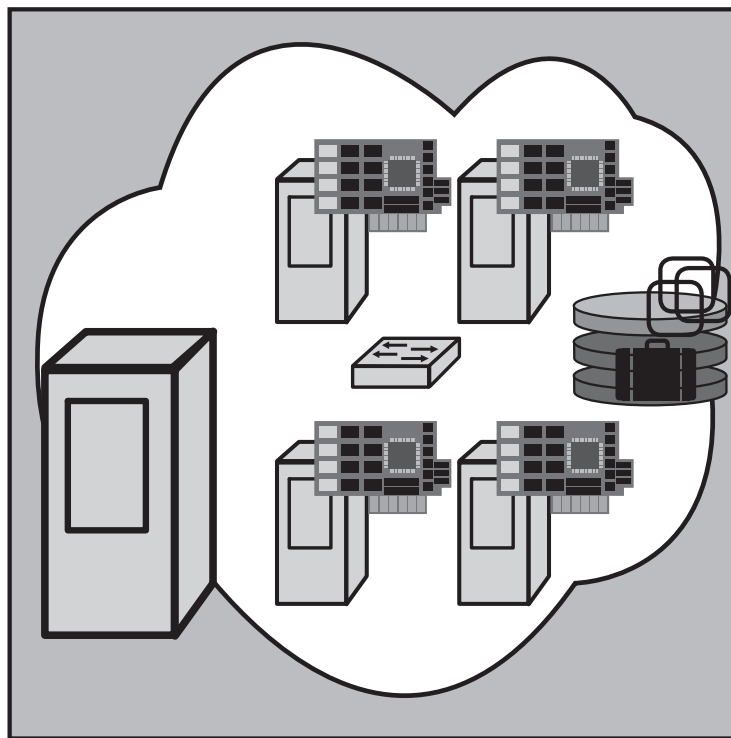


# Virtualisierung: Sicherheit in virtuellen Server-Umgebungen

von Dipl.-Inform. Oliver Flüs, Dr. Simon Hoff, Dipl.-Inform. Daniel Meinhold



Mit dem Einsatz von Server-Virtualisierung sind konkrete Erwartungen an eine verbesserte Wirtschaftlichkeit der IT verbunden:

- **Kosteneinsparungen durch Reduzierung der Hardware-Kosten für Server**
- **Einfacheres Management durch vereinheitlichte Infrastruktur**
- **Erhöhte Verfügbarkeit durch High-Availability-Konzepte mit minimierter**

**Hardware-Abhängigkeit, neue Optionen bzgl. Behandlung von Notfällen im Server-Bereich**

- **Steigerung der Effizienz und Qualität durch vereinfachte Test- und Entwicklungsumgebungen**

Im Rahmen dieses Artikels werden die betroffenen technischen Kernkomponenten und deren Zusammenspiel in Bezug auf die IT-Sicherheit betrachtet. Neben po-

tentiellen Gefährdungen sowie möglichen Maßnahmen wird hierbei auch auf veränderte IT-Betriebs- und Geschäftsprozesse hingewiesen, denn mit der Einführung der Virtualisierung ergeben sich weitreichende Änderungen, die nicht nur den Server-Betrieb betreffen.

## Schwerpunktthema



Dipl.-Inform. Oliver Flüs verfügt über langjährige Kenntnisse im Betrieb von IT-Infrastrukturen. Als Leiter des Competence Center IT-Service der ComConsult Beratung und Planung GmbH bearbeitet er seit Jahren Projekte in den Bereichen Services im IT-Bereich. Zu diesen Themengebieten ist er regelmäßig als Referent bei der ComConsult Akademie tätig, unter anderem als Schwerpunktreferent zu TCP/IP-Aspekten, in der Trouble Shooter-Seminarreihe sowie im Rahmen der Sicherheitsseminare.



Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.



Dipl.-Inform. Daniel Meinhold ist Consultant bei der ComConsult Beratung und Planung GmbH. Dort ist er in den Bereichen Telekommunikationssysteme, Virtualisierung und IT-Sicherheit tätig. Neben diesbezüglichen Praxiserfahrungen in zahlreichen Projekten ist er für die Planung und Durchführung entsprechender Testszenerien im ComConsult-eigenen Labor zuständig.

## Virtualisierung: Sicherheit in virtuellen Server-Umgebungen

### 1. Auswirkungen auf die IT-Landschaft

Die Auswirkungen der Server-Virtualisierung auf die administrativen und betrieblichen Prozesse können erheblich sein. So werden womöglich durch die Server-Virtualisierung Ressourcen zusammengeführt, die im Unternehmen oder der Behörde bisher zum Teil durch verschiedene Verantwortungsbereiche abgedeckt werden, z.B. Server- und Netzbetrieb. Server- und auch Netzkomponenten sind virtualisiert innerhalb von physischen Servern untergebracht. Hierbei gilt es vor allem die Frage der Zuständigkeiten zu klären. Bisher bewusst getrennte Rollen und Kontrollfunktionen fallen nun zusammen und betreffen den Netz- und Server-Betrieb genauso wie die IT-Sicherheit oder Revision. Hinzu kommt der Betrieb der Virtualisierungslösung selbst: Wird diese vom Server-Betrieb gepflegt oder durch einen anderen, ggf. eigenen Bereich? Aus einer Sicherheitsperspektive sind dabei unmittelbar die potentiellen Zugriffsmöglichkei-

ten der Virtualisierungsadministratoren zu berücksichtigen, die ohne differenzierte Berechtigungskonzepte eine umfassende Kontrolle über eine Vielzahl von Servern erhalten.

### Wirtschaftliche Aspekte dominieren die Server-Virtualisierung

Die Server-Virtualisierung findet aufgrund der vordergründigen wirtschaftlichen Thematik „Einsparung von Hardware“ häufig schneller Einzug in das Rechenzentrum als es dem IT-Betrieb unter Umständen lieb ist. Die Verantwortlichen sind sich dabei oft nicht aller Konsequenzen bewusst. Mit Erfahrung beherrschte Szenarien auf Basis dedizierter physischer Server werden durch den neuen Ansatz der Virtualisierung zum Teil im Rekordtempo abgelöst. Die neu eingeführte Technik mit gleicher Qualität zu beherrschen wie die „althergebrachte“ ist zwar nicht unmöglich, erfordert aber Einarbeitungszeit und Tests, für welche die beobachteten typischen Einführungsphasen oft zu kurz sind.

In dieser Zeit kann man bestenfalls an der Oberfläche des nötigen Wissens gekratzt haben, bis die virtualisierte Lösung in den produktiven Betrieb geht.

Dabei birgt eine derart weitgehende Umstellung im technischen Bereich auf Grund der in heutigen IT-Umgebungen zwangsläufigen Vielzahl von Abhängigkeiten etliche Risiken – nicht zuletzt auch aus sicherheitstechnischer Sicht. Von der Virtualisierung sind neben den technischen Aspekten sowohl IT-Betriebsprozesse als auch Geschäftsprozesse betroffen. Für alle diese Bereiche stellen sich bekannte Fragen im Sinne des Risiko- und insbesondere Sicherheitsmanagements neu. Beispielsweise sind veränderte Deployment-Prozesse ebenso zu berücksichtigen wie geeignete Maßnahmen zur Absicherung einer SAN-Umgebung. Diese Punkte müssen in bestehende Sicherheitskonzepte eingearbeitet oder in Form eines Sicherheitskonzepts für die Virtualisierung berücksichtigt werden, denn trotz

## Virtualisierung: Sicherheit in virtuellen Server-Umgebungen

gewisser Analogien können die bisherigen Konzepte nicht unverändert übernommen werden. Anschließend müssen die Konzepte in geeignet modifizierten betrieblichen Abläufen im IT-Service umgesetzt werden. Nur bei Berücksichtigung dieser Aspekte können die Vorteile der Virtualisierung sinnvoll in die Umgebung integriert werden. Bei Nichtbeachtung bzw. diesbezüglich unzureichender Vorbereitung droht hingegen ein deutlicher Abfall des verantwortlich garantierbaren Sicherheitsniveaus.

#### Virtualisierung: Gemeinsame Nutzung von Ressourcen

Das Sicherheitsniveau ist in virtualisierten Umgebungen zunächst durch die Schwächung eines der Grundpfeiler der IT-Sicherheit betroffen, nämlich der konsequenten Trennung von Ressourcen bei hohen oder unterschiedlichen Anforderungen an Verfügbarkeit, Integrität und Vertraulichkeit von gespeicherten oder im Rahmen von Kommunikationsflüssen transportierten Daten. Über Jahre hat es sich die IT-Sicherheit zur Aufgabe gemacht, über differenzierte Verfügbarkeitsbetrachtungen und nötigenfalls

Unterscheidung verschiedener Sicherheitszonen Ressourcen zu isolieren und abzusichern, um die IT-Nutzer und ihre Daten auf diese Weise vor Angriffen zu schützen. Je höher die Ansprüche an Sicherheit im engeren Sinne oder Verfügbarkeit, umso wahrscheinlicher war der Einsatz dedizierter Hardware und separierter Kommunikationswege. Um das Risiko „Mensch“ zu minimieren, ging dies oft mit einer Verteilung der Administrationsrechte für unterschiedliche Systeme auf unterschiedliche Verantwortliche einher.

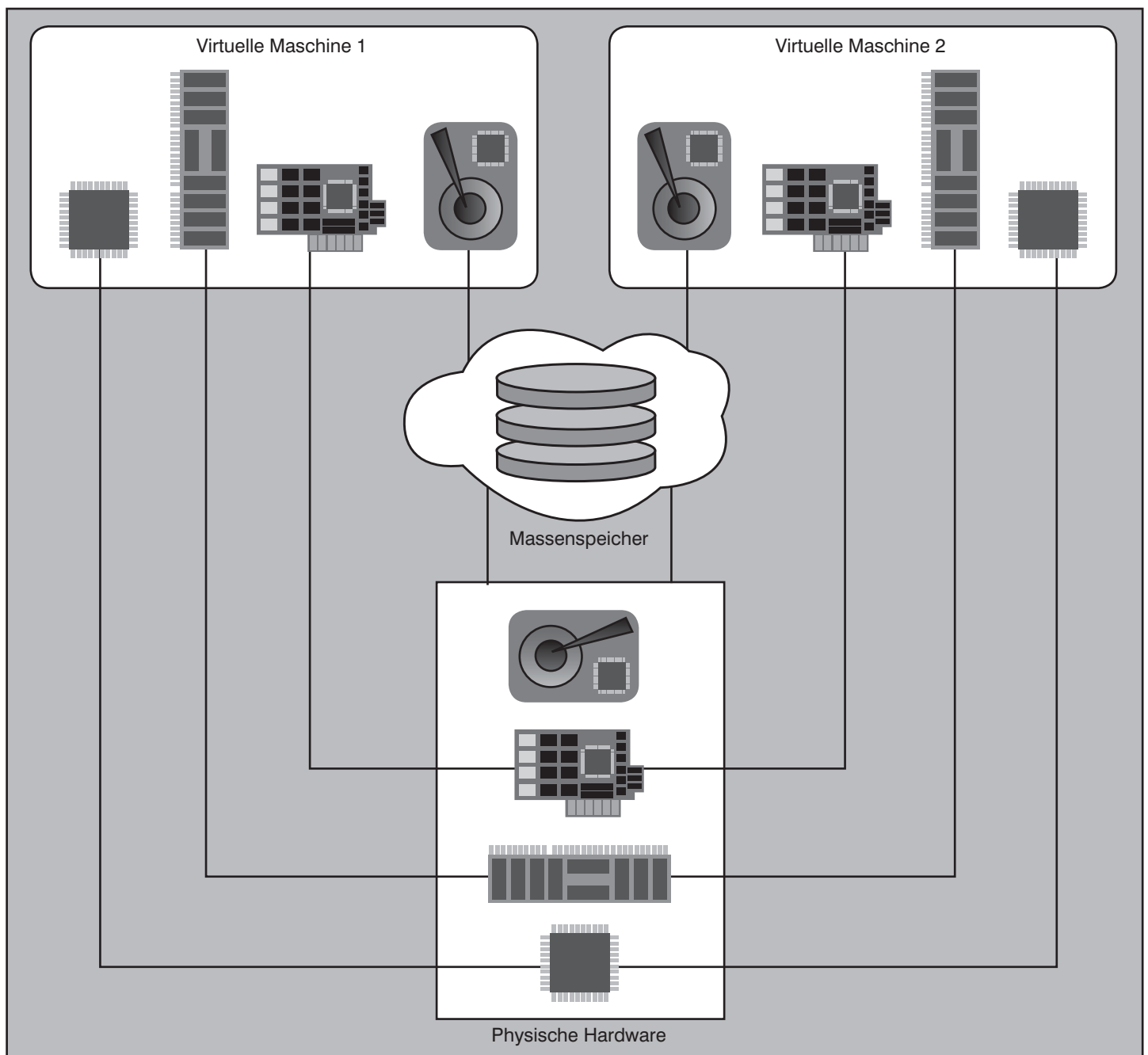


Abbildung 1: Ressourcenteilung zwischen physischen und virtuellen Systemen

Virtualisierung: Sicherheit in virtuellen Server-Umgebungen

Zusammen mit der Einführung einer Server-Virtualisierung werden Hardware-Ressourcen jedoch wieder zusammengeführt. Damit wird die vorhandene physische Hardware nicht länger einem System dediziert zur Verfügung gestellt, sondern wird potentiell von mehreren Systemen (Abbildung 1) genutzt. Die Verwaltung obliegt einer Software, die zur Virtualisierungsbasis gehört. Wenn die bisherigen Separierungsstrategien nicht völlig widersinnig waren, ergeben sich bei diesem rückwärtigen Schritt zur gemeinsam genutzten Basisplattform sofort gezielte Fragen. Hinzu kommt die ständig zunehmende Komplexität der IT-Systeme, deren Beherrschung durch den Übergang von physischen zu virtuellen Systemen nicht erleichtert wird, denn Virtualisierung bringt einen erhöhten Abstraktionsgrad in IT-Planung und Betriebsalltag. Endet dies in einem Verlust von Transparenz und Überblick, ist ein gezielter Umgang mit Sicherheitsrisiken fraglich - hier muss man sich vorsehen!

**2. Grundlage Risikoanalyse**

Das nicht selten vorzufindende Argument, dass eine Virtualisierung zu mehr Sicherheit führe, gilt per se nicht. In diesem Zusammenhang wird oft das Beispiel angeführt, dass es sicherer sei, einen physischen Server mit drei virtuellen Servern und je einem Dienst zu betreiben als einen physischen Server mit drei Diensten. Das für die Betrachtung korrekte physische Pendant zum genannten virtuellen Szenario besteht jedoch aus drei physischen Servern mit je einem Dienst, sollen nicht die berühmten Äpfel und Birnen verglichen werden. Mindestens aus Sicht der Streuung des Ausfallrisikos sind drei dedizierte physische Server die sicherste Lösung. Die maximale Separierung in unterschiedliche Sicherheitszonen setzt ebenfalls eine solche Konstellation voraus. Doch damit soll diese Art der Diskussion auch ein Ende haben: Pauschalitäten dieser Art führen in der IT-Praxis zu nichts.

Der Sicherheitsanspruch und der Einsatz von Mitteln müssen stets in ein zum konkreten Bedarf passendes gesundes Verhältnis gesetzt werden. Damit ist keine Lösung in jedem Fall sofort „die bessere“. Begrenzte Ressourcen bei Geld und Personal sind abzuwägen, und die Bewertung des erreichten oder erreichbaren Sicherheitsniveaus hängt auch in virtuellen Umgebungen von diversen Faktoren ab (siehe auch BSI IT-Grundschutz-Kataloge Maßnahme M 2.392 „Sicherer Einsatz virtueller IT-Systeme“). Die Wahl der Technik ist dabei nur eine zu berücksichtigende Größe.

Grundsätzlich führt die Verkettung aus physischem und virtuellem System im ersten Schritt sowohl aufgrund der Architektur als auch der zusätzlichen Komplexität zu einem geringeren Sicherheitsniveau, da ein Mehr an Software-Komponenten auch ein Mehr an denkbaren Schwachstellen bedeutet. Inwiefern eine Lösung den Anforderungen genügt, muss bei jeder Technik über eine gezielte Risikoanalyse und hieraus hervorgehender Maßnahmenwahl sicher gestellt werden. Als Basis dienen hierzu eine umgebungsspezifische Festlegung konkreten Sicherheitsbedarfs sowie ein solides Wissen um die Prüfpunkte und Möglichkeiten der jeweiligen technischen Basis.

**3. Gefährdungen und Maßnahmen**

Insgesamt ist die logische Konsequenz des Wegfalls bzw. Ersatzes von Hardware eine deutliche Verschiebung der Risiken in Richtung Software. Teilweise können bestehende Konzepte und Best Practices zur IT-Sicherheit für virtuelle Server-Umgebungen übernommen werden; andere Bereiche müssen hingegen (wie im Folgenden beschrieben) neu erarbeitet oder zumindest angepasst werden.

Für die Absicherung der Umgebung, physisch wie virtuell, gelten im Allgemeinen die bisherigen Grundsätze, wobei zusätzliche Gefährdungen und entsprechende Maßnahmenkataloge berücksichtigt werden müssen.

Zu den Angriffsvektoren bzw. Risiken im Zusammenhang mit dem Einsatz einer Server-Virtualisierung zählen insbesondere die nachfolgenden Punkte. Zu unterscheiden ist dabei nach von einem Fehler betroffener Ebene der Virtualisierungslösung (bestehend aus der Hardware der Virtualisierungsbasis und der Software-Ebene der Virtualisierungsbasis, d.h. Host-System bzw. Hypervisor) und den auf dieser Basis laufenden virtuellen Servern. Je nach Zusammenwirken von verschiedenen Teillösungen aus Sicht des Anwenders kann sich dabei die Auswirkung auf ein Gesamtsystem aus verschiedenen, auf unterschiedlicher Hardware realisierten Servern erstrecken:

- Hardware → Host-System/Hypervisor

Ein Fehler in der Hardware der Virtualisierungsbasis kann direkte Auswirkungen auf die Verfügbarkeit des Host-Systems haben und sich damit potentiell auf eine Vielzahl virtueller Server auswirken.

- Host-System/Hypervisor → virtuelle(r) Server

Ein Fehlerzustand der Software der Virtualisierungsbasis (bei fehlerfrei funktionierender Hardware) kann je nach Umfang der betroffenen virtuellen Servern ein Gesamtsystem als Ganzes unbrauchbar machen (Beispiel: VMware ESX Lizenzfehler im August 2008<sup>1</sup>).

**Jetzt Leser werden**



**Der Netzwerk Insider**

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.

Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

<sup>1</sup>siehe <http://kb2.vmware.com/kb/1006716.html>

Virtualisierung: Sicherheit in virtuellen Server-Umgebungen

- Virtuelle Maschine → andere virtuelle Maschine(n)

Eine Überbeanspruchung von Ressourcen (ob beabsichtigt oder nicht) kann sich auch auf andere virtuelle Maschinen negativ auswirken, soweit die Virtualisierungsbasis hier keine strikt getrennte Ressourcenzuordnung realisiert. Auch können Fehler in der Virtualisierungssoftware einen Einbruch von einer virtuellen Maschine aus in eine fremde virtuelle Maschine begünstigen. Dies kann je nach Art und Umfang einen erfolgreichen Angriff auf eine einzelne virtuelle Serverlösung darstellen oder ein Gesamtsystem betreffen dem der angegriffene Server aus Anwendersicht angehört.

- Virtuelle Maschine → Host-System/Hypervisor

Angriffe können weiterhin aus der virtuellen Maschine direkt auf den Hypervisor zielen und damit womöglich in der Kompromittierung des Gesamtsystems enden.

- Virtuelle Maschine → Storage

Sofern die virtuelle Maschine Zugriff auf von mehreren Servern genutzten Storage hat, z.B. mittels iSCSI oder virtualisierten Host-Bus-Adaptoren (HBAs), müssen Vorkehrungen getroffen werden, dass kein Zugriff auf fremde Datenbestände möglich ist. Diese Notwendigkeit gilt auch in nicht virtuellen Umgebungen, jedoch ist gemeinsame Nutzung gleicher Storage-Hardware in virtuellen Umgebungen typischer, womit dieser Gesichtspunkt stärker zu bewerten ist.

- Extern → Host-System/Hypervisor

Angriffe von außen, die sich direkt an das Host-System richten, können im schlimmsten Fall ebenfalls eine vollständige Kompromittierung des Host-Systems bedeuten.

Diese Liste illustriert (ohne Anspruch auf Vollständigkeit) die Komplexität der Gefährdungslage. Hinzu kommen je nach Umgebung weitere Systeme, zu denen Abhängigkeiten bestehen. Im Folgenden werden die Herausforderungen an die IT-Sicherheit für die verschiedenen Bereiche der Server-Virtualisierung genauer betrachtet.

**3.1 Überwachung innerhalb der Virtualisierung**

Die „Verdichtung“ der Infrastruktur erfor-

dert nicht zwingend neue Werkzeuge, jedoch müssen bisher genutzte Werkzeuge der neuen Situation angepasst werden, um die Kontrolle über die IT-Landschaft zu behalten. Die Server-Infrastruktur endet durch den Einsatz der Virtualisierung nicht länger am physischen Server, der entsprechend im Monitoring und der Dokumentation (z.B. physisches und logisches Design) abgebildet werden muss. Die Notwendigkeit einer geeigneten Überwachung und Dokumentation gilt umso mehr in virtuellen Umgebungen, da sich die Server-Anzahl mit der Server-Virtualisierung erfahrungsgemäß erhöht. Die Gründe für erhöhte Server-Anzahlen liegen sowohl im einfacheren Deployment neuer Server z.B. für Test- und Entwicklungssysteme als auch in der Isolation von Diensten, die bisher auf einem gemeinsam genutzten physischen Server liefen.

Die genannten Aspekte zeigen bereits, dass dem Management und der Überwachung der virtuellen Infrastruktur besondere Aufmerksamkeit gewidmet werden muss. Die Herausforderungen liegen dabei in der hohen Dynamik einer virtuellen Infrastruktur, die bisher überwiegend statisch in Form von fest zugeordneten Ressourcen vorlag. Mittels dynamischer Verteilung von virtuellen Servern ist dieses Gesetz aufgehoben.

Neben der Virtualisierungsinfrastruktur selbst, die überwacht werden muss, sind Werkzeuge erforderlich, die den Datenfluss innerhalb der virtuellen Umgebung überwachen. Dieser Verkehr ist für klassische Monitoring-Lösungen, welche Daten an physischen Infrastruktur-Elementen ermitteln, unsichtbar (beispielsweise die Auslastung einzelner virtueller Switch Ports). Aber auch die Überwachung einzelner Applikationen und deren Performance bzw. Antwortzeit ist zu berücksichtigen, da die virtuelle Maschine sich eine gemeinsame physische Hardware mit weiteren virtuellen Maschinen teilen muss, die ebenfalls Einfluss auf die Leistung haben können. An dieser Stelle sind neue Me-

chanismen zur Ressourcenplanung und Kontrolle notwendig.

Da die meisten Funktionen in Form von Software abgebildet sind, ist auch das Risiko der Fehlbedienung höher, da beispielsweise das Kappen einer Netzanbindung, das Ausschalten von Servern oder der Rollback eines Snapshots nur weniger Mausklicks bedarf. Diese Risiken können durch angepasste und eingeübte Prozesse vermindert werden. Die größte Herausforderung besteht somit im Betrieb der Lösung.

**3.2 Sicherheit des Host-Systems**

Das Fundament der Server-Virtualisierung sind die Host-Systeme, auf denen die virtuellen Maschinen betrieben werden. Der oft thematisierte GAU besteht in der vollständigen Kontrolle des Host-Systems durch einen Angreifer und damit potentiell der Kontrolle über eine Vielzahl von virtuellen Maschinen. Hiermit ist das Thema der Verfügbarkeit unmittelbar verbunden, denn der Ausfall eines Host-Systems bedeutet nicht länger nur den Verlust eines Servers, sondern den Ausfall von x Servern in Form virtueller Maschinen. Dieses Risiko gilt es durch entsprechende Verfügbarkeitskonzepte (z.B. Verwendung von Clustern) zu minimieren, wobei speziell das Thema Cluster mit all seinen Facetten (Split-Brain-Syndrom, Fencing, Heartbeat, Cluster-fähige Dateisysteme etc.) nicht zur Vereinfachung des Gesamtsystems beiträgt.

Das Host-System (Hypervisor oder (Standard)-Betriebssystem plus Hypervisor, siehe Abbildung 2) wird damit zum Single Point of Failure. Neben einem direkten Angriff auf das Host-System kann ein Angriff auch anhand einer virtuellen Maschine erfolgen. Dass dies keine rein akademischen Risiken sind, wurde bereits mehrfach erfolgreich demonstriert (siehe (New) Blue Pill<sup>2</sup>, SubVirt<sup>3</sup>, etc.). Neben der vollständigen Kompromittierung sind aber auch partiell erfolgreiche Angriffe zu betrachten, z.B. Zugriff auf Arbeitsspeicher

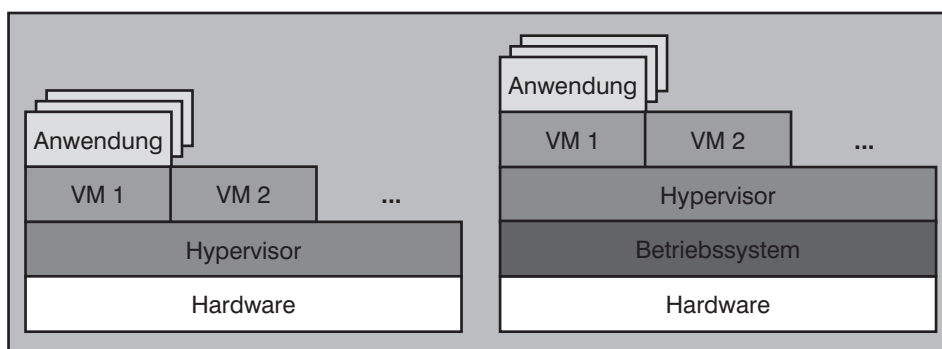


Abbildung 2: Hypervisor „Bare-Metal“, Typ 1 (links) oder auf Basis eines Betriebssystems, Typ 2 (rechts)

<sup>2</sup>siehe <http://bluepillproject.org/>

<sup>3</sup>siehe <http://www.eecs.umich.edu/virtual/papers/king06.pdf>

Virtualisierung: Sicherheit in virtuellen Server-Umgebungen

oder Netzwerk, welches ein Ausspähen von sensiblen Daten ermöglicht, oder Angriffe vom Typ DoS (Zuweisung von mehr Ressourcen als vorgesehen, Blockade von bestimmten Funktionen wie Shutdown der virtuellen Maschine etc.). Auch wenn diese Risiken prinzipiell zu berücksichtigen sind, muss man sie dennoch relativieren. Bevor man sich explizit diesen technisch anspruchsvollen Angriffen widmet, sollte das Augenmerk auf Design und Implementierung nach „Best Practices“ und zugehörigem Management liegen. Dennoch existieren bereits Ansätze, diesen Angriffsvektor z.B. durch die Nutzung von TPM-Chips (Trusted Platform Module) zumindest zu erschweren.

Potentielle Risiken können bereits durch die Wahl der Virtualisierungsplattform verringert werden. Um die Angriffsfläche möglichst gering zu halten, empfiehlt sich generell ein Hypervisor, der direkt auf der Hardware („bare metal“) aufsetzt (Typ 1, Abbildung 2, links) und kein zusätzliches Betriebssystem als Plattform verwendet (Typ 2, Abbildung 2, rechts). Durch jede auf diese Weise eingesparte Zeile Quellcode wird nicht nur die Angriffsfläche verringert, sondern auch die Stabilität erhöht. Außerdem reduziert sich der Aufwand zur Absicherung, da für das Betriebssystem eines Typ-2-Hypervisors dedizierte Sicherheitsmaßnahmen (wie Härtung, Schutz vor schadenstiftender Software, etc.) umgesetzt werden müssen.

Beispiele für einen Typ-1-Hypervisor sind VMware ESXi („i“ für integrated) und Microsoft Hyper-V. Erwähnenswert ist dabei der Unterschied im Speicherplatzbedarf: während dieser bei VMware ESXi bei 32 MB liegt, kann Microsoft Hyper-V - auch bei Verwendung der Core-Server-Rolle - noch mind. 1 GB beanspruchen<sup>4</sup>. Produkte vom Typ 2, die ja auf Standardbetriebssystemen aufbauen, sind beispielsweise VMware Server oder Microsoft Virtual Server.

Für beide Virtualisierungsvarianten, sowohl Hypervisor vom Typ 1 als auch vom Typ 2, existieren zusätzliche Konfigurationsempfehlungen und Checklisten, welche die Sicherheit der Systeme erhöhen können. Ausgehend von den jeweiligen Unterlagen der Hersteller sowie einer Vielzahl von Online-Publikationen liefern speziell die Unterlagen des US-Verteidigungsministeriums (bzw. der Defense Information Systems Agency, kurz DISA) hilfreiche Informationen<sup>5</sup>. Aktuell besteht allerdings eine durchaus kontroverse Diskussion in der Virtualisierungsgemeinde über den Umfang und die Verantwortung des Herstellers der Virtualisierungslösung bzgl. der Sicherheit.

3.3 Sicherheit des Gastsystems

Das Host-System bzw. der Hypervisor stellt nur die Plattform für die produktiven Server bzw. Dienste dar. Neben den traditionellen Gefährdungen für physische Server, wie beispielsweise Viren und andere Programme mit Schadensfunktion, sind Gefährdungen zu berücksichtigen, die mit den Gastsystemen verbunden sind. Dies betrifft beispielsweise die Performance, wenn z.B. ein Fremdsystem unbeabsichtigt oder missbräuchlich Ressourcen-intensive Operationen durchführt. Hinzu kommt die Schnittstelle vom Gastsystem zum Hypervisor - zum einen in Richtung anderer virtueller Maschinen, zum anderen in Richtung des Host-Systems selbst. Dass diese Schnittstelle durchaus eine Gefährdung darstellt, zeigt ein Blick in das Verwundbarkeitsverzeichnis Common Vulnerabilities and Exposures (CVE)<sup>6</sup>: Hier werden für 2008 mindestens zehn solcher Schwachstellen in Produkten von VMware oder Xen aufgeführt<sup>7</sup>.

In diesem Kontext findet sich auch der irreführenden Begriff „Rogue VM“ (analog zu „Rogue Access Points“), der besagt, dass virtuelle Maschinen unerwartet und ohne Genehmigung eingebunden werden können. Dies ist grundsätzlich falsch, da ohne Zugriff und explizite Konfiguration keine virtuelle Maschine in das Gesamtsystem eingebunden werden kann. Wahrscheinlicher sind menschliche Fehler (oder böswillige Absicht) durch an das Netz angebundene Systeme mit virtuellen Maschinen, die z.B. zu einem Rogue-DHCP-Server führen. Dies

ist jedoch kein spezifisches Problem der Virtualisierung, auch wenn dies dadurch ggf. begünstigt wird und das Troubleshooting erschweren kann.

Um die Sicherheit der Gastsysteme zu gewährleisten, gelten vorwiegend die bereits bewährten Maßnahmenkataloge, welche beispielsweise die folgenden Punkte umfassen:

- Härtung des Betriebssystems
- Installation eines Anti-Virus-Programms
- Regelmäßige und zeitnahe Aktualisierung des Betriebssystems
- Beachtung der Sicherheitshinweise der jeweiligen Applikation
- Regelmäßige Sicherung des Systems einschließlich Übung der Wiederherstellung
- Monitoring, Dokumentation und Information über aktuelle Sicherheitslücken

Zusätzlich sind jedoch auch neue Maßnahmen zu berücksichtigen und bisherige ggf. neu zu bewerten. Dies beinhaltet z.B. die folgenden Maßnahmen:

- Entfernen nicht benötigter virtueller Hardware
- Aktualisierung der Virtualisierungs-Software innerhalb der virtuelle Maschine (z.B. VMware Tools)
- Isolation von Diensten, die bisher gemeinsam auf einer physischen Hardware liefen
- Regelmäßige und zeitnahe Aktualisierung der Applikationen

Jetzt Leser werden



## Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.

Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

<sup>4</sup>siehe <http://technet.microsoft.com/en-us/library/cc753802.aspx>

<sup>5</sup>siehe <http://iase.disa.mil/stigs/stig/index.html>

<sup>6</sup>siehe <http://cve.mitre.org/>

<sup>7</sup>siehe auch Untersuchung zur Sicherheit in virtuellen Umgebungen: <http://taviso.decsystem.g/virtsec.pdf>

Virtualisierung: Sicherheit in virtuellen Server-Umgebungen

- Intensiveres Testen von Patches anhand der Virtualisierung einschließlich Wiederherstellung des vorherigen Zustandes (Snapshot- und Rollback-Funktion)

**3.4 Sicherheit des virtuellen Netzes**

Bezüglich der Sicherheit der Netzinfrastruktur muss berücksichtigt werden, dass in virtualisierten Systemen neben der Server-Landschaft auch die Vernetzung der Server virtualisiert wird. Für den internen Schutz solcher virtualisierten Netze stehen entsprechend virtualisierte Sicherheitselemente (wie z.B. IDS/IPS oder Firewall) zur Verfügung.

Bezüglich der Funktionsweise virtueller Switches, möglicher Topologien im Zusammenspiel zwischen virtuellen und physischen Netzelementen und der Isolation unterschiedlicher Sicherheitszonen wurde bereits detailliert im Netzwerk Insider vom November 2008 eingegangen, auf den an dieser Stelle verwiesen wird<sup>8</sup>. Abbildung 3 illustriert den Aufbau virtueller Sicherheitszonen, d.h. virtuelle Netze, die durch virtualisierte Sicherheitselemente geschützt werden.

Die Komplexität der Konfiguration virtueller Netze dürfte damit in Zukunft der physischen Infrastruktur in nichts nachstehen. Aktuell müssen virtualisierte Sicherheitsprodukte (wie sie derzeit von einigen Herstellern forciert werden) außerdem noch skeptisch betrachtet werden. Diese stellen derzeit in der Regel keinen Ersatz für physische Komponenten dar, sondern können ggf. als Ergänzung betrachtet werden. Dies hat zunächst zwei Gründe:

- Performance: Insbesondere Anforderungen im Gigabit-Bereich, für die bisher spezielle Hardware zum Einsatz kam, können aktuell nicht durch virtualisierte Sicherheitsprodukte realisiert werden. Beispielsweise haben Produkte im Bereich Unified Threat Management (UTM), die neben Firewall-Funktion weitere CPU-intensive Aufgaben wie Pattern-Analysen, Viren-Überprüfungen bündeln, erhebliche Leistungsanforderungen.
- Sicherheit: Diese Produkte sind neu und damit bisher wenig erprobt. Ihre Zuverlässigkeit müssen sie daher noch unter Beweis stellen. Weiterhin handelt es sich um normale virtuelle Maschinen. Somit gelten für sie die gleichen Gefährdungen wie für andere virtuelle Gastsysteme bzw. die gesamte virtuelle Infrastruktur.

zung von virtuellen Servern ist jedoch die im Folgenden beschriebene Dynamik und Mobilität der Systeme.

**3.5 Besondere Berücksichtigung der Dynamik und Mobilität**

In der traditionellen Server-Nutzung ist die Zuordnung von Sicherheitsmaßnahmen zu einem Server meist eher statisch. Der Server wird konfiguriert und verrichtet für einen längeren Zeitraum seinen Dienst. Das Bündel von Sicherheitsmaßnahmen, das auf den Server und die dort laufenden Anwendungen angewendet wird, muss nur bei gravierenden Änderungen des Systems (also meist selten) angepasst werden.

Bei Nutzung virtueller Server ist dies jedoch ein hochgradig dynamischer Prozess!

Der Aufenthaltsort eines Servers ist in einer virtuellen Umgebung nicht länger statisch. Das Aufsetzen eines virtuellen Servers reduziert sich umgangssprachlich auf einen Doppelklick. Der virtuelle Server kann dann mit entsprechenden Bordmitteln der Virtualisierungslösung (z.B. VMware VMotion, Citrix oder Microsoft Live Migration) sogar ohne Unterbrechung des laufenden Betriebs auf einen anderen

physischen Server migriert werden. Dieses Verschieben von virtuellen Maschinen zwischen verschiedenen Host-Systemen im laufenden Betrieb (nur Arbeitsspeicher oder auch Festplattendateien) kann beispielsweise aufgrund eines Ausfalls oder einer Ressourcenoptimierung erfolgen.

In bisherigen physischen Infrastrukturen sind Sicherheitsarchitekturen hochgradig von physischen Gegebenheiten abhängig, wie z.B. Switches, NICs oder anderen Sicherheitselementen. Eine virtualisierte Umgebung erfordert, dass dieser Sicherheitskontext dynamisch auf allen potentiellen Host-Systemen zur Verfügung steht und dabei die Abhängigkeiten zu anderen Systemen berücksichtigt werden.

In der Konsequenz bedeutet dies:

- Speicherinhalte und ggf. auch der gesamte Server samt Massenspeicher (Beispiel: VMware Storage VMotion) müssen über das Netz transportiert werden.

In der Standardkonfiguration erfolgt dieser Transport oft im Klartext. Je nach Schutzbedarf der transportierten Daten müssen also Sicherheitsmaßnahmen

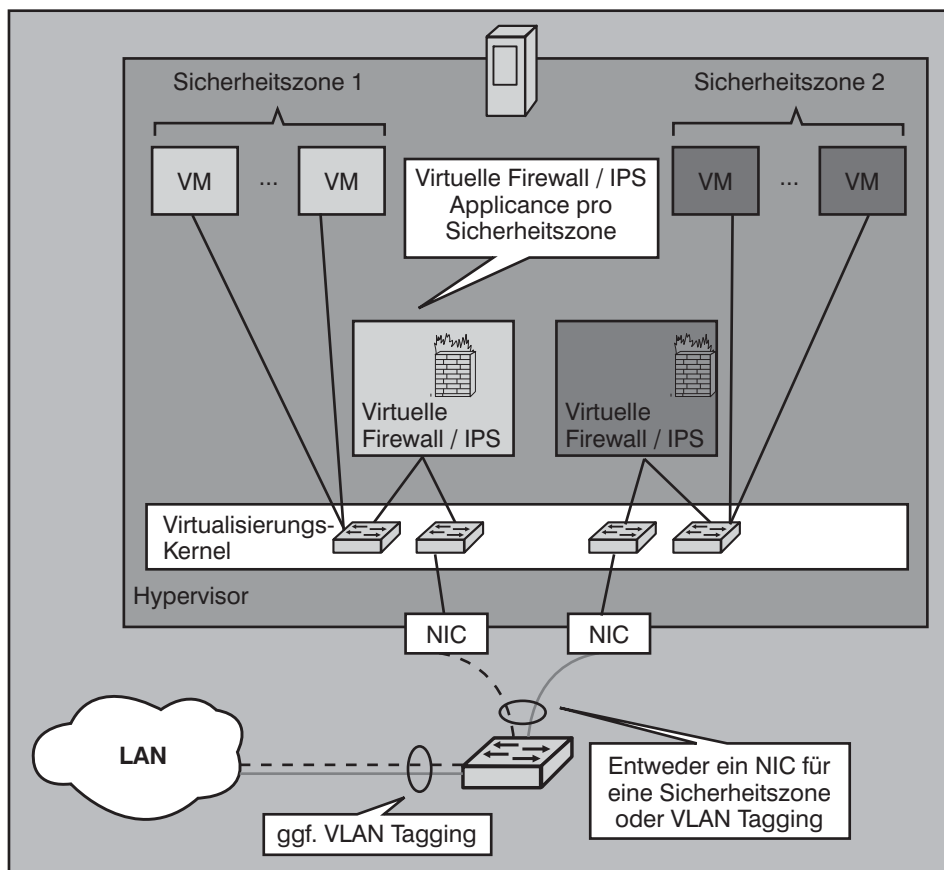


Abbildung 3: Virtualisierung von Sicherheitszonen

Besonders kritisch für die sichere Vernet-

<sup>8</sup>siehe <http://www.comconsult.com/papers/Sicherheitszonen-in-LAN-und-Rechenzentrum.pdf>

Virtualisierung: Sicherheit in virtuellen Server-Umgebungen

umgesetzt werden. Zu nennen sind hier die zusätzliche Verschlüsselung des Netzverkehrs (z.B. per IPsec) oder zumindest die Nutzung eines separaten physischen Netzes bzw. VLAN für das Verschieben virtueller Server zwischen physischen Servern.

- Der Sicherheitskontext muss am Quell- und Zielort identisch sein.

Dabei muss neben den auf den physischen Server angewendeten Sicherheitsmaßnahmen insbesondere die virtualisierte Netzumgebung des virtuellen Servers berücksichtigt werden. Dies beinhaltet beispielsweise zunächst Konfiguration und Regelwerk einer virtualisierten Firewall. Wenn ein Server im laufenden Betrieb umgezogen wird, muss neben dem Zustand des Servers auch der komplette für den Server relevante Zustand einer entsprechenden Firewall umziehen (etwa Informationen, welche Sitzungen aktuell bestehen). Analog müssen Switch-Konfigurationen (z.B. VLANs, QoS-Parameter, etc.) übertragen werden und Aspekte des Monitorings (z.B. Traffic-Verbrauch, der anhand flüchtiger Zählerwerte festgehalten wird) berücksichtigt werden.

Cisco adressiert dieses Thema Serverübergreifender Netzkomponenten und damit auch Sicherheitskontexte aktuell beispielsweise mit dem Nexus 1000V.

VMware hat mit vShield Zones jetzt ein Konzept vorgestellt, das die Umsetzung von Sicherheitsvorgaben für die virtuellen Maschinen auch dann sicherstellen soll, wenn einzelne virtuelle Server zwischen physischen Servern migriert werden. Im Frühjahr 2009 soll hierzu ein Betaprojekt starten.

Es ist weiterhin zu erwarten, dass auch andere Hersteller in diesem Bereich Produkte auf den Markt bringen werden und neben der Thematik dynamischer Sicherheits- und Netzkontexte auch folgende Bereiche abdecken:

- Management (Skalierbarkeit, Integration in physische Netzinfrastruktur, etc.)
- Monitoring (z.B. via SNMP oder Netflow)
- Funktionsumfang (QoS, AAA, ACLs, etc.)

**3.6 Sicherheit der Datenspeicher und des Speichernetzes**

Ein virtueller Server (bzw. der Massenspeicher eines virtuellen Servers) besteht in

der Regel nur noch aus einzelnen Dateien. Diese können bei ungenügender Absicherung z.B. auf mobile USB-Datenträger kopiert werden. Der Angreifer verfügt damit über ein vollständiges Abbild des Servers, das er offline analysieren kann. Dieses Abbild muss der Angreifer nicht zwangsläufig booten und weitere Sicherheitsmaßnahmen, wie z.B. Bootloader-Passwort oder Betriebssystem-Login überwinden, um an die Daten zu gelangen. Stattdessen kann er unter Umständen das Image direkt in die Verzeichnisstruktur (z.B. als zusätzlichen Laufwerksbuchstaben) einbinden und erhält auf diese Weise Zugriff auf die Daten.

Bei der Verwendung eines Speichernetzes (SAN) ergeben sich zudem folgende Risiken:

- Auf IP-basierte Speichersysteme (z.B. iSCSI) vererben sich zunächst automatisch alle Gefährdungen von IP.
- Daten der virtuellen Maschinen (z.B. der Inhalt des Arbeitsspeichers) bzw. vollständige virtuelle Server werden i.d.R. unverschlüsselt über das Netz transportiert. Vertraulichkeit sowie Daten- und Hostintegrität sind also gefährdet. Im Fall von IP-basierten Speichersystemen sind Übertragungswege und Netzkomponenten nicht zwingend reserviert für Speicherverkehr, sondern werden von verschiedensten anderen Verkehrstypen gemeinsam genutzt.
- Anhand von Manipulationen kann ein Zugriff auf nicht erlaubte Datenpartitionen erfolgen (z.B. Daten anderer Sicherheitszonen).

Der letzte Punkt ist eine mögliche Konsequenz, wenn Speicherplatz als zentrale Ressource Systemen unterschiedlicher Sicherheitszonen zugewiesen wird. Ein gesondertes SAN für eine DMZ oder verschiedene Fachabteilungen ist zumindest nicht die Regel. Wird beispielsweise

ein solcher Server der DMZ kompromittiert, besteht die Gefahr, dass dieser Server Zugriff auf Datenpartitionen erhält (z.B. mittels IQN/WWN Spoofing), die eigentlich einem Server z.B. der Personalabteilung vorbehalten sind. Diese Gefährdung besteht zunächst generell, sie wird jedoch durch virtuelle Server deutlich erhöht.

Zu den möglichen Maßnahmen gehören:

- Aufbau eines zumindest logisch getrennten dedizierten Netzes für Speichieranbindung und Management
- Berücksichtigung von Zonierungen innerhalb des Speichernetzes (SAN Zoning, Virtuelle SANs, etc.), so dass entsprechende Sicherheitszonen gebildet werden können
- Authentisierung zwischen Client und Server (z.B. beidseitiges CHAP bzw. DH-CHAP)
- Verschlüsselung auf Ebene des Netzes (z.B. per IPsec oder IEEE 802.1AE) oder sogar Verschlüsselung auf Ebene des Speichermediums

**4. IT-Sicherheitsmanagement und Virtualisierung**

Die beschriebenen technischen Aspekte der Absicherung virtueller Server haben unmittelbare Konsequenzen für das IT-Sicherheitsmanagement und die Gestaltung von Sicherheitskonzepten.

Zunächst muss, wie bereits erwähnt, die Server-Virtualisierung in den Sicherheitskonzepten Server, Betriebssysteme und Anwendungen berücksichtigt werden (Abbildung 4). Die in diesem Artikel beschriebene Komplexität legt die Erstellung eines eigenständigen Sicherheitskonzepts mit einem spezifischen Maßnahmenkatalog für den Umgang mit Server-Virtualisierung nahe.

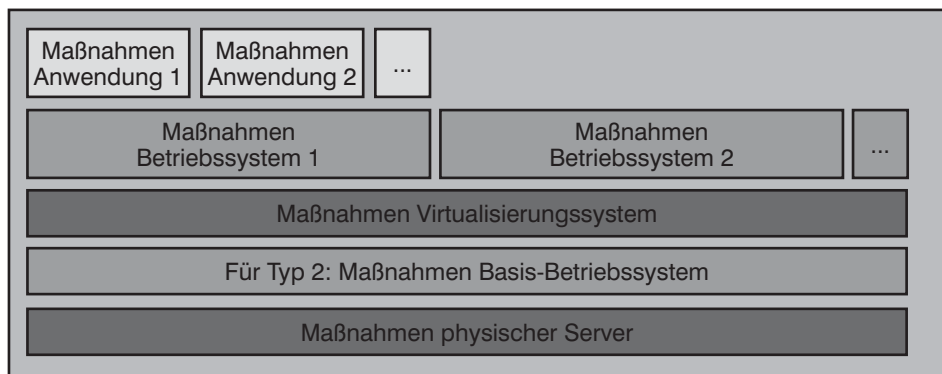


Abbildung 4: Berücksichtigung der Server-Virtualisierung in Sicherheitskonzepten

Virtualisierung: Sicherheit in virtuellen Server-Umgebungen

Insbesondere müssen Datensicherungskonzepte und Notfallvorsorgekonzepte für den Umgang mit Server-Virtualisierung angepasst werden. Außerdem steigen meist durch einen Kumulationseffekt die Sicherheitsanforderungen an die physischen Server. Auch hier müssen die bestehenden Sicherheitskonzepte und Betriebsprozesse ggf. entsprechend erweitert werden, bzw. es wird die Anzahl der virtuellen Server pro physischem Server begrenzt (und zur Vorgabe für den Durchschnittsfall erklärt), bis zu der ein möglicher Kumulationseffekt nicht berücksichtigt werden braucht.

Die Flexibilität und Dynamik der Server-Virtualisierung hat unmittelbare Auswirkungen auf die Vorgehensweise bei der Feststellung des Schutzbedarfs und der Auswahl der auf ein IT-System anzuwendenden Sicherheitsmaßnahmen.

Grundlage einer praktikablen sicheren Server-Virtualisierung ist dabei die Normierung von virtuellen Servern. Dies beinhaltet zunächst Konfigurationsvorgaben an das Betriebssystem auf den virtuellen Servern sowie die Festlegung der Anwendungsbereiche und der Dienste. Unabhängig von dem für die konkreten virtuellen Server bestimmten Schutzbedarf (beispielsweise unter Verwendung der BSI-Methodik) wird von vorneherein festgelegt, dass als Ausgangspunkt nur einer der normierten virtuellen Server herangezogen werden darf. Dieser kann bei Bedarf noch gezielt weiter abgesichert werden. Andere Formen der Diversifizierung von Sicherheitskonfigurationen für virtuelle Server werden nicht zugelassen.

Wer diese Strategie zur sicheren Grundkonfiguration von virtuellen IT-Systemen verlässt, handelt sich unweigerlich eine unüberschaubare Sammlung aus Einzelösungen ein, die schon bei dedizierten Servern nicht zu empfehlen ist. Im Fall virtueller Systeme mit der Addition von zu härtender Virtualisierungsbasis (Hard- und Software) und zu härtenden virtuellen Maschinen entstünde eine Matrix aus möglichen Kombinationen, die sicherheitstechnisch nicht mehr mit verhältnismäßigem Aufwand bewertbar und aktualisierbar ist (Patch-Management, Change Management unter Aufrechterhaltung des erforderlichen Sicherheitsniveaus).

Für jeden auf die beschriebene Weise normierten virtuellen Server kann ein Maßnahmenbündel spezifiziert werden, indem beispielsweise die anwendbaren Maßnahmen der entsprechenden Bausteine der BSI IT-Grundschutzkataloge ausgewählt werden. Dabei kann im Rahmen der Nor-

mierung sofort ein Maßnahmenbündel für den normalen Schutzbedarf (Mindesthärtung) sowie ein hierauf aufbauendes erweitertes Maßnahmenbündel für den erhöhten Schutzbedarf (Basishärtung für erhöhten Schutzbedarf) festgelegt werden. Die wesentlichen Vorgaben können dann als Konfigurationsrichtlinie für jedes Gastbetriebssystem festgelegt werden.

Werden die so geschaffenen Umgebungsstandards für normierte virtuelle Server der Varianten „Schutzbedarf normal“ bzw. „Schutzbedarf erhöht“ in geeigneter Form verwaltet und bei der Serverimplementierung vervielfältigt, tut eine gelegentliche „Übererfüllung“ der Sicherheitsanforderungen bei Einsatz eines Profils für den erhöhten Schutzbedarf aufwandstechnisch

nicht weh. Einrichtungsaufwand ist auf diese Weise kein Gegenargument gegen normierte virtuelle Server zur Optimierung der Effizienz im Sicherheitsmanagement. Für die praktische Umsetzung bietet die Virtualisierung hierzu mittels entsprechender „VM-Bibliotheken“ eine einfache Möglichkeit virtuelle Server auf Basis obiger Konfigurationsrichtlinien zu hinterlegen und bei Bedarf zu klonen, um eine höchstmögliche Übereinstimmung mit den Konfigurationsrichtlinien zu erzielen.

Anschließend können Vorgaben für die Abbildung der normierten virtuellen Server auf den physischen Servern gemacht werden. Hier muss beispielsweise festgelegt werden, ob man virtuelle Server, die unterschiedlichen Vertrauensbereichen zuzu-

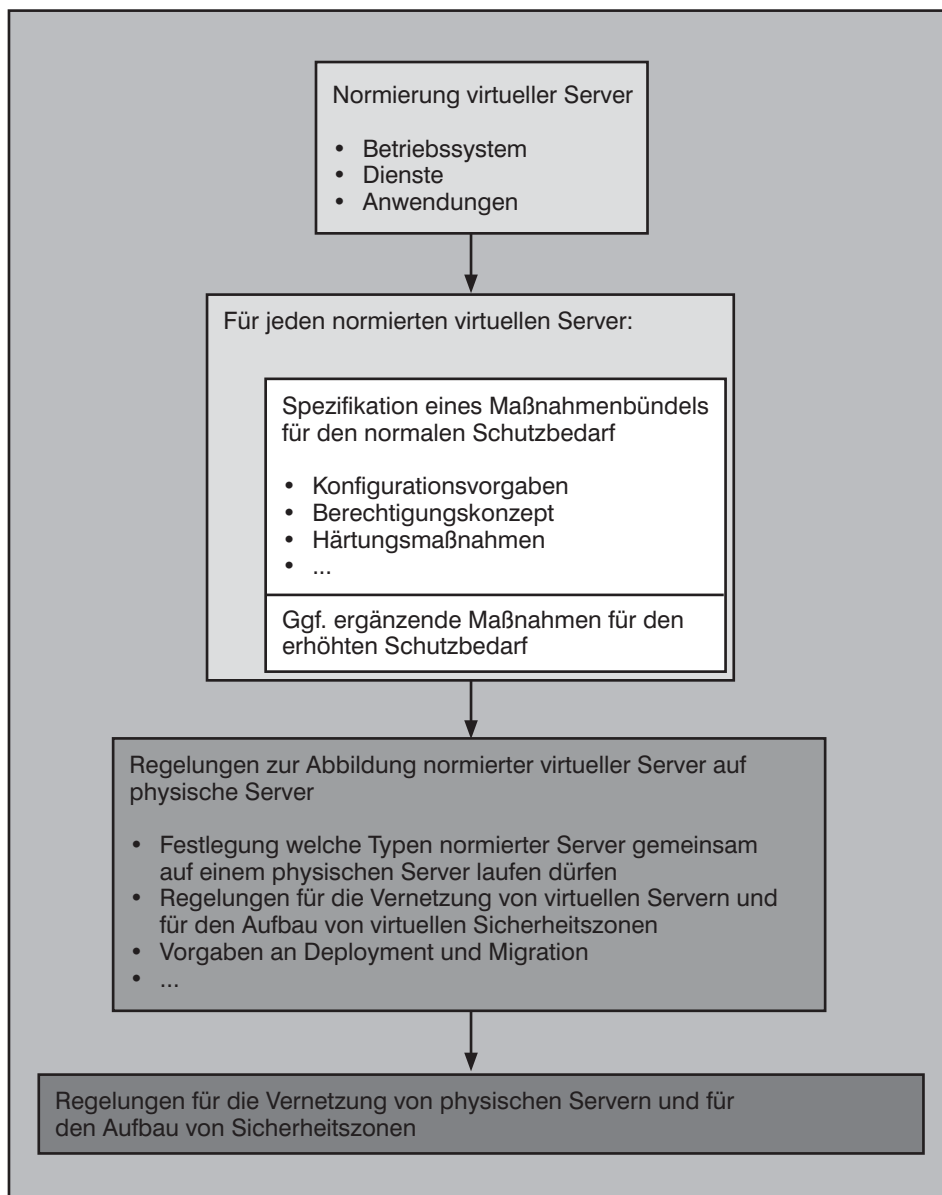


Abbildung 5: Strukturierte Vorgehensweise bei der Absicherung virtueller Server-Umgebungen

Virtualisierung: Sicherheit in virtuellen Server-Umgebungen

ordnen sind, auf einem physischen Server laufen lassen darf oder nicht. Auf dieser Basis können dann die (virtuelle) Vernetzung der normierten virtuellen Server spezifiziert und Regelungen für die Migration zwischen verschiedenen physischen Systemen erarbeitet werden. Dies beinhaltet neben Maßnahmen für die Konfiguration der virtuellen Switches (z.B. kein Promiscuous Mode auf virtuellen Switches) ggf. auch die Gestaltung virtueller Sicherheitszonen verbunden mit Vorgaben an das Regelwerk virtualisierter Firewalls.

Insgesamt ist für jeden physischen Server festzulegen, welche virtuellen Server bzw. Typen von virtuellen Maschinen auf ihm laufen dürfen. Der Schutzbedarf der physischen Server ergibt sich dann durch Vererbung des Schutzbedarfs der einzelnen virtuellen Systeme unter Berücksichtigung eines Kumulationseffekts. Dieser Kumulationseffekt kann – auch wenn die einzelnen virtuellen Systeme nur einen normalen Schutzbedarf haben – einen erhöhten Schutzbedarf eines physischen Servers bedingen, weil sich das Gefährdungspotential mit der Anzahl der virtuellen Systeme entsprechend erhöht. Abbildung 5 zeigt die beschriebene Vorgehensweise im Überblick.

Im Rahmen der Ergänzung und Überarbeitung der Sicherheitskonzepte sollte auch geprüft werden, ob allgemeine Policies durch den Einsatz von Virtualisierung betroffen sind. Ein Beispiel in diesem Zusammenhang sind Compliance-Anforderungen, wie sie für Kreditkartenverarbeitende Unternehmen in Form des Regelwerks PCI DSS (Payment Card Industry Data Security Standard) relevant sind. Hier ist unter anderem der Punkt 2.2.1 im Zusammenhang mit der Virtualisierung von Interesse. Dieser besagt: „Implementieren nur einer primären Funktion pro Server.“ Je nach Auditor gab es in diesem Zusammenhang bisher Unklarheiten, wie dies in einer virtuellen Umgebung zu betrachten ist, da hier mehrere Funktionen auf einem physischen Server untergebracht sind, die Funktionen dennoch isoliert in virtuellen Maschinen ablaufen können. Um in diesem Punkt Abhilfe zu schaffen, ist z.B. VMware der PCI-Gruppe im November 2008 beigetreten. In Zukunft wird das Thema Virtualisierung also auch hier konkrete Berücksichtigung finden.

5. Fazit

Die Server-Virtualisierung lässt sich nicht auf eine reine Serverkonsolidierung reduzieren. Es handelt sich vielmehr um eine neue Architektur mit Auswirkungen auf den gesamten IT-Verbund, angefangen

beim IT-Sicherheitsprozess über die Umgestaltung von IT-Sicherheitskonzepten bis hin zur Umsetzung entsprechender Maßnahmen.

Dabei liegt die Herausforderung in der Beherrschbarkeit der abstrahierten IT-Infrastruktur und weniger in Gefährdungen durch ausgefeilte, besonders für die Virtualisierungstechnik erdachte Angriffe. Zur Notwendigkeit, sich mit einer neuen Generation von Produktlösungen für den Serverbereich zu beschäftigen, kommt die Problematik, dass bislang über eigenständige Geräte unterscheidbare Teile der IT-Infrastruktur in einem Gesamtsystem verschmelzen. Die Übersicht geht leichter verloren, und die Kontrolle auf Funktionalitäten der Kommunikation und Zuständen der Server muss neu gelernt werden. Kombiniert sich dies mit einer Vielzahl an Konfigurationsalternativen, so steht man leicht vor einem sicherheitstechnisch unkontrollierbaren Gebilde. Abhilfe schaffen hier festgelegte (Umgebungs-)Standards und Prozesse sowie ein hoher Automatisierungsgrad bei der Nutzung entsprechender Werkzeuge. Kritisch sind die Seiteneffekte, die sich aus der Dynamik und Mobilität der virtuellen Server ergeben. Hier werden höchste Anforderungen an das Configuration Management und das Release Management mit unmittelbaren Auswirkungen auf die IT-Sicherheit gestellt. Ohne konsequente Standardisierung in Aufbau, Deployment, Vernetzung und Migration virtueller Server droht ein deutlicher Verlust an Sicherheit.

6. Abkürzungen

AAA	Authentication, Authorization, Accounting
ACL	Access Control List
CHAP	Challenge Handshake Authentication Protocol
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
DH-CHAP	Diffie Hellman - Challenge Handshake Authentication Protocol
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone, Demilitarisierte Zone
DoS	Denial of Service
HBA	Host Bus Adapter
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IQN	iSCSI Qualified Name
iSCSI	internet Small Computer System Interface
LAN	Local Area Network
NIC	Network Interface Card
QoS	Quality of Service
SAN	Storage Area Network
SNMP	Simple Network Management Protocol
TPM	Trusted Platform Module
UTM	Unified Threat Management
VLAN	Virtual LAN
VM	Virtual Machine, Virtuelle Maschine
WWN	World Wide Name

## Jetzt Leser werden



### Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.

Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>