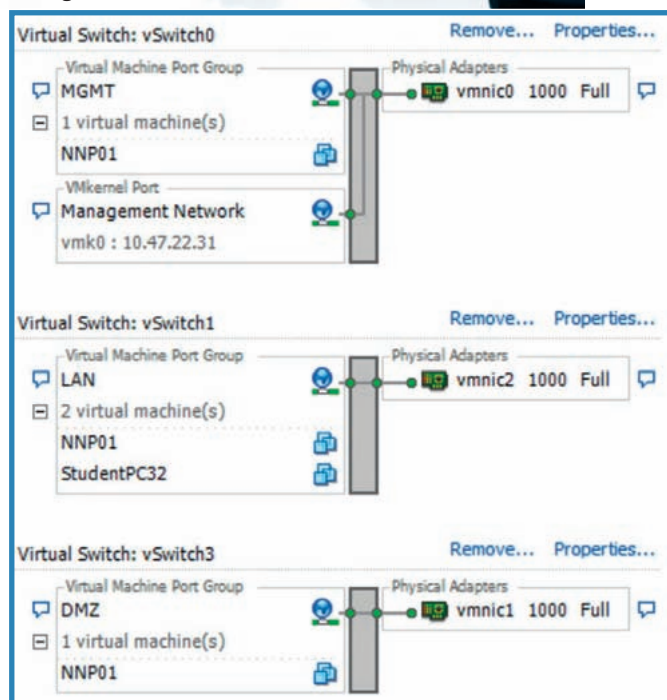


Malwareschutz auf virtuellen Maschinen

Antivirenlösungen auf virtuellen Maschinen können das Gesamtsystem erheblich verlangsamen. Bei knapp kalkulierten Ressourcen fällt die Entscheidung oftmals für einen Verzicht auf die Schutzprodukte. Scanner, die den Netzwerkverkehr überwachen, können strategisch eingesetzt werden und mit überschaubarem Ressourcenbedarf einzelne Maschinen oder Gruppen gegeneinander abgrenzen.

GESICHERT: Die Abbildung zeigt die Verbindung der Scaninterfaces von Norman Network Protection mit den virtuellen Switches vSwitch1 und vSwitch3 sowie die Verbindung des Managementinterfaces mit dem vSwitch0.



Die Virtualisierung von Servern ist aus größeren Netzwerken nicht mehr wegzudenken und wird in immer mehr Unternehmen genutzt. Mehrere Server werden dafür logisch vervielfältigt und dem Netzwerk von einer physikalischen Hardwarekomponente aus zur Verfügung gestellt. Jeder der virtuellen Server hat ein eigenes Betriebssystem, sie alle laufen als Gäste auf einer gemeinsam genutzten Hardware, dem Host-System. Dies spart Kosten für Hardware und senkt den Energieverbrauch; außerdem macht die Bereitstellung neuer Server erheblich weniger Aufwand, da beispielsweise die leidige Strippenzieherei entfällt. Selbst Hochverfügbarkeit lässt sich in solchen virtuellen Umgebungen relativ einfach realisieren, indem virtuellen Maschinen die Möglichkeit zugestanden wird,

sich dynamisch auf der Hardware zu bewegen.

HOHER RESSOURCENBEDARF

Allerdings sind virtuelle Maschinen nicht so stark voneinander abgegrenzt wie physikalische Server. Angreifer können Sicherheitslücken in einem virtuellen System dazu nutzen, um auf andere Systeme zuzugreifen. „Besonders gefährdet sind unternehmenskritische Anwendungen und Daten, da nach einer Virtualisierung oftmals Anwendungen, die auf physischen Systemen unterschiedlichen Sicherheitsanforderungen unterliegen, auf derselben physikalischen Hardware laufen.

In virtuellen Host-Systemen sollte deshalb jede einzelne Maschine mit einer eigenen Antivirenlösung geschützt und gegen die anderen Maschinen abgegrenzt werden“, sagt Jörg

Lützenkirchen, Consultant bei der Norman Data Defense Systems GmbH.

Mit der Anzahl der Maschinen auf dem Host wächst dann auch die Zahl der Virenschutzprodukte. Die Grundauslastung der Hardware steigt allein durch die Anzahl der Virenscanner; gleichzeitig nimmt der Ressourcenbedarf der Scanner durch das Anwachsen der Signaturdatenbanken unaufhaltsam zu. Beide Faktoren werden bei der Dimensionierung der Hosts in der Praxis oftmals nicht ausreichend berücksichtigt; Hersteller-Empfehlungen veranschlagen den Ressourcenbedarf der Virenschutzlösungen häufig zu niedrig oder gar nicht. Die Folge ist eine erhebliche Verlangsamung des Gesamtsystems. Um dieses Versäumnis bei der Planung der Virtualisierungs-Infrastruktur wieder auszugleichen, wären zusätzliche Ausgaben für Hardware nötig, die das Budget für das Projekt, vor allem in kleineren und mittelständischen Unternehmen, erst einmal nicht mehr hergibt. Damit die Performance nicht beeinträchtigt wird, wird deshalb häufig vollständig auf Virenschutz verzichtet; die damit verbundenen Risiken werden in Kauf genommen.

NETZWERKSCANNER

Diese Risiken können laut Lützenkirchen kostengünstig und ressourcenschonend verringert werden, indem in virtualisierter Form netzwerktransparente Virenschutzprodukte



JÖRG LÜTZENKIRCHEN, Consultant bei Norman Data Defense Systems GmbH

verwendet werden, die den Datenverkehr scannen. „Strategisch eingesetzt, reicht eine Lösung wie Norman Network Protection aus, um den jeweiligen Voraussetzungen entsprechend einzelne Maschinen oder Gruppen gegeneinander abzugrenzen. Deren Ressourcenbedarf ist insofern kalkulierbar, als er nur einmal statt mehrmals anfällt und das System daher erheblich weniger stark und mit deutlich geringerer Progression belastet“, sagt Lützenkirchen.

Im Fall der Norman-Lösung werden alle für die Malware-Übertragung relevanten Proto-

kolle wie CIFS, SMB/SMB2, HTTP, FTP, SMTP, POP3, RPC, TFTP und IRC gescannt und auf Wunsch BitTorrent und MSN geblockt. Eine URL-Blockliste kann manuell gepflegt werden. Der Netzwerkverkehr lässt sich auf mehreren Schichten nach den Kriterien IP-Adresse, MAC-Adresse oder VLAN-ID blockieren beziehungsweise sperren.

Für die Abgrenzung bestehen grundsätzlich zwei Möglichkeiten: Dem virtualisierten Netzwerks Scanner werden physikalische Netzwerkkarten zugewiesen, über die zwei Segmente, also Clients, Server oder Netzwerkbereiche, physikalisch zusammengeschaltet werden. Dabei wird der Netzwerkverkehr zwischen den Segmenten gescannt. Alternativ lassen sich mit Norman Network Protection zwei V-Switches verbinden und durch die gesicherte Verbindung wieder zusammenschalten. Die Abbildung auf der linken Seite zeigt die Verbindung der Scanner interfaces von Norman Network Protection mit den virtuellen Switches vSwitch1 sowie vSwitch3 und die Verbindung des Management interfaces mit dem vSwitch0. In dieser Konstellation wird der Traffic einzelner virtueller Maschinen oder Gruppen von vSwitch1 zu den Systemen des vSwitch3 gescannt und gefiltert. Dies ermöglicht die Erkennung und Isolierung der Malwarequelle und verhindert, dass sich Malware über das gesamte System hinweg ausbreiten kann. (kl) ■

Wir sind Experten für De-Mail bei Behörden und Unternehmen.

Registrieren Sie jetzt vorab Ihre De-Mail Adresse! Natürlich kostenlos und unverbindlich.

➔ www.francotyp.de/de-mail

Diesen Dienst bieten wir Ihnen gemeinsam mit Mentana-Claimsoft an, einem Unternehmen der FP-Gruppe. Für Fragen steht Ihnen unser Team gerne zur Verfügung: 05063 / 577570.




DE-MAIL VON
FRANCOTYP-POSTALIA
DIE MAIL, DIE GANZ SICHER MEHR KANN.



Francotyp-Postalia Vertrieb und Service GmbH • Triftweg 21-26 • 16547 Birkenwerder