Bestandsaufnahme

Mobile Endgeräte effektiv und sicher verwalten: MDM-Systeme im Vergleich

Kai-Oliver Detken, Simon Schlenker

Mobile-Device-Management-Lösungen (MDM) erfreuen sich zunehmender Beliebtheit, nimmt doch der mobile Gerätepark eines Unternehmens immer mehr zu. Allerdings ist es schwer, aus der Vielfalt der Angebote die richtige Lösung auszuwählen. Zusätzlich verstehen nicht alle Anbieter oder Hersteller das Gleiche unter einer MDM-Lösung. Es wurden daher eine aktualisierte Bestandsaufnahme der verfügbaren Lösungen vorgenommen und die vielversprechendsten von ihnen getestet.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer, Simon Schlenker Mitarbeiter im Bereich Systemmanagement der Decoit GmbH in Bremen

Smartphones sind schon lange nicht mehr aus dem Geschäftsalltag wegzudenken. Dabei werden sie kaum noch in ihrem ursprünglichen Arbeitsgebiet – der Telefonie – eingesetzt, sondern dienen vielmehr als kleine und leistungsfähige Computer. Wie selbstverständlich werden sie in die Unternehmensnetze eingebunden, Kontakte und Termine mit ihnen synchronisiert sowie sensible Daten ausgetauscht. Dabei ist das Angriffsrisiko ähnlich gestiegen wie der Unternehmenseinsatz. Speziell im Android-Umfeld werden aufgrund der hohen Verbreitung Trojaner, Spyware oder Ransomware geschrieben, die wertvolle Daten entwenden oder den Betrieb erschweren sollen. Hinzu kommt die Problematik, dass eine Trennung zwischen privater und geschäftlicher Nutzung oftmals nicht vorgenommen wird, was wiederum die Verwaltung der Geräte erschwert.

MDM-Systeme sind daher notwendig und auch inzwischen vielfältig im Markt vorhanden. Sie sollen die Verwaltung aller mobilen Geräte ermöglichen und gleichzeitig den Sicherheitsstandard des Unternehmens erhöhen. Jedoch gilt es vorab die Anforderungen und damit den Funktionsumfang eines solchen Systems zu definieren, denn jedes MDM-System besitzt andere Schwerpunkte und Einsatzmöglichkeiten. Nach einer ersten Bestandsaufnahme in NET 9/2016 war es daher wieder an der Zeit, den dynamischen MDM-Markt zu untersuchen.

Auswahlkriterien und Testumgebung

Um aus der großen Zahl der MDM-Lösungen ein für das eigene Unternehmen passende System herauszusuchen, müssen erst einmal die eigenen Anforderungen bekannt sein. Für die Testumgebung wurden daher im Vorfeld folgende Randbedingungen festgehalten:

- Es müssen iOS- und Android-Geräte gleichermaßen verwaltet werden können.
- Eine zentrale App-Verwaltung zum Installieren und Update der Geräte muss vorhanden sein.
- Die Sicherheitslösung muss mit dem BYOD-Konzept (Bring Your Own Device) vereinbar sein.
- Geschäftliche und private Daten müssen voneinander getrennt werden können.
- Aus Sicherheits- und Verwaltungsgründen ist eine On-Premise-Lösung vorgesehen.

Zur genaueren Unterscheidung und zum detaillierten Vergleich sind weitere Kriterien festgelegt worden. So wurde die Vorgehensweise, um ein Gerät auszurollen und die Funktionen dazu (zentrale Konfiguration, Festlegen eines Passwortes, Netzkonfiguration, VPN-Verbindung usw.) mit einbezogen. Des Weiteren wurden Gruppenprofile, Massenaktionen, Ortung, Sperren und Löschen eines Geräts, Zurücksetzen des Passworts, Erkennung der Gerätekonfiguration, Einteilungsmöglichkeiten, Funktionen zum Senden einer Nachricht und die Option zum Pausieren der Client-Verwaltung miteinander verglichen. Dabei wurde Wert auf Übersichtlichkeit der angewandten Richtlinien, empfohlener Apps und Historie, ebenso wie auf die Art der Benachrichtigung und der Dokumenten-Container gelegt. Alle Herstellerlösungen wurden einem praktischen Test unterzogen. *Tabelle 1* fasst die ausgewählten MDM-Systeme zusammen, die sich aus einer größeren Vorauswahl von 58 Herstellern herauskristallisiert haben.

Als Testgeräte wurden zwei Android-Geräte verwendet, die unterschiedliche Zugriffsberechtigungen besaßen und über WLAN mit dem Internet ver-

Produkt	Hersteller	Open Source	zentrale App-Verteilung	Security-Lösung	BYOD-Lösung	iOS	Android	On Premise/ Cloud
Enterprise Mobility	Endpoint Protector	nein	ja	ja	ja (Container)	ja	ja	ja/nein
Flyve MDM	Teclib-Flyve	ja	ja	ja	ja	angekündigt	ja	ja/nein
Mobile Security	Securepoint	nein	ja	ja	ja	ja	ja	nein/ja
Sophos Mobile	Sophos	nein	ja	ja	ja (Container)	ja	ja	ja/ja

Tabelle 1: Übersicht der gestesteten Herstellerlösungen

bunden waren (*Bild 1*). Alle Hersteller stellten für die Testumgebung eine entsprechende Testlizenz zur Verfügung. Die MDM-Lösung von Endpoint Protector erfordert für iOS-Geräte zusätzlich ein APNS-Zertifikat (Apple Push Notification Service) und für Android-Geräte einen GCM-Schlüssel (Google Cloud Messaging).

Herstellerlösungen

Die Securepoint-MDM-Lösung (www.securepoint.de) wird vorerst nur als Cloud-Lösung angeboten. Sie wirbt neben einer schnellen Einrichtung vor allem mit dem Thema Sicherheit, wie der Name Mobile Security erahnen lässt. Wenn ein Firmengerät das sichere Firmen-WLAN verlässt, baut die App automatisch eine VPN-Verbindung zur Cloud-Firewall des Herstellers auf und soll damit auch in unsicheren WLANs geschützt sein. In der App selbst gibt es einen Diagnosebericht über das Gerät und eine Übersicht über die zugeordneten Richtlinien. In der Geräteübersicht (*Bild 2*) bekommt man einen groben Überblick seiner angemeldeten Geräte inkl. einiger Statistiken, wie z.B. Eigentümer (COPE/BYOD, COPE – Corporat-Owned, Personally Enabled, unternehmenseigenes Gerät, das der Mitarbeiter einrichtet und pflegt), Modell, Benutzer, Profil oder den letzten Kontakt mit dem Gerät. Ein gerootetes Gerät wird hier ebenfalls gekennzeichnet.

Die Einrichtung sämtlicher Optionen gestaltet sich schnell und einfach. Die Verwaltung der Geräte inklusive der Apps und Profileinstellungen ist jedoch noch zu träge, da das Pushen der Apps und Profile nicht einwandfrei funktioniert. Positiv zu vermerken sind die stetig sichere Verbindung per VPN, der gesteuerte Netzverkehr und die Kommentare neben fast jeder Option, die eine kurze Erläuterung abgeben. Die VPN-Verbindung kann nach Wunsch pausieren, wenn dies im MDM-System in einem zugehörigen Profil erlaubt ist. Leider gab es bei der Deinstallation des Client keine Benachrichtigung in der Weboberfläche und das Gerät wurde weiterhin als aktiv angezeigt.

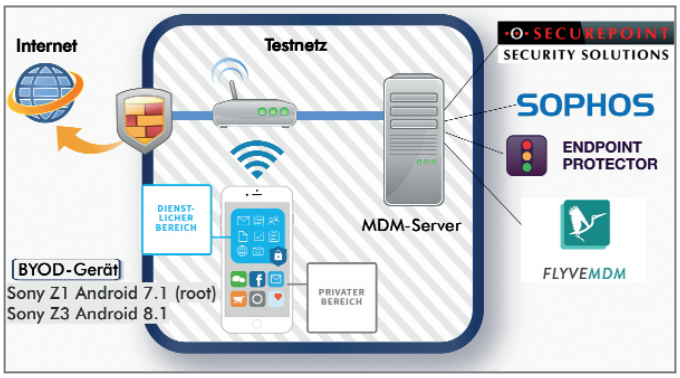

Bild 1: Testumgebung für die Systeme zum Mobile Device Management (MDM)

Die MDM-Lösung von Sophos (www.sophos.com) ist Teil eines Unified-Endpoint-Managements, so dass auch Personalcomputer und Internet-of-Things-Geräte (IoT) mit eingebunden werden können. In der Teststellung wurde nur das Produkt „Mobile" untersucht. Je nach Lizenzierung wird dabei das Device- und Application-Management um eine Container- und Sicherheitslösung ergänzt, so dass DSGVO-Konformität sichergestellt werden kann. Zudem besteht die Möglichkeit, eine ActiveDirectory-Synchronisierung einzubinden.

Über das Webinterface lassen sich die Endgeräte bequem über einen fünfschrittigen Einrichtungsassistenten im Untermenü „Mobile" hinzufügen. In diesem kann wahlweise das iOS- oder Android-Gerät direkt einem zuvor erstellten Benutzer und einer Gerätegruppe zugeteilt werden. Es wird ebenfalls der Besitzer festgelegt (COPE/BYOD). Anschließend lässt sich der Registrierungstyp auswählen, indem zwischen der Geräteregistrierung an sich und der integrierten Container-Lösung mit zuvor definierten Richtlinien gewählt wird.

Das Dashboard von Sophos besteht aus vier Kategorien. Die Erste enthält Statistiken und ist in Übersicht, Berichte und Aufträge unterteilt. Die Übersicht besteht aus anpassbaren Widgets, die selbst zusammengestellt und über Berichte exportiert werden können. Unter Aufträge sind alle Aktionen zwischen Server und Geräten aufgelistet. Dieser Reiter lässt Aktionen durch eine überschaubare Darstellung und Sortierung sehr gut nachvollziehen. Die zweite Kategorie betrifft das Management und beinhaltet eine Benutzerverwaltung sowie eine Geräte- und Gruppenübersicht. Die dritte Kategorie enthält die Konfigurationen, aufgeteilt in Profile, Auftragspakete, Apps, Dokumente und Compliance-Richtlinien. In der letzten Kategorie werden App-Gruppen definiert und Einstellungen eingerichtet.

Der Endpoint Protector (www.endpointprotector.de) wirbt mit vollständigem Schutz und detaillierter Kontrolle der mobilen Geräte sowie der Unternehmensdaten. Zusätzlich soll eine klare Abgrenzung zwischen geschäftlichen und privaten Mitarbeiterdaten geschaffen werden. Mittels E-Mail, SMS oder QR-Code können die Geräte registriert werden. Eine Massenregistrierung per Excel-Tabelle

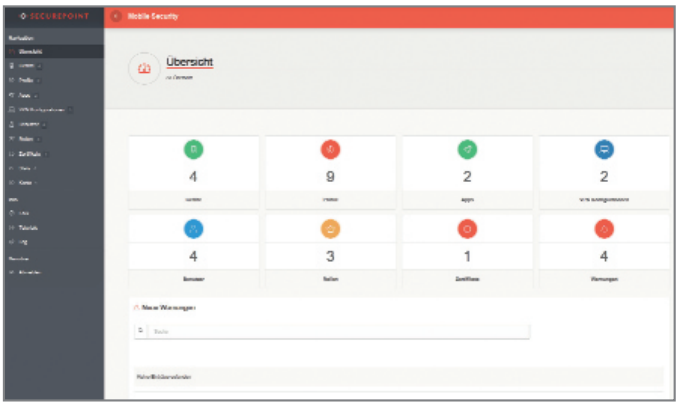

Bild 2: Securepoint Mobility Security Dashboard

ist für größere Umgebungen ebenfalls möglich. Um ein Gerät sicher hinzuzufügen, muss man im Client einen One Time Code (OTC) zur Anmeldung verwenden.

An erster Stelle befindet sich das „Cockpit", das eine Übersicht über Statistiken der Geräte, wie die Anzahl, den letzten Standort oder den Lizenzstatus, erstellt. Hier befindet sich auch die Geräteeinrichtung. Das Untermenü „Mobile Geräte" gibt eine detailliertere Übersicht über die Geräte und beinhaltet die meisten Einstellungen. Diese sind in 13 Reiter unterteilt. Hier kann auch das jeweilige Gerät von der Verwaltung ausgenommen und zu einem beliebigen Zeitpunkt wiederaufgenommen werden.

In der Android-App gibt es zwei Kontrollkästchen, um Lokalisierungskosten und hohe Standortgenauigkeit zu erlauben, sowie einen Button, um den Standort zu melden. Wünschenswert wäre hier eine Übersicht empfohlener Apps sowie eine Aktionshistorie zwischen Server und Gerät mit den angewandten Richtlinien. Eine Container-Lösung zur direkten Trennung zwischen privaten und Unternehmensdaten ist bisher nicht enthalten.

Die Lösung Flyve MDM von Teclib (**www.teclib-edition.com**) wirbt mit einem Open-Source-Konzept, einer schnellen und einfachen Einrichtung sowie einer kompletten Google-Unabhängigkeit. Das MDM-System ist ein Plugin eines Open-Source-basierten IT-Asset-Management- und Service-Desk-Systems, dem GLPI (Gestionnaire Libre de Parc Informatique). Leider reagierte Teclib nicht bei einer Demoanfrage.

Die Einrichtung ist sehr umfangreich. Es wird neben der virtuellen Maschine (VM) mit der GLPI-Basis das Plugin „Fusion Inventory" benötigt. Des Weiteren ist eine zusätzliche VM mit „Mosquitto" zur Kommunikation zwischen Android-Gerät und Server notwendig. Mehrere Dokumentationen, die leider nicht immer vollständig sind, begleiten die Installation. Neben der Verwaltung im GLPI lässt sich zusätzlich das Web-Dashboard installieren. Zum Hinzufügen eines Client wird eine E-Mail mit einem QR-Code und einem Link verschickt.

Über die Adresse der eingerichteten VM lässt sich GLPI über den Webbrowser erreichen. Das Mobile Device Management ist als Plugin über das Untermenü des GLPI in der Weboberfläche erreichbar. Um das Web-Dashboard nutzen zu können, muss Port 3000 angegeben werden. GLPI enthält umfangreiche Einstellungsmöglichkeiten und detaillierte Informationen über die einzelnen Geräte. Persönlich anpassbare Ansichten helfen dabei, die wichtigsten Informationen zusammenzufassen und den Überblick zu behalten. Der Client-Agent musste allerdings aus einem öffentlichen Git-Verzeichnis heruntergeladen werden, da die App aus dem App Store wieder entfernt wurde (Stand: April 2019). Einen Container zur getrennten Nutzung von privaten und geschäftlichen Daten oder Anwendungen sowie eine Option zum manuellen Synchronisieren gibt es nicht.

Testergebnisse

Securepoint Mobile Security erfüllt die Voraussetzung, iOS- und Android-Geräte zu unterstützen. Auch die zentrale App-Verteilung entspricht den gesetzten Anforderungen. Die Erwartungen an ein BYOD-Konzept sind allerdings nicht erfüllt worden, da z.B. eine Container-Lösung fehlt. Gleichzeitig ist die fehlende Option, die MDM-Lösung auch on Premise betreiben zu können, für die Autoren ein Ausschlusskriterium.

Sophos Mobile ist ein ausgereiftes MDM-System mit hilfreichen Extras, wie der Integration von ActiveDirectory und dem Self Service Portal (SSP). Besonders hervorzuheben sind die detaillierten Einstellungsmöglichkeiten, mit denen flexibel auf individuelle Anforderungen eingegangen werden kann. Ebenso auffällig ist die hohe Anzahl an Android-Einstellungen im Vergleich zu iOS. Die Anforderungen werden in allen Punkten erfüllt. Leider gibt es nicht bei allen Optionen oder Features einen Kommentar, der die jeweilige Funktion kurz erläutert. Dafür ist eine einsehbare Online-Dokumentation sehr detailliert hinterlegt.

Endpoint Protector hinterlässt auf den ersten Blick einen umfangreichen Eindruck. Durch die vielen Möglichkeiten der Geräteregistrierung wird ein einfacher Einstieg ermöglicht. Bei genauerem Hinschauen sind jedoch Schwächen erkennbar, wie die fehlende Root-Erkennung, die fehlerhafte App-Verteilung oder die sicherheitsrelevante, aber wirkungslose Festlegung des Eigentümers. Hier sollten nachfolgende Versionen auf jeden Fall Abhilfe schaffen.

Der fehlende Support und der mittlerweile nicht mehr im App Store enthaltene Agent sowie die teilweise fehlerbehaftete Weiterleitung etlicher Links bei Flyve MDM lassen an einem ernsthaften Einsatz zweifeln. Zusätzlich stürzte im Test gelegentlich das Dashboard ab. Da iOS bisher nicht und Android nur von Version 4.4 bis 7.1.2 unterstützt werden, kann Flyve MDM momentan nicht empfohlen werden. Die Lösung hat zwar gute Ansätze, fühlt sich aber nach einer Alpha-Software an. Es besteht noch erheblicher Entwicklungsbedarf.

Fazit

Die vier getesteten MDM-Lösungen verfolgen den gleichen Ansatz, unterscheiden sich jedoch im Detail deut-

Anforderungen		Securepoint	EPP	Sophos	Flyve MDM
Open Source		nein	nein	nein	ja
Lizenzmodell		Cloud	Cloud & Lokal	Cloud & Lokal	Lokal
iOS / Android		ja	ja	ja	angekündigt / bis Android 7.1
BYOD		auf COPE ausgelegt	ja	ja	indirekt möglich
	Container	nein	nein	ja	nein
Rollout		Email, QR	Email, Weblink, SMS, QR	Email, QR	Email, QR
	mit Vorkonfiguration	ja	ja	ja	nein
Passcode		ja	ja	ja	ja
Netzwerkvorkonfig.		nein	ja	ja	nein
VPN		open VPN	nein	ja Dritte	nein
Gruppenprofile		ja	ja	ja	ja
Massenaktion / Auftragspakete		umständlich	ja	ja	ja
Operationen	Ortung	ja	ja	ja	ja
	Sperren	ja	ja	ja	ja
	Löschen	ja	ja	ja	ja
	PW zurücksetzen	ja	ja	ja	ja
	Kamera deaktiviert	ja	ja	ja	ja
Gerätekonfig.-erkennung		ja	ja	ja	ja
Richtlinien		gering	sind Einstellungen	sehr detailliert	gering
Nachricht senden		ja verfällt	nein	ja archiviert	nein
Extras		VPN, Exchange ActiveSync	Geofence, AD, vCard	self Portal, AD, DokuContainer, Exchange ActiveSync	anpassbare Ansichten
Root-Erkennung		ja	nein	ja	ja
Client als		Geräteadmin	Geräteadmin	Geräteadmin	Geräteadmin
	Richtlinienübersicht	ja	nein	nur Bestätigung	ja
	empfohlene Apps	nein	nein	ja	ja
	Dokumentencontainer	nein	nein	extra	kein Container
	Historie	ja	nein	nein	ja
	notification	durchgehend	keine	teils	ja
Pausierung		nein	ja	ja	nein
Einteilungsmöglichkeiten		Rolle, Benutzer, Profile, (Tag)	Benutzer, Richtlinien	Gerätegruppen, Profile, Benutzer	Benutzer

Tabelle 2: Detaillierter Vergleich der untersuchten Herstellerlösungen für Mobile Device Management

lich. Sophos Mobile hebt sich als einziges MDM mit einer integrierten Container-Lösung und durch eine Vielzahl an detaillierten Einstellungsmöglichkeiten für iOS und Android ab, während Securepoint mit dem Thema Sicherheit durch eine integrierte VPN-Verbindung mit White- und Blacklisten für den Netzverkehr punktet. Endpoint Protectors Mobile Device Management besitzt ein gutes Grundkonzept, das allerdings noch einige Wünsche offenlässt. Beispielsweise ist keine Unterscheidung zwischen COPE- und BYOD-Eigentümer oder Root-Erkennung möglich. Flyve MDM verfolgt mit seiner quelloffenen Lösung zwar einen guten Ansatz, muss jedoch stark weiterentwickelt und insbesondere um eine integrierte BYOD-Lösung erweitert werden, bevor ein ernsthafter Einsatz infrage kommen kann. Da momentan nur veraltete Android-Versionen unterstützt werden, ist dies allerdings derzeit nicht absehbar. *Tabelle 2* fasst die Ergebnisse noch einmal im Detail zusammen. *(bk)*