



Bildquelle: Fotolia

# Virtualisierung nach Mass einsetzen

Sind Virtualisierung und Green-IT bloss Schlagworte oder echte Lösungsansätze für die anstehenden Herausforderungen? Wo und wie kann Virtualisierung sinnvoll eingesetzt werden? Und wie sieht es mit der Sicherheit und den tatsächlichen Kosten aus? Kaspar Geiser



**Kaspar Geiser**

ist Managing Director und  
Mitinhaber der Aspectra AG  
kaspar.geiser@aspectra.ch

Die Virtualisierung kann durchaus als Aspekt von Green-IT bezeichnet werden. Die Hersteller versuchen zwar den Ausdruck «Green-IT» für sich zu beanspruchen und preisen unter diesem Label Hardware an, die weniger Energie verbraucht. Dies ist aber nicht sehr sinnvoll und eine kurzfristige Angelegenheit. Wer selbst Rechenzentren betreibt, weiss, was es bedeutet, sich auf Hardwarestandards einzulassen. Pro Serverbaureihe muss der Betreiber Ersatzteile wie Prozessoren, Ventilatoren, Netzteile und Harddisks vor Ort zur Verfügung haben («Spare Park»), die nach Möglichkeit kompatibel mit verschiedenen Generationen der jeweiligen Baureihe sind. Wird nun eine neue Green-IT-Linie eingeführt, muss der Spare Park erweitert werden, was hohe Kosten mit sich bringt. Des Weiteren fehlt es bei der Einführung von neuen Baureihen jeweils an Erfahrungswerten. Was die Energiekosten betrifft, sind diese mit effizient arbeitenden Servern wohl 10 Prozent tiefer. Doch aufgrund der im europäischen Vergleich in der Schweiz noch immer tiefen Stromkosten, werden dadurch die IT-Budgets nur sehr gering entlastet. Aus ökologischen und ethischen Gesichtspunkten höher zu bewerten als der Energiebedarf im Betrieb ist zudem die Produktion der Server: Wurden diese

unter fairen Anstellungsbedingungen und unter Berücksichtigung der endlichen Ressourcen produziert? Die Virtualisierung dagegen kann durchaus für sich behaupten, etwas zur Reduktion von Strom und Platz und somit zur Verringerung des Ressourcenverbrauchs beizutragen. Da virtuelle Systeme nur bedingt von der eingesetzten Hardware abhängig sind, kann mittels Virtualisierung auch auf bestehenden «alten» Servern gearbeitet und somit bestehende Hardware besser und länger genutzt werden. Doch auch die Virtualisierung darf nicht blauäugig eingesetzt werden. Sicherheit und tatsächliche Kosten können gefährliche Stolpersteine sein.

«Die Virtualisierung darf nicht blauäugig eingesetzt werden. Sicherheit und tatsächliche Kosten können gefährliche Stolpersteine sein.»

### IT-Sicherheit von virtuellen Umgebungen

Mit der Virtualisierung kann so ziemlich alles, was die IT benötigt, realisiert werden. So können ganze N-Tier-Architekturen mit einer minimalen Anzahl von Hardware- und Netzwerkkomponenten gebaut werden. Für den Anwender sieht es aus, als hätte er verschiedene Server und Netzwerke in verschiedenen Zonen (DMZ, privaten Zonen) zur Verfügung, die sowohl physisch wie auch logisch voneinander getrennt sind. Führt man dieses Spiel weiter, können auf derselben Infrastruktur sogar die Firewalls zwischen den einzelnen Zonen als «dedizierte» Systeme betrieben werden.

Was heisst das nun in Bezug auf die Sicherheit? Durch die Nutzung von gemeinsamer Hardware fließen folglich auch die Daten über dieselben Netzwerke, die nur durch die Virtualisierungssoftware getrennt werden. Das bedeutet: Physisch betrachtet könnte ein Datenstrom zwischen zwei privaten Zonen, zum Beispiel vom Datenbankserver zum Applikationsserver ebenso gut in einer DMZ auftauchen, was grundsätzlich nicht wünschenswert ist. Natürlich geschieht dies nicht von selbst. Ursprung ist, wie so oft in der Sicherheitsthematik, eine menschliche Fehlmanipulation.

Auch bei der Virtualisierung ist der Mensch der grösste Risikofaktor. Doch welche Fachperson zeichnet verantwortlich? Ist es der Architekt, der das System kreiert hat, der Firewall-Administrator, der Hardwarepezialist, der Betriebssystempezialist oder der Softwareentwickler? Im Zusammenhang mit der Virtualisierung lässt sich diese Frage noch schwerer beantworten als in klassischen Systemarchitekturen.

### Was kosten virtuelle Systeme?

Auf den ersten Blick ist die Virtualisierung der IT für die Kostenrechnung eines Unternehmens durchaus attraktiv, da die Anzahl Server und der damit verbundene Stromverbrauch sowie der dafür benötigte Platz reduziert und zugleich die Hardware-Wartungskosten gesenkt werden können. Es gilt aber zu beachten, dass noch immer der Mensch die grösste Investition innerhalb der IT ist. Mit der Einführung der Virtualisierung gilt es zu entscheiden, ob alles intern mit den eigenen Mitarbeitenden gelöst wird, oder ob die Leistung extern eingekauft werden soll. Wird der interne Weg beschritten, müssen zuerst die Verantwortlichen definiert werden. Dabei ist fest-

zustellen, dass hierfür sowohl Netzwerktechniker wie auch Linux- oder Windows-Spezialisten geeignet sein können.

Die Annahme, dass durch den Einsatz von virtualisierten Umgebungen bei den genannten technischen Ressourcen gespart wird, ist in der Praxis ein Trugschluss und könnte – besonders auf die Sicherheit bezogen – fatale Folgen für das Unternehmen haben. Aufgrund des Einsatzes von virtuellen Architekturen kann auf das Patchen der einzelnen Betriebssysteme, die virtuell betrieben werden, nicht verzichtet werden. Daher sind auch unter dem Einsatz von virtuellen Systemen nach wie vor Experten in den Bereichen Sicherheit, Betriebssystem und Applikationsentwicklung vonnöten. Wählt man für die Umsetzung von Virtualisierungsprojekten den externen Weg, drängt sich die Frage auf, wer der richtige Partner für die Umsetzung sein könnte: Soll die Herkunft des Lieferanten beispielsweise in der Hardwarebranche liegen, darf es ein Consultant sein oder sind es gar IT-Sicherheitsfirmen, die sich damit beschäftigen? Einige Virtualisierungssoftware-Hersteller erteilen zwar Zertifizierungen, doch daraus kann noch nicht abgeleitet werden, ob diese Partner tatsächlich auch für die vom Kunden benötigte Sicherheit eine adäquate Lösung bereitstellen können. Bei solchen Projekten werden oft die komplexen Abhängigkeiten auf nur einem einzigen System simuliert. Daher ist für die Beteiligten nicht mehr klar ersichtlich, was nun wo und wie miteinander verbunden ist. Hinzu kommt die Gefahr, dass, wenn es den Partner einmal nicht mehr gibt, intern keiner weiss, zu welchem Zeitpunkt was wo ausgeführt wurde. Egal welchen Weg man wählt, die zur Umsetzung nötigen Kosten sind sicherlich nicht unwesentlich und sollten genauestens berechnet werden, um im Nachhinein nicht

►



Wie grün ist «Green-IT»? Sind Virtualisierung und Green-IT bloss Schlagworte oder echte Lösungsansätze für die anstehenden Herausforderungen?

Bildquelle: Aspectra



Wie viele Server passen ins Boot? Das Sicherheitsrisiko steigt mit der Anzahl virtueller Server stetig an, da Fehlkonfigurationen nicht bloss einen einzelnen Kunden, sondern ganze Gruppen beziehungsweise Server betreffen können.

Bildquelle: Aspectra

zum Schluss kommen zu müssen, dass die Virtualisierung mehr kostet, als sie bietet, beziehungsweise gegenüber dedizierten Architekturen mehr Aufwand verursacht.

#### Wo soll mit Virtualisierung gearbeitet werden?

Nach Prüfung erwähnter Risiken und Kosten stellt sich die Frage, in welchen IT-Bereichen nun tatsächlich mit der Virtualisierung gearbeitet werden soll. Die Antwort sieht für Dienstleistungsanbieter wie Hosting-Provider nicht zwingend gleich aus wie für die internen IT-Leistungserbringer. Beim Hosting-Provider geht es primär darum, Kosten zu sparen und möglichst vielen Kunden ein «dediziertes» System anbieten zu können. Dabei kommen die genannten Risiken für den Kunden natürlich voll zum Tragen, und eine Kontrolle der angebotenen Lösung erweist sich für den Leistungsabnehmer als schwierig.

Für interne Leistungsanbieter ist dies unter Umständen etwas einfacher: Hier zählt vor allem die Inbetriebnahmezeit, also jene Zeit, die verstreicht, bis den Entwicklern oder anderen internen «Kunden» ein System zur Verfügung gestellt werden kann. Somit müssen auf der Basis der Netzwerksicherheit Zonen gebildet werden, in denen virtuelle Systeme auf gemeinsamer Hardware angeboten werden. Trotz der Möglichkeiten der Virtualisierung ist auf die Trennung von Firewall und Server sinnvollerweise nicht zu verzichten. Aus sicherheitsrelevanten Überlegungen ist es somit sowohl für Hosting-Provider als auch für die internen IT-Abteilungen ratsam, eine physische Trennung von Netzwerk und Server mit jeweils dedizierter Hardware zu vollziehen.

Die Anforderungen an den Betrieb steigen. Die Virtualisierung darf nicht blauäugig eingesetzt werden. Sicherheit und tatsächliche Kosten können gefährliche Stolpersteine sein. Aber schon nach einigen Monaten tummeln sich bereits mehrere – unter Umständen voneinander komplett unabhängige – «Kunden» auf einer virtuellen Umgebung. Dies stellt hohe Anforderungen an den Betrieb, weil bei geplanten

Arbeiten oder Zwischenfällen eine Vielzahl von Leistungnehmern avisiert und die Arbeiten sehr genau koordiniert werden müssen. Diese Problematik stellt sich vor allem Hosting-Providern, die in einer virtuellen Umgebung die verschiedensten Arten von Kunden haben und Lösungen betreiben. Das Sicherheitsrisiko steigt mit der Anzahl virtueller Server stetig an, da Fehlkonfigurationen nicht bloss einen einzelnen Kunden, sondern ganze Gruppen beziehungsweise Server betreffen können. Auch der Betrieb wird feststellen, dass hinsichtlich des Back-ups und Recoverys die Komplexität mit der Anzahl der vorhandenen virtuellen Systeme steigt respektive die Anforderungen an die Back-up- und Recovery-Umgebung steigen. Ein Beispiel hierfür sind die unterschiedlichen Back-up-Zyklen der Systeme (täglich, wöchentlich, monatlich).

#### Sachlich abwägen, ob und wie virtualisiert wird

Die Virtualisierung ist eine nützliche Ergänzung in der IT-Landschaft. Die eigene IT-Produktion komplett auf ein virtuelles System umzustellen, ist sowohl aus Kostengründen, insbesondere aber aus sicherheitstechnischen Überlegungen nicht sinnvoll. Speziell Hosting-Provider beziehungsweise IT-Anbieter mit mehreren voneinander unabhängigen Kunden müssen sich sehr genau überlegen, wie und wo der Einsatz von virtuellen Systemen überhaupt möglich ist. Sicherheit hat ihren Preis – dies trifft insbesondere bei Virtualisierungsprojekten zu. Die Lösungen und die Einhaltung von Sicherheitsrichtlinien sind komplexer als bei dedizierten und voneinander physisch getrennten Systemen. Auf ein Vermischen von Sicherheits- und Serversystemen sollte aber in jedem Fall verzichtet werden, da faktisch keine Gewaltentrennung zwischen Netzwerk und Serveradministration vollzogen werden kann. Auch die Anzahl Kunden, die auf einer gemeinsamen Hardware betrieben wird, sollte nicht zu hoch sein, damit bei geplanten und ungeplanten Arbeiten der IT-Betrieb nicht beeinträchtigt wird. ■