OKTOBER 2014

ISSN 1864-0907 • 7,- €

IT-SICHERHEIT

Made in Germany

Titelbildcomposing: © frank peters/ Dan Race - Fotolia.com

Datensicherheit

Endpoint Security

ATP

Backdoor

Data Leakage

Compliance

Verschlüsselung

Patch Management

Powered by:

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

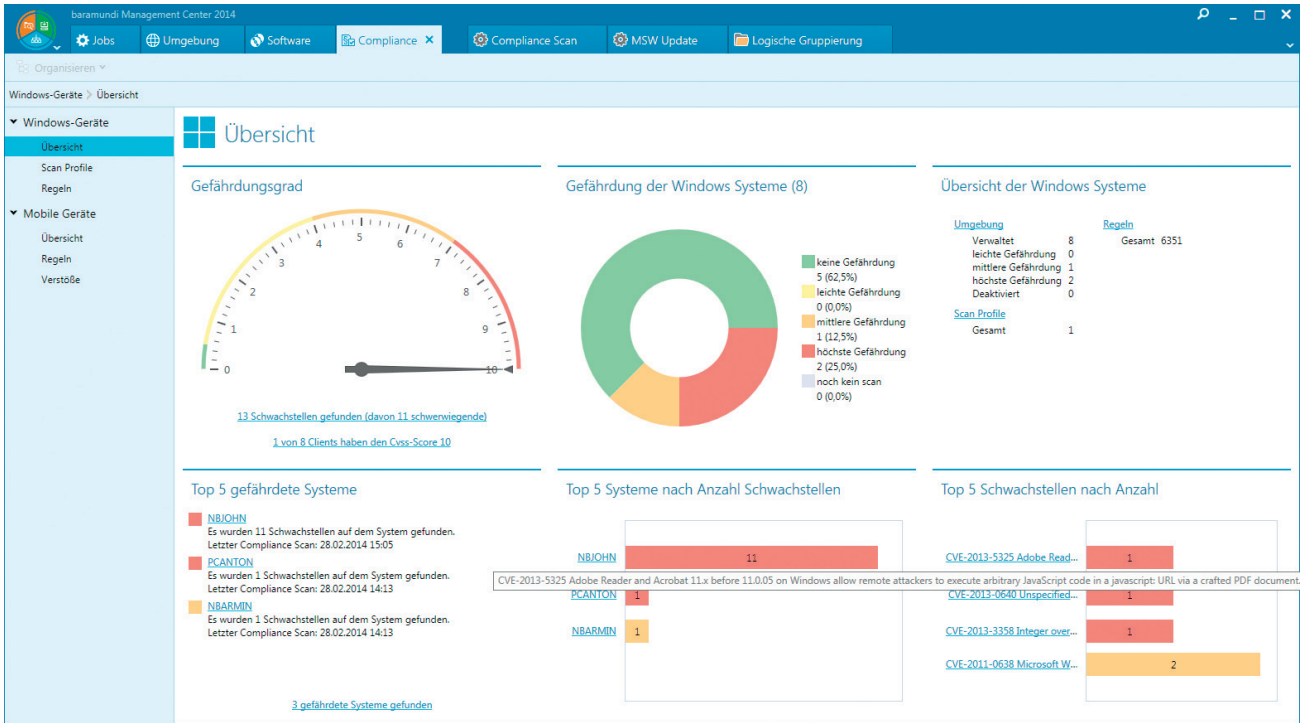
Vogel Business Media

Eine Publikation von IT-BUSINESS

Security Insider

Safety First: Automatisiertes Schwachstellenmanagement

Eine Sicherheitslücke auf einem einzelnen Rechner bringt die Sicherheit der gesamten Unternehmens-IT in Gefahr. Doch einem IT-Administrator ist es in der Praxis nicht möglich, alle Clients und Server fortwährend zu prüfen und zu patchen. Abhilfe schafft automatisiertes Schwachstellenmanagement, integriert in eine Client-Management-Software.



Übersicht über den Zustand der IT-Umgebung im Compliance-Dashboard der baramundi Management Suite

Auf jedem Windows-Rechner und Server lauern potentiell tausende Schwachstellen – Tendenz steigend: 2013 wurden jede Woche rund 100 neue Sicherheitslücken in der National Vulnerability Database des US-CERT dokumentiert. Jede könnte als Einfallstor für Angreifer dienen. Schwachstellen werden für sogenannte Reverse-Angriffe genutzt, die etablierte Sicherungen wie Firewall und Virenscanner aushebeln. Ein Beispiel: Einem Mitarbeiter wird eine manipulierte Datei zugespielt, die sich eine Lücke im PDF-Reader zunutze macht und so einen Schadcode auf dem Rechner ausführen kann. Dieser macht den Rechner zum willigen Sklaven des Angrei-

fers. Da die Verbindung aus dem Unternehmen heraus aufgebaut wird, greift die Firewall nicht ein. Neben korrumpierten Dateien werden auch manipulierte Webseiten oder bösartige Online-Anzeigen eingesetzt.
Im Rahmen eines wirkungsvollen IT-Sicherheitskonzepts ist es daher essentiell, Sicherheitslücken auf allen Geräten zu erkennen und alle nötigen Patches unverzüglich, flächendeckend und zuverlässig einzuspielen.

Automatisierte Schwachstellenanalyse

Dazu müsste der Administrator laufend Datenbanken und Blogs auf Meldungen über Schwachstellen durchsuchen, diese bewerten, die eigenen Rechner prüfen, Updates paketieren, testen, verteilen und erfassen, ob die Verteilung erfolgreich war. Ohne automatisierte Hilfsmittel ist dies de facto nicht möglich. Ein automatisiertes Patch-Management für Microsoft-Produkte schließt zwar einige Lücken, deckt aber längst nicht jede Software ab. Hilfreich ist ein Scanner, der die Rechner im Unternehmensnetzwerk regelmäßig auf die Einträge in den Schwachstellendatenbanken prüft. Der IT-Administrator erhält so einen umfassenden Überblick. Sinnvoll ist dabei eine Drill-Down-Möglichkeit, zum Beispiel nach den Clients mit den meisten oder den gefährlichsten Lücken.

Integration in Client-Management

Für das schnellstmögliche Schließen der Lücken stehen ebenfalls automatisierte Hilfsmittel zur Verfügung. Neben Microsoft-Patches sollten diese zumindest Updates für weit verbreitete und daher bei Angreifern populäre Anwendungen anderer Hersteller abdecken. Aktuelle Softwarepakete für zahlreiche Applikationen sind auch als Managed Software von Client-Management-Herstellern verfügbar. Essentiell ist dabei, die Verteilung nicht nur anzustoßen, sondern auch eine Rückmeldung, ob diese erfolgreich war. Im Idealfall sind diese Lösungen mit dem Schwachstellenscanner in einer ganzheitlichen Client-Management-Software zusammengefasst, so dass der gesamte Prozess zügig ablaufen kann.
Ein derartiges automatisiertes Schwachstellenmanagement sorgt für eine größtmögliche Aktualität der Client-Systeme und Server im Unternehmen. Es kann allein aber keinen umfassenden Schutz bieten, sondern muss Teil einer umfassenden Sicherheitsstrategie sein. In einer größeren Umgebung sollte diese automatisiert umgesetzt werden, um einheitliche Standards an allen Geräten durchzusetzen. Dazu gehören standardisierte Abläufe ebenso wie ein zentrales Backup, das Verschlüsseln von Datenträgern oder der Schutz vor nicht autorisierten Anwendungen. Flankierend müssen auch die Endanwender für Gefahren sensibilisiert und darüber informiert werden, welche Verhaltensweisen zum Schutz vor Angriffen beitragen.
In ein derartiges Sicherheitskonzept sollten auch Smartphones und Tablets eingebunden werden. Es bietet sich an, auch diese Aufgabe über eine integrierte Lösung für Client- und Mobile-Device-Management abzudecken, um einheitliche Standards auf allen Geräten im Unternehmen durchzusetzen. ■

Der Autor Armin Leinfelder ist Produktmanager bei der baramundi software AG.