



# Kooperation für mehr Sicherheit

*Angriffe durch Viren oder Würmer nehmen kontinuierlich zu. Die IT-Industrie arbeitet daher daran, Sicherheitsprobleme bereits auf der Ebene vor den Servern abzufangen und so eine sicherere Infrastruktur aufzubauen. Das Ziel ist somit die möglichst enge Verzahnung von Security-, Netzwerk- und IT-Lifecycle-Management.*

(erschienen in LanLine Spezial III/2005, S. 34-37; Autor: Thomas Schumacher/ Mike Goedecker)

Sicherheit ist heute für Unternehmen ein ständiger Wettlauf mit der Zeit. Ein Berg von Aufgaben ist abzutragen, um das Netzwerk vor Hackern, Spionen und anderen Sicherheitsbedrohungen zu schützen. Insbesondere Viren und Würmer stellen eine ständige Bedrohung für Unternehmen aller Größenordnungen dar. Neben den Desktops greifen sie Server, IT-Infrastruktur und auch mobile Endgeräte an. Die Schäden durch Ausfallzeiten gehen in die Millionen, verursacht durch Produktivitätsverlust und Kosten zur Prävention. Die wachsende Intelligenz der Schädlinge und ihre Eigenschaft, sich selbst weiterzubreiten, machen Angriffe immer gefährlicher. Zwar haben alle von Ernst & Young im Rahmen einer Untersuchung befragten Unternehmen Antivirenprogramme im Einsatz, aber das allein reicht nicht aus. Antivirus-Lösungen stoßen seit langem an ihre Grenzen, da sie auf Signaturen basieren, mit deren Hilfe sie Viren und Würmer identifizieren. Sie erkennen daher nur bekannte Bedrohungen und können keinen Schutz vor „DayZero“ Angriffen und den von ihnen verursachten Denial-of-Service Effekten bieten.

In großen Firmen kommen ständig neue Endgeräte und Mitarbeiter hinzu. Den Über-

blick zu behalten fällt vielen IT-Verantwortlichen schwer und ist in vielen Fällen geradezu unmöglich. Daher taucht immer öfter ein weiteres Problem auf: Server, Desktops und Laptops entsprechen nicht dem aktuell geforderten Sicherheitsniveau des Unternehmens. Insbesondere bei mobilen Mitarbeitern, die außerhalb der Unternehmensnetzwerke surfen, können sich deshalb Schädlinge einschleichen. Unterwegs ist der Laptop meist ausschließlich durch die Signatur basierten Verfahren geschützt. Taucht nun ein unbekannter Schädling auf – ein so genannter Day-Zero Exploit – kann das Sicherheitssystem des Laptops nicht entsprechend reagieren, da es den Schädling nicht kennt. Sobald der mobile Anwender sich erneut im Unternehmensnetzwerk anmeldet, kann sich der Virus/Wurm ungehindert ausbreiten: dann ist die Katastrophe da.

## Quarantäne erhöht Sicherheit

Security ist nicht an einer Ebene im Netzwerk festzumachen, sinnvoll ist vielmehr eine mehrstufige Strategie. Dabei kommt den Systemen direkt vor den Servern eine besondere Bedeutung zu. Quasi als „Abfangjäger“ stellen Router und Switches die letzte Verteidigungslinie gegen Angriffe dar.

In einem hochgradig sicheren System sollten Rechner erst dann ins Netzwerk gelangen dürfen, wenn sie auf Übereinstimmung mit den Sicherheitsrichtlinien eines Unternehmens geprüft wurden. Auf diese Weise könnte ein Administrator zum Beispiel 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. Ansätze dieser Art finden immer stärkere Akzeptanz und werden z.B. durch die Trusted Computing Group mit ihrer Spezifikation zur Netzsicherheit „Trusted Network Connect“ unterstützt.

Einer der interessantesten Ansätze kommt von Cisco, die mit „Network Admission Control“ oder kurz NAC, eine Initiative ins Leben gerufen haben, um Netze besser vor Bedrohungen, sowohl internen als auch externen, zu schützen. NAC ist Teil der „Cisco Self-Defending Network“-Initiative, mit der Netzwerke einen automatischen Schutz vor Bedro-

hungen erhalten sollen. 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 ist es allerdings 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. Die dazu notwendigen Vorgänge sind zeit- und kostenaufwendig und gefährden die Unternehmenssicherheit, wenn sie unterbleiben. 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 (Layer 3) und so Infizierungen einschleppen können. Genau dieses Problem adressiert NAC. Zudem verfügt NAC über eingebaute Mechanismen, um Probleme selbstständig zu beheben, sodass ein Gerät wieder auf vollständige Netzwerkverbindung zurückgesetzt werden kann. Im Zusammenspiel mit den Lösungen von Altiris bietet die Cisco-Technologie eine einfache Möglichkeit, NAC einzuführen und gleichzeitig die Gesamtkosten für die Informationstechnologie in einem Unternehmen unter Kontrolle zu halten.

Die Funktionsweise von NAC

NAC ist aus einer Reihe einzelner Komponenten zusammengesetzt, mit denen die Zugangsrichtlinien erstellt und verwaltet werden können. Zum einen ist das der Cisco Trust Agent (CTA) – eine von Cisco Systems entwickelte Schnittstelle (API) mit deren Hilfe sich Informationen über das aktuelle Sicherheitsniveau des Endgerätes abfragen lassen. Diese werden über eine gesicherte Verbindung zum nächsten Cisco Netzwerkzugangsgesamt übertragen, das dann die Zugangskontrolle regelt. Cisco hat die Cisco Trust Agent Technologie an die führenden Antivirus-Softwarehersteller – Symantec, TrendMicro, Network Associates – und den Partner IBM lizenziert. Diese Unternehmen integrieren CTA in ihre Produkte und machen sie so für Unternehmen verfügbar. Mithilfe des CTA lassen sich Informationen, über die auf dem Endgerät installierte Antivirus-Software und die derzeit verwendeten Signatur-Dateien, abfragen. Die Integration des CTA in den Cisco Security Agent erweitert die Abfragemöglichkeiten auf Versionsinformationen des Betriebssystems, Patch- und Hotfix-Level. Endgeräte, die nicht den notwendigen Patchlevel aufweisen, können so leicht identifiziert und isoliert werden.

Eine Schlüsselrolle nehmen in diesem Konzept Netzwerkzugangsgesamte ein – das sind Router, Switches, Wireless Access Points oder dedizierte Sicherheits-Appliances, mit deren Hilfe die Sicherheitsrichtlinien durchgesetzt werden. Diese Geräte fordern von jedem am Netzwerk teilnehmenden Endgerät Informationen über das aktuelle Sicherheitsniveau und leiten dieses zur Überprüfung an Richtlinienserver weiter. Anhand der dort hinterlegten

Unternehmens-Sicherheitsrichtlinie entscheidet der Server, ob das Endgerät Zugang erhält (permit), der Zugang verweigert (deny), es in Quarantäne genommen (quarantine) oder der Zugang stark eingeschränkt (restrict) wird. Die Umsetzung der Entscheidung erfolgt dann wieder im Netzwerkzugangsgesamt. Als dritte Komponente werten Richtlinienserver die Informationen über das Sicherheitsniveau der Endgeräte aus und wählen die jeweils notwendige Zugangsbeurteilung. Der Cisco Secure Access Control Server (ACS), ein Authentisierungs-, Autorisierungs- und Accounting-Server, ist die Basis des Richtlinienserver-Systems. Er arbeitet direkt mit den AV-Richtlinienservern der Cisco NAC-Partner zusammen, die weitere produktspezifische Auswertungen ermöglichen. Als letztes Element wird das Management System mit CiscoWorks VPN/Security Management Solution (VMS) für die Einrichtung/Verwaltung der Cisco NAC Infrastruktur eingesetzt sowie CiscoWorks Security Information Management Solution (SIMS) für die Auditierung und das Reporting. Die Cisco NAC Partner bieten zusätzliche Verwaltungs-/ Audittools für ihre Produkte an.

### **Integration in Managementlösung**

Für die effiziente Umsetzung von NAC und ähnlichen Ansätzen ist es unabdingbar, dass IT-Manager ihr weltweites Netzwerk kennen und schnellen Zugriff auf alle Systeme haben. Quasi per Knopfdruck müssen sie in der Lage sein, den Status jedes einzelnen angeschlossenen Gerätes überprüfen zu können. Altiris hat sich daher am NAC-Programm beteiligt, damit Unternehmen in der Lage

sind, den Cisco Trust Agent in ihre Infrastruktur zu integrieren und so Softwareanwendungen, Updates, Patches oder Konfigurationsänderungen mittels einer einheitlichen Managementlösung zentral zu überwachen und zu steuern. Mit Health Check stellt man eine Lösung bereit, mit der sich sämtliche Komponenten einer Installation auffinden und registrieren lassen. Eine tief gehende Analysefunktion informiert den Administrator über den Status eines Gerätes und hilft bei der Vorbereitung eventuell notwendiger Aktionen. Diese lassen sich im Vorfeld definieren, wobei eine beliebige Kombination von Elementen aus der Altiris Datenbank für das Konfigurationsmanagement sowie aus dem Patch Repository möglich ist. Mit dem Konfigurationsmanagement „Provisioning“ kann eine solide Ausgangsbasis festgelegt werden, die als Grundlage für einen reibungslosen Betrieb der angeschlossenen Komponenten dient. Mittels Client- und Server-Management „Remediation“ bietet man eine integrierte Lösung für das Patch Lifecycle Management zur Verfügung.

Sämtliche Komponenten eines Netzwerkes, die von den vordefinierten Sicherheitsrichtlinien eines Unternehmens abweichen, werden an vordefinierte Richtlinien automatisch angepasst. In vier Schritten begegnet man den Herausforderungen, die einen IT-Lifecycle umfassen und ermöglicht den Aufbau einer kompletten Quarantäne-Umgebung für ein Netzwerk:

Der erste Schritt ist die Vorbereitung: Werkzeuge erleichtern die Planung und Umsetzung von NAC. Sie ermöglichen die Identifizierung und das Lösen bekannter Sicher-

heitsbedrohungen, kartieren die aktuelle Netzwerkkonfiguration für die Planung notwendiger Änderungen, automatisieren die Quarantäne bei VLAN-Rollouts und sorgen für die Installation und Konfiguration der CTA. Darüber hinaus erzeugen sie eine ACS-Ausnahmeliste, indem sie bereits im Vorfeld Geräte identifizieren, die nicht CTA-fähig sind (dazu zählen beispielsweise Drucker), schätzen die Auswirkungen der Quarantäne-Richtlinien ab und ermitteln, welche Computer vor der NAC-Implementierung aufzurüsten sind.

Als zweiter Schritt folgt das Prüfen: Hier entscheidet sich, welche Geräte (verwaltet, nicht verwaltet oder nicht verwaltbar) Netzwerkzugang erhalten. Dazu dient die Erstellung von Richtlinien zum Sollzustand (der „Gesundheit“) Diese richtlinien greifen auf CMDB und das Patch Repository zurück.

Drittens folgt das Blockieren: hier vereinfacht die Managementlösung die Verwaltung von NAC. Eine abgestufte Upgrade-Strategie dient dazu, Randumgebungen so lange mit NAC-ähnlicher Funktionalität sicher zu machen, bis das Unternehmen Legacy- oder Nicht-Cisco Netzwerkgeräte aufgerüstet hat. Bei einer auffällig hohen Zahl von geblockten Rechnern kann die Lösung automatisch einen Alarm auslösen. Webbasierte Berichte helfen, die NAC-Leistung über die Zeit zu verfolgen und zu verbessern.

Den vierten und letzten Schritt bilden Abhilfemaßnahmen: der Zugriff auf die Systemmanagementlösungen ermöglicht es, Geräte aus der Ferne und auf Basis von Richtlinien aufzurüsten. Dies vereinfacht den Prozess, einen Computer so schnell wie möglich an ein Netzwerk anzubinden.

## Fazit

Sicherheit im Unternehmen darf nicht als isolierte Komponente betrachtet werden, wenn ein Unternehmen global aufgestellt ist und mit Kunden, Partnern, Outsourcing-Partnern oder Application Service Providern verbunden ist. Dabei ist die Zeit der Vogel-Strauß-Unternehmenspolitik unwiederbringlich vorbei: neue gesetzliche Regelungen wie Basel II oder die derzeit diskutierten Gesetzesentwürfe zur Managerhaftung machen das Ignorieren des Problems zu einer hochbrisanten Angelegenheit. Wer künftig als Geschäftsführer nicht nachweisen kann, alles Notwendige getan zu haben, kann schnell neben seinem Job auch noch Haus und Hof verlieren.

Computersicherheit ist ein wesentlicher Aspekt im Rahmen des IT Lifecycle-Managements. Integrierte Lösungen für das Aufspüren möglicher Sicherheitslöcher, ein ausgefeiltes Patch-Management und Module für die Überwachung von Vorgängen im Sicherheitsbereich sowie automatisierte, regelbasierte Anwendungen für notwendige Reparaturen sind unerlässlich. Das Ziel solcher Initiativen wie eines quarantänefähigen Netzwerkes ist es dabei, einerseits Verwaltungs- und Betriebskosten zu senken, andererseits aber gleichzeitig die Sicherheit von Computer-Ressourcen zu erhöhen.