



Systemmanagement: Der Weg ist das Ziel

Security- und Konfigurationsmanagement müssen Hand in Hand gehen, um größtmögliche Sicherheit zu erreichen. Voraussetzung dafür sind spezielle Softwarelösungen, mit denen sich alle IT-Assets eines Unternehmens über den gesamten Lebenszyklus kontrollieren und verwalten lassen.

(erschienen in Network Computing Security Guide März 2006, S. VI; Autor: Michael Naunheim/ Thomas Schumacher)

Mit der in den letzten Jahren stetig gewachsenen Bedeutung der IT haben auch die potenziellen Gefährdungen und vor allem die damit verbundenen wirtschaftlichen Risiken enorm zugenommen. Bedrohungen wie Viren und Würmer oder unberechtigte Zugriffe auf Unternehmensrechner stellen eine ständige Bedrohung für Unternehmen aller Größenordnungen dar.

Prinzipiell lassen sich zwei Arten von Sicherheitsbedrohungen unterscheiden: diejenigen, die Ausfälle erzeugen – wie Viren und Würmer - und diejenigen, die Systeme entblößen und unautorisierten Zugriff ermöglichen, der wiederum den Diebstahl von Informationen zur Folge haben kann. Ständig eröffnen neue Formen von Viren, Würmern, Trojanern oder Spyware Sicherheitslöcher in Betriebssystemen oder Internet-Browsern und bieten Hackern die Möglichkeit, wichtige Unternehmensdaten abzugreifen oder sonstige Schäden anzurichten.

Gelegentlich stellen sogar Quellen eine Bedrohung dar, die auf den ersten Blick völlig harmlos erscheinen: ein gutes Beispiel hierfür ist die Diskussion um einen versteckten Kopierschutz auf Musik-CDs von SONY BMG, der als eine Art Spyware eine potenzielle Sicherheitslücke für Hacker eröffnet hat. Anhand dieses Beispiels wird deutlich, dass jedes noch so gut geschützte Netz irgendwann ein Loch aufweisen kann.

Einbeziehung des Konfigurationsmanagements

Einzelne Lösungen wie Antivirusprogramme oder eine Firewall sind längst nicht mehr in der Lage, eine IT-Infrastruktur effizient zu schützen. Schlimmer noch: sind einige kritische Bereiche gut geschützt und andere nicht, so ist trotz des betriebenen Aufwands der Effekt gleich null – die Ressourcen sind immer noch angreifbar.

Es liegt auf der Hand: wenn schon ein einzelner ungeschützter oder nicht aktuell gepatchter PC das gesamte Netzwerk gefährden kann, dann ist das Wissen um jede Komponente der Infrastruktur absolute Voraussetzung für maximale Sicherheit. Was nützt es, den Haupteingang zu vernageln, wenn die Hintertür sperrangelweit offen steht?

Daher ist es notwendig, jedes einzelne Rechnersystem kontinuierlich auf dem neuesten Stand zu halten. Dies betrifft nicht nur Antivirensoftware sondern vor allem Anwendungen, Betriebssysteme und den Gesamtstatus des Systems. Besonders wichtig dabei ist eine optimale Kooperation von Security- und Systemkonfigurations-Management.

Administratoren benötigen Werkzeuge, mit denen sie durch Trendanalyse die sprichwörtliche Nadel im Heuhaufen finden können. Ziel ist es, die enorme Komplexität der Aufgabe zu reduzieren.

Konfigurationsmanagement – also das Wissen, welche Assets mit welchen Eigenschaften im Unternehmen anzutreffen sind – ist daher Voraussetzung für größtmögliche Sicherheit: Welches Notebook ist gepatcht? Welche Betriebssystemversionen und Anwendungen sind installiert? Welche Server sind von der gerade entdeckten Schwachstelle betroffen? Nur, wenn solche Informationen ständig automatisch abgerufen und ausgewertet werden, können die verantwortlichen IT-Mitarbeiter durch Aktualisierungen die bedrohten Systeme wieder sicher machen.

Eine Lösung für sieben Sicherheitsprobleme

Moderne Softwarelösungen sind heute im Zusammenspiel mit unternehmensweiten Sicherheitsrichtlinien in der Lage, einen Großteil der anfallenden Aufgaben zu automatisieren und so den Sicherheitslevel konstant hochzuhalten. Altiris hat die Client Management Suite (Level 2) erweitert sowie die Total Management Suite neu auf den Markt gebracht, damit IT-Organisationen gleichzeitig die Bewertung, Überwachung und Kontrolle von Sicherheitslücken durchführen können. In ihnen sind nun die wichtigsten Funktionen vereint, um den sieben vorrangigen Sicherheitsproblemen zu begegnen:

1. Antivirus-Status
2. Status von Sicherheits-Patches

3. Branchenbekannte Schwachstellen
4. Status der persönlichen Firewall
5. Sicherheitseinstellungen des Systems
6. Unautorisierte Software
7. Unautorisierte Hardware

Eine leistungsfähige Sicherheitslösung erfordert eine kontinuierliche Überwachung und Pflege aller sieben Sicherheitsbereiche. Neben Tools für Web Administration und Application Metering sind daher auch die Komponenten Auditing, Deployment sowie Patch Management durch die Suite abgedeckt.

Sicherheit beginnt vor den Servern

In einem nachhaltig sicheren System sollten Rechner erst dann ins Netzwerk gelangen dürfen, wenn sie auf Übereinstimmung mit den Sicherheitsrichtlinien eines Unternehmens geprüft wurden. Ein Administrator kann mit den Altiris-Lösungen beispielsweise festlegen, dass nur PCs mit aktuellen Virendefinitionen, laufender Firewall und einem Betriebssystem mit neuesten Patches vollständigen Zugang zum Netz erhalten. Rechner, die bei einer solchen Prüfung durchfallen, werden abgewiesen oder in ein Quarantäne-Subnetzwerk, ein VLAN, umgeleitet. Erst, wenn sie auf den neuesten Stand gebracht wurden bzw. „gereinigt“ sind, dürfen sie wieder ins Unternehmensnetzwerk.

Security lässt sich also nicht an einer Ebene im Netzwerk festmachen. Sinnvoll ist vielmehr eine mehrstufige Strategie. Dabei kommt den Systemen vor den Servern eine besondere Bedeutung zu. Quasi als „Abfangjäger“ stellen Router und Switches vor dem eigentlichen Unternehmensnetzwerk die letzte Verteidigungslinie gegen Angriffe dar. Hier werden nach vordefinierten

Sicherheitsregeln Datenpakete analysiert und gefiltert.

Die Altiris Sicherheitslösungen unterstützen dabei den „Network Admission Control“-Ansatz (kurz NAC) von Cisco, der als Teil der „Cisco Self-Defending Network“-Initiative für Netzwerke einen automatischen Schutz vor Bedrohungen sicherstellen soll. Die Sicherheit wird verbessert, indem das Netzwerk selbst den Zugang für Endgeräte wie PCs, Server oder PDAs reguliert, die nicht den Sicherheitsstandards einer Organisation entsprechen. Dazu bietet die Lösung einen Mechanismus, mit dem der Netzwerkzugang auf Basis definierter Sicherheitsrichtlinien blockiert werden kann.

Dabei bleibt es dem Administrator und den eingesetzten Werkzeugen überlassen, welche Gerätezustände als "gesund" oder "ungesund" eingestuft werden. Systeme, die nicht konform mit den Sicherheitsrichtlinien sind, sind schwierig zu identifizieren, isolieren und nur aufwendig wiederherzustellen. Bisher können infizierte Systeme beispielsweise erst bei der Anmeldung an einer Windows-Domäne auf Sicherheit überprüft werden. Dieser Zeitpunkt ist jedoch viel zu spät, da die Geräte bereits Kontakt zum Netzwerk haben und so Infizierungen einschleppen können. Genau dieses Problem adressiert NAC und verfügt zudem über eingebaute Mechanismen, um Probleme selbstständig zu beheben, sodass ein Gerät wieder auf vollständige Netzwerkverbindung zurückgesetzt werden kann. Im Zusammenspiel mit den Altiris Lösungen bietet die Cisco-Technologie eine einfache Möglichkeit, mehr Sicherheit zu erreichen und gleichzeitig die Gesamtkosten unter Kontrolle zu halten.

Sicherheit – kein Zustand, sondern eine Aufgabe

Wenn man sich intensiv mit der Materie befasst wird schnell klar, dass Sicherheit kein erreichbarer Zustand ist, sondern eine kontinuierliche Aufgabe, die niemals endet. Unternehmen sind gezwungen, ein aktives Sicherheitsmanagement zu praktizieren, denn Sicherheit ist für viele deutsche Firmen eine gesetzliche Vorgabe. Das zum 1. Mai 1998 in Kraft getretene Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) verpflichtet börsennotierte AGs und größere GmbHs zur Einrichtung eines Risiko-Management-Systems sowie zur Erstellung eines regelmäßigen Risikoberichtes, der auch die Vorsorge mit Blick auf die Unternehmensdaten einschließt. Darüber hinaus sind spätestens mit der Kreditvergabe-richtlinie Basel II Maßnahmen der IT-Sicherheit auch ein Faktor bei der Bewertung der Kreditwürdigkeit eines Unternehmens.

Vollständige Sicherheit lässt sich allerdings auch mit der besten verfügbaren Software nicht erreichen, dafür sind die Bedrohungen einfach zu komplex. Viele Netzwerkadministratoren wären aber bereits froh, wenn sie durch intelligentes und konsequentes Systemmanagement die größten Risiken ausschließen oder zumindest minimieren könnten. Mit den besprochenen Systemmanagement-Tools liegt dafür eine gute Basis vor.

*Autor: Michael Naunheim
Altiris EMEA Alliance Marketing
Manager*