

# Sicherheit und Kosten der Virtualisierung

*Einer der jüngsten und meist diskutierten IT-Trends ist die Virtualisierung. Doch wie sieht es betreffend Sicherheit und anfallenden Kosten tatsächlich aus?*

KASPAR GEISER

Vom Hardware- über die Betriebssystem-Hersteller bis hin zu den Applikations-Entwicklern loben alle die Möglichkeiten der Virtualisierung. Eines der wichtigsten Argumente ist immer wieder die Kostenersparnis, welche durch eine bessere Hardwareauslastung, eine schnellere Inbetriebnahme der Systeme oder einfachere Wartung erreicht wird. Doch schauen wir genauer hin.

## Risiken beachten

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 Netzwerk-Komponenten gebaut werden. Für den Anwender sieht es aus, als hätte er verschiedene Server und Netzwerke in verschiedenen Zonen (DMZ, privaten Zonen) zur Verfügung, welche 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, welche nur durch die Virtualisierungs-Software getrennt werden. Das bedeutet: physisch betrachtet könnte ein Datenstrom zwischen zwei privaten Zonen, z.B. vom Datenbank-Server zum Applikations-Server ebenso gut in einer DMZ auftauchen, was grundsätzlich nicht wünschenswert ist. Natürlich geschieht dies nicht von selbst.

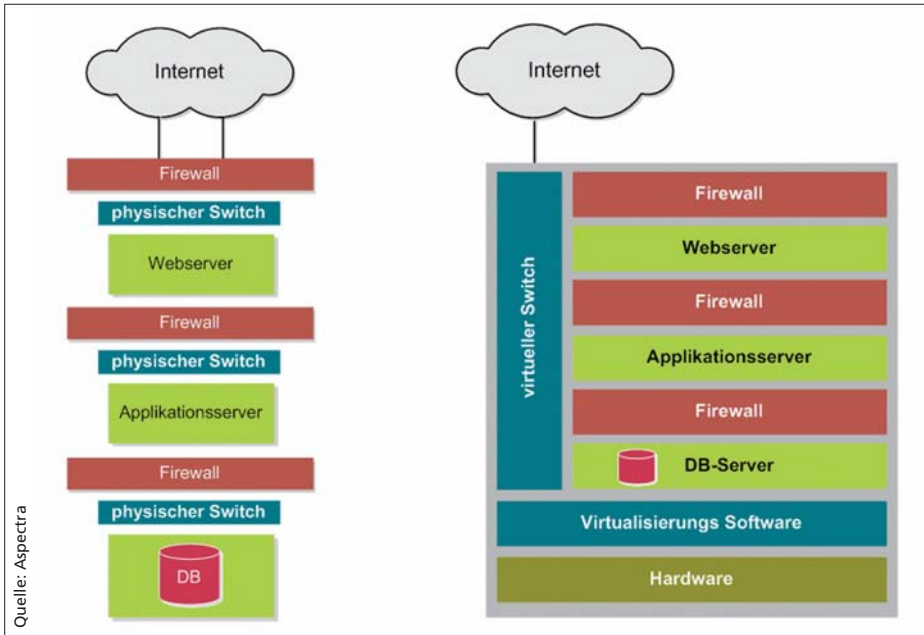
Ursprung ist, wie so oft in der Sicherheits-Thematik, eine menschliche Fehlmanipulation. Auch bei der Virtualisierung ist der Mensch der grösste Risikofaktor. Doch welche Fachperson zeichnet sich verantwortlich? Ist es der Architekt, der das System kreiert hat, der Firewall-Administrator, der Hardware-Spezialist, der Betriebssystem-Spezialist oder der Software-Entwickler? Im Zusammenhang mit der Virtualisierung lässt sich diese Frage noch schwerer beantworten als in klassischen Systemarchitekturen.

## Die Kostenfrage

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 eige-



*Tummeln sich diverse, voneinander unabhängige Kunden in unterschiedlichen virtuellen Umgebungen auf einem System, so erschwert dies die Wartung massiv.*



### n-Tier-Architekturen mit und ohne Virtualisierung

nen Mitarbeitenden gelöst wird oder ob die 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 nach sich ziehen. Aufgrund des Einsatzes von virtuellen Architekturen kann auf das Patchen der einzelnen Betriebssysteme, welche 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 Applikations-Entwicklung vonnöten.

Wählt man für die Umsetzung von Virtualisierungs-Projekten den externen Weg, drängt sich die Frage auf, wer der richtige Partner für die Umsetzung sein könnte: Soll die Herkunft des Lieferanten z.B. in der Hardwarebranche liegen, darf es ein Consultant sein oder sind es gar IT-Sicherheitsfirmen, die sich damit beschäftigen? Einige Virtualisierungs-Software-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 es für die Beteiligten nicht mehr klar ersichtlich, was nun wo und wie miteinander verbunden ist. Hinzu kommt die Gefahr, dass wenn der Partner einmal nicht mehr existiert, 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 zum Schluss zu kommen, dass die Virtualisierung mehr kostet als bietet bzw. gegenüber dedizierten Architekturen mehr Aufwand verursacht.



*Vier Assen hat man mit virtuellen Systemen nicht zwingend im Ärmel. Je nach Anwendungszweck birgt Virtualisierung aber enormes Potential.*

## 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 Inbetriebnahme-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 den Möglichkeiten der Virtualisierung ist auf die Trennung von Firewall und Server sinnvollerweise 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.

### Anforderungen an den Betrieb 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, da bei geplanten Arbeiten oder Zwischenfällen eine Vielzahl von Leistungsnehmern 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 bzw. Server betreffen können.

Auch der Betrieb wird feststellen, dass hinsichtlich des Backups und Recovery die Komplexität mit der Anzahl der vorhandenen virtuellen Systeme ansteigt bzw. die Anforderung an die Backup- und Recovery-Umgebung steigen. Ein Beispiel hierfür sind die unterschiedlich geforderten Backup-Zyklen der Systeme (täglich, wöchentlich, monatlich).



*Die Verlockung ist gross, anstelle dedizierter Systeme auf die vermeintlich kostengünstigere Virtualisierung zu setzen.*

### Sachlich abwägen

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 bzw. 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 seinen Preis – dies trifft insbesondere bei Virtualisierungsprojekten zu. Die Lösungen bzw. die Vorgabe von Sicherheitsrichtlini-

en 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, welche auf einer gemeinsamen Hardware betrieben werden, sollte nicht zu hoch sein, damit bei geplanten und ungeplanten Arbeiten der IT-Betrieb nicht beeinträchtigt wird.

*Der Autor Kaspar Geiser ist Technischer Direktor und Mitinhaber der Aspectra AG in Zürich.*