Test: Schwachstellen und Sicherheitslücken in Windows finden mit der baramundi Management Suite

Andrej Radonic, 27.10.2015

Tags: Sicherheit, Patch-Management, Compliance

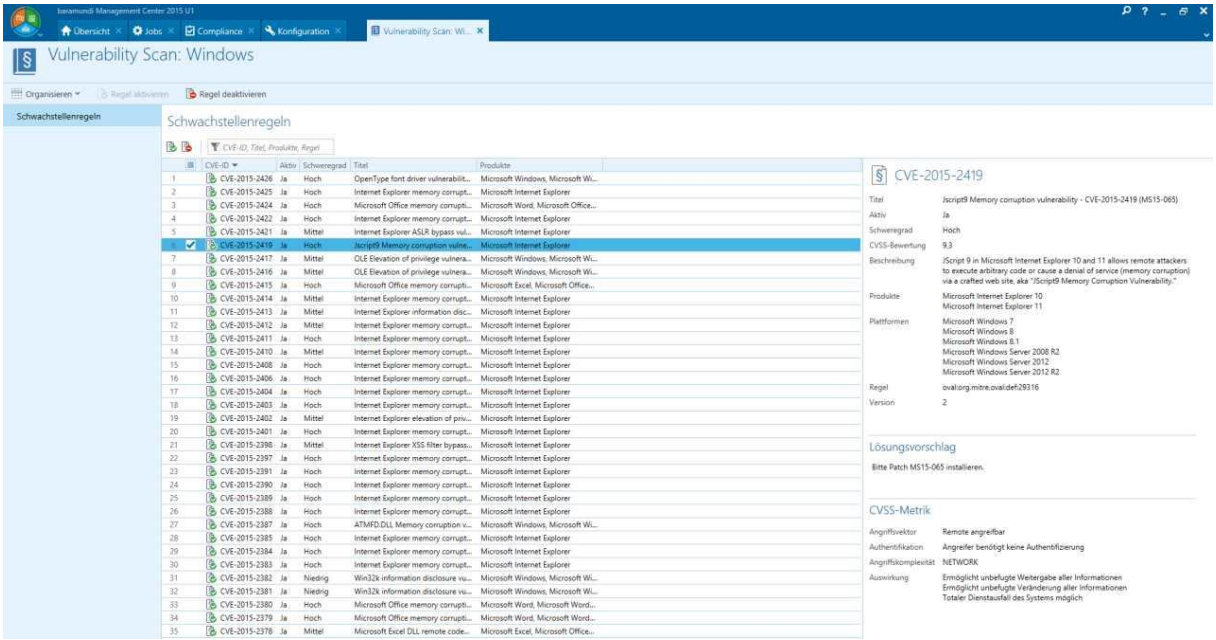
Die baramundi Software AG ergänzte seine Management Suite in der Version 2014 R2 um eine Schwachstellen-Prüfung. Diese Funktion des Compliance-Moduls soll Admins dabei helfen, Lücken zu schnell zu erkennen und zu beheben: Detaillierte Auswertungen geben Auskunft über Schwachstellen und Abweichungen von Konfigurationsvorgaben.

Auch wenn das integrierte Patch- und Update-Management die Clients automatisch aktualisiert, so bleiben oftmals doch Schwachstellen und Konfigurationsfehler in den verwalteten Systemen bestehen und von Administratoren unerkannt. Hier springt das Compliance-Modul ein, indem es auf Grundlage einer eigenen Wissensbasis die Systeme tiefergehend prüft und dabei zusätzlich die Konfiguration ins Visier nimmt.

Bekannte Schwachstellen und abweichende Konfigurationen finden

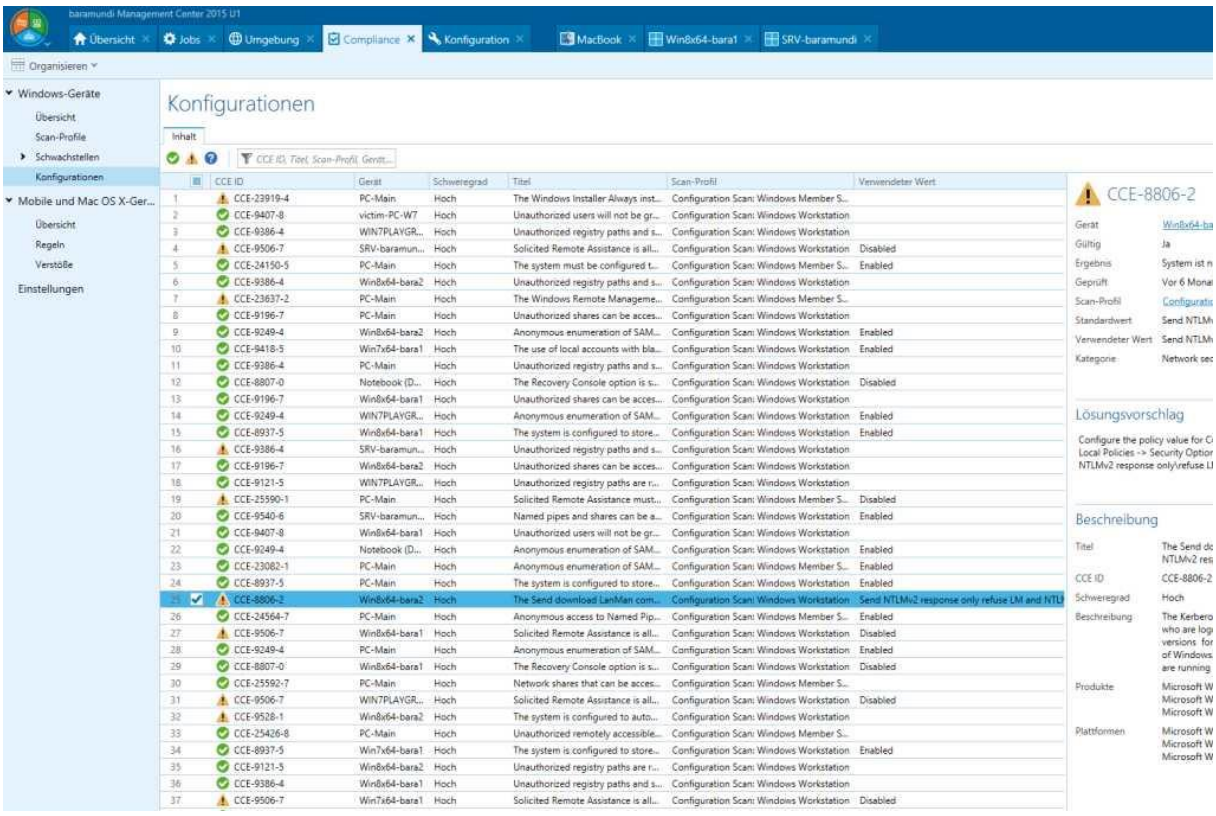
Während das Patch-Management seine Updates ausschließlich von den Herstellern bezieht, konsultiert der Schwachstellen-Scanner mehrere öffentliche Vulnerability-Datenbanken wie die CVE Dictionary (Common Vulnerabilities and Exposures). Derzeit werden täglich etwa 7000 Einträge vom baramundi Management Server (bMS) automatisch heruntergeladen und für die Client-Scans verwendet.

Die Datenbasis umfasst dabei sowohl Schwachstellen von Betriebssystemen als auch von allen gängigen Applikationen, vom Web-Browser bis zum PDF-Reader.



baramundi Compliance sucht Sicherheitslücken auf Basis eines täglich aktualisierten Schwachstellenkataloges.

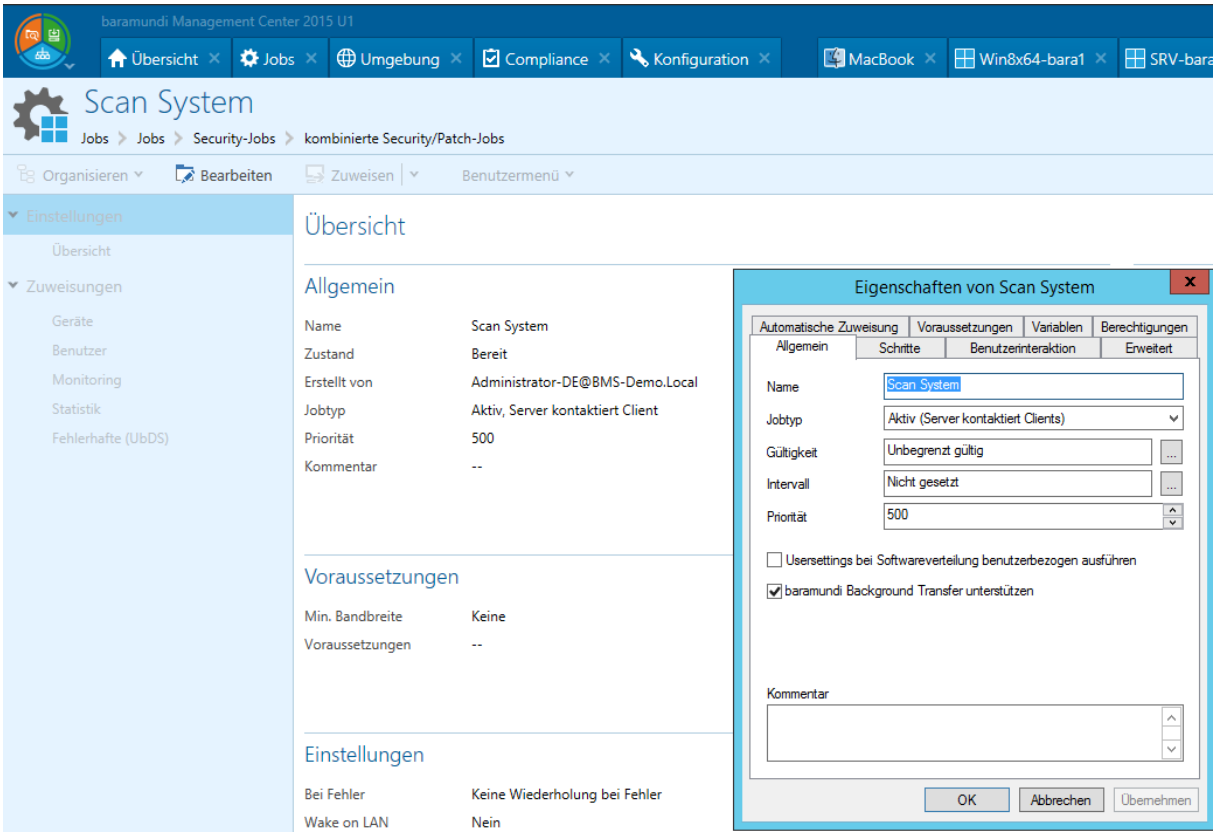
Mit dem Compliance-Modul kann der Administrator zudem nach Abweichungen von Konfigurationsvorgaben suchen. Zwar konfigurieren Systemverwalter typischerweise alle wichtigen Client-Einstellungen zentral über Gruppenrichtlinien, aber ein hohes Sicherheitsniveau kann jedoch nur garantiert werden, wenn überprüft wird, ob die Richtlinien auf allen Clients angekommen sind.



Der Konfigurations-Check prüft Windows-Systeme auf Basis eines umfassenden Regelkatalogs.

Automatische Prüfungen über Jobs

baramundi-typisch steuert der Administrator die Compliance-Scans über Jobs. Das Modul enthält bereits solche für Vulnerability und Configuration Scan. Letzterer ist nach Client-Gruppen (Workstations, Member Server, Domain Controller) unterteilt.



Compliance-Scans werden als Jobs definiert und ausgeführt und lassen sich mit Bedingungen verknüpfen.

Der Administrator kann also sofort loslegen, indem er in der Übersicht die entsprechenden Jobs startet und anschließend die Auswertung durchgeht. Zusätzlich kann er selbst Scan-Profile zusammenstellen, in welchen er die Prüfungen definiert und bei Bedarf Bedingungen hinzufügt (beispielsweise welche Bandbreite beim Client zur Verfügung steht oder welche OS-Version installiert ist). Schließlich legt er noch die Zeitsteuerung fest und ordnet den Job Gruppen von Geräten zu, auf die er angewandt werden soll.

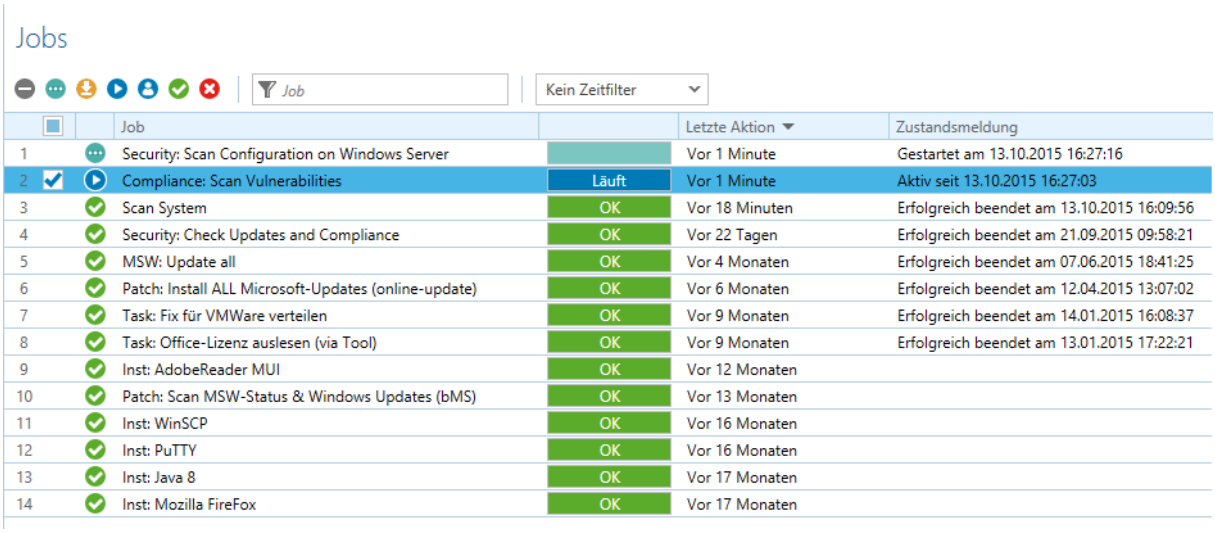
Compliance-Scan und Updates im regelmäßigen Wechsel

Sinnvollerweise kombiniert baramundi Prüf- und Update- bzw. Patch-Vorgänge miteinander. So wird der Job *Update System and Check Security* mitgeliefert, welcher die Schritte

- Software aktualisieren
- Microsoft Patches verteilen
- Vulnerability Scan

direkt hintereinander ausführt.

Den Best Practices folgend, führt das Management-Tool den Compliance-Scan und die Patch-/Update-Läufe alternierend aus. Bewährt hat sich ein wöchentlicher Rhythmus, in dem zunächst das Update erfolgt und einige Tage später wieder ein vollständiger Schwachstellen-Check, der durch das Update eventuell zurückgelassene Lücken oder in der Zwischenzeit entstandene Probleme aufdeckt.



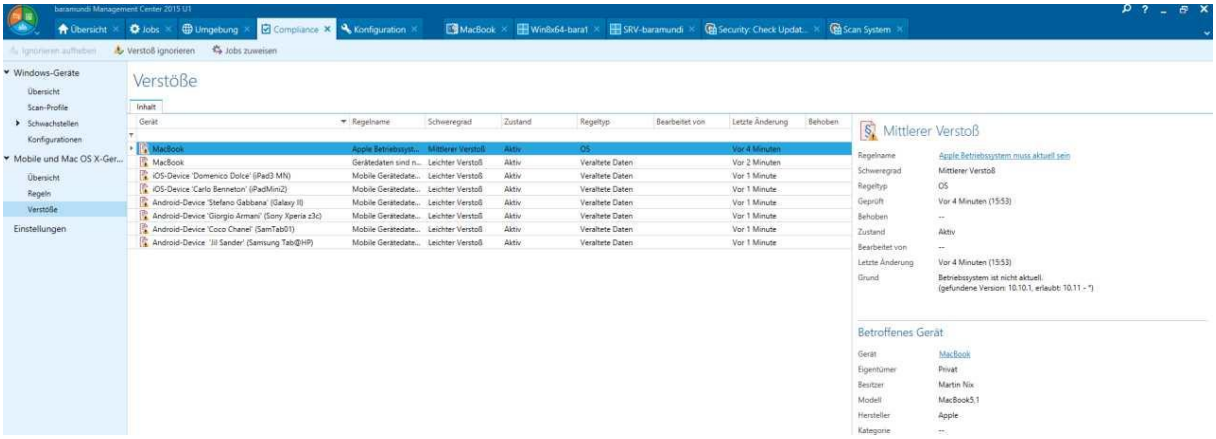
Jobs für Compliance-Scans prüfen die Clients zeitgesteuert auf Schwachstellen und Konfigurationsverstöße.

Compliance für Mobilgeräte und Mac OS Systeme

Da die baramundi Management Suite neben Windows auch Apple Mac OS X und mittels integriertem MDM auch iOS-, Android- und Windows-Mobilgeräte verwalten kann, umfasst das Compliance-Management auch diese Geräteklassen. Allerdings sind hier keine Konfigurations-Prüfregeln und Schwachstellen-Datenbanken vorhanden, vielmehr definiert der Administrator alle Regeln und deren Bedingungen selbst.

Er kann dabei Einschränkungen für Apps sowie den Umgang mit Jailbreaks definieren, Betriebssystemversionen prüfen sowie die Geräte regelbasiert und automatisch inventarisieren.

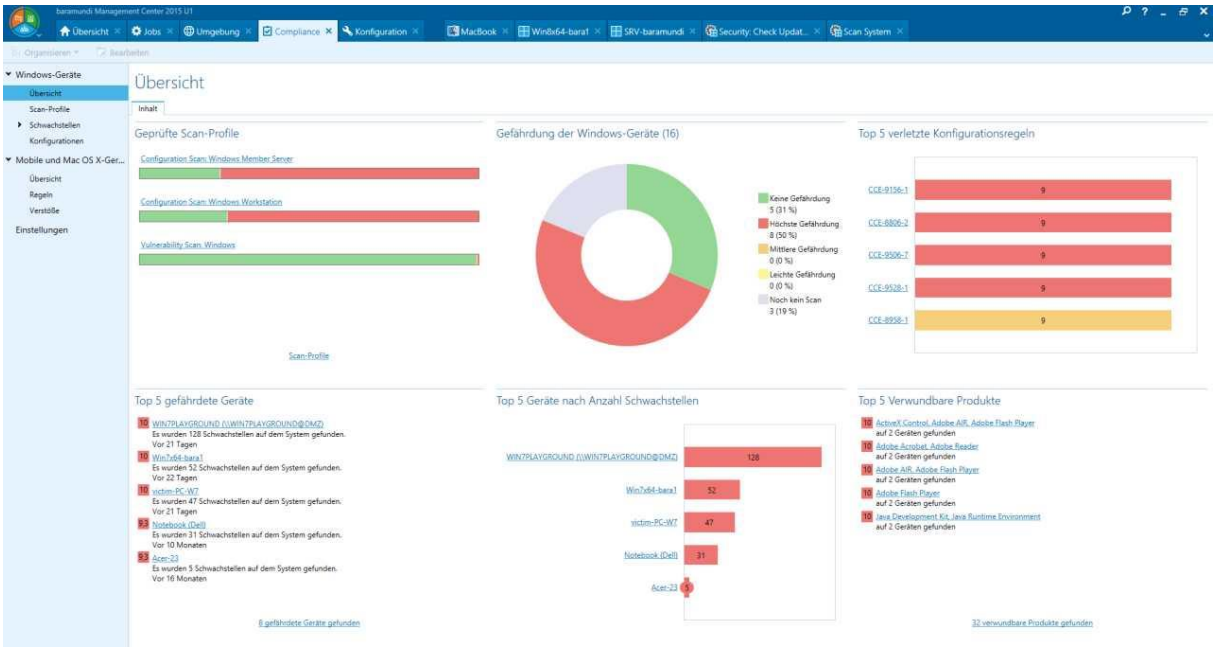
Als Reaktion auf einen festgestellten Verstoß kann man Aktionen veranlassen: eine Hardware- und/oder eine Software-Inventarisierung starten, Geräte sperren oder Entsperren, Scripte ausführen, Apps und Profile installieren oder deinstallieren.



baramundi Compliance prüft auch Apple Mac OS X Computer auf Verstöße.

Dashboard für den Compliance-Überblick

Das baramundi Management Center (bMC) konsolidiert alle Scan-Ergebnisse übersichtlich im Compliance-Dashboard. In einer grafischen Übersicht erhält man einen aktuellen Überblick über die Sicherheitslage, gestaffelt nach den Kriterien Verletzung von Konfigurationsregeln, verwundbarste Software, Geräte mit dem höchsten Gefährdungspotential sowie Geräte mit den meisten Schwachstellen. Letzteres ist meist ein Hinweis auf Probleme mit dem Update-Management der betreffenden Systeme.



Das Compliance-Dashboard fasst alle Scan-Ergebnisse zusammen und liefert einen Sofortüberblick über die Sicherheitslage.

Listendarstellungen erlauben einen Drill-down nach Rechner, Schwachstelle oder Gefährdungsgrad. Bei jedem Gerät befindet sich zudem eine detaillierte Compliance-Übersicht, welche nicht nur die Risiken und wichtigsten Schwachstellen, sondern auch eine Liste mit verwundbarer Software und fehlerhaften Konfigurationen anzeigt.

Keine Brücke zwischen Compliance und Update

Während sich die Module *Compliance* und *Patches* ideal ergänzen, existiert kein Automatismus, der Updates abhängig von entdeckten Schwachstellen priorisiert und einspielt. Eine solche Funktionalität ist erst für eine künftige Version geplant.

baramundi unterbreitet dem Adminstrator Lösungsvorschläge zur Beseitigung gefundener Sicherheitslücken.

Allerdings lassen sich viele Sicherheitslücken und Fehlkonfigurationen prinzipiell nicht automatisch beseitigen, vielmehr verlangen sie nach manueller Analyse und Behebung. Das Compliance-Modul liefert den Sysadmins daher zu jeder gefundenen Schwachstelle Referenzen auf externe Informationsquellen sowie Lösungsansätze wie Patches oder neue Versionen.

Lizenzen und Preise

Das baramundi Compliance Management kann nur als Erweiterungsmodul der baramundi Management Suite erworben werden. Die Kosten für das Paket bemessen sich nach den gewählten Modulen sowie der Anzahl der verwalteten Clients. Den Preis nennt der Hersteller auf Anfrage.

Copyright © WindowsPro