Security-Virtualisierung

Die Virtualisierung von IT-Security erfährt derzeit einen neuen Hype – Hersteller bieten bisher nur als Hardware-Appliances erhältliche Produkte zunehmend auch als betriebsfertiges Image für gängige Virtualisierungslösungen an, was bis vor kurzem noch mit dem Hinweis auf Support-Herausforderungen stringent abgelehnt wurde. Doch die neue Flexibilität hat auch Schattenseiten, die man organisatorisch abfangen muss.

Von Tim Cappelmann, Lehrte

In der Vergangenheit hat manch ein Anbieter ausschließlich "speziell gehärtete Hardware-Systeme" ausgeliefert – nicht selten bestanden diese Appliances aber de facto lediglich aus einem Standard-Server, einer produktspezifischen Frontblende und einem ISO-Image auf beigefügter DVD. Nun greift das Marketing der führenden Hersteller die Security-Virtualisierung als neuen Mega-Trend auf – und die Vorteile liegen zunächst auf der Hand: Unternehmen haben bereits Mittel in hochverfügbare Hypervisor investiert und mit der dritten Generation der Bladeserver sowie dynamischer Hardwarezuweisung steht längst eine effiziente und skalierbare Serverplattform im eigenen Rechenzentrum zur Verfügung.

In diesem Umfeld könnte man leicht auch IT-Security-Technik betreiben, die vormals ihren sicheren Platz in einer "demilitarisierten Zone" (DMZ) auf separaten Servern gefunden hat. Doch bei der Virtualisierung von IT-Security sollte man spezielle Designaspekte beachten. Denn mit der Virtualisierung ergeben sich einige Herausforderungen, die es schon weit vor der Anschaffung von Produkten zu berücksichtigen lohnt.

Zwei Arten Virtualität

Virtualisierte IT-Security lässt sich in zwei Gruppen gliedern: Zum einen existieren virtuelle Instanzen innerhalb standardisierter Securityprodukte. In dieser Kategorie versprechen Hersteller Vorteile insbesondere in der administrativen Zugriffskontrolle, der Mandantenfähigkeit und der Vereinfachung der technischen Policies. Vormals standen beispielsweise virtuelle Firewallinstanzen nur großen

Providern zur Verfügung – heute halten virtualisierte Firewalls auch Einzug in die Enterprise-Produktlinien für klassische Unternehmensnetzwerke.

Hersteller ermöglichen so den Betrieb mehrerer gekapselter Firewallinstanzen mit eigenständigen Routing-Prozessen und Regelwerken pro Instanz. Virtuelle Firewalls ziehen vermehrt unter den Namen "Virtual Domain" (Fortinet) oder "Virtual System Extension" (Checkpoint) in den Netzwerkkern ein. Diese virtuellen Firewalls können jeweils Kunden, Aufgaben oder Abteilungen zugeordnet werden und ermöglichen letztlich speziellere und übersichtlichere Regelwerke. Diese Instanzen arbeiten streng gekapselt und unzugänglich innerhalb des jeweiligen Herstellercodes.

Erwünschte Vermischung

Zum anderen werden auch Security-Produkte selbst für den Betrieb auf einem Standard-Hypervisor angeboten – zum Beispiel für VMWare ESXi oder Microsoft HyperV. Solche virtuellen Appliances versprechen geringere Kosten durch eingesparte Serverhardware, Klima- und Stromleistung oder auch einfach(er) umzusetzende Hochverfügbarkeit. Denn im Gegensatz zu proprietären Appliance-Cluster-Failover-Mechanismen sorgt der bestehende Hypervisor heute schon zuverlässig für einen ständig verfügbaren Serverdienst und notwendige Redundanzen.

Oft eignen sich virtualisierte Securityprodukte zudem auch bestens dafür, sich zwecks Reglementierung für ohnehin schon längst virtualisierte Serverlandschaften in den Datenpfad einzuklinken, was mit externen (physischen) Appliances oft schwierig wäre. So bieten etablierte Hersteller ihre jüngst virtualisierten Produkte speziell zum Schutz virtueller Serverfarmen an: f5 Networks liefert seine "Big IP Local Traffic Manager" genauso virtualisiert aus wie Checkpoint seine "Secure Gateway Virtual Edition" oder Fortinet die "Fortigate-VM"-Firewalls.

Unerwünschte Vermischung

In beiden Virtualisierungs-Kategorien ergeben sich jedoch (zumindest zunächst) Probleme in der klaren Abgrenzung von Security-Zonen: Wenn viele Netzsegmente unterschiedlichen Schutzbedarfs mit der Infrastruktur des Hypervisors oder dem Standard-Netzwerkequipment verschaltet werden, ist jetzt besondere Aufmerksamkeit geboten! Was zuvor in eigens für die "demilitarisierte Zone" (DMZ) vorgesehenen Schränken zusammengefasst wurde, verteilt sich je nach administrativem Geschick nun auf diversen aktiven Komponenten im Rechenzentrum.

Diese Komponenten werden nicht zwangsläufig von Security-Administratoren eingerichtet, sondern unterliegen meist der Betriebsverantwortung der

Netzwerkabteilung – am Hypervisor werden die sensitiven DMZ-Segmente nun in Form virtueller Netze konfiguriert, dort halten vorrangig die Server-Administratoren die Richtlinienkompetenz. Was zuvor durch abgeschlossene Racks und farbig gekennzeichnete Patchkabel eindeutig der Security zuzuordnen war, geht nach der Virtualisierung innerhalb bestehender Infrastrukturen auf und auch leichter unter.

Security-Zonen werden an die physischen Knoten mittels VLANs herangeführt – diese lassen sich jedoch nicht eindeutig bezüglich ihres Schutzbedarfs kennzeichnen. Bei der Nutzung virtualisierter Securityprodukte und auch im Fall virtueller Securityinstanzen muss dem Security-Verantwortlichen daher zukünftig eine erweiterte Sicht auf die nunmehr beteiligten Netzwerkkomponenten, Hypervisor und Servertechnik eingeräumt werden.

Unglücklicherweise benötigen die beteiligten Server einer Virtualisierungsinfrastruktur auch direkte Layer-2-Verbindungen für mögliche Failover beim Ausfall einzelner Nodes. So werden VLANs als Träger von Security-Segmenten durch den Einsatz der Virtualisierung nun tendenziell im gesamten Rechenzentrum verbreitet – jedes beteiligte Bladecenter, jeder beteiligte Switch trägt dann auch die sensitiven DMZ-Subnetze, die Zeit des abgeschlossenen DMZ-Schranks ist damit endgültig vorbei.

Mit zunehmender Betriebsdauer und Serverumzügen im RZ schleichen sich gerne Fehler in der Netzwerkkonfiguration ein: Nahezu in jedem Datacenter finden sich VLANs, die als "Konfigleichen" ewig auf Ports gebunden bleiben, obwohl diese dort längst nicht mehr benötigt werden. Die Schaltung von VLANs unterliegen in den meisten IT-Organisationen nicht einmal offiziellen Change-Management-Prozessen gemäß den ITIL-Empfehlungen.

Folgerungen

Die Ausbreitung virtueller Netze innerhalb der Rechenzentren muss nach der Integration von Security-Zonen jederzeit überprüfbar sein und auch regelmäßig durch "Config-Dumps" an die Security-Verantwortlichen berichtet werden. Das ist mit aktuellen Netzwerkmanagement-Stationen durchaus automatisiert möglich: Diese lesen die VLAN-Port-Zuordnungen aus der Management-Information-Base (MiB) der Switches aus und können auch mit dem API des Hypervisors umgehen. So lässt sich die vollständige Verschaltung von DMZ-VLANs in einer Baumstruktur übersichtlich darstellen – auch unter Einbeziehung der virtuellen Segmente auf dem Hypervisor. Diese Informationen sollten bei Security-Virtualisierung zukünftig auch die Security-Verantwortlichen interessieren.

Im Prinzip könnte den skizzierten Herausforderungen nach möglichst trennscharfer Abgrenzung auch durch eine ausschließlich für die DMZ vorgesehene Virtualisierungsinfrastruktur begegnet werden: Mindestens zwei Nodes tragen dann die virtuellen Maschinen für einen redundanten Betrieb und werden in einer eigens dafür vorgesehenen Security-Zone aufgebaut. Um bei Ausfall eines Servers weiterhin Verfügbarkeit der Dienste zu realisieren, muss die Hardwareausstattung dieser Server jedoch deutlich über dem Normalbedarf dimensioniert werden. Diese Insellösung trägt so zwar den Security-Anforderungen Rechnung – rechnet sich jedoch nicht: Denn Virtualisierung wird erst bei hoher Auslastung der Hardware wirtschaftlich, die Ressourcen vieler CPUs werden innerhalb der DMZ aber oft gar nicht benötigt.

Ganz andere Fragestellungen ergeben sich in der genannten zweiten Kategorie betriebsfertiger virtueller Security-Appliances, denn hier muss man auch den standardisierten Hypervisor selbst noch kritisch hinterfragen:

> Ist ein Ausbrechen aus dem Gastsystem mit Securityaufgaben möglich? Der unbedachte Einsatz von Gastwerkzeugen schafft hier womöglich Übergänge zur virtuellen Securityappliance, wo eigentlich keine hingehören.
> Wie wird mit Snapshots virtueller Firewalls umgegangen und wo werden diese gespeichert? Eingefrorene Systeme können bewegt werden, sind logisch jedoch nicht ausgeschaltet – eventuell vorgesehene Sicherheitsfunktionen des Herstellers greifen daher womöglich nicht.
> Ein weiteres Themengebiet ist die Live-Migration von virtuellen Appliances: Wie lässt sich hier verhindern, dass Maschinen mit hohem Schutzbedarf auf dafür nicht vorgesehene Trägerhosts verschoben werden? Das wäre in etwa so, als würden heikle DMZ-Maschinen durch unbekannte Arbeiter auf einen fremden LKW verladen – und zwar weiterhin im Betrieb unter laufender Notstromversorgung.
> Zudem spiegeln die Managementwerkzeuge des Hypervisors die Konsole des Gastsystems in einem Web-GUI oder ein Java-Interface. Die Zugriffskonzepte der bestehenden Virtualisierungsinfrastruktur müssen daher in jedem Fall für das neue Aufgabenfeld "IT-Security-Betrieb" neu überdacht werden.

Fazit

Die hier angeführten Probleme sind letztlich nur organisatorisch zu lösen – IT-Security ist eine Querschnittsfunktion innerhalb der IT-Organisation und muss auch so implementiert werden. Wenn DMZ-"Gäste" auf einen bestehenden Hypervisor umziehen, erscheint dies wirtschaftlich sinnvoll – die Betriebskosten sollten sich durch Skalierungseffekte und Einsparungen in der Beschaffung von Hardware nahezu sofort

senken lassen. Die in der Folge neu an der Security-Leistungserbringung beteiligten Komponenten müssen dann aber administrativ den Security-Verantwortlichen zugänglich sein, die Richtlinienkompetenz sollte sauber definiert und entsprechende Kontrollmöglichkeiten eingeführt werden. An vielen Stellen kann man bestehende Change-Management-Prozesse aus ITIL zusammen mit einem Vier-Augen-Prinzip als Lösungsansatz heranziehen.

Wichtig bleibt festzuhalten, dass man schon weit vor einer Entscheidung zur Virtualisierung von IT-Security die Fragestellungen hinsichtlich einer ständigen Auditierbarkeit aller beteiligten Systeme und Verfahren beantworten kann und sollte. Dazu müssen die Netzwerkkomponenten im Rechenzentrum, die beteiligte Serverhardware nebst Storage und der Hypervisor selbst in den Scope der Untersuchung rücken. Die Projektverantwortlichen müssen sich dabei organisatorisch auf ein mögliches Kompetenzgerangel einstellen und vorher sauber die Zuständigkeiten definieren.

All diese Fragen sollten schon Bestandteil der Designentscheidung sein und die Grundsatzentscheidung pro oder contra Security-Virtualisierung wesentlich beeinflussen. Bei einer ehemals physisch sauber getrennten DMZ wird es nach der Security-Virtualisierung erstmalig zu Schnittmengen kommen: Operativer Betrieb und Security-Design müssen gemeinsame Wege finden, um im Change-Management handlungsfähig zu bleiben, aber zugleich auch jede Konfiguration hinsichtlich der Sicherheitsimplikationen zeitnah zu bewerten. Das hierzu notwendige Betriebskonzept sollte man weit vor eventuell zu treffenden Produktentscheidungen entwerfen

Dipl.Ing. (FH) Tim Cappelmann, MBA ist Leiter Managed Services bei der AirITSystems GmbH.

Erschienen in <kes 05/2011>
***<kes> – Die Zeitschrift für Informations-Sicherheit** (Printausgabe: ISSN 1611-440X).*