Mit automatisiertem Schwachstellenmanagement Sicherheitslücken schnell erkennen und schließen

Mut zur Lücke – nein danke!

Eine Schwachstelle auf einem einzigen Rechner im Unternehmen genügt, um die Sicherheit der gesamten IT-Umgebung und damit der sensiblen Firmendaten zu gefährden. Doch dem IT-Administrator ist es in der Praxis nicht möglich, alleClients und Server laufend auf alle bekannten Lücken zu prüfen. Abhilfe schafft automatisiertes Schwachstellenmanagement mithilfe einer Client-Management-Software.

Von Armin Leinfelder, baramundi software AG

Vollkommen fehlerfreie Software gibt es nicht. Potenziell kann jeder Fehler ein Sicherheitsrisiko darstellen und eine Hintertür öffnen, die für Angriffe genutzt werden kann. Im Jahr 2013 wurden jede Woche rund 100 neue derartige Schwachstellen in Betriebssystemen und Anwendungen entdeckt und in der National Vulnerability Database des US-CERT dokumentiert.

Mut zur Lücke ist vor diesem Hintergrund für IT-Administratoren keine Tugend. Schließlich tragen sie die Verantwortung für die Sicherheit der Daten und einen störungsfreien Betrieb. Kundendaten, Geschäftszahlen, Entwicklungsunterlagen – die Konsequenzen eines erfolgreichen Cyberangriffs können den Betrieb lahmlegen und Firmeninterna offenlegen. Neben finanziellen Verlusten und einem Imageschaden für das Unternehmen drohen im ungünstigsten Fall sogar staatsanwaltschaftliche Ermittlungen. Zum Beispiel wenn der Verdacht auf einen Verstoß gegen Datenschutzrichtlinien besteht.

Längst sind für schadensträchtige Cyberangriffe auch keine weitreichenden Programmierkenntnisse mehr erforderlich. Viele Attacken gehen inzwischen auf das Konto von Kriminellen, die auf im Internet verfügbare Exploits zurückgreifen. Derartige Angriffssoftware, die gezielt eine bekannte Schwachstelle ausnutzt, wird im Internet gratis oder gegen Bezahlung angeboten. Verfügbar ist sogar eine grafische Benutzeroberfläche, sodass Angriffe auch für mittelmäßig begabte Hacker kein Problem mehr darstellen.

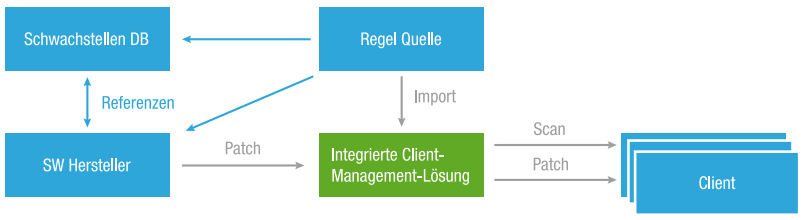
Firewall und Virenscanner bieten inzwischen einen sehr wirkungsvollen Schutz gegen in der Vergangenheit populäre Angriffsmethoden. Da diese Sicherheitsvorkehrungen kaum noch auszuhebeln sind, haben sich Angreifer inzwischen auf Attacken über die Hintertür verlegt. Bei diesen Reverse-Angriffen werden Firewall und Virenscanner einfach umgangen, indem eine Sicherheitslücke in einer Software ausgenutzt wird. Ein Beispiel: Über eine E-Mail mit einem sensationell günstigen Angebot wird ein Mitarbeiter auf eine präparierte Webseite gelockt, die sich eine Lücke im Flash-Player zunutze macht und so einen Schadcode auf dem Rechner ausführen kann. Dieser lässt den Rechner eine Verbindung nach außen zum Server des Angreifers aufbauen, die ihn zum willigen Sklaven des Angreifers macht. Da die Verbindung aus dem Unternehmen heraus aufgebaut wird, greift die Firewall nicht ein.

Neben präparierten Webseiten werden auch manipulierte Dateien (z. B. Office-Dokumente, PDFs) eingesetzt. Es wurden auch bereits Angriffe über bösartige Anzeigen auf eigentlich harmlosen Internetseiten ausgeführt. Oft verwenden Angreifer auch Informationen aus sozialen Netzwerken, um ihre Opfer gezielt in die Falle zu locken und sie zum Öffnen einer bestimmten Datei oder zum Klick auf einen Link zu bewegen. Und egal wie detailliert die Verhaltensregeln des Unternehmens und die Warnungen der Admins auch sein mögen: Irgendwann macht ein Mitarbeiter vorsätzlich oder fahrlässig einen Fehler und geht einem Angreifer auf den Leim. Nötig sind daher auch technische Schutzmaßnahmen gegen solche Angriffsmethoden.

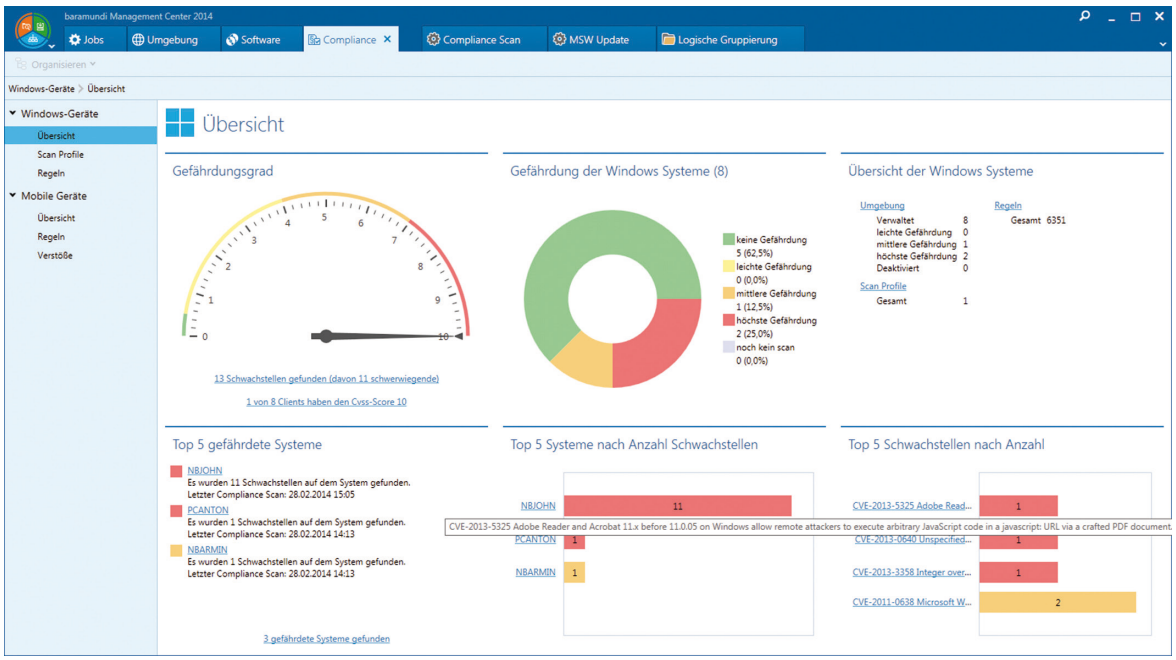
Vorsorgeuntersuchung für die IT

Solange eine Schwachstelle nicht bekannt ist und im Verborgenen zwischen Millionen Zeilen Programmcode schlummert, sind die von ihr ausgehenden Gefahren äußerst gering. Die Schwachstelle ähnelt einem offenen Fenster, das noch niemand entdeckt hat. Gefährlich wird es, sobald sie weithin bekannt sowie in einschlägigen Schwachstellendatenbanken dokumentiert ist, was oft dann passiert, wenn der Softwarehersteller einen Patch bereitgestellt hat. Denn auch potenzielle Angreifer und Exploit-Entwickler lesen diese Datenbanken, analysieren die vom Hersteller bereitgestellten Patches und können daraus Rückschlüsse ziehen, wie sich die Lücke ausnutzen lässt.

Solange der Patch nicht auf allen betroffenen Geräten eingespielt wurde, sind daher über die Schwachstelle wirkungsvolle Angriffe ausführbar, gegen die kaum Gegenwehr möglich ist. Am offenen Fenster lehnt nun eine Leiter, die Zahl der Attacken unter Ausnutzung der Lücke steigt stark an. Für einen wirksamen Schutz gegen Angriffe ist es daher essenziell, Sicherheitslücken auf allen Geräten zu erkennen und alle nötigen Patches unverzüglich, flächendeckend und zuverlässig einzuspielen.



Komponenten und Abläufe einer integrierten automatisierten Schwachstellenmanagement-Lösung



Ein Compliance-Dashboard macht Schwachstellen in der eigenen IT-Umgebung transparent.

Ohne automatisierte Hilfsmittel ist diese Anforderung angesichts der großen Zahl von Geräten, eingesetzter Software und Sprachversionen de facto nicht zu erfüllen. Der Administrator müsste 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. Ein automatisiertes Patch-Management für Microsoft-Produkte reicht alleine nicht aus: Es 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, die anerkannte Sicherheitsorganisationen pflegen, laufend aktualisieren und online zur Verfügung stellen. In diesen Datenbanken werden die Schwachstellen bewertet und nach Gefährdungspotenzial markiert. Ein solcher Schwachstellenscan findet bei minimiertem Ressourcenverbrauch im Hintergrund statt und beeinträchtigt den angemeldeten Nutzer am Client nicht bei der Arbeit. Gleichzeitig nimmt er potenziellen Angreifern den Vorsprung: Der IT-Administrator erhält einen umfassenden Überblick über etwaige Lücken. Eine gute Lösung bietet eine Drill-Down-Möglichkeit, zum Beispiel nach den Clients mit den meisten oder den gefährlichsten Lücken.

Updates und Patches zentral verteilen

Für das schnellstmögliche Schließen der Lücken stehen ebenfalls automatisierte Hilfsmittel zur Verfügung. Im Idealfall sind diese mit dem Schwachstellenscanner in einer integrierten, ganzheitlichen Client-Management-Software zusammengefasst, sodass der gesamte Prozess vom Aufspüren der Lücken bis zur Patch-Verteilung in einer einheitlichen Lösung zügig ablaufen kann.

Neben Microsoft-Patches sollte eine Lösung für das Schwachstellenmanagement mindestens auch Updates für häufig genutzte Anwendungen wie Adobe Reader, Java oder Firefox zentral und automatisiert verteilen, die aufgrund ihrer großen Verbreitung bei Angreifern besonders populär sind. Aktuelle Softwarepakete für zahlreiche Anwendungen sind auch als Managed Services von Client-Management-Herstellern verfügbar. Darüber hinaus lässt sich jede Software, die mit einer Client-Management-Lösung automatisiert nach Original-Setup-Verfahren verteilt werden kann, mit dieser automatisiert patchen.

Es genügt für ein wirksames Schwachstellenmanagement aber nicht, von einer Lücke zu wissen und eine Patch-Installation anzustoßen. Essenziell ist auch das Wissen darüber, ob das sicherheitsrelevante Update tatsächlich auf allen Clients angekommen ist. Installationen können fehlschlagen, vom Benutzer blockiert werden oder ein Notebook im Außeneinsatz könnte nicht erreichbar sein. Die eingesetzte Lösung für die Patch-Verteilung muss daher eine Rückmeldung zum Installationsstatus sowie zu etwaigen Fehlern geben.

Wichtiger Baustein Schwachstellenmanagement

Ein automatisiertes Schwachstellenmanagement sorgt für mehr Transparenz und eine größtmögliche Aktualität der Client-Systeme und Server im Unternehmen. Ebenso wie eine Firewall allein, kann es 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 und automatisiertes Backup von Daten und Benutzereinstellungen, 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, die inzwischen in nahezu jedem größeren Netzwerk zu finden sind, 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.