LANline

9,– €

Januar 2014
20. Dezember 2013

ITP VERLAG

IT ■ Netze ■ Infrastruktur www.lanline.de

Client-Management

Consumerization und Android-Sicherheit

User-Orientierung

Desktops as a Service

Mit Marktübersicht Thin Clients

MDM-Test Baramundi BMS 8.9
Mobilgeräte komplett integriert verwalten

Infrastructure as a Service
Kriterien für die IaaS-Auswahl

Sonderdruck für Baramundi

MDM-Test Baramundi BMS 8.9

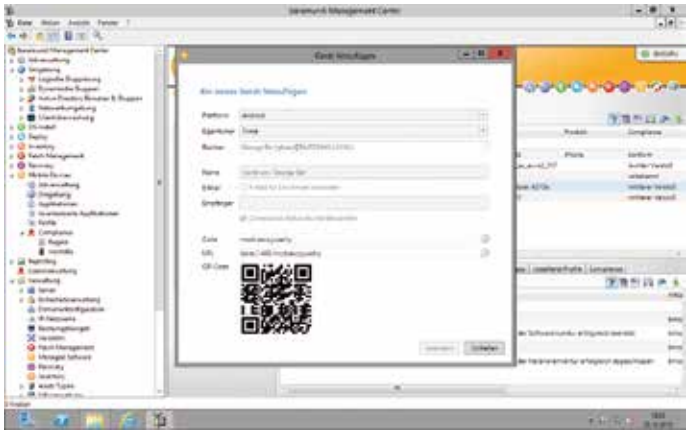
Mobilgeräte komplett integriert verwalten

Tablets, Smartphones und andere Mobile Devices sind aus dem Geschäftsleben nicht mehr wegzudenken. Wer sich als IT-Verantwortlicher mit der Verwaltung der vielen unterschiedlichen Systeme auseinandersetzen muss, braucht die passende Software. Gut, wenn diese komplett in das Client-Lifecycle-Management (CLM) eingebunden ist wie bei der Baramundi Management Suite.

Administratoren sehen die rasante Verbreitung der mobilen Endgeräte eher skeptisch denn euphorisch. Der Grund für die Zurückhaltung liegt in der Sorge begründet, dass die vielen kleinen Computer, die sich mit dem Unternehmensnetzwerk verbinden, als Gefahr für die Stabilität erweisen könnten. BYOD (Bring Your Own Device) – die oft in den Medien genannte Flexibilität der Benutzer, ihre eigenen Geräte ins Büro mitzubringen – ist mancherorts nicht einmal durch eine Betriebs- oder Dienstvereinbarung gedeckt und wird dennoch munter betrieben. Wenn jeder seine Arbeitsgeräte künftig mitbringt, so eine oft gehörte Meinung, könne es der Unternehmensleitung ja nur recht sein, das spare schließlich Geld.

Die IT jedoch muss den immer bunteren Gerätepark verwalten und überwachen. Es gilt, unerwünschte Apps zu entdecken und den Benutzer zu motivieren, dass betreffende Programm zu löschen. Allerdings sollen dem Anwender wichtige Programme möglichst ohne Aufwand zur Verfügung stehen, sofern die Geräte nicht durch eine Rooted- oder Jailbreak-Firmware ein Sicherheitsrisiko darstellen. Das Sperren und gezielte Löschen der Geräte über die Verwaltungskonsole stehen ebenfalls auf der Wunschliste der Administratoren.

Das Augsburger Unternehmen Baramundi hat im Gegensatz zur Mehrheit der Marktbegleiter nicht den eher einfacheren Weg über die Integration einer Speziallösung gewählt, sondern ein komplett selbstentwickeltes MDM in seine Client- und Server-Management-Suite integriert. Administratoren und IT-Support-Mitarbeiter sind in diesem Fall nicht gezwungen, zwischen den beiden Management-Welten zu wechseln: Die Verwaltung von PCs, Thin Clients, Servern und Mobilgeräten erfolgt mit der Baramundi Management Suite (BMS) über eine einzige Plattform. Während die Software ausschließlich als MMC unter Windows arbeitet, ist das Modul „Baramundi Mobile Devices“ in der Lage, Systeme mit Apple IOS ab Version 5, Android 2.2 und höher sowie Windows Phone 8 anzusprechen und zu verwalten. Unterstützung für Blackberry oder Symbian gibt es nicht.



Für das Enrollment (Neuaufnahme) nutzt die Software einen QR-Code, um die notwendigen Konfigurationseinträge einzulesen.

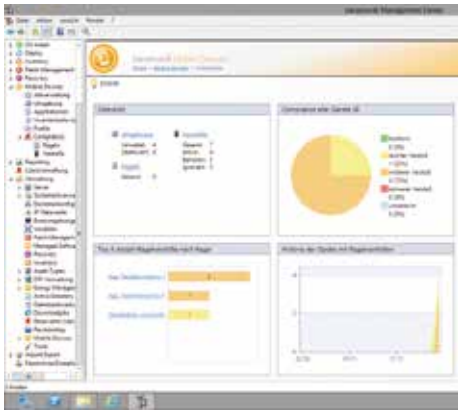
Einrichtung auf dem Server

Da „Mobile Devices“ lediglich einen Zweig in der MMC der Suite darstellt, muss das Grundsystem auf einem aktuellen Windows Server 2008 SP2 oder höher mit Microsoft SQL Datenbank bereits installiert sein, um die Funktionalität nutzen zu können. Für den Test setzten wir eine vorinstallierte virtuelle Maschine des Herstellers mit der aktuellen BMS-Version 8.9 auf Basis eines Windows Server 2012 ein.

Damit Mobilgeräte über die jeweiligen Push-Dienste auf das System zugreifen können, mussten wir eine der beiden virtuellen Netzwerkkarten mit der DMZ verbinden. Den externen Router galt es im Anschluss so zu konfigurieren, dass er die TCP-Ports 2195, 2196, 5223, 443 und 5228 bis 5230 von der festen IP-Adresse auf die NIC weiterleitet. Der erste Konfigurationsschritt ist die Sicherstellung, dass eine Certificate Authority (CA) die zur IP-Adresse passenden Zertifikate ausstellt. Dies erfolgt über die Verwaltung im Zweig „Mobile Devices“ und über die IIS-Verwaltungskonsole. BMS verfügt zwar über einen eigenen Web-Service, jedoch ist die IIS-Verwaltungskonsole für die Konfiguration der SSL-Kommunikation nutzbar. Das Zertifikat ist, sofern man IP-Adresse oder Hostname verändert, neu auszustellen – ein Vorgang, der nur wenige Minuten dauert.

Zur Speicherung von Apps auf dem lokalen Server muss der Administrator nun einige Verzeichnisse anlegen und die Pfade der Software bekanntmachen. Es folgt die Erzeugung eines Apple-Push-Zertifikats. Dieses muss der Administrator auf der Apple-ID-Seite unter „APN CSR“ erstellen und die erzeugte bCert-Datei an Ba-

ramundi mailen. Die Datei wird von Baramundi als so genanntem MDM-Vendor signiert und zurückgeschickt. Dieses Zertifikat wird nach zwölf Monaten seine Gültigkeit verlieren. Deshalb ist es beruhigend zu wissen, dass die MDM-Software bereits drei Monate vor dessen Ablauf die Verlängerung oder Erneuerung anmahnt.



Eine grafische Übersicht erleichtert die Kontrolle der Einhaltung von Compliance-Regeln.

Für Android-Apps reichen die Anlage eines Pfads und die Erstellung eines Google-Code-Accounts. Zur Verwaltung von Windows Phones muss der Administrator lediglich einen Dateipfad für die Apps anlegen und darin einen Baramundi-Agent im XAP-Format abspeichern.

Wie kommt der Client auf das System?

Bevor auch nur eine einzige Regelung oder Prüfung mit einem mobilen Endgerät stattfinden kann, gilt es, die Client-Komponente auf dem Endgerät zu installieren. Das Procedere variiert je nach Hersteller ein wenig. Für Android- und Apple-Geräte muss der Benutzer oder der Administrator den „Baramundi Mobile Agent“ über die jeweilige Store-Plattform herunterladen. Folglich ist bereits an dieser Stelle die Verwendung einer ID für Apple oder Google erforderlich, da sonst kein Zugriff auf den Store zulässig ist. Apple begrenzt die Anzahl von Geräten pro Apple ID auf zehn Systeme. Sofern ein Administrator in seinem Unternehmen weniger Systeme betreut, wäre grundsätzlich eine zentrale Verwaltung durch die IT denkbar. Da dies in der Realität selten der Fall sein dürfte, ist im Fall von BYOD ein Zusammenspiel zwischen der IT und dem Gerätebesitzer erforderlich.

Auf Windows Phone 8 müssen Benutzer oder Administrator in den Einstellungen im Zweig „Unternehmens-Apps“ den Server-Namen oder die IP-Adresse sowie den Active-Directory-Benutzernamen des Besitzers eingeben. Die Installation der Agent-Software beginnt nach der Eingabe. Wer MDM ohne Microsoft Exchange einsetzt, wird in diesem Dialogfenster möglicherweise Lehrgeld in Form von Zeitverlust durch „Trial and Error“ zahlen. Nur wenn im AD das Feld „E-Mail“-Adresse mit einem gültigen Wert gefüllt ist, beispielsweise login@domäne, kann ein Windows-Phone-8-Client sich mit dem AD verbinden.

Ist der Agent installiert, muss unter Android noch sichergestellt sein, dass der Agent als „Geräteadministrator“ definiert ist. Aktuelle Android-Versionen setzen das notwendige Häkchen in den Einstellungen automatisch, ältere Android-2.x-Geräte benötigen hier möglicherweise eine Benutzeraktion. Mit dem Setzen des Häkchens erlaubt der Besitzer der App, alle Gerätedaten zu löschen, das Passwort zum Entsperren des Displays zu ändern, die Passwortregeln festzulegen, das Display selbst zu sperren und Zugriffsversuche zu protokollieren.

An dieser Stelle sind alle MDM-Lösungen, die mit Android arbeiten, auf die Zusammenarbeit mit dem Benutzer angewiesen. Deaktiviert dieser die Option, so ist die MDM-Software machtlos. Damit – darauf haben wir schon im Zusammenhang von Tests anderer MDM-Lösungen schon verwiesen – entspricht das Sicherheitskonzept der heutigen Mobilsysteme eher dem Stand bei Desktops zu Windows-9x-Zeiten.

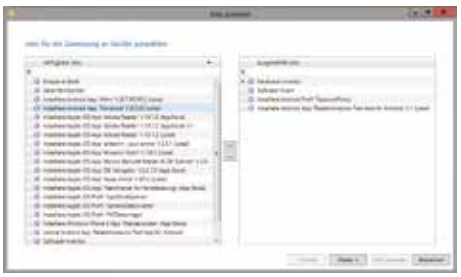
Zur Integration der Geräte auf dem Server klickt der Administrator auf den Aktionsbefehl „Gerät hinzufügen“. Nun möchte die Software wissen, um was für eine Geräteplattform es sich bei dem neuen Client handelt und welchem AD-Benutzer dieser zuzuweisen ist. Eine weitere und entscheidende Frage folgt: Gehört das neue Gerät der „Firma“ oder handelt es sich um ein „Privat“-Gerät? Diese Information ist spätestens dann von Bedeutung, wenn es darum geht, die Inhalte über den „Wipe“-Befehl komplett aus der Ferne zu löschen.

Anschließend zeigt die Software einen zusammenfassenden Dialog an, der einen Code und einer URL für die Konfiguration des Agents anzeigt. Praktischerweise ist in dem Dialogfenster auch ein QR-Code, der URL und Code gemeinschaftlich repräsentiert. Die Agent-Software bietet die Möglichkeit, über die im Gerät eingebaute Kamera diesen QR-Code einzulesen. Anschließend ist die Verbindung zum Management-Server eingerichtet.

Testgeräte und Inventardaten

Nach gut zwei Stunden hatten wir unsere Testgeräte – ein Nokia Lumia 620 mit Windows Phone 8, ein Apple Iphone 4S mit IOS 7, ein Samsung Galaxy Tab 2 P3110 mit Android 4.1.2 und ein älteres HTC Explorer A310 mit Android 2.3.5 – mit dem MDM-Client ausgestattet und für jeden fiktiven Besitzer eines Geräts einen Benutzer im AD angelegt. Der Agent bietet auf jeder Plattform identische Funktionen: die Anzeige, ob das Gerät sich „compliant“ (regelkonform) gegenüber den Richtlinien verhält, einen Info-Button zur Anzeige der Softwareinformationen sowie den „Kiosk“, über den der Anwender bereitgestellte Programme auf Wunsch selbsttätig herunterlädt.

Die Server-Software selbst besteht aus mehreren Zweigen in der MMC. In der Übersicht zeigt die Konsole alle derzeit verwalteten Geräte, deren Status und Informationen zur Hardware an. Wer sich intensiver mit den Hardwaredaten auseinandersetzen möchte, wird sich darüber freuen, dass sich die Ansicht per Mausklick zu Excel exportieren lässt. Neben



Der Administrator kann mehrere Jobs gleichzeitig losschicken.

der wichtigsten Information, der IMEI-Nummer, listet die Hardware mehr als 50 weitere Parameter auf. Eigene Variablen kann der Administrator in der Verwaltung anlegen, beispielsweise für Informationen wie das Kaufdatum oder die Kostenstelle.

Der Zweig „Applikationen“ bietet dem IT-Verantwortlichen die Möglichkeit, in Abhängigkeit zur Plattform Programme bereitzustellen. Für IOS und Windows Phone besteht dies in der Auswahl einer App über den jeweiligen Store oder das Einbinden einer Installationsdatei über das Dateisystem. Für Android beschränkt sich die Funktionalität auf die Auswahl von lokalen APK-Dateien. Insgesamt erklärt sich die App-Verwaltung weitgehend von selbst und ist intuitiv in der Bedienung.

Das Wipe-Kommando kann die Software auch automatisch versenden.

Die Lizenzverwaltung lizenzpflichtiger Apps beschränkt sich auf das Setzen des Status auf „verbraucht“ oder „frei“. Baramundi unterstützt das „Volume Purchase Program“, über das Unternehmen IOS-Lizenzen für kostenpflichtige Programme gesammelt für Mitarbeiter erwerben. Die Profilverwaltung, die notwendigen Grundeinstellungen für ein Gerät hinsichtlich seiner WLAN-Einstellungen, Sicherheitsparameter wie notwendige Passcodes, die Sperre von Speicherkarten oder die Erlaubnis, die Gerätekamera zu verwenden, ist in der aktuell vorliegenden Version noch an externe Programme gebunden. Für IOS kommt das bekannte Iphone-Konfigurationsprogramm von Apple zum Einsatz, für die anderen Systeme Baramundis „Configuration Utility“. Das als Datei erzeugte Profil wird in die Management-Software importiert. In der kommenden Version, so versicherte uns der Hersteller, wird es diese Teilung nicht mehr geben. IT-Verantwortliche konfigurieren dann die „Mobile Profiles“ direkt aus der Management-Konsole.

Jobs und Compliance

Die Applikations- und Profilbereitstellung geschieht über die so genannte Jobverwaltung. Hier kann der Administrator jedem Gerät Aufgaben zuweisen und diese über eine Intervallsteuerung automatisieren. Eine Softwareinventur ist beispielsweise ein lohnendes Ziel für eine wiederkehrende Aufgabe. Ob ein Job ausgeführt wird oder nicht, kann der Administrator von der Erfüllung eines Compliance-Status abhängig machen.

Um eine App unter Android zuzuweisen, muss der Benutzer möglicherweise die Sicherheitseinstellungen seines Geräts anpassen, da in der Standardeinstellung eine Installation aus „unbekannter Herkunft“ nicht zulässig ist. Dies ist jedoch keine funktionelle Einschränkung, die Baramundi anzulasten wäre – sie liegt an der Android-Plattform im Allgemeinen. Eher unschön ist jedoch der Umstand, dass in der MDM-Datenbank der Eintrag gespeichert wird, der Benutzer hätte die Installation der App abgebrochen. Die Agent-Software macht den Besitzer darauf aufmerksam, dass eine Installation oder ein Update ansteht.

Die möglicherweise wichtigste Ansicht ist jedoch der Zweig „Compliance“. Über selbst definierbare Regeln – wie beispielsweise „Software XYZ darf nicht auf einem Gerät vorhanden sein“ – stellt der Administrator sein Regelwerk in einer Wizard-gestützten, selbsterklärenden Oberfläche zusammen. Bei der Anlage einer Regel wählt er zunächst aus, ob es sich um eine App-Beschränkung, eine Rooting/Jailbreak-Kontrolle, eine OS-Versionsprüfung oder um eine Regel zur Zeitspanne von Inventarisierungsaufträgen handelt. Jede Regel ist nach demselben Schema gestrickt: Er muss die Bedingung festlegen, die Zielplattform angeben und die dazugehörige Reaktion aus der Jobauflistung wählen. Denkbare Szenarien sind: „Entdeckt der Agent einen Jailbreak auf einem Iphone, so wird das Gerät automatisch gelöscht“; oder, weniger dramatisch: „Ist das Tablet schon seit mehr als drei Tagen nicht mehr in Verbindung getreten, so markiere dies als ‚leichten Verstoß’.“

Wie bei allen MDM-Plattformen, kommt es zu gewissen zeitlichen Abweichungen, abhängig davon, wie ausgelastet die Push-Dienste der Plattformhersteller sind. Wer also einen Job losschickt, darf sich nicht wundern, wenn dieser nicht sofort zur Ausführung kommt, dabei können schon einmal einige Minuten vergehen.

Fazit

Das Mobile-Device-Management in der Baramunid Management Suite 8.9 ist eine solide Lösung, die sich nahtlos in die Verwaltung von Servern und Clients einfügt. Die Compliance-Prüfung, das weitgehend problemlose Enrollment mit dem QR-Code und die Intervallsteuerung dürften jedem Administrator gut gefallen. Kleinere funktionale Lücken, die derzeit noch umständliche Workarounds erfordern, will der Hersteller in Kürze geschlossen haben. Der Preis ist nach der Anzahl benötigter mobiler Clients gestaffelt und liegt zwischen zehn und 25 Euro zuzüglich der Basis-Lizenzen für die BMS.

Thomas Bär, Frank-Michael Schlede/wg

Thomas Bär auf LANline.de: **BÄR**

Frank-Michael Schlede auf LANline.de: **Frank-Michael Schlede**

Info: Baramundi
Tel.: 0821/56708-0
Web: www.baramundi.de