Sonderdruck aus COMPUTERWOCHE ONLINE vom 19. September 2013

IDG

COMPUTERWOCHE

www.computerwoche.de

Mobile Device Management mit baramundi

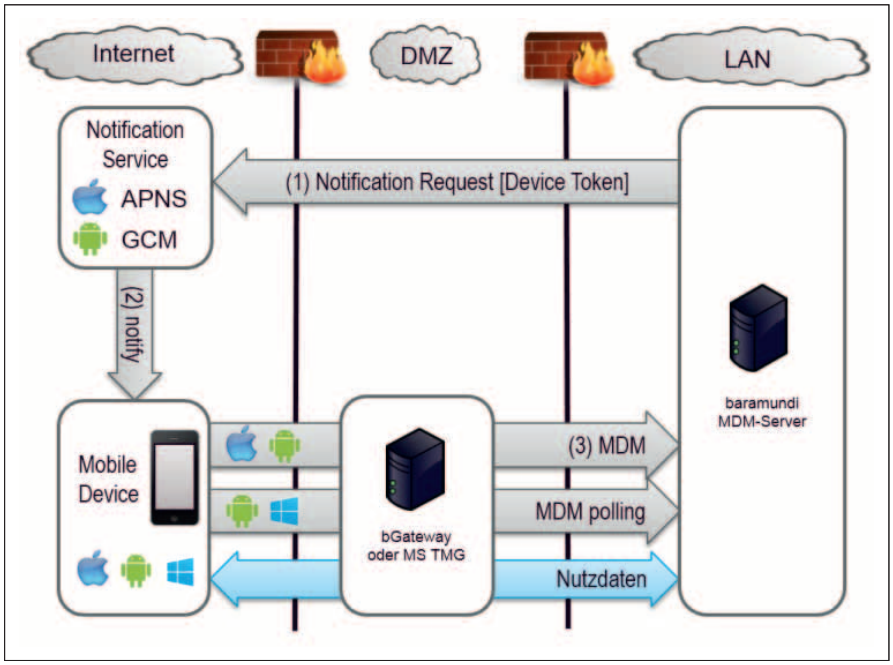
baramundi verwaltet mit seinem Modul für Mobile Device Management (MDM) als Teil seiner Client Management Suite neben iOS- und Android-Geräten nun auch Smartphones mit Windows Phone 8.

Von Andrej Radonic

Angesichts der rasant zunehmenden Nutzung von Smartphones und Tablets in Unternehmen erkennen IT-Abteilungen allmählich die Notwendigkeiten und Herausforderungen der neuen Client-Generation. Diese bringt eine neue Betriebssystem-Vielfalt von Apple iOS über Android, Blackberry bis Windows Phone mit sich, welche spezialisierte Werkzeuge für ein zentrales MDM unumgänglich macht.

Zwei Ansätze kristallisieren sich am Markt heraus: Auf der einen Seite Standalone-Management-Pakete wie AirWatch oder Mobileiron, auf der anderen Seite um MDM erweiterte etablierte Lösungen für netzweites Client- und System-Management.

Den zweiten Ansatz verfolgt die baramundi Software AG aus Ausgburg. Sie erweitert ihre Lösung um baramundi Mobile Devices (bMD) als modularen Bestandteil der umfassenden Verwaltungssoftware baramundi Management Suite. baramundi weitet damit das Client-Lifecycle Management von der Einführung über die Nutzung bis hin zur Löschung konsequenterweise auf Mobilgeräte aus. Mit der kürzlich veröffentlichten Version 8.9 ist neben der Unterstützung für iOS- und Android-Geräte nun auch Support für Windows Phones an Bord.



Die Architektur des baramundi-Systems abstrahiert von den Eigenheiten der Plattform-Anbieter. Foto: baramundi

Systemübergreifende Architektur

Die vorherrschenden mobilen Betriebssysteme sind technisch sehr unterschiedlich gestrickt – dies betrifft beim zentralisierten Management vor allem die Anbindung an den jeweiligen App-Stores sowie die Kommunikation zwischen Serveranwendungen und dem Endgerät. Eine der wesentlichen Aufgaben der baramundi MDM Lösung besteht darin, eine einheitliche Sicht auf diese Systeme zu schaffen – für eine zentrale Verwaltung der Mobilsysteme unter Berücksichtigung der verschiedenen Kommunikationswege, die die unterschiedlichen Anbieter vorsehen.

Im Gegensatz zu normalen PCs im Unternehmens-LAN bewegen sich die mobilen Geräte auch im Mobilfunknetz oder in einem fremden WLAN hinter einer Firewall und sind daher vom Server aus nicht direkt zu erreichen. Daher findet der Verbindungsaufbau immer vom Gerät zum

Die MDM-Funktionen sind nahtlos in das baramundi Management Center integriert. Foto: baramundi

Server statt. So muss nur der eine Management-Server aus dem Internet erreichbar sein, nicht jedes einzelne Gerät vom Server aus. Da aber der MDM-Server alle Vorgänge steuert und daher auch den Verbindungsaufbau auslösen können muss, bieten die Plattformhersteller Apple und Google einen Notification Service in der Cloud an, worüber der bMD-Dienst die mobilen Geräte benachrichtigen kann. Daraufhin meldet sich das Gerät bei seinem zugewiesenen Management Server zurück. Windows Phones können über einen direkten Polling-Mechanismus mit dem bMD-Server in Verbindung bleiben.

Entscheidender Aspekt aus Sicht der Compliance und des Datenschutzes: bMD ist eine On-Premise-Lösung und integriert dabei die Herstellerdienste so, dass keine schützenswerten Daten für die Management-Steuerungen bei den jeweiligen Herstellersystemen landen. Sämtliche Nutzdaten finden auf direktem Weg vom Management Server (und dessen Gateway) hin zum Endgerät.

Zentraler Management-Server

Da der bMD-Service als Modul ausgeprägt ist, wird neben einem Lizenzschlüssel eine Komplettinstallation der baramundi Management Suite als Basis benötigt. Diese setzt einen dedizierten Windows Server (2008, 2008 R2, 2012, 2012 R2) sowie eine Oracle oder MS SQL Datenbank (wird bei Bedarf in einer Express-Variante mitgeliefert) voraus. Zudem stellt der Administrator üblicherweise eine Anbindung an das Active Directory her, damit die Benutzerdaten im baramundi-System verfügbar sind.

Sind diese Voraussetzungen geschaffen, müssen für die Inbetriebnahme des MDM-Moduls einige Basis-Setups durchgeführt werden. Vor allem wird für die Absicherung der Kommunikation ein SSL-Zertifikat benötigt (kann extern eingespielt oder selbst signiert werden), welches im MDM Modul hinterlegt sowie an den jeweiligen Port des MDM-Servers gebunden wird. Der baramundi-Server kann dabei die Rolle der Zertifizierungsstelle (Certificate Authority/CA) übernehmen. Zudem muss ein Gateway eingerichtet werden, damit die Mobilgeräte aus dem Internet mit dem Unternehmens-internen Service kommunizieren können. Hierfür kommt entweder ein baramundi-eigener Dienst auf einem dedizierten Server in der DMZ zum Einsatz, oder der Administrator verwendet einen bereits vorhandenen Microsoft Forefront Service (TMG). Für die Kommunikation mit den Geräten sowie den APIs der Hersteller-Benachrichtigungsdienste sind zudem diverse Ports zu öffnen.

Client Management für Smartphones

Das bMD fügt dem baramundi Management Center den neuen Knoten Mobile Devices zu. Darunter finden sich die bereitgestellten Funktionsbereiche für Jobverwaltung, Übersicht über die Geräteumgebung und die Applikationen, sowie die Profile und die Compliance-Prüfung.

Damit Smartphones und Tablet-PCs verwaltungsmäßig erfasst und remote administriert werden können, wird ein Agent auf jedem Endgerät benötigt. baramundi stellt hierfür in den jeweiligen AppStores den baramundi Mobile Agent (bMA) kostenfrei zur Verfügung. Diese App stellt dem Anwender ein Selbstbedienungs-Portal namens Kiosk zur Verfügung und signalisiert ihm seinen individuellen Compliance-Status.

Erfassung mobiler Geräte

Damit das MDM eine Verbindung zu den Mobilgeräten herstellen kann, müssen diese im ersten Schritt im System registriert werden. Je Device legt der Administrator hierzu zunächst einen neuen Gerätedatensatz an, in welchem er den Gerätetyp, den Besitzer und den Besitzstatus (Firma oder Privat) angibt. Zudem kann das Gerät einem Benutzer aus dem Active Directory zugeordnet werden. Bei Windows Phone ist diese Zuordnung Pflicht, da sie für die Authentifizierung im Rahmen des Enrollment benötigt wird.

Das MDM präsentiert dem Administrator anschließend einen Anmelde-Token sowie einen passenden QR-Code. Am Mobilgerät erfasst er dann in der Anmeldemaske der baramundi App den QR-Code über die Kamera und bestätigt die Geräte-Aktivierung.

Alternativ versendet das MDM-System eine Mail an den Anwender; mit einem Klick auf den Bestätigungslink öffnet sich der Enrollment-Dialog in seiner App, wo er zum Abschließen der Anmeldung nur noch den Aktivieren-Button drücken muss.

Microsoft bietet in Windows Phone 8 ein alternatives Verfahren an: Statt zuerst die bMD App zu laden, kann der Phone-Anwender die seitens Microsoft integrierte Unternehmens-App starten. Von hier aus gibt er die vom MDM vorgegebenen Anmeldedaten an. Danach wird automatisch das sogenannte „Unternehmens-Hub" – der eigentliche baramundi Mobile Agent – geladen und installiert.

Der Enrollment-Prozess installiert ein Konfigurationsprofil auf dem Endgerät, welches unter anderem die Verbindungsparameter und das Sicherheitszertifikat enthält.

Jobs übernehmen Geräte-Verwaltung

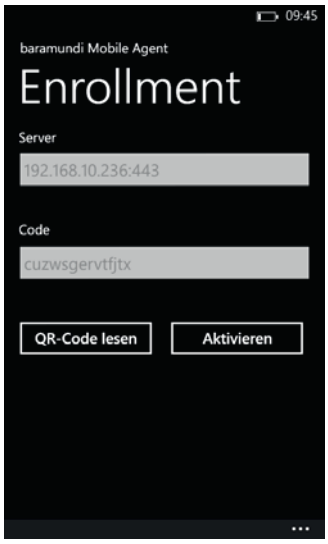
Der MDM-Administrator kann nun mit der eigentlichen Geräte-Verwaltung beginnen. Sämtliche Administrationsbefehle – für das Installieren oder Deinstallieren von Apps oder Profilen, für die Geräte-Sperrung oder -Entsperrung sowie die Inventarisierung – erfasst er dazu als sogenannte Jobs.

In diesen Jobs können Parameter der jeweiligen Aktion konfiguriert werden, so zum Beispiel eine regelmäßige Wiederholung oder welchen Compliance-Grad ein Gerät als Voraussetzung für die Ausführung des Jobs erfüllen muss.

Jobs können wahlweise vom Administrator auf Geräte zugewiesen oder dem Benutzer im Kiosk zur Verfügung gestellt werden, beispielsweise als Liste empfohlener Mobil-Anwendungen, die der Anwender bei Bedarf selbst installieren kann.

Während das Definieren und Ausführen von Jobs vom bMD im Management Center einheitlich gestaltet und geregelt ist, bieten die Geräte-Hersteller sehr unterschiedliche Steuerungsmöglichkeiten, z.B. beim Installieren und Deinstallieren von Apps:

- Bei Appes iOS müssen App-Installationen immer vom Benutzer bestätigt werden. Das System erlaubt ausschließlich die Deinstallation von Apps, die im MDM registriert sind. Benutzer-Apps können nicht entfernt werden.
- Android erfordert immer eine Bestätigung des Benutzers für Installation und Deinstallation.
- Windows Phone erlaubt keine App-Deinstallation durch MDM-Systeme, jedoch können Installationen wahlweise auch ohne Benutzerinteraktion durchgeführt werden.



Anmeldevorgang am baramundi Server auf einem Windows Phone 8. Foto: baramundi

Verfügbare Jobs werden dem mobilen Benutzer in der baramundi App im Kiosk-Bildschirm signalisiert und können von ihm mit einem Tap ausgelöst werden, sofern eine Benutzeraktion notwendig ist.

Geräte-Inventarisierung verschafft automatisierten Überblick

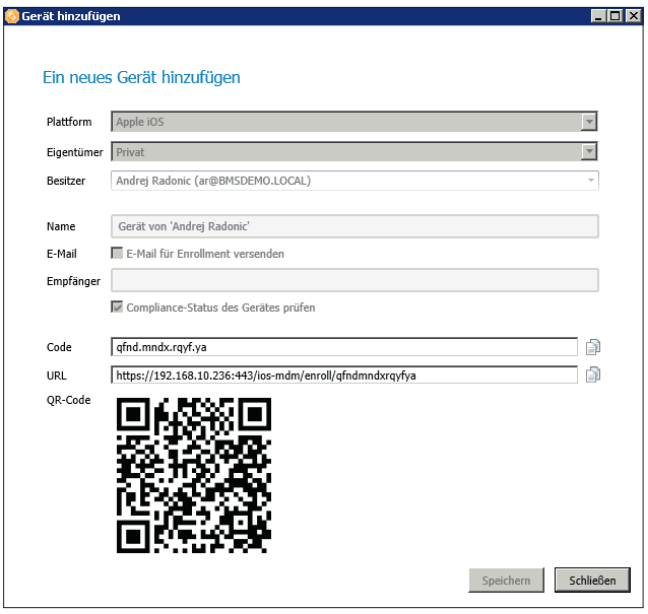
Für sämtliche administrativen Aufgaben benötigt der baramundi-Systemadministrator genaue Informationen über die in den zu verwaltenden Geräten verbaute Hardware, die installierten Softwarepakete (Apps) sowie die auf den Devices vorhandenen Einstellungen.

Für diese Zwecke nutzt er die automatische Inventarisierung des MDM. Sie erfolgt getrennt für Hardware und Software als Job-Ausführung und kann in vorgegebenen Abständen automatisch wiederholt werden, um zwischenzeitliche Veränderungen zu erfassen. Die Inventarisierung kann automatisch nach einem Geräte-Enrollment erfolgen oder zu beliebigen Zeitpunkten manuell ausgelöst werden. Der Inventarisierungsprozess wird dem Geräte-Benutzer im Kiosk als Job signalisiert.

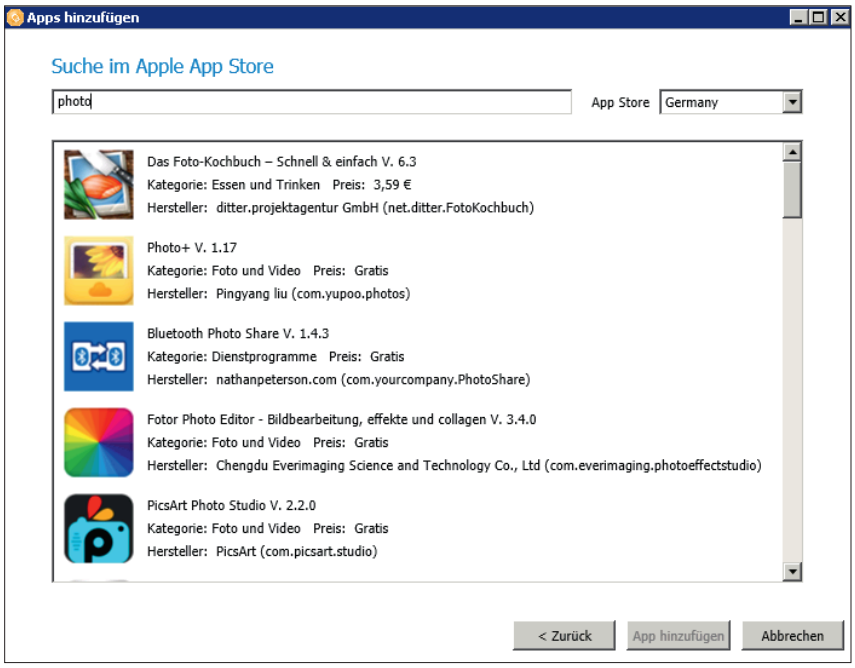
Zentrale App-Verteilung trifft auf uneinheitliche Gerätefunktionen

Bevor Applikationen an mobile Geräte verteilt werden können, müssen die Apps dem System erst einmal bekannt sein. Der Administrator hat bei iOS- und Windows-Phone-Geräten zwei Alternativen zur Verfügung: Entweder er lädt diese direkt aus den jeweiligen App-Stores über die in bMD integrierte App-Suche direkt auf den baramundi Management Server. Unternehmens-Apps, die über den App-Store nicht zur Verfügung stehen, muss er dagegen zunächst in das MDM importieren und kann sie dann wie gewohnt verteilen.

Im Gegensatz dazu erfordert die Verteilung von Android-Apps immer lokal verfügbare Quellen in Form von apk-Dateien. Der einfachste Weg, diese zu beschaffen, besteht



Ein neues Mobilgerät kann mit wenigen Handgriffen im baramundi-System angemeldet werden. Foto: baramundi



Apps können über die integrierte App-Store-Suche dem Managementsystem hinzugefügt werden. Foto: baramundi

darin, die gewünschten Apps auf einem Smartphone zu installieren und sie anschließend mit einem Tool wie App-Saver als apk-Dateien auf die SD-Karte zu sichern, um sie von dort aus in das bMD-Ablageverzeichnis zu kopieren.

Eine wichtige Rolle bei der App-Verteilung kommt der Software-Inventarisierung zu: Das baramundi-Managementsystem unterscheidet strikt zwischen denjenigen Apps, die es auf einem Gerät vorfindet, und den Apps, die es selbst im zentralen Repository versammelt hat: So können bei iOS nur solche Apps deinstalliert werden, die auch über den bMD installiert wurden.

Remote Konfiguration über Profile

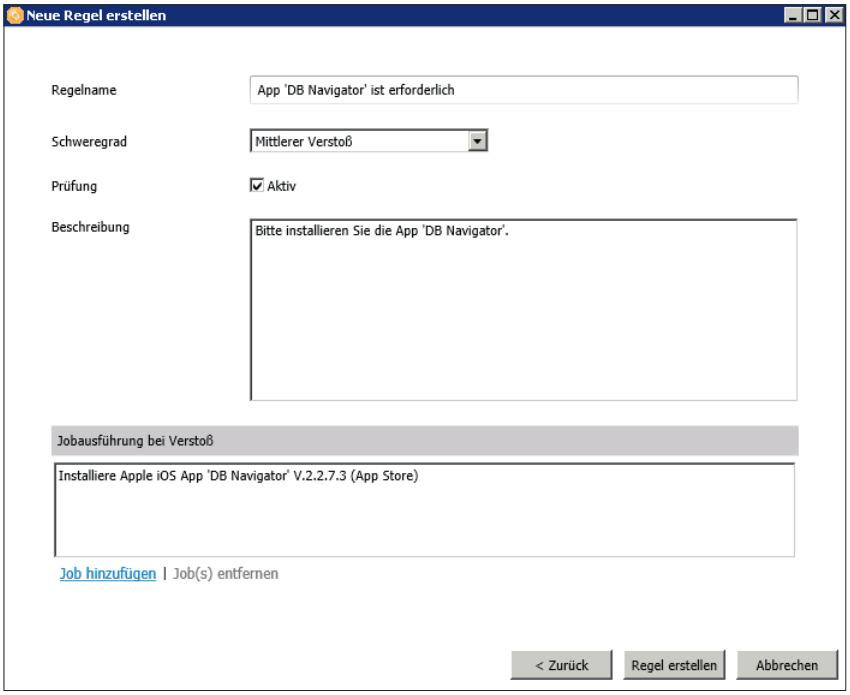
Profile sind Sammlungen von Mobilgeräteeinstellungen, welche als Konfigurationspaket an ein Mobilgerät übertragen und eingerichtet oder von diesem gelöscht werden können. Während geräteseitig teilweise durchaus weitgehende Möglichkeiten vorgesehen sind, z.B. die Vordefinition von WLAN-Verbindungen, das Sperren von System-Apps wie Youtube und Siri, sind auch hier wieder die Möglichkeiten sowie die Art der Profilgenerierung stark vom jeweiligen System abhängig. Windows Phone bietet dabei die wenigsten Optionen. So kann etwa die Kamera bei iOS und Android deaktiviert werden, bei Windows nicht.

Profile rollt der Administrator ebenfalls über Jobs aus. Um diese zu erstellen, muss er die gewünschten Konfigurationen mit einem betriebssystemspezifischen Tool erstellen, als Datei speichern und vor der Generierung des jeweiligen Jobs importieren. Für iOS-Handys wird das iPhone-Konfigurationsprogramm von Apple benutzt. Für Android und Windows Phone stellt baramundi das baramundi Configuration Utility bereit.

Automatisierte Überwachung der Compliance

Wichtigste Aufgabe des Mobil-Administrators ist, für einen korrekten, regelkonformen Gerätestatus zu sorgen. Hierbei hilft ihm das Herzstück des baramundi MDM: das Compliance Dashboard. Es verhilft automatisiert zu einem umfassenden und aktuellen Überblick über wichtige Einstellungen, installierte Apps und ihre Versionen sowie die

Die baramundi Software ermöglicht im Compliance Dashboard einen aktuellen Überblick über die Konformität der Mobilgeräte im Unternehmen. Foto: baramundi



Über eine Compliance Regel lässt sich sowohl ein bestimmter Versionsstand einer App prüfen als auch deren Einhaltung durchsetzen – durch eine automatische Installation der App. Foto: baramundi

Einhaltung definierter Regeln, z.B. das Verbot von Jailbreaks.

Die gewünschten Benchmarks legt der Administrator als Regelsatz im System an. Die Einhaltung der betreffenden Regeln wird vom Server in definierbaren Abständen sowie immer dann neu geprüft, wenn sich durch neue Gerätedaten der Compliance-Zustand eines Gerätes verändert hat.

Als Resultat erhält er im Dashboard eine aktuelle Ansicht des momentanen Compliance-Zustandes seiner Mobil-Umgebung, mit einer Unterteilung nach dem Schweregrad von festgestellten Verstößen. Von hier aus kann er durch benutzer- oder gerätebezogenen Drilldown den Einzelheiten direkt auf den Grund gehen.

Die Reaktion auf Regelverstöße kann entweder interaktiv durch den Administrator oder vollautomatisch erfolgen, sobald eine Regelverletzung vom System ermittelt wird. Dies ist umso wichtiger, da es je nach Gerätetyp und den darauf zugelassenen oder vorhandenen Funktionen schwierig oder teilweise unmöglich ist, Regelverstöße von vorneherein zu verhindern. Über die Compliance-Prüfung können solche Verstöße zeitnah automatisiert erfasst und Gegenmaßnahmen in Gang gebracht werden. Wurde zum Beispiel ein Jailbreak erkannt, führt das MDM die hinterlegten Gegenmaßnahmen automatisch aus: wahlweise wird das Exchange-Profil entfernt oder alternativ der Geräteinhalt mit einem Remote Wipe gelöscht.

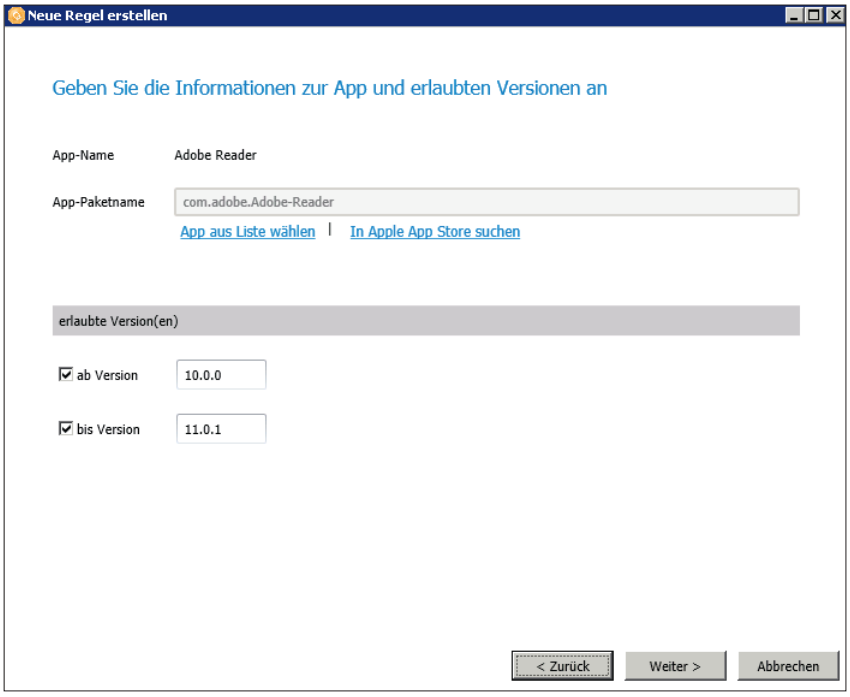
baramundi erlaubt es, bei der Compliance-Regeldefinition nach erwünschten und unerwünschten Apps zu unterscheiden. Die betreffende Regel kann dann sinnvollerweise mit einer passenden Gegenmaßnahme verknüpft werden. Mit diesem Mechanismus ist der Administrator in der Lage, die (teilautomatisierte) Verteilung von Apps zu organisieren. Beispiel: Eine App muss einen Mindest-Versionsstand aufweisen. Ist dies nicht der Fall, wird der User automatisch im Kiosk zur Installation dieser Version aufgefordert. Ein automatisierter Abgleich mit aktuellen Versionsständen in den App-Stores führt bMD allerdings nicht durch.

Über diesen Mechanismus können Unternehmen ebenso ein (indirektes) Blacklisting von Apps mit differenzierten Regeln vornehmen, nämlich anhand diverser Bedingungen wie Version, System, Hersteller, Kategorie und Besitzstatus (Firma versus Privat). Der Anwender wird dann jeweils zur Deinstallation aufgefordert und ein entsprechender Hinweis in der Auswertung angelegt.

In Ergänzung zur Dashboard-Ansicht stehen über die in der baramundi Management Suite standardmäßig installierte Reporting-Engine verschiedene Reports zur Verfügung, um einen umfassenden Überblick über den Geräte- und Compliance-Status zu erhalten.

Kiosk bindet User in Compliance-Durchsetzung ein

Nicht nur der Administrator ist am Compliance-Zustand aller verwalteten Endgeräte interessiert, idealerweise sollten sich auch die Endanwender ein Bild über die Com-



Über den Regel-Typ Versionsprüfung kann automatisiert die Einhaltung vorgegebener App-Versionen überwacht und ... Foto: baramund

pliance des eigenen Geräts machen können. So zeigt der baramundi-Agent dem Benutzer im App-Kiosk alle Regelverstöße an, wie beispielsweise unerlaubte Firmware-Manipulationen oder unerwünschte Apps. Das Wissen über vom MDM festgestellte Regelverstöße erlaubt es dem Endanwender, selbstständig für die notwendigen Korrekturen zu sorgen und damit den vorgeschriebenen Regelzustand wieder herzustellen.

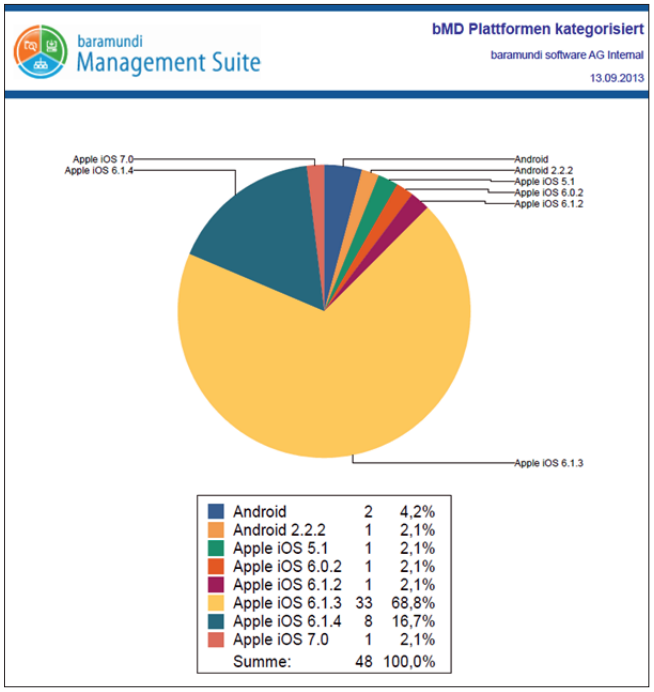
Der Kiosk kann außerdem dafür genutzt werden, dem Endbenutzer eine Auswahl derjenigen Apps zur Verfügung zu stellen, die auf der Whitelist des Unternehmens stehen und damit den eigenen Richtlinien genügen.

Fazit: Weitgehend schlüssig umgesetzt

Der Anspruch der Augsburger, eine kompakte zentrale System-Management-Lösung auf die Beine zu stellen, die das MDM-Thema nahtlos integriert, ist weitgehend schlüssig umgesetzt. Systemadministratoren finden eine sehr umfassende Lösung vor, welche in einheitlicher Weise durch die Unterstützung von Android, iOS und Windows Phone einen Großteil der im Einsatz befindlichen Mobilgeräte zu verwalten mag. Hier schlägt sich die Erfahrung mit zentralisiertem Client-Management auch bei Mobile-Clients nieder. Zudem spricht für baramundi das strikt auf deutsche Rechtsprechung ausgerichtete System. Bei Software von ausländischen Lieferanten ist dies nicht immer gegeben.

Die Kiosk-Funktion ermöglicht geräteübergreifend den Anwendern einen Überblick über Gerätestatus und verfügbare Apps. Foto: baramundi

baramundi hat nach eigenem Bekunden dabei nicht den Anspruch, jedes Feature-Battle gegen Wettbewerber zu gewinnen. So fehlen einige Features, die man anderweitig vorfindet wie beispielsweise Policies für den externen Mobilzugriff auf das Unternehmensnetz. Negativ bei der



... bMD Reports liefern detaillierte Übersichten über die Mobilgeräte-Umgebung. Foto: baramundi

baramundi-App für iOS fällt auf, dass die Standort-Bestimmung aktiviert sein muss, was laut Hersteller jedoch ab iOS 7 nicht mehr der Fall sein wird.

Die Probleme und Schwächen von MDM generell liegen derzeit eher in den Mobil-Betriebssystemen selbst begründet - hier fehlen außer zahlreichen weitergehenden Management-Features in den jeweiligen APIs zudem auch Standards, um MDM-Systemen das Leben leichter zu machen und für mehr Durchgängigkeit, Sicherheit und Compliance bei der Mobilgeräte-Ausstattung zu sorgen.

Aufgrund des Modul-Charakters dürfte die Lösung vor allem für baramundi-Bestandskunden interessant sein sowie für Unternehmen, welche auf der Suche nach einer allumfassenden Client-Management-Software sind.

Lizenzen und Preise

baramundi Mobile Devices kann als Erweiterungsmodul der baramundi Management Suite erworben werden. Der Lizenzpreis für das Paket bemisst sich nach den gewählten Modulen sowie der Anzahl der verwalteten Clients (PC, Server, Mobilgeräte). Den Preis nennt der Hersteller auf Anfrage. Berechnungsbeispiel: Für 500 verwaltete Clients und einer Auswahl von gängigen Modulen ergibt sich ein Lizenzgesamtpreis von rund 20.000 Euro.

Sonderdruck aus COMPUTERWOCHE ONLINE für

baramundi software AG

Beim Glaspalast 1
86153 Augsburg

Telefon: +49 (821) 5 67 08 - 380
E-Mail: request@baramundi.de
www.baramundi.de

baramundi
software AG