



# Virtualisierung zehn Jahre nach dem Hype

Um die Leistung der Server effizient nutzen und jeder Anwendung ihre Umgebung zur Verfügung stellen zu können, kam vor gut zehn Jahren der Trend zur Virtualisierung auf. Was ist in dieser Zeit passiert? Welche Konzepte waren erfolgreich? Wo sind die Grenzen? Kaspar Geiser

Ende der 90er-Jahre boomte der Server- und Rechenzentrumsbau. Immer noch grössere und leistungsfähigere Systeme kamen auf den Markt. Das Internetzeitalter brach an, und unzählige Webapplikationen schossen aus dem Boden. Um die vorhandene Leistung der Server zu optimieren, kam die Virtualisierung auf. Der Begriff Virtualisierung musste die letzten zehn Jahre für verschiedene Funktionen und Lösungen erhalten. Heute wird dieser vornehmlich als eine Methode bezeichnet, Ressourcen eines Servers mit den Komponenten CPU, RAM, Disk und Netzwerk zusammenzufassen oder aufzuteilen und diese einer Anwendung zur Verfügung zu stellen. Die Konzepte der «grossen» wie IBM und SUN, die auf der jeweils eigenen Hardware basierten, waren bereits vor zehn Jahren ausgereift, aber auch teuer und nur auf der jeweils eigenen Hardware verfügbar. Die Entwicklung von Virtualisierungslösungen für kleine, aber auch günstige Systeme startete bereits in den 80er-Jahren.

Als wohl kommerziell erfolgreichstes Unternehmen in der Virtualisierung von x86-basierten Systemen kann VMware bezeichnet werden. 1998 gegründet, kam 2001 deren Version 1.0 ESX Server auf den Markt. Doch mit der günstigen Software war es noch nicht getan. Die Hardwarehersteller sahen und sehen sich noch immer gezwungen, die richtige Antwort auf die Virtualisierung zu geben. Immer wieder bündeln die Hersteller Server, Storage und Netzwerk und preisen dieses als DIE Basis für Virtualisierung an. Doch IT-Verantwortliche tun gut daran, sich die Hardwarebasis zu schaffen, die für ihr Unternehmen beziehungsweise ihre Anforderungen nötig ist. Der Grundsatz «klein anfangen» ist hier ganz bestimmt ein guter Ratgeber. Wer sich vor zehn Jahren Hardware beschaffte, zum Beispiel ein Bladesystem und ein Storage à la EMC, und diese mit den nötigen Reser-

ven für das Wachstum versah, bezahlte dies teuer. Meistens werden aber teure Systeme nicht so schnell ersetzt. So sass man also auf teurer, stromintensiver und unflexibler Hardware und konnte die Möglichkeiten der Virtualisierung nur innerhalb des vorhandenen Rahmens nutzen. Wer jedoch mit kleinen einzelnen Systemen startete, konnte problemlos neue und schnellere Systeme hinzunehmen und dabei die älteren Rechner ersetzen.

## 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, private 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 ist verantwortlich? Ist es der Architekt, der das System kreiert hat, der Firewall-Administrator, der Hardware spezialist, der Betriebssystemspezialist 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, was intern mit den eigenen Mitarbeitenden realisiert wird und welche Leistung extern eingekauft werden soll. Wird der interne Weg beschritten, müssen zuerst die Verantwortlichen definiert werden. Dabei ist festzustellen, 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

**Kaspar Geiser** ist Geschäftsführer und Inhaber der Aspectra AG.

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. Wenn der Partner einmal nicht mehr existiert, kommt die Gefahr hinzu, dass 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 soll-

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 Inbe-

### Anforderungen an den Betrieb und Sicherheitsrisiken steigen

Wie so oft kommt der Appetit erst beim Essen: Ist einmal das erste Dutzend virtueller Systeme in Betrieb, wird die Hardware stark ausgebaut. 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 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 IT-Betrieb wird feststellen, dass hinsichtlich des Back-ups und Recovery die Komplexität mit der Anzahl der vorhandenen virtuellen Systeme steigt, beziehungsweise die Anforderung 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 Server-Administration 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. <



Nicht nur die Hardware entwickelte sich, die Virtualisierung ist mittlerweile erwachsen und bezahlbar.

Bildquelle: Vladir09 - Fotolia.com

ten genauestens berechnet werden, um im Nachhinein nicht 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

triebnahme-Zeit, also jene Zeit, 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.