

Neue Risiken durch Virtualisierung?

Traditionelle Serverumgebungen stehen in dem Ruf, wenig energie- und ressourceneffektiv zu sein. Als kostensparend beworben werden hingegen Virtualisierungslösungen. Doch welche Vorteile bringt die Virtualisierung gemessen an den realen Verhältnissen in mittelständischen Unternehmen wirklich? Bergen virtualisierte Umgebungen vielleicht sogar erhöhte Sicherheitsrisiken?

Montagsmorgen in einem mittelständischen Unternehmen. Die Mitarbeiter fahren ihre Computer hoch und lesen zunächst die E-Mails. Das bedeutet Arbeit für den E-Mail-Server des Unternehmens, der nun zu beinahe 100 Prozent ausgelastet ist. Danach allerdings liegen die teuren Ressourcen größtenteils brach, denn die Auslastung geht nicht über 15 bis 20 Prozent hinaus. Was für einen E-Mail-Server gilt, hat auch für andere Dienste Gültigkeit. Und so bleiben etwa 80 bis 85 Prozent der Leistungsfähigkeit aller Server in Unternehmen ungenutzt. Das kostet Platz, Geld, Energie und trägt obendrein zur Klimaerwärmung bei.

Virtualisierung ist nicht nur in aller Munde, sondern sie steht auch bei IT-Profis und -Entscheidern von deutschen Unternehmen ganz oben auf der To-Do-Liste. Zu Recht, denn Virtualisierung verbessert nicht nur signifikant die Effizienz, sondern auch die Verfügbarkeit von Ressourcen und Anwendungen in einem Unternehmen.

Leistungsfähige Computerhardware wurde ursprünglich zur Ausführung eines einzelnen Betriebssystems und einer einzelnen Anwendung entwickelt, etwa für Mailserver, Printserver, Datev oder dergleichen. Doch damit sind die Maschinen heutzutage überhaupt nicht ausgelastet. Mittels Virtualisierung kann man nun mehrere virtuelle Maschinen auf einem physischen Computer ausführen. Die Ressourcen eines einzelnen Computers können dabei von mehreren Umgebungen gemeinsam genutzt werden. Verschiedene virtuelle Maschinen können unterschiedliche Betriebssysteme und mehrere Anwendungen auf demselben physischen Computer verwenden. Durch Virtualisierung werden Programme und ihre Daten von den Hardwareressourcen entkoppelt. Dadurch ist es möglich, diese Ressourcen in einem Pool zu sammeln und den Applikationen nach Bedarf zuzuweisen. Mittels einer dynamischen Verteilung der Lasten auf einem oder auch zwischen verschiedenen Servern kann eine bessere Auslastung der Ressourcen sichergestellt werden.

VIRTUALISIERUNG

ist ein Verfahren, mit dem ein leistungsstarker physischer Server in mehrere sogenannte virtuelle Server aufgeteilt wird. Jeder dieser virtuellen Server arbeitet völlig eigenständig und kann individuell konfiguriert werden. Die Einbindung neuer Applikationen respektive neuer virtueller Server ist dadurch vergleichsweise einfach möglich.



Marco Neumueller, Manager bei der STZ Object-IT, sagt: „Virtualisierung wird den Servermarkt weiter signifikant verändern. Seit gut zwei Jahren ist die Virtualisierung ein Megatrend, welcher sicherlich bis spätestens zum Jahre 2012/13 den Infrastrukturmarkt beherrschen wird.“

Es wird sehr häufig damit geworben, dass eine Virtualisierungslösung immer mit Kosteneinsparungen einherginge. Dies trifft allerdings nur bedingt zu und würde – um sofort eine Kosteneinsparung sehen zu können – voraussetzen, dass dem Paradigma „Eine Applikation – ein Server“ in jedem Unternehmen Rechnung getragen wird. In der Realität wird jedoch bereits heute aus Kostengründen ein Server für mehrere Applikationen verwendet. Schließlich wollen Ausrüstung, Kühlung und Strom ebenfalls bezahlt sein. Die oftmals beworbene Reduzierung der Anzahl an Servern trifft somit nur in seltenen Fällen zu. Bei der Einführung einer Virtualisierungsumgebung benötigt man in den meisten Fällen dieselbe Anzahl an neuen Servern.

Kosten sparen auf den zweiten Blick

Virtualisierung bringt zeitgleich aber auch viele Vorteile. So sorgt sie etwa für Geschäftskontinuität und eine einfache Lösung zur Wiederherstellung im Verlustfall. Die IT-Infrastruktur in einer Firma zeichnet sich zumeist dadurch aus, dass verschiedene Server unterschiedlichen Alters vorhanden sind. Auf diesen Servern laufen Betriebssysteme und Anwendungen parallel. Doch welche typischen Probleme ergeben sich hieraus? Abgesehen davon, dass sich manche Softwarelösungen nicht miteinander vertragen, finden die vorgesehenen Updates in aller Regel äußerst selten zeitgleich statt. Wird eine Software auf einem Server gewartet, führt dies zu Ausfällen aller anderen Dienste auf dieser Maschine. Im Resultat können die Mitarbeiter dann beispielsweise nicht mehr mit ihrer Branchensoftware arbeiten. Durch die Trennung der Dienste in einer virtuellen Umgebung können die Mitarbeiter nun auch während eines Updates ihre Software verwenden.

Sollte sich einmal ein Server dauerhaft verabschieden, so ist die Wiederherstellung eines virtuellen Servers relativ rasch und

grundsätzlich sogar im laufenden Betrieb möglich, zumal ein solcher lediglich aus einigen Dateien besteht, die zuvor aber selbstredend gesichert werden mussten. Der virtuelle Server lässt sich auf dem neuen physischen Server binnen kürzester Zeit wieder reaktivieren. So spart man Kosten – aber eben erst auf den zweiten Blick.

Ein durchaus heikles Thema ist heutzutage auch die Sicherheit. Kann Virtualisierung mehr Sicherheit bieten, oder wird sie gar zum Sicherheitsrisiko? Virtualisierung schottet theoretisch Server und Applikationen zuverlässig voneinander ab und erhöht dadurch die Sicherheit. Im Falle eines Angriffs können die Systeme sogar gestoppt und von außen analysiert werden. Doch eine Attacke auf die Virtualisierungsplattform selbst stellt ein enormes Risiko dar.

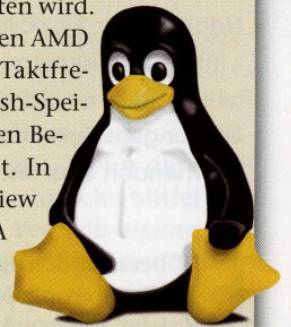
Wie jede andere Software haben auch Virtualisierungslösungen Sicherheitslücken. Der schlimmste Fall träte ein, wenn eine Attacke über eine virtuelle Maschine eine andere auf dem gemeinsamen Host angreift. Dabei nutzt ein Angreifer eine Schwachstelle in einer virtualisierten Applikation aus und übernimmt eines der virtuellen Gastsysteme. In einem zweiten Schritt müsste der Eindringling über eine weitere Schwachstelle in der Virtualisierungssoftware selbst aus dieser virtuellen Maschine in die Verwaltungskomponente eindringen. Gelänge es ihm, diese unter seine Kontrolle zu bringen, könnte er alle anderen Geräte dieses physischen Servers kompromittieren.

Doch selbst wenn man für jede Applikation einen eigenen physischen Server betreiben würde und einem Hacker das Eindringen in einen gelänge, so ist die Wahrscheinlichkeit groß, dass er auch in der Lage wäre, alle anderen zu kompromittieren. Wichtig ist somit immer, ganz gleich ob mit Virtualisierung oder ohne, die Server bestmöglich vor fremdem Zugriff von außen zu schützen. Virtualisierung stellt insgesamt gesehen somit nicht zwingend ein höheres Sicherheitsrisiko dar als bereits ohne sie besteht. ◀

Marco Henry V. Neumueller

Einstieg in Virtualisierung

Eine Preis-Offensive im Thin-Client-Markt gestartet hat der Hersteller VXL Instruments Moosburg mit seinem neuen, virtualisierungsfähigen Einstiegsgerät Itona TC1330, das zum Netto-Listenpreis von 195 Dollar (umgerechnet rund 134 Euro) angeboten wird. Der neue Thin Client verfügt über einen AMD Geode GX-Prozessor mit 466 MHz Taktfrequenz, 256 MB RAM und 64 MB Flash-Speicher und ist mit einem Linux-basierten Betriebssystem (Sylph-OS) ausgestattet. In der Firmware sind neben Vmware View 3.1 auch Clients für die Protokolle ICA und RDP sowie PNAgent-Unterstützung integriert. ◀ www.vxl.net



Zertifizierung

Ausbau der Partnerschaft: Kurz nachdem Vmware in seinem neuen Partnerprogramm vier Kompetenzen für Virtualisierungslösungen unterscheidet, erreicht die Profi Engineering Systems AG im Oktober als eine der Ersten die Zertifizierung in „Infrastrukturvirtualisierung“. Daneben unterscheidet Vmware drei weitere Kompetenzen: „Business Continuity“, „Desktopvirtualisierung“ und „Virtualisierungsverwaltung“. ◀ www.profi-ag.de