An der kurzen Leine halten

Was versprechen Managementsysteme für mobile Endgeräte? Und was halten sie?

Kai-Oliver Detken

Durch die Nutzung mobiler Endgeräte in Unternehmen wächst der IT-Schutzbedarf. Während sich frühere Angriffe vor allem gegen öffentliche Server richteten, verlagern sie sich heute nicht nur auf die Firewall und das VPN-Gateway, sondern wenden sich auch direkt gegen Endgeräte, die sich zeitweilig außerhalb des sicheren Netzes befinden. Denn wer sie kompromittiert, erlangt in vielen Fällen zugleich einen bequemen Zugang ins Unternehmensnetz. Anforderungen und Maßnahmen an mobile Endgeräte in Sicherheitsstandards (z.B. ISO 27001, IT-Grundschutz) fokussieren bisher den Einsatz innerhalb einer Arbeitsumgebung, berücksichtigen jedoch nicht deren Nutzung in Umgebungen verschiedener Betreiber. Neben mehr Interoperabilität wäre daher eine Distributionsplattform hilfreich, die Software an mobile Endgeräte sicher verteilt, die Patche der Endgeräte überwacht und die Installation von Schadsoftware verhindert.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Mobile Endgeräte werden zunehmend mit integrierten Anwendungen wie Terminplanung, elektronischen Notizblöcken oder E-Mails eingesetzt. Dabei werden auch sensible Unternehmensdaten auf den elektronischen Begleitern mitgenommen. Allerdings sind die mobilen Endgeräte im Unterschied zu normalen Arbeitsplatzrechnern schlechter in herkömmliche betriebliche IT-Infrastrukturen integrierbar. So erfolgen Zugriff und Synchronisation der Daten durch spezielle Software. Auch reichen die wenigen vorhandenen Sicherheitsmechanismen kaum aus, um vertrauliche persönliche oder geschäftskritische Daten zu schützen. Der Verlust eines Gerätes bringt daher fast immer auch den Verlust der Vertraulichkeit der Daten mit sich.

Folgende Entwicklungen lassen sich im mobilen Umfeld ausmachen:

- Mobile Endgeräte: Die technische Entwicklung ermöglicht sowohl eine zunehmende Integration von Funktionen und Schnittstellen in mobile Endgeräte als auch die Zusammenführung ursprünglich verschiedener Geräteklassen wie z.B. Mobiltelefon und PDA (Personal Digital Assistant). Zudem werden die Geräte immer leistungsfähiger, und der Grad der Vernetzung wächst sowohl quantitativ durch die Anzahl zur Verfügung stehender Kommunikationskanäle als auch qualitativ durch höhere Übertragungsraten.
- Dienste: Es ist eine verstärkte Verbreitung von echten mobilen Diensten festzustellen. Das heißt, es werden immer mehr Dienste eingesetzt, die sich der spezifischen Eigenschaften und Fähigkeiten (z.B. GPS-Daten) der mobilen Endgeräte bedienen. Neue Benutzungsparadigmen wie „Digital Lifestyle“ oder „Ubiquitous Computing“ verändern dabei die Anforderungen an mobile Services. So spielen hier Bedienbarkeit und Kommunikationsfähigkeit eine wichtige Rolle. Der Wunsch nach aktuellen und ständig verfügbaren Informationen führt zum mobilen Internet und in vielen Fällen auch zu neuen Anwendungsfeldern.

Anforderungen an mobile Endgeräte

Die Bedrohungslage hat sich verändert. Angriffe, wie sie heute bei Desktop-PCs und anderen Rechnersystemen bekannt sind, werden in Zukunft in deutlich stärkerem Umfang auch bei mobilen Endgeräten auftreten. Monokulturen von Soft- und Hardware können diese Bedrohungslage zusätzlich verschärfen. Da der Einsatzbereich eines mobilen Endgerätes vom Arbeitsgerät bis hin zum persönlichen Lifestyle-Produkt reicht, entwickeln sich neue Anwendungsaspekte. Im Vergleich zu klassischen Rechnern entstehen durch die Veränderung der Benutzungsparadigmen und aufgrund neuer Anwendungsszenarien neuartige Bedrohungen.

Ebenso ergeben sich aus den neuen Sicherheitskriterien zur Absicherung eines Unternehmensnetzes neue Anforderungen an mobile Endgeräte. Speziell die Mobilität sowie diverse nutzbare Schnittstellen (*Bild 1*) machen sie leichter angreifbar, auch die Nutzung unterschiedlicher Netzzugänge ist nicht wie herkömmlich im administrativen Alltag handhabbar:

- Recovery: Notebooks lassen sich z.B. mithilfe einer Recovery-Partition auf einer lokalen Festplatte oder durch einen externen Datenträger wiederherstellen. Damit ist es möglich, bei intakter Hardware Fehler im Bereich des Betriebssystems oder der Anwendungssoftware zu beheben. Mobile Endgeräte lassen sich über eine Speicherkarte leicht mit einem neuen System versorgen.

- Remote-Installation: Erfordert ein Minimalbetriebssystem mit den nötigen Treibern für die Konnektivität, so dass das Endgerät eine Verbindung zur Zentrale aufnehmen und die benötigten Programme von dort installieren kann. Notwendig ist eine Softwareverteillösung (MDM – Mobile Device Management), die über Firmengrenzen hinweg funktioniert.
- Patch-Level: Damit ein mobiles Endgerät die Erlaubnis erhält, sich mit dem Firmennetz zu verbinden, sollte es einen bestimmten Patch-Level nachweisen können. Die Patche kann z.B. eine Softwareverteillösung bereitstellen. Je nach Strenge der Sicherheitsrichtlinien kann das in einer Quarantänezone erfolgen.
- Quarantänezone: Dieser vom Firmennetz getrennte Bereich besitzt einen Mechanismus für die Softwareverteilung und hält alle aktuellen Patche sowie Daten für sicherheitsrelevante Services wie Antiviren- oder Antispy-Definitionen vor. Das mobile Gerät muss diesen Bereich passieren, um in das lokale Netz zu kommen.

Die Authentifizierung der mobilen Mitarbeiter erfolgt auf Benutzer- und Hardwareebene. Sie überprüft, ob das Gerät im Firmennetz erlaubt ist und ob der jeweilige Teilnehmer eine Berechtigung besitzt. Diese Leistungsmerkmale versprechen MDM-Systeme, die zudem das zentrale Management der Mobilgeräte ermöglichen.

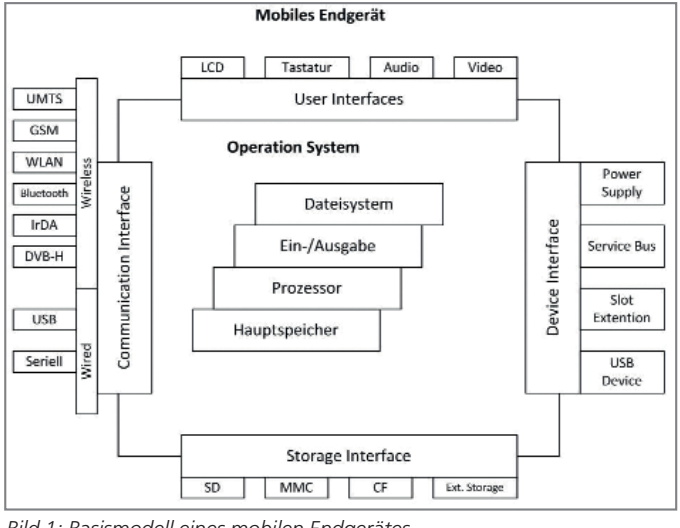

Bild 1: Basismodell eines mobilen Endgerätes

MDM-Anforderungen

Auf dem Markt gibt es inzwischen einige MDM-Systeme, die vorgeben, Sicherheitsmaßnahmen für mobile Endgeräte zentral umsetzen zu können. Doch nicht alle von ihnen zielen auf die IT-Sicherheit als Hauptschwerpunkt ab. Manche geben sich z.B. bereits mit der einheitlichen Verwaltung der mobilen Systeme zufrieden. Und auch dies gestaltet sich nicht trivial, wenn verschiedene Plattformen im Einsatz sind, die meistens auf proprietären Betriebssystemen aufsetzen. Hinzu kommt, dass die Smartphones hauptsächlich für den Consumer-Be-

reich entwickelt werden und deshalb keine einheitlichen Managementmöglichkeiten vorsehen – mit Ausnahme von Blackberry-Geräten.

MDM-Systeme sollen in erster Linie folgende Aufgaben wahrnehmen:

- alle mobilen Geräte eines Unternehmens erfassen;
- Software, Daten und Unternehmensdaten auf dem neuesten Stand halten;
- Zugriffsschutz sicherstellen.

Diese Aufgaben lassen sich unterschiedlich bzw. in manchen Fällen gar nicht umsetzen. So ist z.B. eine Softwareverteilung von Apps ohne Anwenderinteraktion schwierig. Das liegt daran, dass die Verteilung von Apps eigentlich nur über sog. App-Stores vorgesehen ist. Eine Unternehmenslösung müsste also einen internen App-Store anlegen, der stellvertretend die Apps des Unternehmens beim Hersteller einkauft und zur Verfügung stellt. Bei Android lassen sich zwar auch ohne den sog. Play Store neue Apps installieren. Aber dies wird als Sicherheitsproblem angesehen – speziell, wenn die Apps von unbekannten Drittanbietern kommen. Daher sollte das MDM-System diese Möglichkeit eigentlich deaktivieren.

Die größte Herausforderung aber ist es, unterschiedlichste Betriebssysteme auf einen gemeinsamen Nenner zu bringen. Dies ist jedoch aufgrund der Vielzahl der Systeme und Versionen kaum möglich. Trotzdem sollte man sich ein MDM-System aussuchen, das möglichst viele Systemvarianten unterstützt, da man dann bei späteren Betriebssystemwechseln auf weniger Engpässe stößt. Es ist aber zu empfehlen, nicht mehr als zwei verschiedene Systeme zuzulassen. Durch die geringere Komplexität kann man auf einen höheren Funktionsumfang zurückgreifen und ist weniger eingeschränkt.

Die BYOD-Problematik (Bring your own Device) und damit verbunden die Vielfalt der zu verwaltenden Endgeräte verschärft die Situation noch. In den USA ist BYOD schon wesentlich verbreiteter. Amerikaner gehen gewohnheitsmäßig sehr pragmatisch an solche Dinge heran: Bewährt sich der Einsatz von BYOD und arbeitet man so kostengünstiger und effizienter, wird der neue Arbeitsstil beibehalten. An die IT-Sicherheit wird dabei kaum ein Gedanke verschwendet. Hauptsache ist, dass die Apps, die man privat lieb gewonnen hat, ohne Probleme im Unternehmensumfeld eingesetzt werden können.

Der Administrator muss allerdings nun auch diese fremden Geräte mit in die Unternehmensrichtlinien einbinden. Folgendes hat er dabei zu beachten:

- Auf den Geräten muss eine bestimmte Betriebssystemversion laufen, die den Sicherheitsrichtlinien des Unternehmens entspricht und auch verwaltet werden kann.
- Das Gerät darf weder „gerootet" (Android), noch „gejailbreaked" (Apple iOS) sein.
- Absicherungsmaßnahmen für den Zugang zu dem Gerät sind zu überprüfen. Es muss zwingend ein „Device Look" eingerichtet sein, so dass der Benutzer nur über eine PIN-Eingabe das Gerät bedienen kann.
- Unternehmensdaten müssen sicher auf das Gerät übertragen, aber dort auch sicher abgelegt werden können.
- Beim Ausscheiden des Mitarbeiters müssen die Daten wieder sicher entfernt werden können, ohne dass die privaten Daten verloren gehen.

Diesen Bedingungen muss sich ein Privatanwender beugen, will er sein Smartphone oder seinen Tablet-PC im Unternehmen nutzen. Zur Erleichterung der Administration und zum Ausrollen einer zentralen Sicherheitsrichtlinie ist dabei der Einsatz eines MDM-Systems zwingend erforderlich.

MDM-Systembeispiele

In der *Tabelle* werden verschiedene MDM-Systeme aufgeführt, die alle unterschiedliche Schwerpunkte und Ausrichtungen besitzen. Während die einen sich nur auf ein mobiles Betriebssystem festlegen, versuchen andere, möglichst alle Varianten zu unterstützen.

Eine Datentrennung von privaten und geschäftlichen Informationen wird bei

MDM-Systeme	unterstützte Betriebssysteme	Patch-Management	Sicherheits-funktionen	Datentrennung
MobileIron	iOS, Android, Blackberry, Symbian, Windows Mobile	Quarantänezone, Patch-Updates	Repository-Monitoring, Lock-Funktionalität	keine Datentrennung, Remote-Vollzugriff auf das Endgerät
Matrix42	iOS, Android, Blackberry, Symbian, Windows Mobile	Portalseite zum Patch-/Rollenmanagement	rollenbasierter Zugriff, Remote-Datenlöschung	firmenspezifische Apps, Löschen von Firmendaten
AirWatch	iOS, Android, Blackberry, Symbian, Windows Mobile	App-Katalog für Patch-Updates	zentrale Definition von Policys, rollenbasierte Gruppen	Unterscheidung zwischen internen und öffentlichen Apps
Baramundi	iOS, Android, Windows Phone	Inventarisierung mobiler Endgeräte, Patch-Updates	zentrales Management, IT-Compliance, Lock-Funktionalität	Unterscheidung zwischen Firmen- und Privatgerät
Lookout	iOS, Android	Cloud-Portal, kein Patch-Management, AV-Funktionalität	Sperren und Löschen von Daten	keine Datentrennung
Samsung Knox	Android	zentrales Patch-Management	Remote auf Werkszustand zurücksetzen, Rechte remote setzen, Secure Boot, Verschlüsselung	Trennung durch verschiedene Profile, extra Firmen-Container
BizzTrust	Android	Quarantänezone, Patch-Updates	Gerätezustand remote ermitteln, Policy Enforcement, Trusted Network Communications, Verschlüsselung	Container isoliert die Daten (privat und geschäftlich) klar voneinander
Auralis	iOS	zentrale Verwaltung, Patch-Updates über Mobilfunkschnittstelle	Lock-Funktionalität, zentrale Definition von Policys, Verschlüsselung	keine Datentrennung
Sophos	iOS, Android, Blackberry, Symbian, Windows Phone, Samsung Safe	zentrale, rollenbasierte Verteilung und Verwaltung von Apps, AV-Funktionalität, Quarantänezone	IT-Compliance, Lock-Funktionalität, Content-Management, Verschlüsselung	App-Management, Bereitstellung von Apps für Benutzer oder Gruppen, keine Datentrennung
AppTec 360	iOS, Android, Windows Phone, Samsung Safe, Samsung Knox	Cloud-Lösung zur zentralen Verwaltung, Patch-Management, Inventarisierung, AV-Funktionalität	Wiederherstellen der Daten auf neuem Gerät, Lock-/Asset-Funktionalität, Verschlüsselung	App-Management, verschlüsselte Container, Kioskmodus

Vergleich verschiedener MDM-Systembeispiele

wenigen Lösungen angeboten. Dabei könnte man durch den Einsatz unterschiedlicher Container beide Welten voneinander isolieren und die Gefahr für das Unternehmen gering sowie die Flexibilität für den Nutzer hoch halten. Auch die sichere Verschlüsselung der mobilen Daten oder eine Integritätsüberprüfung des Endgerätes ist noch kein Funktionsstandard.

Neben der Benutzerverwaltung und der zentralen Software- und Policy-Verteilung sollte auch die Hardware vom jeweiligen MDM-System auf Sicherheit überprüft werden. Dies ist beim BizzTrust-Ansatz in *Bild 2* mithilfe des Trusted Computing realisiert worden, indem eine Verschlüsselung eingesetzt und das Endgerät über einen TNC/MAP-Server abgefragt wird. Solange dies nicht der Fall ist, kann auch ein laufendes AV-System das Kompromittieren von Endgeräten nicht verhindern. Um zusätzlich die Integrität des Endgerätes sicherstellen zu können, müssten entsprechende TPM-Chips (Trusted Computing Module) verbaut sein. Diese sind aber in heutigen Smartphones Mangelware, da die Hersteller und Provider vornehmlich den Consumer-Massenmarkt adressieren.

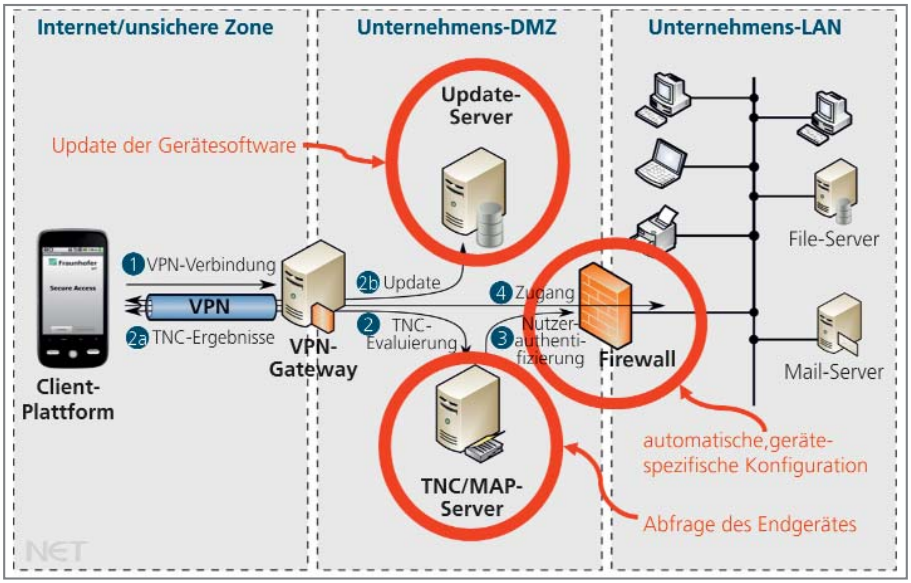

Bild 2: Funktionsweise von BizzTrust (1 – Nutzer verbindet sich mit dem VPN, 2 – Evaluierung der Client-Konfiguration via TNC, 2a – Bitte updaten/OK, 2b – Update der Client-Software, 3 – Server erhalten Nutzerinfos, 4 – User kann auf Dienst zugreifen) (Quelle: www.bizztrust.de)

Fazit

MDM-Lösungen sind in relativ großer Vielfalt vorhanden. Aber längst nicht alle erfüllen die Anforderungen zur Absicherung der vorhandenen Smartphone- und Tablet-PC-Hardware. Der Fokus liegt in den meisten Fällen auf der zentralen Verwaltung mit entsprechenden Softwareupdates, die es dem IT-Administrator ermöglichen sollen, der mobilen Geräteschar Herr zu werden. Zwar bringt die kontinuierliche Aktualisierung von Betriebssystemen und Apps eine erhöhte IT-Sicherheit – die Hardwareintegrität oder Betriebssystemlücken werden aber nach wie vor außen vor gelassen, weshalb vorhandene Schutzmaßnahmen immer noch ausgehebelt werden können.

Ein weitere Frage ist, ob das zukünftige MDM-System in die vorhandene Verwaltung von Client- und Serversystemen integriert oder als separates System betrachtet werden soll. Wie hier vorgestellt, gibt es eine Reihe an Speziallösungen, die sich ausschließlich um mobile Endgeräte kümmern und losgelöst von vorhandenen Managementlösungen implementiert werden müssen. Die Marktführer im Bereich Client- und Serverlösungen sind bisher noch nicht so weit, geeignete mobile Lösungen anbieten zu können. Firmen, die sich ausschließlich auf mobile Endgeräte und deren Vielfalt an Betriebssystemen spezialisiert haben, scheinen momentan im Vorteil zu sein. *(bk)*