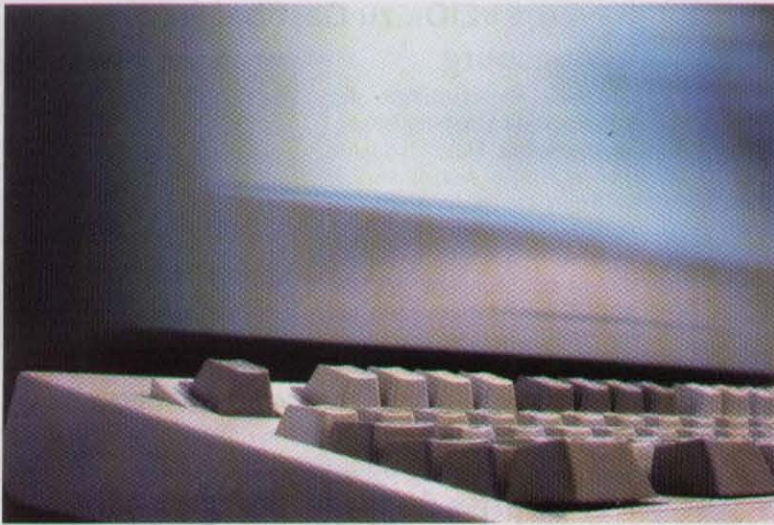


Auch Virtuelles braucht Schutz

Virtuelle Systeme erobern die IT: Sie sollen flexibler sein und die Ressourcen besser nutzen. Dabei tun sich aber neue Sicherheitslücken und -bedrohungen auf, die gestopft werden müssen, wenn der virtuelle Ausflug nicht zum Albtraum werden soll.

von johann baumeister* | werner.fritsch@informationweek.de

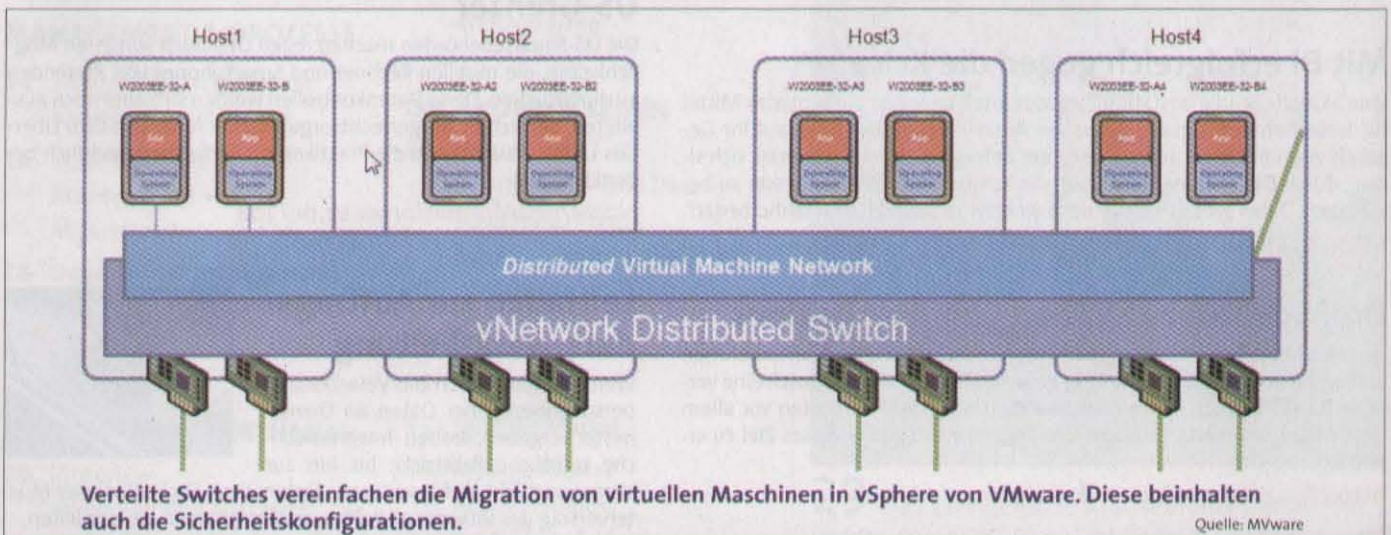


Durch Virtualisierung wird eine Abstraktionsschicht zwischen Systemen eingebracht, die die physischen Ressourcen von den Nutzern entkoppelt. Das ist im Prinzip nicht neu, erlebt derzeit aber in unterschiedlichen Bereichen eine breite Akzeptanz. Unterschieden wird nach den Verfahren der Server-, der Desktop-, der Applikations- und der Präsentations-Virtualisierung.

Die Zielsetzungen der unterschiedlichen Virtualisierungstechniken sind verschieden, ihre Sicherheitsbedrohungen auch. Bei der Servervirtualisierung packt man kurzerhand mehrere Serverimages zusammen. Dies spart Hardware, Platz, Strom und sonstige Infrastukturressourcen des Rechenzentrums. Gleichzeitig wird der Host, der nun zum Träger vieler virtueller Server wird, zum single point of failure. Fällt er aus, so zieht er zwangsläufig alle seine virtuellen Gäste in den Abgrund. Dabei spielt es eigentlich keine Rolle, ob dieser Ausfall aufgrund eines Sicherheitsangriffs, eines Hardwaredefekts oder einer temporären Überlastung auftritt. Aus der Sicht des Benutzers oder Unternehmens ist der Dienst eben nicht verfügbar – und nur das zählt. Die Absicherung muss daher auch in alle Richtungen greifen.

Virtuelle Security Appliances in virtuellen Maschinen

Um die Server gegen Angriffe abzusichern, wird meist auf bekannte Hilfsmittel wie Firewalls und Intrusion Prevention Tools zurückgegriffen. Diese Einrichtungen können auch im Kontext einer virtuellen Maschine eingesetzt werden und verrichten hier ihre Dienste. In der bestehenden Umgebung mit physischen Servern werden oftmals Security Appliances, wie etwa eine Fi-



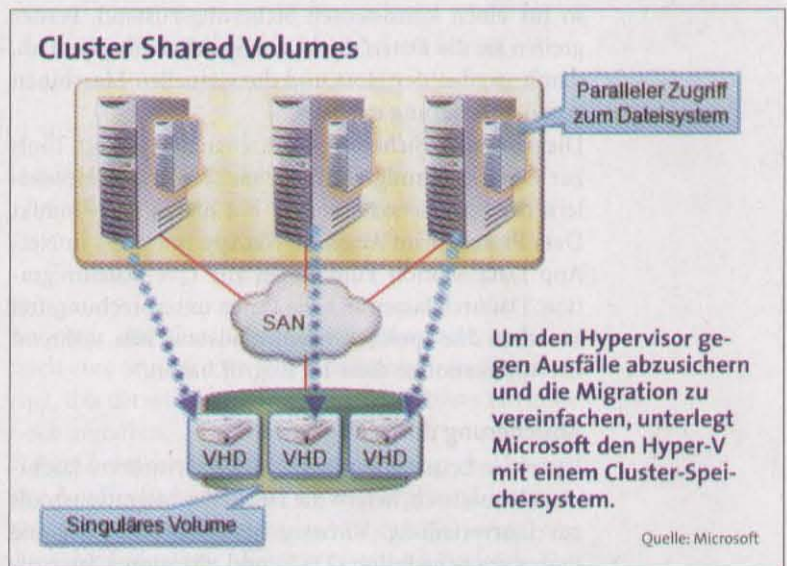
rewall, ein Intrusion Prevention System oder ein Malware Scanner zwischen zwei Serversysteme in deren Kommunikationskanal geschaltet. Dies kann auch weiterhin beibehalten werden. Dem Trend der Virtualisierung folgend gehen manche Hersteller nun dazu über, diese Security Appliances virtuell nachzubilden. Die **Hersteller Checkpoint und Gateprotect** beispielsweise liefern virtuelle UTM Appliances zur Sicherung von VMware-Umgebungen. Diese virtuellen Security Appliances laufen dann in einer virtuellen Maschine auf einem Hypervisor. Doch das bleibt nicht ohne Auswirkungen auf den gesamten Sicherheitsstatus. Was passiert beispielsweise, wenn zwischen zwei virtuellen Maschinen eine virtuelle Security-Appliance ihren Dienst verrichtet und eine der virtuellen Maschinen auf einen anderen Host migriert wird? Beim Umzug einer virtuellen Maschine auf einen anderen Host ändert sich auch die Verbindung zwischen den beiden. Daher muss bei der Migration von virtuellen Maschinen auch die Sicherheitstechnik berücksichtigt werden. Dieses Problem geht VMware mit den vShield Zones an. Diese beruhen auf einem Set an Sicherheitseinrichtungen für virtuelle Umgebungen. Bei der Migration der virtuellen Maschinen behalten diese die vorgenommenen Sicherheitseinstellungen. Technisch basiert das Konzept auf externen Sicherheitsappliances. Dieser verwalten dann die Sicherheitseinrichtungen für die vShield Zones.

Absicherung des Hosts

Ein besonderes Augenmerk gilt aber dem Hostsystem. Da der Hypervisor, wie beispielsweise der VMware ESX-Server, der Microsoft Hyper-V oder der Citrix XenServer, die Träger der virtuellen Maschinen darstellen, müssen sie besonders abgesichert werden. Gelingt es einem Angreifer, den Host zu kompromittieren, so bleibt das selten ohne Auswirkungen auf die virtuellen Gäste. Um die Sicherheit der Systeme zu gewährleisten, liefert VMware unter VMSafe verschiedene Sicherheitskonzepte. Dabei handelt es sich um einen Verbund von Sicherheitsvorkehrungen zum Schutz der virtuellen Maschinen, die im Kontext des ESX-Servers laufen.

Patchverteilung bei virtuellen Systemen

Ein weiterer Aspekt betrifft die Versorgung der virtuellen Maschinen mit den Security Updates und Patches. Die traditionellen Update- und Patch-Techniken greifen nur, wenn die virtuelle Maschine zum Zeitpunkt des Patchens aktiv ist. Da aber virtuelle Maschinen sehr schnell aktiviert und auch deaktiviert werden können, ist dies nicht immer gegeben. Damit weisen virtuelle Maschinen oftmals einen älteren Sicherheitsstand auf. Die **Marktforscher von Gartner** haben beispielsweise festgestellt, dass circa 60 Prozent der virtuellen Systeme einen niedrigeren Sicherheitsstatus aufweisen als ihre physikalischen Pendanten. Dennoch kommen auch hier die Hersteller mit den ersten Lö-



sungen speziell für virtuelle Maschinen. McAfee beispielsweise liefert sein Tool Total Protection for Virtualization und Matrix42 kümmert sich um das Patch Management.

Absicherung gegen den Ausfall

Neben diesen Ausfällen aufgrund von Sicherheitsangriffen stehen jene, die durch ein Hardware- oder Software-Problem verursacht werden. Sie gilt es ebenfalls abzufedern. Ferner gelten bezüglich der Sicherung der Systeme im virtuellen Kontext andere Bedingungen. Zwar lassen sich prinzipiell auch virtuelle Systeme durch die gleichen Techniken und Verfahren sichern wie physische Server, doch das führt schnell zum Engpass. Aufgrund der höheren Auslastung der Hosts im Vergleich zu den traditionellen physischen Servern fehlen dem Virtualisierungs-Host oftmals die Reserven zur Durchführung des Backups. Dies gilt vor allem dann, wenn in mehreren virtuellen Maschinen die Backupläufe parallel ausgeführt werden sollen. Des Weiteren wird das Netzwerk oftmals zum Engpass.

Sicherung durch den Host

Aus diesem Grund erfolgt bei virtuellen Infrastrukturen die Sicherung der virtuellen Maschinen meist durch den Host oder das Speichersystem. VMware bietet dafür mehrere Techniken. So können mit vSphere die virtuelle Maschinen für den Zeitraum der Sicherung unterbrochen (suspendiert) werden, weitere Varianten stellen ESX-Snapshot und VCBBackup dar. Hinter VCBBackup verbergen sich Funktionen zur Sicherung von virtuellen Maschinen durch eine separate Sicherungssoftware. Diese kommuniziert dann über ein Interface mit VCBBackup. Um die Daten in virtuellen Umgebungen in einem konsistenten Zustand zu sichern, sind allerdings Zusatzwerkzeuge erforderlich. Diese kommunizieren zum einen mit den Applikationsdiensten in der virtuellen Maschine und sorgen →

so für einen konsistenten Sicherungszustand. Ferner greifen sie die Daten direkt am Speichersubsystem ab, damit werden der Host und die virtuellen Maschinen von der Sicherung entlastet.

Die passenden Sicherungswerkzeuge und weitere Tools zur Datensicherung kommen meist von den Herstellern der Speichersysteme. HP hat hierzu das Produkt Data Protector im Angebot. NetApp integriert in NetApp Data Motion Funktionen zur Live-Datenmigration. Dadurch lassen sich die Daten unterbrechungsfrei zwischen den Speichersystemen austauschen, während die Applikationen diese im Zugriff haben.

Absicherung durch Migration

Um einen Leistungsengpass bei den virtuellen Maschinen abzusichern, liefern die Hersteller Migrationstools zur Lastverteilung. VMware hat dazu sein Dynamic Resource Scheduling (DRS) und vMotion, Citrix offeriert XenMotion und die Essentials for Hyper-V. Seit der Version 2008 R2 des Windows Server unterstützt auch Microsoft die Live Migration. Die Grundlagen dazu liefern wiederum die Cluster Shared Volumes. Die Migration einer virtuellen Maschine hilft auch bei geplanten Wartungsarbeiten. Auch bei einem Ausfall des Hosts kann somit die Last von einer anderen Serverhardware übernommen werden.

Sicherung des Desktops

Die Sicherung des Desktops ist ungleich einfacher, überschneidet sich teilweise auch mit der

Absicherung der Server. Da virtuelle Desktops in der Regel auf zentralen Servern laufen, kann die Absicherung gegen Angriffe über die traditionellen Sicherheitseinrichtungen erfolgen. Wird der virtuelle Desktop bei jedem Start aus einem Image neu gezogen, so vereinfacht sich auch die Sicherung des Desktops. Denn selbst wenn es einem Angreifer gelingt, den Desktop zu kapern, so lässt sich das durch einen Neustart einfach beheben. Gleichzeitig allerdings muss dann der Server, auf dem die Desktops laufen, umso besser abgesichert sein. Dazu sind wieder die bereits erwähnten Verfahren heranzuziehen. Bei der Sicherung gegen Hardwareausfälle wiederum sind oftmals die Verfahren der Server anzuwenden.

Anders hingegen ist der Aspekt der Lastverteilung mit der Absicherung gegen Engpässe verbunden. Dies erfolgt meist durch vorgeschaltete Lastverteiler, die dann die Last auf einen Server verteilen, der noch Reserven besitzt. Die Datensicherung kann durch die traditionellen Konzepte erfolgen. Da virtualisierte Desktops auf zentralen Speichern operieren, entfallen die Sicherungen von lokalen Daten. Hinsichtlich der Sicherungen der Konfigurationen oder der User Sessions ist dies eine Aufgabe, die in den jeweiligen Virtualisierungssystemen enthalten sein muss. ■

* **Johann Baumeister** ist IT-Journalist in Brunthal bei München.