

# Sicher Virtualisieren

Risiken der Virtualisierung  
professionell managen



# Sicher Virtualisieren

## Risiken der Virtualisierung professionell managen

### SICHERE VIRTUALISIERUNG

Virtualisierung hat sich zum Mega-Trend in der Informationstechnologie entwickelt. Vorbei sind die Zeiten, in denen Virtualisierungslösungen eher rudimentären Charakter besaßen und vornehmlich in Testumgebungen zum Einsatz kamen. Lösungen von heute sind den Kinderschuhen entwachsen und präsentieren sich im professionellen Format. Kein Wunder also, dass gegenwärtig auch in Produktivumgebungen virtualisiert wird, was das Zeug hält. Ob mittelständische Betriebe, Körperschaften öffentlichen Rechts oder weltweit operierende Konzerne – alle sind dabei.

Voraus gingen Zeiten bemerkenswerter Dynamik. Als VMware im Jahr 1999 mit der Einführung der ersten Lösung für x86-Plattformen ein Ausrufezeichen setzte, ließen andere Anbieter nicht lange auf sich warten. Rasch formierte sich ein Zirkel weiterer Innovationstreiber, der eine clevere, funktionale Raffinesse nach der anderen in den Mikrokosmos der Virtualisierung einbrachte. Das Big Picture der Virtualisierung gewann so fließend an Reife und in der Folge ebenso auch an Akzeptanz und Nachfrage. Alles prima, oder? Nicht ganz, denn der rasanten Entwicklung fiel ein kleines, aber wichtiges Detail zum Opfer: die IT-Sicherheit.

Virtualisierung ist im Hinblick auf die IT-Sicherheit „nicht ganz ohne“. Denn neben dem Plus an Möglichkeiten holen sich Unternehmen und Organisationen zugleich etliche neue Sicherheitsfragen ins Haus. Ein Effekt mit Tragweite, denn für die meisten existieren schlichtweg keine praxiserprobten Rezepte oder Konserven. Im Klartext: Die Sicherheit konnte der rasanten Entwicklung immer neuer Features nicht mehr folgen und ist buchstäblich abgehängt worden. Das stellt Verantwortliche vor ernsthafte Schwierigkeiten. Nahezu rat- und hilflos stehen sie einem Bündel explosiver, offener Punkte gegenüber.

### VIELE SICHERHEITSFRAGEN – KAUM ANTWORTEN!

- Wie kann ich verhindern, dass Mitarbeiter unser virtualisiertes, laufendes SAP-System auf einem USB-Stick mit nach Hause nehmen (Offline-Hacking)?
- Wie bekomme ich in meiner virtuellen IT-Infrastruktur eine saubere Trennung von Netzen und Systemen hin?
- Kann ich den Webserver in unserer DMZ zusammen mit unserem internen ERP-System auf derselben Virtualisierungsinfrastruktur sicher betreiben?
- Wie passen meine bisherigen Betriebskonzepte zur virtuellen Welt? Sind Anpassungen vorzunehmen?
- Wie migriere ich richtig und sicher?
- Wie sieht die Rechtestruktur für die Administratoren der Virtualisierungsinfrastruktur aus?
- Brauche ich zusätzlich noch Backup, wenn ich doch Snapshot-Möglichkeiten habe? Welche Gefahren bergen Snapshots?
- Kann ich einen Serverpark auf einer einzigen Maschine laufen lassen, auf der sich alle virtuellen Maschinen den gleichen Arbeitsspeicher teilen?
- Wie kann ich feststellen, ob meine virtualisierten Umgebungen „safe“ sind?

Als wäre das nicht Zwickmühle genug, wird in Kürze sogar noch eins draufgesetzt: Nach den Epochen der „Partitionierung“, „Konsolidierung“ und „Automatisierung“, befindet sich Virtualisierung aktuell auf dem Sprung in die Ära der „Serviceorientierung“, vielfach geläufiger unter der Bezeichnung „Cloud Computing“ (siehe Grafik). Und bereits jetzt zeichnet sich ab, dass mit der Einführung und dem Betrieb von Cloud Computing ein ganzer Komplex neuer Sicherheitsfragen zusätzlich zu den bereits bestehenden auf uns zukommen wird. Die Aufrechterhaltung definierter Sicherheitsniveaus wird also immer schwieriger!

### DIE EVOLUTION DER VIRTUALISIERUNG



### WAS ABER TUN?

Eine Möglichkeit bestünde im „Back to the roots“, also im Rückbau virtualisierter Infrastrukturen zurück zu realen, physischen Umgebungen: Aber wäre „Virtual To Physical“ wirklich eine ernstzunehmende Alternative? Wohl kaum! Der Nutzen der Virtualisierung ist so überwältigend, dass ein Zurück in alte Zeiten objektiv nicht wirklich in Frage kommt.

Wie wäre es stattdessen mit IT-Security Standard Methoden? Das BSI hilft hierbei mit dem BSI-Standard 100-2 (IT-Grundschutz-Vorgehensweise) für die komplette IT inklusive der virtuellen IT-Systeme und zeigt darüber hinaus mit dem BSI-Standard 100-3 (Risikoanalyse) wie Maßnahmen für die virtuelle Infrastruktur evaluiert werden können. Wermutstropfen: Es gibt in den aktuellen Grundschutzkatalogen (wie auch in der ISO 27001) noch keine Konserven für eine solche virtuelle Infrastruktur.

### WAS IST ZU TUN? WIE GENAU KANN NETWORKERS HELFEN?

Networkers schließt aktuell im Auftrag des BSI die Erstellung solcher Konserven für virtuelle Infrastrukturen ab (Baustein Virtualisierung, Veröffentlichung in 2009/2010 im Grundschutzkatalog).

Nutzen Sie jetzt schon die Best Practice-Maßnahmen, die morgen zum Standard werden. Networkers unterstützt Sie mit:

- Innovationsworkshops zum Aufzeigen kundenspezifischer Potentiale der Virtualisierungs- und Cloud-Technologien,
- Beratung bei Design, Sizing, Werkzeugwahl und Lizenzierung,
- Aufbau kundenspezifischer Virtualisierungs- und Cloudlösungen,
- Service Level Agreements (SLA) zur Übernahme oder Unterstützung des IT-Betriebs und
- Auditierungen virtualisierter Umgebungen.

### NETWORKERS IST PRÄDESTINIERT BEI HILFESTELLUNGEN RUND UM DIE FRAGE „SICHERE VIRTUALISIERUNG“:

- Langjähriges Know-how und Erfahrungen in den Bereichen Informationssicherheit, Netzwerk- und Systemtechnik sowie Application Delivery.
- Ganzheitliche Hilfestellung bei Planung und Evaluierung über Aufbau bis hin zum Betrieb.
- Umfassende nachweisbare Zertifizierung in allen genannten Themengebieten.

### ÜBER DIE NETWORKERS AG

Die Networkers AG ist Spezialist für die Planung, den Aufbau und den Betrieb sicherer und leistungsfähiger Applikations- und Netzwerkinfrastrukturen und idealer Partner für alle Fragen rund um die sichere Virtualisierung. Integrale Themenschwerpunkte, wie Informationssicherheit, Datenkommunikation und Virtualisierung beherrschen wir seit vielen Jahren sicher und zuverlässig. Wir sind zertifizierter Partner namhafter Hersteller von Netzwerk-, Infrastruktur- und Sicherheitswerkzeugen. Unsere Kunden sind in vielen unterschiedlichen Branchen aktiv – darunter befinden sich sowohl namhafte Großunternehmen wie auch Unternehmen aus dem Mittelstand. Gerne stellen wir Referenzen zur Verfügung.



### AUTOMATISIERUNG



Phase III  
2006-2008  
Ziel:  
Standardisierung  
von IT-Prozessen

### SERVICEORIENTIERUNG



Phase IV  
2009-2012  
Ziel:  
Flexibilisierung  
IT-Services on-demand



Networkers AG  
Bandstahlstraße 2  
58093 Hagen

fon: 0 23 31 . 80 95 0  
fax: 0 23 31 . 80 95 499

email: [info@networkers.de](mailto:info@networkers.de)  
web: [www.networkers.de](http://www.networkers.de)