

IT Administrator

Das Magazin für professionelle System- und Netzwerkadministration

Sonderdruck für baramundi

Im Test:

baramundi Management Suite 2014



**Im Test:** baramundi Management Suite 2014

Client-Management modular und mobil

von Jürgen Heyer



Die Anforderungen an eine Managementsoftware für Clients wachsen rasant und zudem in zwei Richtungen: Zum einen werden immer mehr Zusatzfunktionen nachgefragt wie ein Schwachstellenmanagement oder eine Schnittstelle zu einer Helpdesk-Lösung, zum anderen stehen nicht mehr nur Desktops und Server im Fokus, sondern auch mobile Geräte. IT-Administrator konnte sich davon überzeugen, dass die neue Version 2014 der baramundi Management Suite dementsprechend vielseitig ausgerichtet ist.

Ein entscheidendes Plus der baramundi Management Suite ist der modulare Aufbau, der es einem Unternehmen erlaubt, zur Minimierung der Kosten und Vermeidung von Ballast genau die Komponenten aus dem breiten Funktionsumfang auszuwählen, die es benötigt. So führt der Hersteller insgesamt 18 Module auf, aus denen sich die Suite zusammensetzt, beginnend bei der Betriebssysteminstallation über die Softwareverteilung und Applikationskontrolle, Patchmanagement sowie Backup bis hin zur Gerätekontrolle, Fernsteuerung und Datensicherung.

Mit der aktuellen Version 2014 der Management Suite hat sich Baramundi von den bisherigen Versionsnummern – die vorherige Version war die 8.9 – verabschiedet und den Funktionsumfang nochmals erweitert. Nun gibt es ein automatisiertes Schwachstellenmanagement für Clients und Server sowie ein integriertes Mobile-Device-Management (MDM) sowie einen erweiterten Patch-Umfang. Neu gestaltet wurde auch die Benutzeroberfläche.

Gerade für den Einstieg interessant ist die Möglichkeit, womöglich mit nur einem Modul und wenigen Clients zu beginnen und dann Schritt für Schritt zu wachsen.

baramundi unterscheidet bei der Lizenzierung nicht zwischen Arbeitsplätzen und Servern. Jedes Modul ist zudem einzeln bepreist und erlaubt so einen kostengünstigen Einstieg.

Da es im Rahmen eines solchen Tests unmöglich ist, alle Funktionen einer derart mächtigen Suite eingehend zu betrachten, haben wir uns in erster Linie auf die genannten Neuerungen konzentriert.

Durchdachte Systemarchitektur und Kommunikation

Von baramundi erhielten wir für den Test eine vorkonfigurierte virtuelle Maschine mit Windows Server 2012 R2 und der baramundi Management Suite. Unterstützt werden die Windows Server-Versionen ab 2008 SP2. Analog zu einer typischen Kundeninstallation waren auch bei uns nur die Module installiert, die wir im Vorfeld ausgewählt hatten. Die für die Datenhaltung benötigte Datenbank SQL Server 2012 war mit auf dem System eingerichtet. Der Hersteller gibt an, dass für bis zu 300 verwaltete Systeme auch die SQL-Express-Version verwendet werden kann. In einer größeren Umgebung mit vielen Clients ist die Datenbank auf einem getrennten Server zu betreiben.

Jedes zu verwaltende Windows-Gerät benötigt einen installierten Dienst, den baramundi Management Agent. Grundsätzlich kontaktiert der Server den Agenten und nicht umgekehrt. Die Softwareverteilung erfolgt von einem Datei-Depot, dem so genannten Distribution Installation Point (DIP), wobei es sich hier letztendlich um eine Installationsfreigabe handelt. Der Agent ist in der Windows-Taskleiste sichtbar.

baramundi Management-Server für zirka 500 zu verwaltende Zielsysteme.

Hardware

Aktueller Prozessor (Dual- oder Quad-Core, je nach Rechneranzahl), mindestens 2 GByte Arbeitsspeicher (4 GByte empfohlen), wenigstens 1 GByte Festplattenplatz für die BMS-Installation sowie zusätzlich Platz für die zu verteilenden Betriebssysteme, Patches und Applikationen (etwa 10 bis 15 GByte).

Software

Als Betriebssystem eignen sich Windows Server 2008 R2 SP1, 2008 SP2, 2012 und 2012 R2. Die PowerShell und das .NET Framework 4.51 sind Voraussetzung. Für die baramundi-Datenbank kommt MS SQL Server 2012 SP1, 2008 R2 SP2 oder 2008 SP3 (im gemischten Modus) in Frage; bei bis zu etwa 300 verwalteten Geräten auch MS SQL Express. Außerdem Oracle ab Version 11 gR2 mit jeweils aktuellem Service Pack.

Systemvoraussetzungen



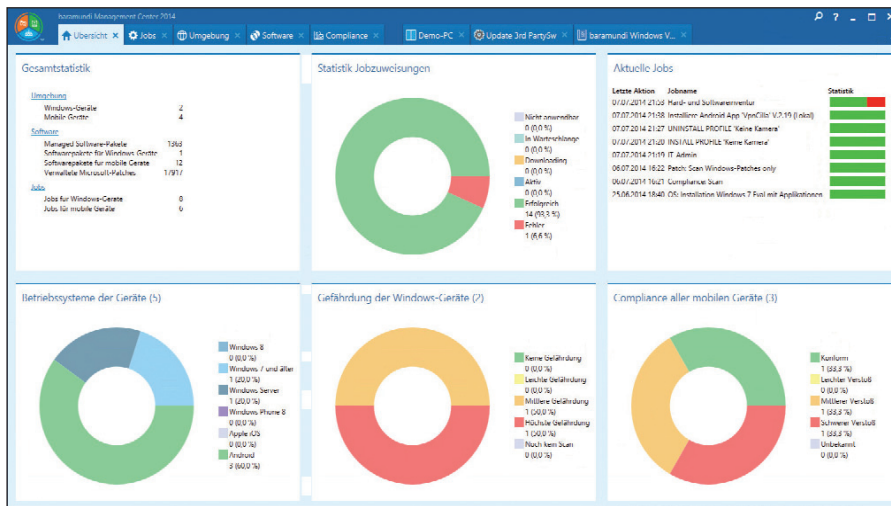


Bild 1: Die Hauptübersicht der Management Konsole liefert über mehrere Bereiche hinweg die wichtigsten Eckdaten zum Status der Umgebung.

bar. Über das Kontextmenü sind verschiedene Informationen abrufbar, über den Punkt "Software-Kiosk" kann der Anwender vom Administrator bereitgestellte Softwareprodukte einrichten. Der Agent kommuniziert mit dem Server über verschiedene Ports für unterschiedliche Zwecke wie CIFS, RDP, VNC, Server Push, Job Transfer und Agenteninstallation. Die meisten der genutzten Ports sind durch den Administrator änderbar.

Bei mobilen Geräten erfolgt die Kommunikation über HTTPS, der Standard-Port 443 ist auch hier umkonfigurierbar. Zu weiteren Details kommen wir später bei der Beschreibung des MDM. An dieser Stelle sei nur erwähnt, dass im mobilen Umfeld im Gegensatz zum Client-Agenten immer das mobile Gerät den Server kontaktiert, da der Server schlichtweg nicht wissen kann, wo sich ein mobiles Gerät befindet. Daher muss der baramundi Server für diese Geräte aus dem Internet erreichbar sein. Da er aber aufgrund seiner Steuerfunktionen durchaus ein attraktives Angriffsziel darstellt und vor fremdem Zugriff geschützt werden muss, lässt sich das so genannte baramundi Mobile Gateway (BMG) zwischenschalten, das am besten in einer DMZ installiert wird. Dieses reicht die Anfragen weiter, schottet den baramundi Server aber ansonsten gegenüber dem Internet ab. Alternativ wird noch das Microsoft Threat Management Gateway (TMG) unterstützt, das aber bereits abgekündigt ist.

Ansprechende Benutzeroberfläche

Die Benutzeroberfläche der Suite besteht aus einer grafischen Oberfläche, dem baramundi Management Center 2014. Dieses wurde optisch an das Design von Windows Server 2012 angepasst. Die einzelnen Themengebiete wie Übersicht, Jobs, Umgebung, Software und Compliance sind als Registerblätter mit Reitern am oberen Rand angeordnet, lassen sich aber auch durch einen Klick auf das Management-Center-Logo links oben als seitliches Menü auflisten.

Die Register erlauben ein paralleles Arbeiten und den schnellen Wechsel zwischen den Aufgaben. Auf jedem Registerblatt befindet sich auf der linken Seite ein Menü mit den einzelnen Haupt- und Unterpunkten. Im Kopfbereich eines je-

den Blatts kann der Administrator auf einen Blick erkennen, wo er sich in der Menüstruktur befindet. Auf einer Übersichtsseite (Dashboard) lassen sich die wichtigsten Informationen auf einen Blick einsehen. Nicht vorgesehen ist es, diese Ansicht individuell anzupassen.

Mobile Geräte einfach integrierbar

Eine wichtige Neuerung der aktuellen Suite ist die Erweiterung um ein Mobile Device Management (MDM). baramundi hat sich entschieden, das MDM selbst zu entwickeln und in vollem Umfang in die Suite zu integrieren, statt eine vorgefertigte Lösung zu verwenden. Dabei fiel uns gleich zu Beginn auf, dass sich das MDM wirklich gleichberechtigt zur normalen Desktopverwaltung einfügt und vom Prinzip her auch identisch zu bedienen ist, sodass niemand umdenken muss, wenn er zwischen den Aufgaben springt. Das MDM unterstützt Systeme mit Apple iOS ab Version 5, Android 2.2 und höher sowie Windows Phone 8. Blackberry wird nicht unterstützt.

Sichere Einrichtung kostet Zeit

Etwas Arbeit bereitet es, den Server so vorzubereiten, dass er mit den mobilen Geräten kommunizieren kann. Dies wiederum ist für alle drei genannten Betriebssysteme zu erledigen. Wie schon eingangs erwähnt, kann der Server ein mobiles Gerät nicht direkt erreichen. Vom funktionalen Ablauf her bedient sich der baramundi Server daher bei Windows Phone 8 des Windows Stores sowie bei iOS und Android des Apple beziehungsweise Goo-

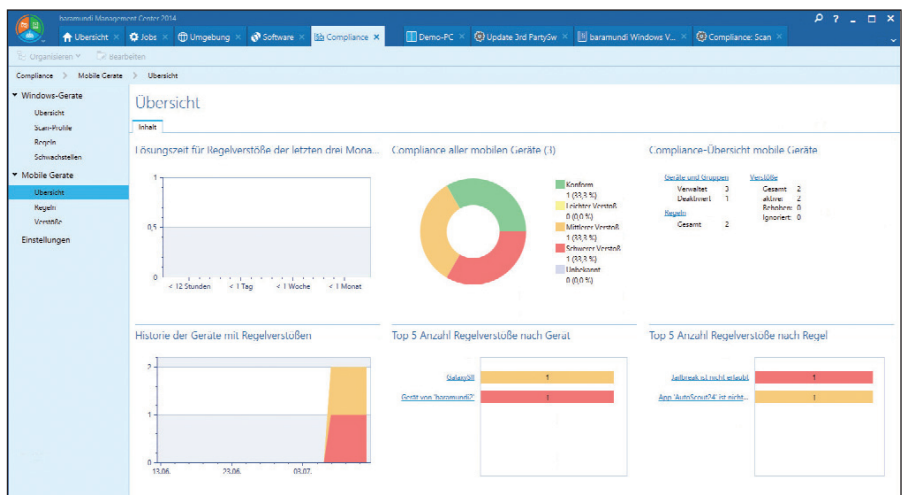


Bild 2: In einer Übersicht präsentiert die BMS die wichtigsten Ergebnisse getrennt für mobile Geräte und Windows-Systeme.

Bild 3: Die sichere Aufnahme eines neuen mobilen Gerätes gelingt mittels QR-Code erfreulich einfach.

gle Push Services, um ein mobiles Gerät darüber zu informieren, dass es sich beim Server melden soll. Damit dies funktioniert, muss der Server oder das oben erwähnte BMG aus dem Internet über einen FQDN erreichbar sein, was sich beim Fehlen einer festen IP-Adresse mit einem DynDNS-Eintrag realisieren lässt.

Außerdem ist der Port 443 für HTTPS (oder ein anderer gewählter Port) über den DSL-Router zum baramundi Server beziehungsweise zum BMG weiterzuleiten. Um die Sicherheit zu gewährleisten, arbeitet die Suite mit Zertifikaten. Dazu muss der Administrator in der Konfiguration der Suite über eine Certificate Authority (CA) ein Zertifikat erstellen, das zum FQDN passt, dieses speichern und anschließend über die IIS-Verwaltungskonsolle für die SSL-Kommunikation einspielen. Nach einem Neustart des Management Servers ist dieses aktiv. Zu beachten ist, dass das Zertifikat nur dann passt, wenn über den FQDN zugegriffen wird. Sollten also in einem Unternehmen mobile Geräte sich sowohl über das Internet melden als auch aus einem internen Netz wie einem WLAN, so ist beispielsweise

ein Proxy einzusetzen, damit die internen Geräte den gleichen FQDN verwenden können.

Komfortable Erfassung per QR-Code

Damit der Administrator Apps verteilen kann, muss er diese auf dem baramundi Server in einem entsprechend angelegten Verzeichnis speichern. Weiterhin benötigt er bei Apple ein Push-Zertifikat, das er auf der Apple-IP-Seite erstellen kann. Dieses muss er dann noch von baramundi signieren lassen. Einfacher geht es bei Android, wo der Administrator einen Google Code-Account anlegen muss, sowie bei Windows Phone, wo es reicht, im App-Dateipfad einen baramundi-Agenten im XAP-Format zu speichern.

Ist der baramundi Server soweit für das MDM vorbereitet, sind noch die aufzunehmenden mobilen Geräte vorzubereiten. Bei Apple und Android ist dazu über den jeweiligen Store der baramundi Mobile Agent zu installieren, bei Windows Phone 8 sind der Servername und der Active Directory-Benutzername anzugeben, um so das Agentensetup zu starten. Ist der jeweilige Agent installiert, geht es nun noch darum, das Gerät beim

baramundi Server zu registrieren, was der Hersteller hervorragend einfach realisiert hat. Dazu muss der Administrator in der baramundi Management Konsole auf dem Registerblatt "Umgebung" den Punkt "Logische Gruppierung" anwählen und dann über das Kontextmenü und den Punkt "Neu" ein mobiles Gerät hinzufügen. Nach Auswahl der Plattform, der Eigentümervorgabe "Firma" oder "Privat" und der Vergabe eines Gerätenamens wird auf dem Monitor ein QR-Code angezeigt, der nur noch mit Hilfe des Agenten auf das mobile Gerät gescannt werden muss. Schon ist das Enrollment erledigt. Wahlweise verschickt der Server eine E-Mail mit dem QR-Code, sofern der Empfänger beziehungsweise das Gerät nicht vor Ort ist.

Im Test hatten wir ein Apple iPad sowie mehrere Android-Geräte (Samsung Galaxy SII, Samsung Tab 2 und Tab 3) zur Verfügung, die wir nach den beschriebenen vorbereitenden Schritten in kürzester Zeit aufnehmen, um dann wie nachfolgend beschrieben einige Jobs laufen zu lassen. Dabei fiel uns auf, dass es für einen Anwender problemlos möglich ist, sein mobiles Gerät wieder der Steuerung durch die BMS zu entziehen. So trägt sich der Agent bei der Installation als Geräte-Administrator ein, wobei der Anwender dieses Haken problemlos entfernen und dann auch den Agenten wieder deinstallieren kann. Es ist also stets eine Kooperation zwischen Administrator beziehungsweise Unternehmen und Anwender notwendig.

Nicht näher eingehen wollen wir auf die Aufnahme von normalen Arbeitsplätzen, was schon lange Bestandteil der Suite ist. Zu beachten ist allerdings, dass nur Windows-Systeme unterstützt werden und kein Linux.

Einfache Steuerung über Jobs und Profile

Das Einstellen von Tätigkeiten erfolgt bei der Suite über Jobs und Aktionen. Beim Anlegen eines Jobs muss der Administrator zuerst auswählen, ob es sich um einen Job für mobile Geräte oder für Windows-Systeme handelt. Typische Aktionen für Windows-Geräte, wie Software verteilen,

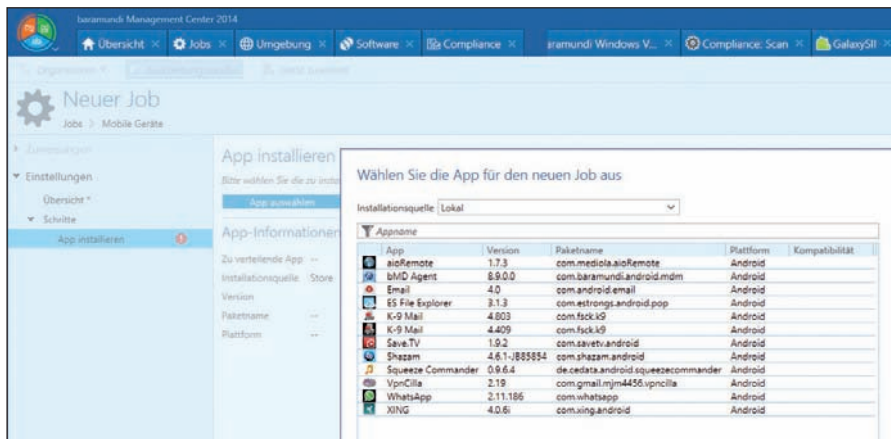


Bild 4: Auf Wunsch verteilt BMS mobile Applikationen, Voraussetzung ist aber, dass das Installieren aus unbekannten Quellen erlaubt wird.

Compliance Scan durchführen oder Energierichtlinie verteilen, sind bereits in großer Zahl vorbereitet. Bei den Mobilgeräten gibt es wesentlich weniger mögliche Aktionen. Hier beschränkt sich das Programm auf die Bereiche App-Verwaltung, Profilverteilung, Inventarisierung und Geräteoperation. Ist ein Job definiert, wird er den Geräten zugewiesen, um so die Ausführung zu veranlassen.

Uns fiel auf, dass die GUI für die Jobdefinition für mobile Geräte dem neu gestalteten Design entspricht, während die Suite beim Job für Windows-Geräte in die bisherige Optik wechselt. Auch ist der funktionale Ablauf etwas unterschiedlich. Das hängt damit zusammen, dass der Server wie schon beschrieben ein mobiles Gerät nicht direkt erreichen kann, sondern den Umweg über den Push-Dienst nehmen muss. Sobald sich der Agent mit dem Server verbunden hat, bekommt er die Jobinformationen übermittelt. Daraufhin führt das mobile Gerät den Job aus und meldet dem Server das Ergebnis.

Sehen wir uns nun die Jobs und Aktionen für mobile Geräte genauer an. Während bei den Windows-Geräten ein Job aus mehreren Schritten bestehen kann, enthält ein Job für mobile Geräte nur eine Aktion, also beispielsweise Apps installieren oder deinstallieren. Die Suite bietet dann die Applikationen zur Installation an, die im oben bereits erwähnten Installationsverzeichnis abgelegt sind. Die Auswahl der Apps lässt sich hier nachträglich ändern, aber nicht die gewählte Aktion. Sollte dies notwendig sein, ist stattdessen ein neuer

Job anzulegen beziehungsweise der nicht mehr benötigte zu löschen. Damit sich eine App installieren lässt, muss der Anwender die Installation aus unbekannten Quellen erlauben, da dies am App Store vorbeiläuft. Das birgt ein gewisses Risiko in sich, da ein Anwender dann auch nicht mehr vor anderen unbekannten Installationsquellen gewarnt wird.

Jobs lassen sich regelmäßig wiederholen und der Administrator kann die Ausführung vom Compliance-Status abhängig machen. Je nach Unterstützung des mobilen Betriebssystems lässt sich das Gerät aus der Ferne sperren, entsperren oder auch löschen. Weiterhin kann eine serverseitige Aktion in Form eines Skripts gestartet werden.

Für die Änderung der Sicherheitseinstellungen und der Gerätekonfiguration dienen die Profile. Hier geht es dar um, beispielsweise die App-Installation zu unterbinden oder die Kameranutzung zu sperren. Auch hier hängen die Möglichkeiten von dem Betriebssystem des Gerätes ab. Dies sind beispielsweise 14 Optionen bei iOS und nur eine bei Android (Kamera verbieten) sowie Windows Phone (SD-Karte deaktivieren). Erfreulicherweise lassen sich aber bei Android die Samsung KNOX-spezifischen Einstellungen steuern (15 Optionen). Im Test definierten wir probeweise einige Einschränkungen wie das Deaktivieren der Kamera sowie die erneute Aktivierung. Dies funktionierte problemlos.

Die Profile dienen auch dazu, Sicherheitsrichtlinien hinsichtlich der Passwortnutzung

zu definieren, die Konfiguration für ein Exchange-Konto zu verteilen sowie dem Anlegen von Wifi- und VPN-Definitionen.

Umfassende Schwachstellenanalyse

Mit der aktuellen Version ist für die BMS ein Compliance Management verfügbar, das sich für Windows-Systeme und mobile Geräte etwas unterschiedlich darstellt. Im Fall der Windows-Systeme handelt es sich um einen Schwachstellenscanner, der unter anderem Registry-Einträge sowie Dateien und deren Eigenschaften überprüft. Zum einen geht es dar um, potenzielle Schwachstellen aufzuzeigen, zum anderen lässt sich damit prüfen, ob eingespielte Patches wirklich gegriffen haben.

Auch können nachträgliche Änderungen, die womöglich eine Schwachstelle wieder öffnen, erkannt werden. Die BMS enthält dazu eine Regeldatenbank, die sich wiederum des offenen OVAL-Repositories (Open Vulnerability and Assessment Language) bedient. Zum Testzeitpunkt enthielt die Datenbank über 6.200 Einträge. Zu jeder Schwachstelle kann der Administrator umfassende Informationen nachlesen, auch sind der Schweregrad, eine Referenz für weitere Informationen sowie gegebenenfalls ein Lösungsvorschlag angegeben. Nach einem Scan der Client-Systeme werden die erkannten Schwachstellen aufgelistet.

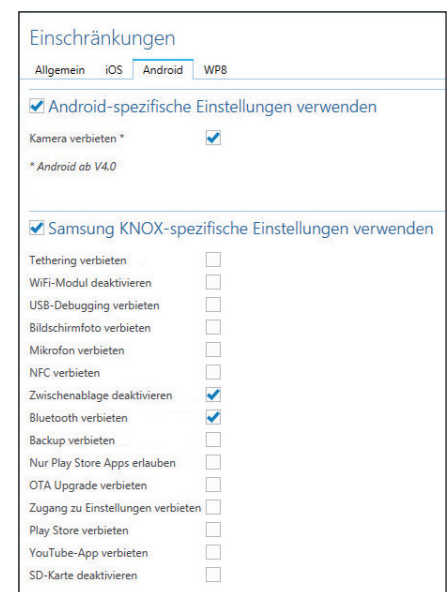


Bild 5: Bei den weit verbreiteten Android-Geräten von Samsung kann die BMS auch die KNOX-spezifischen Einstellungen ändern, was eine Vielzahl an Optionen eröffnet.



Eine Compliance-Übersicht enthält in verschiedenen Diagrammen die wichtigsten Informationen inklusive einer Top 5-Liste der am meisten betroffenen Systeme sowie eine Top 5-Liste der am häufigsten gefundenen Schwachstellen.

Für die mobilen Geräte stellt sich die Compliance-Prüfung etwas anders dar. Hier geht es nicht um allgemein bekannte Schwachstellen, sondern um Regeln, wie ein Gerät konfiguriert sein soll. Dazu muss der Administrator Vorarbeit leisten und zuerst einmal entsprechende Regeln definieren. Dies kann eine unerwünschte App sein oder ein unerlaubtes Rooten des Geräts. Auch lässt sich die Betriebssystemversion einschränken oder vorgeben, wie alt die letzte Inventarisierung sein darf. Zu jeder Regel lässt sich ein Schweregrad definieren, was insofern wichtig ist, da beispielsweise die Ausführung von Jobs von einem Compliance-Verstoß eines bestimmten Schweregrads abhängig gemacht werden kann.

Sind entsprechende Regeln festgelegt und die mobilen Geräte darauf geprüft, finden sich die gefundenen Verstöße in einer Liste. Nicht ganz einfach ist verständlicherweise die Beseitigung der vielfältigen Schwachstellen, manche lassen sich auch gar nicht direkt beheben. Zumindest aber sind die unterschiedlichen Module der BMS wie das Patchmanagement sowie die Softwareverteilung, aber auch das gezielte Ausführen von individuellen Skripten eine wertvolle Hilfe.

Bezüglich des Patchmanagements wurde die Suite übrigens in der aktuellen Version hinsichtlich der Microsoft-Updates erweitert. So können nun neben Sicherheitspatches auch funktionale Updates, zum Beispiel für Office-Produkte, verteilt werden. Damit verdoppelt sich die Zahl der verfügbaren Patches auf rund 13.000. Neue Patches werden schnellstmöglich am Microsoft-Patchday über die BMS bereitgestellt.

Sympathisch offen nach außen

Entgegen manch anderer Suiten, die versuchen, durch proprietäre und schlecht dokumentierte Schnittstellen den Verkauf weiterer Produkte aus dem eigenen Haus zu pushen, gibt sich baramundi weltoffen. So kann ein Administrator die Inventarisierung von baramundi auch dafür nutzen, um beliebige Daten anderen Anwendungen zur Verfügung zu stellen, wenn es beispielsweise darum geht, ein Lizenzvertragsmanagement, ein Asset Management oder ein Helpdesk-System anzubinden.

So besitzt die aktuelle Version der Suite mit "bConnect" eine moderne REST-Schnittstelle auf Basis von HTTPS. Die Vorteile liegen in einer sicheren SSL-Verbindung und der damit verbundenen serverseitigen Authentifizierung sowie der Authentifizierung des Clients per Zugangsdaten. Als Datenformate werden JSON und XML unterstützt. Diese Schnittstelle ermöglicht beispielsweise die Integration der BMS mit der Helpdesk-Software OTRS. Bereits in der Vergangenheit ließen sich die Helpdesk- und Li-

zenzmanagement-Lösungen von USU, Omninet, MIT Solutions sowie Aspera anbinden.

Aus der Kombination mit einer ITSM- und Helpdesk-Lösung ergeben sich vielfältige Ansätze. So können Client-Daten wie die Konfiguration der Rechner direkt im Helpdesk-Tool genutzt werden. Dadurch kann der Support beispielsweise erkennen, ob ein bestimmter PC die Hardwareanforderungen an die installierte oder zu installierende Software überhaupt erfüllt. Der Administrator kann

Produkt

Modulare Software zum Client-Management.

Hersteller

baramundi software AG
www.baramundi.de

Preis

Die baramundi Management Suite wird auf Client-Basis entsprechend der benötigten Module lizenziert. Beispielsweise kostet das MDM-Modul einmalig maximal 25 Euro pro Gerät zuzüglich einer Grundlizenz, das Schwachstellenmanagement höchstens 15 Euro. Für größere Mengen gibt es jeweils Staffelpreise.

Technische Daten

www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator (max. 10 Punkte)

Funktionsumfang der Suite	8
Management von Windows-Systemen	8
Management von mobilen Geräten	7
Compliance-Prüfung	8
Schnittstellenintegration	9

Die Details unserer Testmethodik finden Sie unter www.it-administrator.de/testmethodik

Dieses Produkt eignet sich

optimal für Unternehmen, die eine große Anzahl an Windows-Clients sowie viele mobile Geräte zu versorgen haben.

bedingt für Organisationen, die neben Windows-Clients auch diverse Linux-Systeme zu pflegen haben.

nicht für sehr kleine Betriebe, die bereits ein anderes Client-Lifecycle-Management im Einsatz haben.

baramundi Management Suite 2014

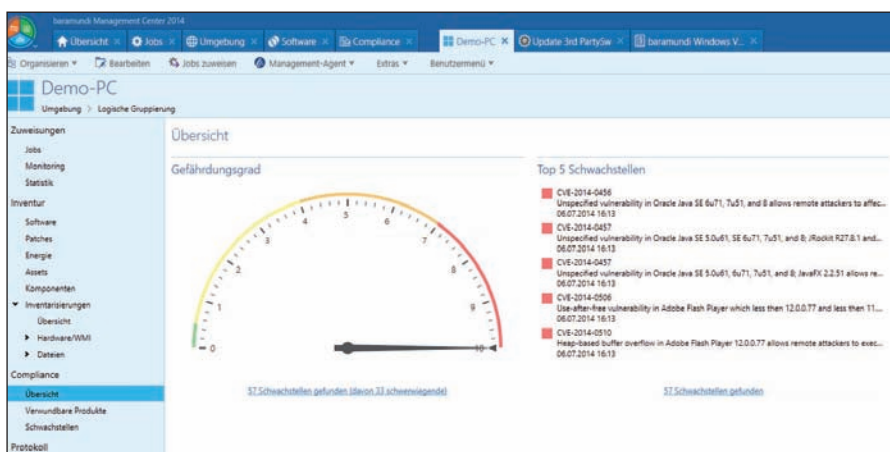


Bild 6: Die Schwachstellenübersicht liefert ein schnelles Ergebnis zur aktuellen Situation und weist auf die wichtigsten gefundenen Schwachstellen hin.



zudem komplette baramundi-Jobs vorbereiten, um etwa einen neuen Client oder häufig benötigte Software zu installieren, und dem Support die Ausführung zugänglich machen.

Weiterhin lässt sich die REST-Schnittstelle leicht in alle gängigen Sprachen, aber auch in Microsoft Office einbinden. Zusätzlich lassen sich viele Aktionen der BMS beispielsweise über VBScript und das Command Line Interface (CLI) automatisieren. Ein weiteres Plus ist die vollständige Dokumentation und Offenlegung der SQL-Datenbank. Alle Tabellen und Spalten sowie deren Schlüssel und Beziehungen zu anderen Tabellen werden ausführlich beschrieben, sodass es auch möglich ist, direkt auf die Datenbank zuzugreifen.

Eine Session-basierte HTTP-Schnittstelle ist httpMOC, die primär lesenden Zugriff auf wesentliche Objekte der BMS erlaubt und die Daten im XML-Format bereitstellt. Die baramundi Management Object Language ermöglicht den Zugriff auf die wesentlichen Objekte der BMS mittels einer Hochsprache

wie beispielsweise VBScript. Der Zugriff basiert auf einem veröffentlichten COM-Interface, sodass auch nahezu jede beliebige andere Programmiersprache verwendet werden kann.

Abschließend ermöglicht die BMS einen einfachen Import und Export per XML, darüber hinaus können die Listenansichten der HTML-Oberfläche nach Excel exportiert und dort weiterverarbeitet werden. Mittels geeigneter Excel-Skripte können aber auch Informationen an die BMS übergeben werden.

Fazit

Mit der Erweiterung der baramundi Management Suite um ein Mobile Device Management und eine Schwachstellenanalyse hat baramundi auf jeden Fall den aktuellen Bedarf getroffen. Nun ist es möglich, aus einem Werkzeug heraus nicht nur die PC-Systeme, sondern auch Smartphones und Tablets zu verwalten. Das MDM prüft die Geräte auf Compliance, sperrt bei Bedarf Funktionen, überwacht die installierten Apps und nimmt gegebenenfalls Änderungen vor. Gut ge-

fallen hat uns die nahtlose Integration des MDM in die Suite, wozu baramundi alles selbst programmiert und sich nicht fertiger Bausteine anderer Hersteller bedient hat. Als sehr wichtig sehen wir im produktiven Umfeld den Einsatz des Mobile Gateways, um den baramundi Server vor Angriffen aus dem Internet zu schützen.

Als sehr interessant erachten wir auch die Schwachstellenanalyse für die PC-Systeme als sinnvolle Ergänzung zum Patchmanagement, um die Geräte umfassend absichern zu können. So gelingt eine Prüfung und Beseitigung aus einem Werkzeug heraus. Gut gefallen haben uns die vielfältigen Schnittstellen zur Anbindung von Software anderer Hersteller wie beispielsweise an Helpdesk-Lösungen oder zur eigenen Auswertung.

Sehr von Vorteil ist der bewusst modulare Aufbau der Suite, der es einem Unternehmen erlaubt, klein einzusteigen und die Nutzung gegebenenfalls später zu erweitern. Entsprechend modular ist auch die Preisgestaltung, die einen Einstieg ebenfalls attraktiv macht. (ln) 