

Rollenbasierte Rechte vereinfachen Verwaltung

Endpunkte im Netz sind kritischer Faktor

Der Zugriff auf das Netzwerk ist unter IT-Managern ein Topthema: 95 Prozent sehen einen erhöhten Bedarf an Zugangskontrollen – deren Steuerung aber immer komplexer wird, wie fast zwei Drittel meinen.

Dies ergab eine Umfrage des Sicherheitsspezialisten Consentry unter 200 Netzwerkkompetenten. Dabei zeigte sich auch, dass Firmen Hackerangriffe zwar mit viel Aufwand abwehren, externe Mitarbeiter und solche von Fremdunternehmen sich aber nahezu uneingeschränkt im LAN bewegen können. Hinzu kommt eine hohe Fluktuation: Den Anteil der vorübergehend tätigen Mitarbeiter als Mittel bis hoch bezeichnen 82 Prozent der Unternehmen mit über 1000 Beschäftigten.

Um die Endpunktkontrolle an diese Anforderungen anzupassen, hat Consentry seine Lanshield Access Control Platform mit Microsofts Network Access Protection (NAP) integriert. NAP zielt wie andere – auch als Network Access Control (NAC) bezeichnete – Produkte auf den Schutz des Netzwerks vor Endgeräten, die nicht den Sicherheitsbestimmungen entsprechen. Im Rahmen der Kontrolle werden dabei etwa die Aktualität von Antivirenprogrammen oder der eingespielten Software-Patches geprüft.

Mit Consentrys Lanshield können die einzelnen Nutzernach dem Netzwerkzugriff

erteilten Rechte einfach anhand der jeweils zugeteilten Rollen definiert werden. So lässt sich etwa festlegen, worauf ein Anwender Zugriff hat und welche Aktionen er dort vornehmen darf. Zudem erweitert Lanshield den Zugangs-Check von Microsofts NAP auf Plattformen, die nicht von dieser unterstützt werden – neben Nicht-Windows-Systemen beispielsweise Drucker oder VoIP-Telefone.

Zentrale Konsole schafft Überblick

Die Kontrolle von Endpunkten – inklusive VoIP- und Smartphones – verbessern wollen auch IBM und Mirage Networks mit ihrer Kooperation: Die Partner kombinieren den Proventia Management Site Protector des von Big Blue übernommenen ISS und Mirages Endpoint Control. Das Produkt-Bundle soll ein zentralisiertes Access-Management erlauben. Laut Mirage-Vize-Präsident Michael D'Eath werde „die gemeinsame Lösung dem Administrator Informationen über die Sicherheit der Endpunkte, die Bedrohungslage und die Einhaltung der Policy anzeigen“.

Die Aktivität der Anbieter ist nicht verwunderlich: Die Marktforscher von Infonetics schätzen, dass sich der Umsatz mit NAC von 323 Millionen Dollar in 2005 im kommenden Jahr mit 3,9 Milliarden mehr als verzehnfacht. Barbara Gengler/sts

Network Access Control: Forescout berücksichtigt bei Policies Anforderungen regionaler Domains

Besucher stellen größtes Risiko für Infrastruktur dar

Mit zwei Appliances für die Netzzugangskontrolle (NAC) sichert Forescout nun auch Filialen mit bis zu 50 Arbeitsplätzen sowie Unternehmen mit bis zu 2500 Stationen ab. Die steuernde Security-Anwendung fährt gefährliche Programme auf Endgeräten herunter – auch auf Macs.

Mit den beiden NAC-Systemen CT-R und CT-2000 erweitert Forescout aus Cupertino sein Produktspektrum nach unten und oben. Laut Forescout-Marketing Ray Wizbowski kostet der Einstieg knapp 5000 Dollar, die Oberklasse startet bei 50 000 Dollar. Leben haucht der Network Access Control die Software Counter ACT ein, die nun in der Version 6.0 vorliegt. „Administratoren können damit automatisch für das Netzwerk riskante Anwendungen stoppen, die auf Systemen laufen, die ins Netz wollen“, benennt Wizbowski ein Highlight. „Zudem röntgt die Version 6.0 auch die Macintosh-Systeme und vereinfacht die Policy-Erstellung.“

Als Schlüsselfaktoren für den Erfolg einer NAC-Technik nennt Wizbowski die Bereitstellung der erforderlichen Informationen, Skalierbarkeit sowie die Richtlinienerstellung und -einhaltung. „Generell sind drei technische Ansätze maßgeblich: Marktführer Cisco agiert

Den Netzzugang von bis zu 2500 Mitarbeitern kontrollieren die Forescout-Appliances – wer mit nicht zugelassenen Anwendungen ins Netz will, den verpfeift Counter ACT beim IT-Leiter oder Chef.

Foto: Forescout



mit einer Switch-basierten Lösung, also einem Stück Infrastruktur. Einige Unabhängige setzten ihre Lösung zwischen den Access-Layer und den Distribution-Layer-Switch – und Forescout bedient sich am Switch auf dem Distribution-Layer.“ Der Vorteil: Bei mehreren Verbindungspunkten reicht dadurch ein Gerät aus.

Für globale Organisationen sieht der Forescout-Manager zwei NAC-Herausforderungen: „Das Primärproblem sind Besucher, die in die Infrastruktur kommen – Gäste, Geschäftspartner oder Lieferanten klinken eben ihr Notebook im Konferenzraum ans Netz.“

Das zweite Problem sei die zunehmend mobile Mitarbeiterschaft: „Es ist sicherzustellen, dass jedes Gerät im Netzwerk den Basis-Sicherheitsrichtlinien gehorcht.“ Dafür empfiehlt er vier Maßnahmen: eine universelle Policy, Endpunktkontrolle,

Definition einer angemessenen Reaktion auf jeden Verstoß und ein nicht disruptives Vorgehen.

Die Definition von Policies ist in Counter ACT Version 6.0 überarbeitet worden. „Es gibt pro Policy einen Entscheidungsbaum für jedes Kriterium. Für ein Antivirus-Update waren bisher drei separate Regeln erforderlich – in der neuen Version nur eine mit drei Check-Boxes.“ Auch Regionen werden berücksichtigt: Für die Kreation einer Richtlinie in der deutschen Domain wird immer auf die übergreifende Policy verwiesen – über eine Wenn-dann-Steuerung gehorcht das granulare Level stets der General-Policy. Der Infonetic-Analyst Jeff Wilson hat sich die Forescout-Lösung angeschaut. „NAC wird eine kritische Infrastrukturkomponente für Firmen aller

Größenordnungen“, so der Principal Analyst. „Counter ACT bringt alles mit für einen breit angelegten Einsatz – einfache Kostenstruktur, leicht zu implementieren und zu warten.“ So werden beispielsweise bei einer Expansion der Lösung einfach die Policies übernommen. „Zunächst läuft jedes Gerät selbstständig“, erläutert Wizbowski. „Aber wir haben eine Schichtarchitektur – über mehrere Geräte wacht der Enterprise Manager, der die Informationen der Geräte aggregiert.“ Für ein Upgrade schiebe dieser also einfach die gültigen Richtlinien und Konfigurationseinstellungen zum neuen Gerät. rr Interview unter www.computerzeitung.de.

Emulex-Manager Chevallier: In zwei Jahren ist Fibre Channel mit acht Gigabit pro Sekunde Usus – SAN-Connectivity-Lösung erhöht Servicequalität

„Reifegrad der Netzwerkvirtualisierung steigt“

Im Frühjahr wird die Emulex-Lösung Vmpilot ausgeliefert, die an Speichernetze (SANs) angeschlossene virtuelle Maschinen einrichtet und migriert. Emulex-Produktmanager Jean-Yves Chevallier stellt die Entwicklung in den generellen Virtualisierungskontext.

Wann werden wir denn in Reinform virtualisierte Rechenzentren sehen, und was sind die Schritte, die ein CIO dafür gehen muss?

Es wird zwei bis drei Jahre dauern, bis komplette End-to-End-Lösungen am Markt sind. Ein IT-Leiter kann heute noch nicht seine endgültige Lösung definieren: Es gibt zu viele Fortschritte in verschiedenen Bereichen – ich denke an die Kooperation Microsoft-Novell auf der Serverseite oder die Innovationen der Pro-

Im Gespräch

Den gemessenen Zeitraum zwischen Fehlfunktionen führt der Emulex-Softwaredirektor **Jean-Yves Chevallier** ins Feld, um eine technische Spitzenposition für seine Host-Bus-Adapter zu reklamieren. „Das bestätigen aber auch die Virtual-Machine-Hersteller.“ Zudem ziehe die Emulex-Managementlösung die Informationen aus Serverbetriebssystem und Fibre-Channel-Netz zusammen. rr



Foto: Emulex

zessorhersteller Intel und AMD. Aber es lohnt sich, virtuelle Server und Speicher einzuführen und mit Host-Bus-Adapter-Technologie zu experimentieren. Generell trägt der Trend ja auch Bedeutung für künftige Anwendungsarchitekturen.

Sie ist kritisch für die serviceorientierte Architektur (SOA)?

Ohne virtualisierte Umgebung oder extrem vielen Extraressourcen kann eine End-to-End-SOA keine Resultate garantieren. **Wie bewerten Sie den Stand der Technolo-**

gie, die zu flexiblen Infrastrukturen führt?

Die Servervirtualisierung nach Art von VMware ist verstanden, für die Virtualisierung der Speicher gibt es viele Lösungen mit höchst unterschiedlicher Qualität hinsichtlich der Services. Die Virtualisierung des Netzwerks zwischen Server und Speicher gewinnt an Aufmerksamkeit – auch der Reifegrad steigt erst jetzt.

Im ersten Quartal 2007 wird die Emulex-SAN-Connectivity-Lösung Vmpilot für den Microsoft Virtual Server 2005 ausgeliefert. Was bringt sie dem Rechenzentrum?

Vmpilot erzeugt virtuelle Maschinen mit SAN-Verbindung und erleichtert Migrationen – es wird also die Zeit und

der Arbeitsaufwand gespart für das Rekonfigurieren von Massenspeichern und Fabrics sowie das Kopieren von Dateien. Und: Der Microsoft Virtual Server dient ja neben der Hardwarekonsolidierung gerade einer höheren Systemauslastung. Die Vorteile der virtualisierten Verbindung sind mehr Servicequalität sowie einfacheres Management und Trouble-Shooting.

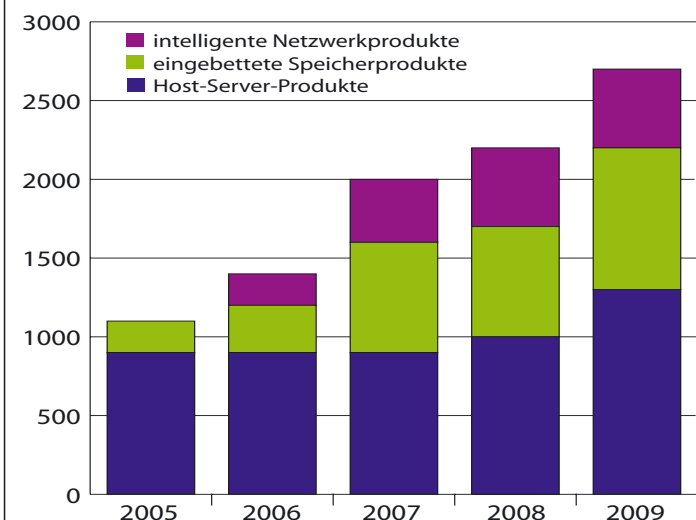
Was verbessert sich im Detail?

Bei der Quality of Service kann die IT-Abteilung Bandbreite oder Geschwindigkeit zu bestimmten virtuellen Maschinen garantieren. Das Management erlaubt eine Rückbelastung für Services auf eine virtuelle Maschine oder eine ganze Gruppe sowie das Zoning – die Unterteilung von Speichernetzen in Teilnetzwerke ist sehr hilfreich für die Absicherung. Und bei der Fehlerbehebung ist die Ursache eines Problems klar identifizierbar – bis hin zur Anwendung die das Speichernetz verletzt hat. Unser Usability-Lab hat mit Großanwendern auch Installation und Betrieb vereinfacht: Niemand muss also dafür extra einen Nobelpreisträger anheuern.

Beim Fibre Channel steigt die Bandbreite. Wie lange reichen die vier Gigabit pro Sekunde?

Ressourcen werden zum Pool

Markt für Storage-Networking-Produkte (in Milliarden Dollar)



Die Konsolidierung und Kosteneinsparung im Rechenzentrum bringt den **Markt für Verbindungstechnik** bei Servern, Speicher und Netzwerken in Schwung. IDC macht aufmerksam auf eine zunehmende Konvergenz der Server-, Speicher- und Fabric-Switch-Virtualisierung: Ergebnis ist eine Utility-Infrastruktur für alle Anwendungen. rr

Quelle: IDC, Gartner, Emulex

COMPUTER ZEITUNG 8/2007

Als erstes wurden alte Anwendungen virtualisiert, wie die Windows NT File Server, wozu wenig Bandbreite erforderlich war. Inzwischen richten sich die Ambitionen auf große Anwendungen – das fing an, als vorletztes Jahr VMware den Support von Solaris angekündigte. Nicht, dass Solaris selbst für viel

Speicherzugriff stehen würde, aber die Anwendungen auf Solaris sind sehr aggressiv beim Speicherzugriff. Deshalb hat sich die Vier-Gigabit-Technologie sehr schnell durchgesetzt, beschleunigt durch die Virtualisierung. Und wegen der virtuellen Server werden es in zwei Jahren acht Gigabit sein. rr



Host-Bus-Adapter verwandelt Emulex in virtuelle Ports. Foto: Emulex