LANline

9,– €

Januar 2015
19. Dezember 2014

ITP VERLAG

IT ▪ Netze ▪ Infrastruktur www.lanline.de

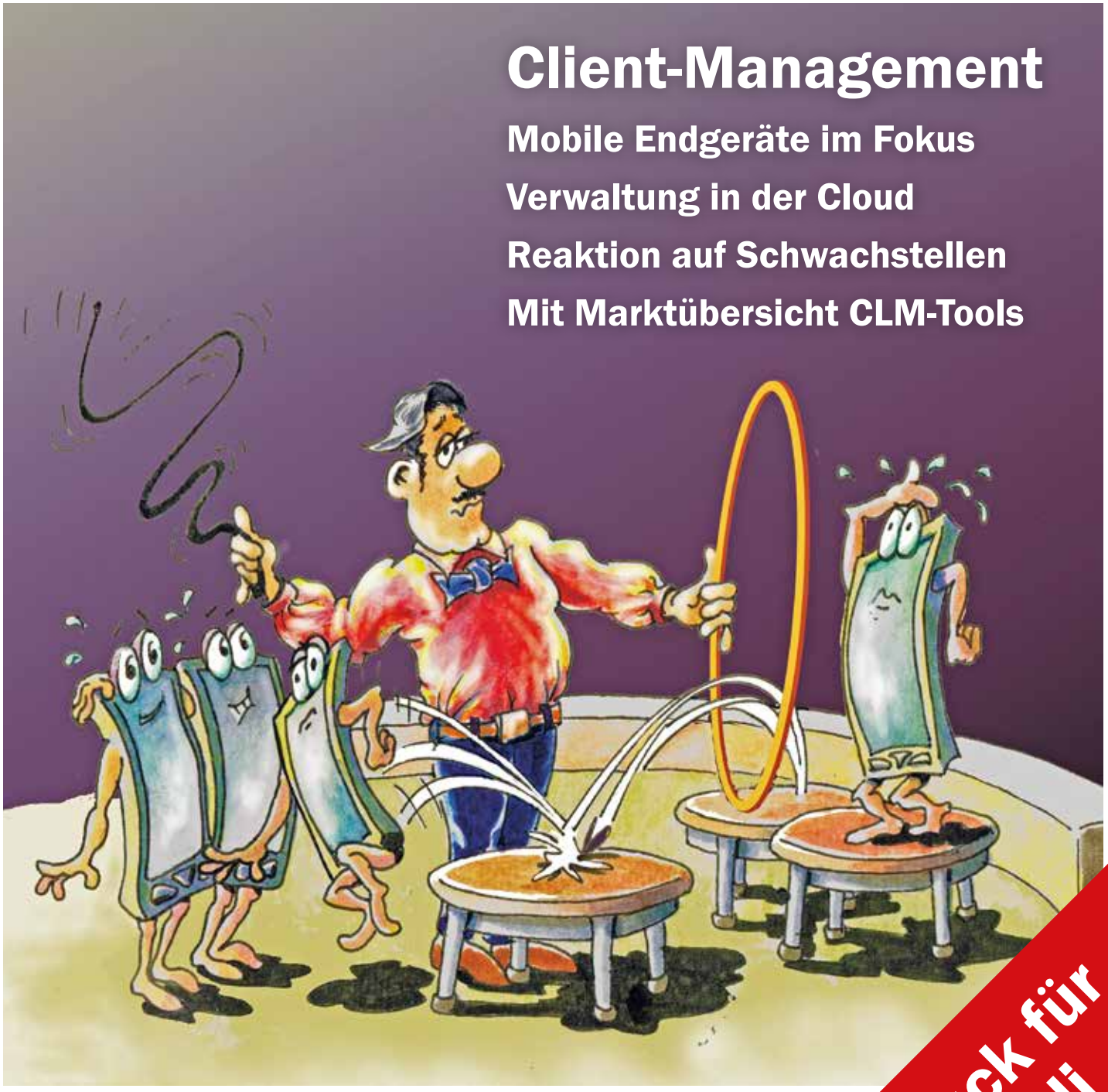
Client-Management

Mobile Endgeräte im Fokus

Verwaltung in der Cloud

Reaktion auf Schwachstellen

Mit Marktübersicht CLM-Tools



Testreihe SDS
Red Hat Storage Server
Scale-out-Speicher mit Cloud-Anschluss

Software-Defined Networking (SDN)
Flexibilität für das Campusnetz

Schwer
Data
Mi

Schwachstellen-Management

Gegen die Lücke

Compliance zu gewährleisten ist eine Kernaufgabe von IT-Verantwortlichen. In diesem Zusammenhang muss unter anderem dafür gesorgt sein, dass die Rechner im Unternehmen möglichst keine gefährlichen Sicherheitslücken aufweisen. Dafür sorgen Lösungen für das Schwachstellen-Management, die als eigenständige Lösung oder als Modul von Client-Management-Software verfügbar sind. Was spricht für eine integrierte Lösung – oder ist die eigenständige Software die bessere Wahl?

Ein unbedachter Klick auf einen E-Mail-Anhang oder einen Link genügt: Die fatale Infektion des Rechners ist passiert. Als ferngesteuerter Teil eines Botnets kommt das Gerät nun für weitere, strafbare Angriffe zum Einsatz – und die Spur der IP-Adresse führt ins eigene Unternehmen. Oder aber Angreifer lesen Passwörter und vertrauliche Dokumente mit, werten sie aus oder laden sie herunter. Dass dieses Worst-Case-Szenario nicht eintritt, dafür sind in Unternehmen und Behörden die IT-Abteilungen verantwortlich.

Angriff durch die Hintertür

Die Zeiten, in denen man zur Abwehr der Angriffe allein auf eine gute Firewall und einen leistungsfähigen Virenscanner setzte, sind schon lange passé. Diese Maßnahmen gilt es durch ein Management von Schwachstellen zu ergänzen. Denn eine Sicherheitslücke in einem der vielen unternehmensweit eingesetzten Softwareprodukte – vom Betriebssystem bis zur Applikation – auf einem der vielen Geräte genügt potenziell, um Opfer eines erfolgreichen Reverse-Engineering-Angriffs zu werden.

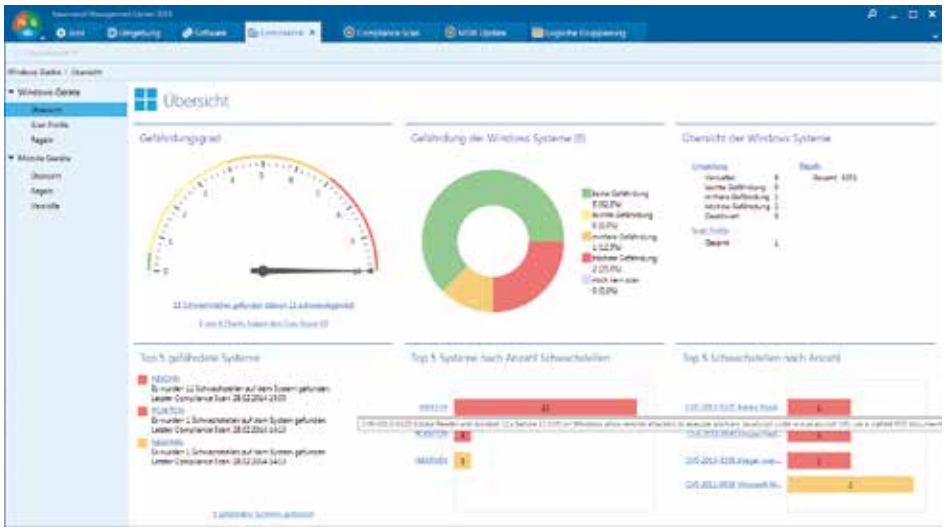
In diesem Szenario schicken Angreifer Mitarbeitern manipulierte Dateien zu oder schieben ihnen eine präparierte Webseite unter. Diese nutzen gezielt eine Sicherheitslücke aus und können so einen Schadcode auf dem Rechner ausführen, der das Gerät zum willigen Sklaven eines fremden Herrn macht – meist sogar, ohne dass der Nutzer vor dem Bildschirm etwas davon merkt. Da die Verbindung aus dem Unternehmen heraus aufgebaut wird, greift auch die Firewall nicht ein. Derartige Angriffe sind mithilfe von Exploits, die sich im Internet finden, auch ohne weitreichende Programmierkenntnisse möglich.

Nötig sind daher ein Management der Schwachstellen und technische Schutzmaßnahmen zur Gefahrenabwehr: Die Administratoren müssen zuverlässig wissen, welche Sicherheitslücken existieren und auf welchen Geräten im Unternehmen welche Lücken bestehen. Nur so können sie abschätzen, welche Risiken vorliegen, und diese beseitigen, zum Beispiel durch Patch-Installationen.

Softwarelösungen für das Schwachstellen-Management liefern diese Informationen gebündelt. Sie prüfen die Rechner im Unternehmen regelmäßig auf Basis der Informationen in Schwachstellen-Datenbanken wie auch anderen Regelwerken und zeigen erkannte Sicherheitslücken übersichtlich an. Ein solcher Schwachstellenscan findet bei niedrigem Ressourcenverbrauch im Hintergrund statt und beeinträchtigt den angemeldeten Nutzer am Client nicht bei der Arbeit. Eine solche Lösung bewertet Schwachstellen nach Schweregrad. Dies versetzt den IT-Administrator in die Lage, gezielt besonders gefährdete Rechner, sehr gefährliche oder weit verbreitete Lücken zu patchen. Gleichzeitig erhält er überhaupt erst eine Übersicht über den Zustand seiner Umgebung, kann Gefahrenpotenziale abschätzen und darüber Rechenschaft ablegen. Neben Sicherheitslücken in Softwareprodukten prüfen Schwachstellen-Management-Lösungen teilweise auch weitere potenzielle Gefährdungen, zum Beispiel die Konfiguration der Geräte.

Zwei Lösungswege

Am Markt verfügbar sind sowohl eigenständige Lösungen, die auf das Aufspüren von Schwachstellen spezialisiert sind, als



Übersicht über erkannte Schwachstellen im Dashboard einer Client-Management-Lösung.

Bild: Baramundi

auch Lösungen, die in eine System-Management-Software integriert sind. Ein wichtiges Kriterium bei der Auswahl einer Lösung ist sicher der Leistungsumfang: Es gilt, die angebotenen Features und möglichen Aktionen zu prüfen. Spezialisierte Lösungen sind hier in Details oft leistungsfähiger als Erweiterungsmodule von Client-Management-Herstellern.

Diesen möglichen Nachteil im Funktionsumfang können integrierte Lösungen mit dem Mehrwert effizienterer Abläufe wieder wettmachen – vor allem, wenn die IT nicht alle Funktionen einer Speziallösung im Alltagsbetrieb benötigt. Wenn es um das schnelle, gezielte Schließen von Lücken geht, ermöglichen es integrierte Lösungen, den gesamten Prozess vom Erkennen der Schwachstelle bis zum Schließen der Lücke in einer Lösung darzustellen. Zur Verteilung eines Patches muss der IT-Administrator hier keine weitere Softwarelösung starten, sondern kann die Remediation direkt aus derselben Oberfläche anstoßen – mit den Vorteilen, die eine Client-Management-Software dabei bietet, also zum Beispiel mit Rückmeldung zum Installationsstatus. So kann der gesamte Prozess vom Aufspüren der Lücken bis zu ihrem Schließen zügig ablaufen.

Client-Management-Anbieter stellen teilweise in ihren Softwarelösungen auch verteilfertig vorbereitete Softwarepakete und Patches als Managed-Software-Services zur Verfügung und ermöglichen so ein schnelles, weitgehend automatisiertes Schließen von Sicherheitslücken. Zudem entfällt der Einrichtungs- und Pflegeaufwand für eine zweite Lösung, die Administratoren müssen sich in keine zweite Benutzeroberfläche einarbeiten. Bei der Zusammenarbeit mit dem Lösungsanbieter und dem Support besteht ein einheitlicher Ansprechpartner für den gesamten Prozess vom Scan bis zur Remediation.

Nicht immer steht für eine Schwachstelle sofort ein Patch zur Verfügung, nicht immer kann eine Software sofort aktualisiert werden, da andere, geschäftskritische Anwendungen mit der aktuellen Version noch nicht funktionieren. In diesem Fall gilt es, Maßnahmen zur Eindämmung der Gefahren zu ergreifen, zum Beispiel eingeschränkte Zugriffsrechte auf Ressourcen im Unternehmen, bis die IT die Sicherheitslücke endgültig schließen kann. Auch diese Schritte lassen sich in einer integrierten Lösung effizienter und eleganter durchführen als mit einer separaten Lösung.

Es bleibt die Frage, ob es sinnvoll ist, sowohl den Schwachstellenscan als auch die Remediation nur einem Produkt anzuvertrauen. Hier bieten Standalone-Lösungen, die unabhängig arbeiten, auf den ersten Blick ein deutliches Mehr an Sicherheit. Betrachtet man diesen Aspekt jedoch im Detail, relativiert sich dies, sofern Schwachstellenscan und Remediation integrierter Lösungen völlig unterschiedliche Mechanismen und externe Datenquellen nutzen: Ersterer verwendet Regeln aus den Datenbanken unabhängiger Organisationen, während bei der Remediation Patches des jeweiligen Herstellers für dessen Software verteilt werden. Somit ist es unwahrscheinlich, dass eine Lücke in einem Tool gleichzeitig auch eine analoge Lücke des anderen zur Folge hat. Darüber hinaus können integrierte Lösungen aber mit den üblichen Vorteilen der Integration punkten.

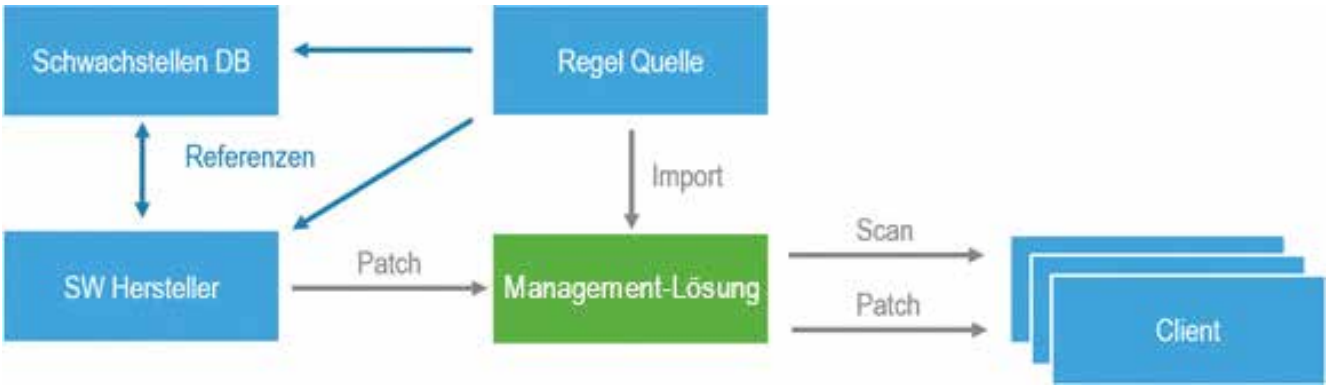
In Unternehmensumgebungen ist auch eine große Zahl mobiler Endgeräte im Einsatz, die Notebooks und Desktop-Clients ergänzen. Auch diese Smartphones und Tablets muss die IT auf Compliance mit Sicherheitsanforderungen und Unternehmensregeln prüfen.

Eine integrierte Lösung, die eine MDM-Funktionalität (Mobile-Device-Management) bietet, ermöglicht ein Schwachstellen-Management aller Endgeräte aus einer einheitlichen Lösung heraus. So lassen sich nicht nur einheitliche Richtlinien plattformübergreifend durchsetzen. Die IT-Administration ist gleichzeitig für Trends wie Mobilität und Consumerization sowie ein verstärktes Zusammenwachsen von Desktop- und Mobilplattformen gut gerüstet.

Fazit

Ein automatisiertes Schwachstellen-Management sorgt zudem für Transparenz im Hinblick auf vorhandene Schwachstellen und versetzt den IT-Administrator in die Lage, über eine Client-Management-Software für eine größtmögliche Aktualität der Client-Systeme und Server im Unternehmen zu sorgen. Eine Integration beider Lösungen in einer Softwaresuite schafft den Mehrwert einheitlicher Abläufe, verringert den Aufwand und ermöglicht, Schwachstellenerkennung und Remediation als einheitlichen Prozess zu betrachten – zu prüfen ist aber, ob der Schwachstellenscan allen unternehmensinternen Anforderungen genügt. Armin Leinfelder/wg

Armin Leinfelder ist Produktmanager bei Baramundi Software in Augsburg, www.baramundi.de.



Schwachstellen-Management und zentrales Client-Management können im Zusammenspiel Remediation-Prozesse beschleunigen. Bild: Baramundi