellungen trifft, sowie mehrere Verwaltungs-Administratoren, die für Teilbereiche zuständig sind. Es sind rollenbasierte und/oder lokationsbasierte Administratoren denkbar.

Notfallmaßnahmen / Notfallübungen

Der Verlust oder Diebstahl eines Smartphones oder Tablets ist gleichbedeutend mit dem Verlust oder dem Diebstahl von Geschäftsdaten. Das Gerät muss schnellstmöglich gesperrt und/oder ferngelöscht werden. Es ist also äußerst wichtig, dass der Benutzer den Verlust so früh wie möglich meldet. Mitarbeiter sollten diesbezüglich in regelmäßigen Abständen sensibilisiert werden. Enthält die MDM-Lösung ein Self-Service-Portal für diese Zwecke, müssen die Mitarbeiter mit dem Umgang vertraut gemacht werden. Außerdem ist ein Notfallplan zu erstellen, der klare Anweisungen enthält, die auch von einem Vertreter des zuständigen Administrators durchgeführt werden können.

Zusätzlich zu der Fernsperrung/Fernlöschung des verlorenen Gerätes muss der Zugang des Smartphones zum Unternehmen in der Verwaltungskonsole komplett gesperrt werden, damit kein unberechtigter Zugriff mehr erfolgt.

Schutzprogramme

Apps zum Schutz vor Malware auf Android-basierten Smartphones arbeiten mit den gleichen Einschränkungen wie alle anderen Apps auch. Sie sind in eine Sandbox eingesperrt und müssen bei der Installation ihre Berechtigungen anmelden. Es besteht keine Möglichkeit mit Systemberechtigungen (Root/Administrator-Rechten) in den Tiefen des Betriebssystems zu agieren.

Schadprogramme werden anhand der Installationsdatei (apk-Datei) erkannt. Durch die Android-Berechtigung „Aktive Apps abrufen" ist die Schutz-App in der Lage, installierte Programmpakete gegen eine Blacklist zu prüfen. Diese Blacklist mit bekannten Malware-Programmpaketen ist entweder im Schutzprogramm enthalten oder wird online abgerufen. So können infizierte Apps „on demand" oder bei der Installation erkannt werden.

Daneben gibt es je nach Ausbaustufe noch weitere Schutzfunktionen, beispielsweise Schutz vor unberechtigtem Zugriff auf Kontaktdaten oder SMS- und Anruffilter. Weitere Schutzfunktionen sind „SIM-Kartenwechsel erkennen und Gerät sperren“ sowie „Remote Wipe“-Funktionalitäten.

Unter iOS ist es grundsätzlich technisch nicht möglich, solche zusätzlichen Schutzmaßnahmen zu installieren. Apple stellt hierfür keine geeigneten Schnittstellen zur Verfügung, sondern wehrt Angriffe über betriebssystemeigene Mechanismen ab.

Zusätzliche Informationen zum Android-Berechtigungssystem finden Sie auf der Internetseite „BSI für Bürger“ unter Exkurs: App-Berechtigungen bei Android.

Konfigurationsempfehlungen (exemplarisch)

Im Folgenden werden einige wenige ausgewählte Konfigurationsempfehlungen für iOS und Android vorgestellt. Sie sollen in späteren Versionen dieses Dokuments erweitert werden. Vorschläge für Konfigurationsempfehlungen, die nicht trivial sind oder eine besondere Bedeutung für die Datensicherheit darstellen, werden gerne entgegengenommen (gerne auch für andere mobile Betriebssysteme).

Die beschriebenen Konfigurationen sind jeweils von einem für das Unternehmen verantwortlichen System-Administrator durchzuführen und per Passwort vor Änderungen durch den Benutzer zu schützen. Sofern möglich sollten die Anpassungen zentral über die MDM-Lösung vorgenommen werden.

Android: Externer Speicher

Die Speicherung dienstlicher Daten auf Standard-SD-Karten sollte nach Möglichkeit verhindert werden, Datendiebe können die Speicherkarte schnell und leicht vor dem Zugriff durch die MDM-Lösung schützen. Prüfen Sie zumindest, ob die gespeicherten Daten auf dem externen Speicher verschlüsselt werden. Prüfen Sie auch, ob ein „Remote Wipe“-Befehl die Daten der SD-Karte überhaupt löscht.

iOS: Konfigurations-Profile

Einstellungen von iOS-basierten Geräten werden über Konfigurations-Profile vorgenommen. Technisch sind das Dateien im XML-Format, die an das Gerät gesendet und dort verarbeitet werden. Wird eine Einstellung durch den Administrator geändert, muss die entsprechende Konfigurations-Datei (.mobileconfig-Datei) erneut an das Gerät (die Geräte) gesendet werden. Verschiedene MDM-Lösungen konfigurieren iOS-Geräte über ein einziges Konfigurations-Profil. Dies hat zur Folge, dass bei der Änderung einer einzigen Einstellung die gesamte Konfiguration erneut verarbeitet wird und eine vollständige Synchronisation der Daten stattfindet. Die Folge ist die erneute (unnötige) Übertragung der Daten. Deshalb ist eine Aufteilung der Konfigurationen auf mehrere Konfigurations-Dateien sinnvoll, was von einigen MDM-Lösungen gemacht wird.

iOS: „Öffnen in ...“

Verschiedene Apps bieten die Option „Öffnen in ...“ (engl. „Open in ...“) für die Bearbeitung von Dateien an. In der Option werden Apps angezeigt, die in der Lage sind, die Dateiinhalte zu verarbeiten. Beispiel: Bei pdf-Dateien hat man u. a. die Möglichkeit, den Inhalt in der „iBooks-“, „Chrome-“ oder „Kindle-“ App zu lesen. Mit „Öffnen in ...“ kann man aber auch Dateien zu einem Speicherdienst in der Cloud (wie beispielsweise „Dropbox“) verschieben.
Wenn möglich, muss diese Option durch die MDM-Lösung deaktiviert werden.