LANline

9,– €

Dezember 2015
24. November

ITP VERLAG

IT ■ Netze ■ Infrastruktur www.lanline.de

Private Cloud und Hybrid Cloud

Siegeszug des „Sowohl … als auch“

Datenschutzkonforme SaaS-Nutzung

Mit Marktübersicht Cloud-Integratoren

Neue Testserie Client-Management
Teil 1: Baramundi Management Suite

Hochverfügbarkeit für Industrie 4.0
Zukunftsszenarien werden Realität

Sonderdruck für Baramundi
Security im Fokus

Testserie Client-Management, Teil 1: Baramundi

Security im Fokus

Client-Management-Suiten umfassen heutzutage Werkzeuge für beinahe alle täglichen Belange der Endgeräte-Administration. So hat der Augsburger Anbieter Baramundi, mit dem wir die neue Testserie der LANline beginnen, seine Management Suite um einen Schwachstellenscanner und eine automatisierte Prüfung des Sicherheitsstatus erweitert.

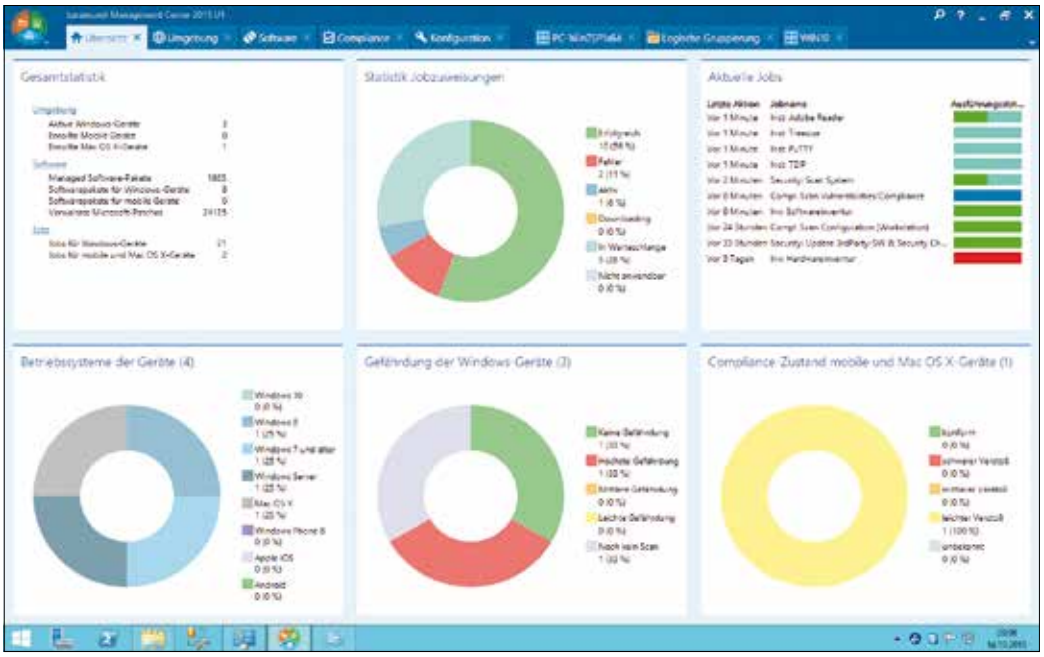
Die Baramundi Management Suite (BMS) ist eine klassische, modular aufgebaute Client-Management-Software für Unternehmen verschiedener Größen. BMS deckt den typischen Lifecycle von Windows-PC-Clients, Windows-Servern und Mobilgeräten ab: von der automatisierten Erstinstallation über die Inventarisierung, Softwareverteilung, Patch-Management, Lizenzüberwachung, Personal Backups, Fernwartung und weitere Support-Aufgaben bis hin zur automatischen Datenlöschung am Ende des Client-Lebenszyklus. Neben Windows-Clients unterstützt BMS auch Mac OS X, jedoch mit reduzierten Client-Management-Basisfunktionen.

Noch recht jung ist das Modul für das Schwachstellen-Management in BMS, vom Hersteller etwas irreführenderweise „Compliance-Management“ genannt. Die Integration eines Schwachstellenscanners in eine Client-Management-Software ist ein logischer Schritt: Während es in sehr großen Unternehmen spezielle Abteilungen gibt, die sich mit der IT-Security auseinandersetzen, dürfte die Mehrheit des deutschen Mittelstands das Thema IT-Sicherheit eher als „Mitaufgabe“ für die Administration definiert haben.

Gegen Sicherheitslücken helfen Antivirusprogramme und Firewall-Systeme nur bedingt, wenn die Fehler im Programm selbst stecken. Laut einer Untersuchung von Kaspersky dauert es durchschnittlich 64 Tage, bis Unternehmen kritische Sicherheitslücken schließen. Derlei Schwachstellen sind jedoch kein Geheimnis: Experten publizieren entdeckte Fehler in Datenbanken, die auf OVAL (Open Vulnerability and Assessment Language) setzen. Doch auch potenzielle Angreifer nutzen diese Informationsquellen. So ist es kaum verwunderlich, dass die Anzahl insbesondere gezielter Angriffe tendenziell zunimmt, obwohl eine adäquate Dokumentation von Lücken in OVAL-Repositories die Betriebssicherheit grundsätzlich erhöht.

Wie können IT-Verantwortliche diese Gefahr abwehren? Das ständige Verfolgen von Publikationen zu Sicherheitslücken der unterschiedlichen Quellen und sofortiges Reagieren durch Installation von Security Patches ist kaum zu stemmen. Automatisiert arbeitende Scanner mit vorgefertigten Regelwerken erlauben auch dem weniger in IT-Sicherheit bewanderten Administrator, in seinem Netzwerk eine Sicherheitsüberprüfung durchzuführen. Gibt die Software dann noch Empfehlungen, was der Administrator unternehmen kann, so ist schon viel gewonnen.

Einen solchen Scanner hat Baramundi bereits mit dem Release 2014 in BMS eingefügt und mit dem aktuellen Update überarbeitet. Der Scanner prüft verschiedenste



Die Ergebnisse der Sicherheitsprüfung sind in der Hauptübersicht der Baramundi Management Suite enthalten. Unseren Windows-10-Testrechner zählte BMS jedoch als Windows-8-System.

Einstellungen, beispielsweise Registry-Einträge, Dateien und deren Eigenschaften. Die Software lädt regelmäßig neue Regelwerke von namhaften Quellen über einen eigenen Dienst bei Baramundi herunter und steuert Schwachstellen-Scans auf allen zu verwaltenden Rechnern auf Basis jeweils aktueller Regeln. Somit ist eine kontinuierliche Überprüfung aller Rechner auf bekannte Sicherheitslücken möglich, auch ohne IT-Sicherheitsexperten im eigenen Unternehmen zu beschäftigen.

Für einen Test stellte uns der Hersteller eine vorkonfigurierte virtuelle Maschine auf Basis von Windows Server 2012R2 mit MS SQL 2014 als Datenbanksystem, AD, DNS und DHCP zur Verfügung. Neben dem Server-System selbst dient ein ebenfalls virtualisierter Windows-7-PC als Test-Client. Einen Rechner mit dem aktuellen Windows 10 Enterprise fügten wir im Test ebenfalls hinzu. Diesen identifizierte BMS zwar als Windows-8-PC, ansonsten ließ er sich jedoch normal ansprechen. Hier hatte möglicherweise die Einstellung der Virtualisierungssoftware Auswirkungen auf die Identifikation: In VMware Workstation 11.1.2 wird die VM als „Windows 8 x64“ betrieben.

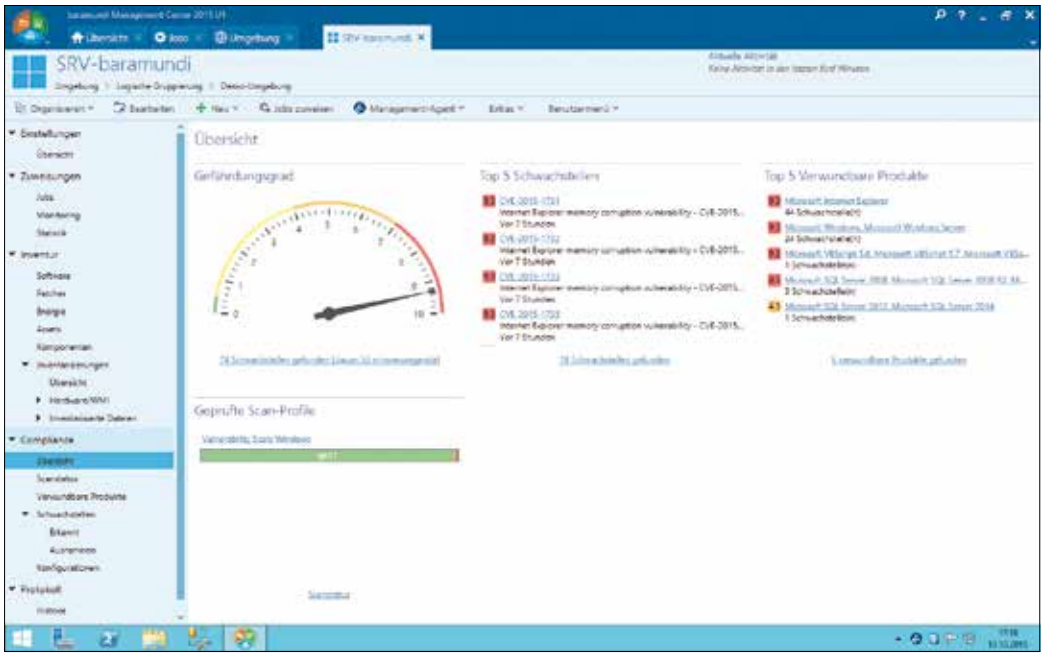
Hallo, Dashboard!

Die Thematik „Compliance“ ist komplett in die BMS-Oberfläche integriert. Administratoren erreichen sie über das Hauptmenü auf der linken Seite. Per Klick gelangt der Anwender auf ein modern gestaltetes Dashboard. Hier zeigt die Software grafisch den aktuellen Gefährdungsgrad der IT-Umgebung an. Dieser bemisst sich nicht etwa an einem rechnerischen Durchschnitt, sondern am Gefährdungsgrad des verwundbarsten Clients. Wie beinahe alle Dashboards, so erlaubt auch diese Ansicht ein zügiges Drill-down bis hin zur genauen Systemansicht. Jedoch haben die Baramundi-Entwickler das Drill-down nicht auf jedes grafische Element angewandt, sondern nur auf unterstrichene Informationen. Als Alternative zum systemorientierten Vorgehen kann der Verantwortliche anhand der Schwachstellen sowie deren Häufigkeit durch die IT-Landschaft navigieren und geeignete Updates ausführen.

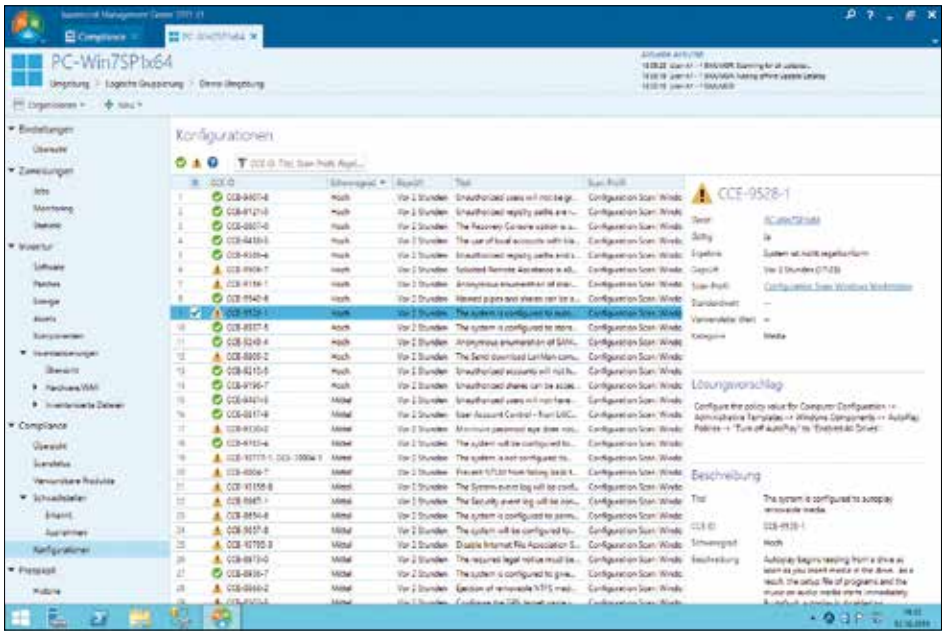
Letztlich wendet der Administrator Scan-Jobs auf einzelne Client/Server-Systeme oder Gruppen an, die dann mit einer vertretbaren zeitlichen Verzögerung von einigen Minuten bis zu einer halben Stunde das Ergebnis an die Datenbank übermitteln. Der gesamte Ablauf und die Bedienung sind insgesamt recht intuitiv. Sehr schnell dürfte sich der Benutzer an die Oberfläche und ihre Bedienungselemente gewöhnt haben. Ab und zu vermissten wir einen „Zurück“-Button, der uns zur vorherigen Ansicht zurückbringen würde.

Der Scan unserer kleinen Testumgebung zeigte sehr schnell, dass fehlende Software-Patches der Hauptgrund für eine „gefährdete Konfiguration“ sind. Für den Windows-10-PC zeigte die Software einen Gefährdungsgrad von 5/10 an. Nur die Werte 0 bis 0,5 würden mit der Farbe Grün hinterlegt, unsere 5 war indes tieforange. Insgesamt sorgen vier Schwachstellen, allesamt mit der Nummer CVE-2005-2128 gelistet, für das eher schlechte Ergebnis.

In den Top 5 der verwundbaren Produkte war im Zusammenhang mit den genannten Schwachstellen nur eines nennenswert: Direct X. Der Lösungsvorschlag für alle diese Missstände war wiederum sehr einfach: Bitte Patch MS05-2005 installieren! Ein Patch aus dem Jahr 2005, der überhaupt nicht für Windows 10 gültig ist? Diese Empfehlung war wohl eher etwas fragwürdig. Wie die Software eine Schwachstelle identifiziert, so der Hersteller, hängt von der OVAL-Beschreibung in den XML-Dateien ab, die das Center for Internet Security bereitstellt. Wie eine Schwachstelle genau benannt wird, beispielsweise durch eine bestimmte DLL-Version oder einen Registry Key, zeigt die aktuelle BMS-Version noch nicht an. Mit dem Service-Release 2 für 2015 soll sich das ändern. Dass ein solcher Scan nicht alle Sicherheitsprobleme automatisch erkennen wird, zeigt ein anderer Fall: wieder



Den Gefährdungsgrad für einen Computer stellt die Software grafisch dar. Tabellarisch aufgelistet erhält der Administrator den Hinweis, welche Programme betroffen sind.



Zu jeder Schwachstelle liefert die Software einen Lösungsvorschlag, entweder auf Englisch oder Deutsch.

der genannte Windows-10-PC, auf dem wir bewusst eine äußerst alte Version von Psexecute von Mark Russinovich ablegten. Psexecute, ursprünglich für Winternals entwickelt, ist ein äußerst praktisches Programm zur Fernausführung von Befehlen. In der Version 1.6 jedoch überträgt die Software Anmeldedaten noch im Klartext – ein Sicherheitsrisiko, neuere Versionen verschlüsseln deshalb die Verbindungsdaten. Doch diese veraltete Version der Software identifizierte der Scanner nicht.

Dieser Hinweis soll die Leistung eines solchen Schwachstellen-Scanners nicht über Gebühr schmälern, denn immerhin prüfte BMS über 6.800 Regeln auf der Workstation. Falsch konfigurierte Passworteinstellungen für lokale Konten bemängelt der Scanner, ebenso das Vorhandensein offenkundig unsicherer, aber weit verbreiteter Anwendungsprogramme, beispielsweise auch die anfällige OpenSSL-Bibliothek (CVE-2010-2939) in den älteren Versionen des VMware-Vsphere-Clients. Neben der regelorientierten Auflistung aller gefundenen Schwachstellen bietet das Modul Compliance-Management zudem eine Ansicht der verwundbaren Lösungen, inklusive einer Darstellung der jeweiligen Anzahl daraus resultierender Schwachstellen. Diese Darstellung erlaubt dem IT-Verantwortlichen eine schnelle Identifikation für das Maß der Dringlichkeit, Updates mittels BMS zu verteilen. Ergibt die Prüfung beispielsweise, dass mehr als 140 Schwachstellen in einem bekannten PDF-Reader im Unternehmen entdeckt wurden, so ist dies sicherlich ein größeres Risikopotenzial als die drei veralteten Textverarbeitungsprogramme in der Version 97.

Bereits mit dem Release 2014 R2 war es Administratoren möglich, Ausnahmen für Schwachstellenregeln auf einer globalen Ebene zu definieren. Mit der aktuellen Version haben die Entwickler bei Baramundi die Funktion erweitert, indem Anwender Ausnahmen hinsichtlich des Geltungsbereichs festlegen können: Neben globalen Ausnahmen können IT-Verantwortliche nun Gruppen oder einen Client-Rechner ausschließen oder Ausnahmen für ganze Untergruppen aufheben.

Die Möglichkeiten zur Einflussnahme auf die Regelwerke sind ansonsten für den Administrator eher begrenzt. In den definierbaren Profilen kann der Administrator lediglich festlegen, welche der rund 6.900 Schwachstellen der Scanner für die gewählten Geräte abprüft und welche nicht. Die Definition eigener Regelwerke, zum Beispiel auf das Vorhandensein einer bestimmten Datei oder Dateieigenschaft, sieht die Software derzeit nicht vor. Mit Blick auf die Zielgruppe – Administratoren, die sich nicht zu sehr mit Security auseinandersetzen wollen – ist dies jedoch eine verschmerzbare Einschränkung.

Üblicherweise verstehen Administratoren unter dem von Baramundi so genannten „Compliance-Management“ nicht etwa die Prüfung auf Schwachstellen oder Fehlkonfigurationen, sondern eine Überwachung im Hinblick auf Regularien, insbesondere Lizenzbestimmungen. In der Tat gibt es für BMS auch ein Software-Asset-Management, jedoch nicht aus eigener Entwicklung: BMS arbeitet hierfür entweder über eine Schnittstelle mit der Cloud-basierten Esam-Software von Amando Software zusammen oder nutzt die lokal zu installierende Lösung Miss Marple, die ebenfalls von Amando entwickelt wurde.

Baramundis eigenes Lizenzierungsmodell für BMS gilt pro Modul und verwaltetem Arbeitsplatz, unabhängig davon, ob es sich um einen Client oder Server handelt. Das Schwachstellen-Management kostet maximal rund 15 Euro, bei Abnahme einer größeren Menge gibt es Staffelpreise.

Insgesamt bietet die Baramundi Management Suite eine ausgewachsene Lösung für die Verwaltung von PCs, Servern, Mac-OS-X-Systemen und Mobilgeräten. Das Augsburger Unternehmen hat seine Suite mit dem „Compliance-Management“-Modul um eine wichtige Erweiterung ergänzt. Zwar gibt es bereits viele Schwachstellenscanner und -lösungen auf dem Markt, doch viele Administratoren wünschen sich eine komplett integrierte Variante. Mit BMS sind nun Softwareverteilung, Schwachstellenprüfung und das Patch-Management unter einem Dach vereint.

Thomas Bär, Frank-Michael Schlede/wg

Thomas Bär auf LANline.de: **BÄR**

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

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