

Virtualisierte Rechenzentren

Konsequenzen für die Sicherheit?



© Shutterstock

Die Konzepte, auf denen die Virtualisierung von Anwendungen und Betriebssystemen beruhen, sind durchaus nicht neu, jedoch hat sich die Geschwindigkeit, mit der sich die Virtualisierung insbesondere von Software-Betriebssystemen durchsetzt, in den zurückliegenden Jahren exponentiell zugenommen.

Virtuelle Maschinen haben endlich ihre Berufung gefunden, erobern rasch die Rechenzentren der Unternehmen und entwickeln sich überall zu einem universellen Hilfsmittel für alle Personen und Teams in IT-Abteilungen.

Was aber ist eigentlich unter einer ‚virtuellen Maschine‘ zu verstehen?

VMware definiert eine Virtualisierung als eine Abstraktionsschicht, die „die physische Hardware vom Betriebssystem entkoppelt“. Wenn

wir heute an virtuelle Maschinen denken, stellen wir uns überwiegend eine Hardware-Plattform vor, auf der mehrere Software-Betriebssysteme laufen. Meist wird dieses Konzept so umgesetzt, dass ein Betriebssystem auf einer Hard-

ware-Box (der Host-Plattform) läuft, während mehrere unabhängige Betriebssysteme gleichzeitig auf virtuellen Hardware-Plattformen (den Guests) laufen.

Die Plattform-Virtualisierung setzt in der Regel eine vollständige Hardware-Segmentierung voraus. Hierbei wird den einzelnen Guest-Plattformen erlaubt, bestimmte Abschnitte der physischen Host-Hardware zu nutzen, ohne dass es zu Konflikten oder zu Beeinflussungen der Host-Plattform kommt. Host und Guests können somit gleichzeitig operieren, ohne sich gegenseitig ins Gehege zu kommen.

Plattform-Virtualisierung

Es gibt in erster Linie zwei Arten der Plattform-Virtualisierung: transparent und ‚host-aware‘. Bei der transparenten Virtualisierung bleibt dem Guest die Tatsache, dass er virtualisiert läuft, verborgen. Der Guest nutzt die Ressourcen, als würden sie nativ auf der Hardware-Plattform laufen – ungeachtet der Tatsache, dass er durch eine zusätzliche Komponente, nämlich den VMM (Virtual Machine Monitor) oder Hypervisor gemanagt wird. Die gängigeren heutigen Arten der Virtualisierung, zum Beispiel auch jene von VMware, implementieren transparente Hypervisor-Systeme. Man kann sich diese Systeme wie Proxys vorstellen: der Hypervisor schaltet sich transparent als Proxy in die gesamte Kommunikation zwischen Guest und Host-Hardware ein, verbirgt dabei aber seine eigene Existenz so vor dem Guest, dass es diesem so vorkommt, als sei er das einzige auf der betreffenden Hardware laufende System.

‚Host-Aware‘ (das heißt host-bewusste) Implementierungen unterscheiden sich hiervon dadurch, dass in den Kernel des Guests ein gewisses Maß an ‚Wissen‘ um die Existenz des Hypervisors eingebaut ist, mit dem auch direkt kommuniziert wird. Xen, eine populäre Virtualisierungs-Implementierung für Linux, nutzt

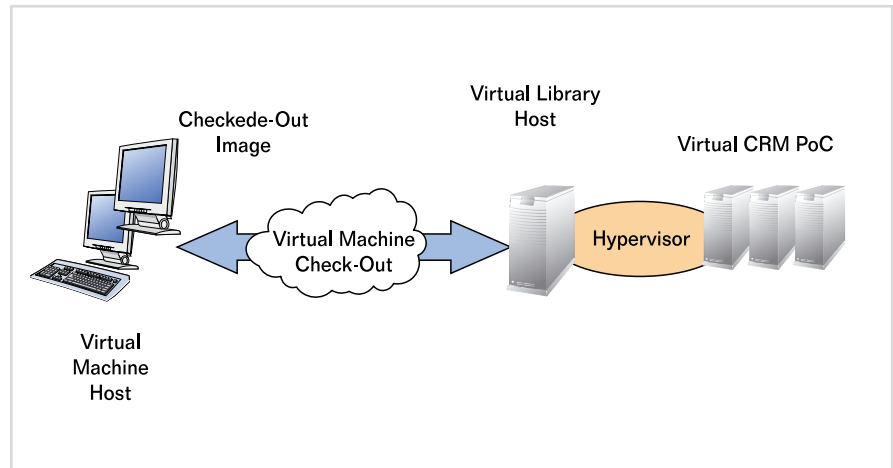


Bild 1: Example Co.'s virtual library check-out system.
(Alle Grafiken von www.f5networks.de)

eine Host-Aware-Architektur, die es notwendig macht, dass spezieller Hypervisor-Befehlscode sowohl im Host als auch in allen virtualisierten Guests aktiv läuft.

Was die wachsende Verbreitung der Virtualisierung vorantreibt, ist unter anderem die Offenheit des Hardware-Supports für VMMs. Die

Zugang zu Virtualisierungs-Umgebungen geschaffen. Die Virtualisierung gibt einem Unternehmen die Chance, eine einzige High-End-Hardwarelösung zu erwerben und auf dieser 20 virtuelle Betriebssysteme laufen zu lassen, anstatt für jede einzelne Betriebssystem-Plattform ein eigenes System zu erwerben.

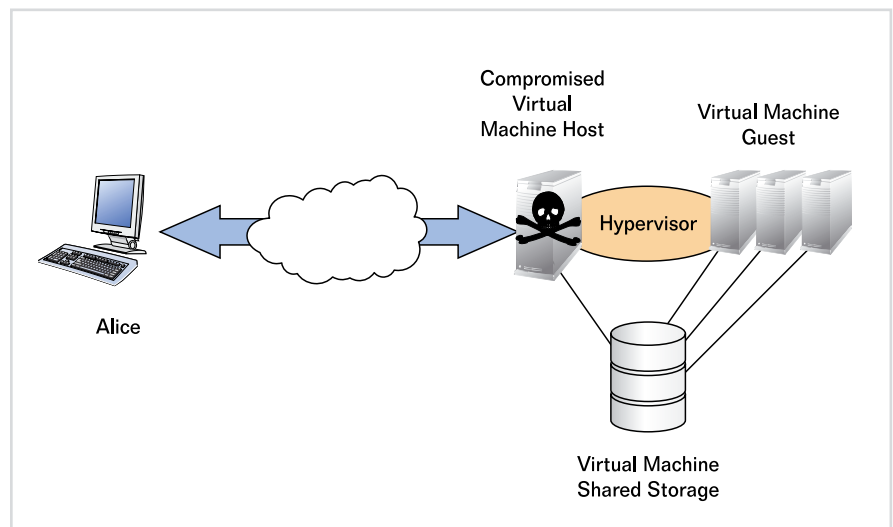


Bild 2: VMware ESX Virtual Switch mit multiplen segmentierten VLANs.

Hardware-Plattformen, die das primäre Host-Betriebssystem ausführen und managen, sind ebenso wie der VMM keine besonderen Devices oder Appliances. Diese Flexibilität, also die Verlagerung der Virtualisierungs-Software auf gewöhnliche Hardware, hat für jeden Anwender einen direkten und kostengünstigen

Virtualisierte Bedrohungsvektoren

Die Vorteile der Virtualisierung liegen auf der Hand: es gibt schlicht mehr Leistung für das gleiche Geld. Nun hat aber alles seine Vor- und Nachteile, und auch die Virtualisierung bildet hier keine Ausnahme.

Die Liste der Pluspunkte ist lang, und die Nachteile liegen eher im Verborgenen. Was kann man Schlechtes daran finden, 20 Server zum Preis eines einzigen laufen zu lassen? Auch wenn man hierin keinesfalls eine ernste Bedrohung sieht, wird die Sicherheit virtueller Maschinen und Umgebungen meist in keiner Weise berücksichtigt. Der Grund hierfür ist nicht etwa, dass die Sicherheit dieser Implementierung technologisch unerforscht wäre. Vielmehr handelt es sich hier um einen Vektor, der den Gruppen, die umfangreiche Virtualisierungen implementieren, in der Regel unbekannt ist. Im Klartext heißt dies: die Virtualisierung wird in aller Regel implementiert, ohne die mit ihr einhergehenden neuen Sicherheitsrisiken in Betracht zu ziehen.

Mit der Virtualisierung kommt eine vollkommen neue Kategorie von Sicherheitsaspekten, Problemen und Risiken ins Spiel. Sicherheits-Administratoren kennen Aussagen wie zum Beispiel „Hardened Operating System“ (sinngemäß: abgesichertes Betriebssystem), „Walled Garden“ und „Netzwerk-Segmentierung“, aus der Welt, in der jeder Applikation ein eigenes System zugewiesen wird. Wie aber können Administratoren diese Konzepte auf die noch vollkommen unerforschten Gebiete der virtuellen Rechenzentren übertragen? Wie können wir uns in neuen Umgebungen schützen, die wir nicht einmal verstehen? Heutige System- und Sicherheits-Administratoren müssen ihren Blick verstärkt auf die virtuelle Sicherheit richten und sich für ein neues Bedrohungs-Szenarium mit seinen verteilten und zielgerichteten Angriffen rüsten.

Es gibt eine Unmenge Sicherheitsrisiken und Überlegungen, mit denen sich die Administratoren virtueller Infrastrukturen auseinandersetzen müssen und auf die sie sich vorbereiten sollten. Viele dieser Aspekte können im Rahmen dieser kurzen Abhandlung nicht einmal angesprochen werden. Darüber hin-

aus gibt es noch zahlreiche Fragen, denen man sich stellen muss, bevor man auf eine vollständig virtualisierte Umgebung umstellt, wie zum Beispiel:

- Wie lassen sich die vorhandenen Analyse-, Debugging- und Foren-

tualisiert ist? Ebnet die Hardware-Virtualisierung den Weg zu einem wirklich sicheren VMM?

- Zum Thema Virtualisierung und gemeinsam genutzte Massenspeicher: Was passiert, wenn man die Virtualisierung bis zur iSCSI-

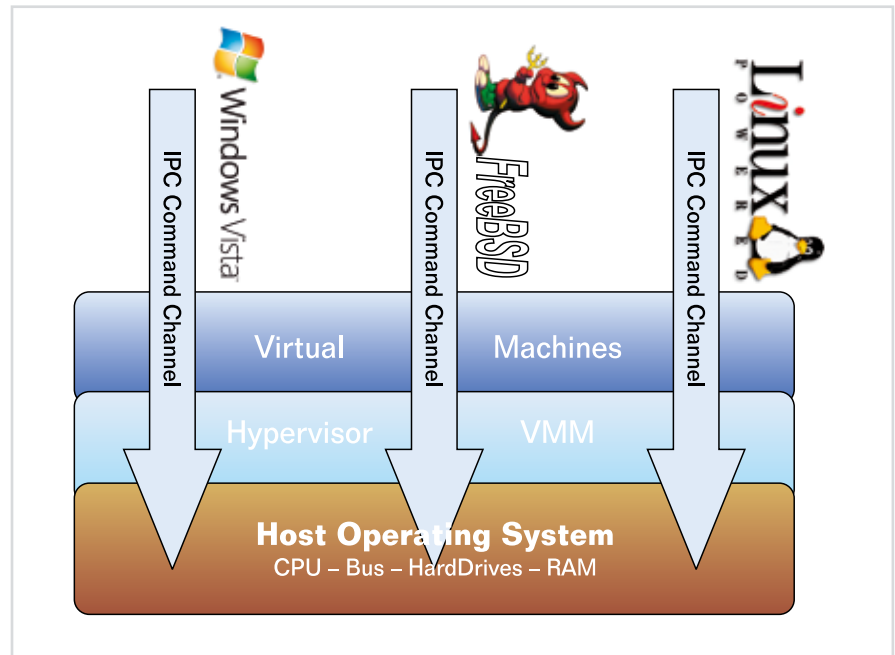


Bild 3: Virtual machine Hypervisor Architectur.

sik-Tools an die Virtualisierung anpassen?

- Welche neuen Tools werden die Sicherheits-Administratoren zwischen all den Virtualisierungs-Plattformen beherrschen müssen?
- Wie wirkt sich das Patch-Management auf die virtuelle Infrastruktur für Guests, Hosts und Management-Subsysteme aus?
- Werden neue Sicherheits-Tools wie etwa eine in die CPUs eingebaute Hardware-Virtualisierung dabei helfen, den Hypervisor zu schützen, indem er aus der Software herausverlagert wird?
- In welcher Weise können bekannte Best Practices zum Thema Sicherheit (etwa No-Exec Stacks) helfen, wenn ein System vollständig vir-

Transportschicht fortsetzt? Öffnet man damit ein Einfallstor, über das die eingebaute SAN-Sicherheit umgangen werden kann?

All diese Fragen gilt es zu beachten, bevor ein Unternehmen komplett auf die Virtualisierung setzt. Vor allem ist bereits heute zu bedenken, wohin einen die Virtualisierung-Sicherheit morgen führen wird. Wir sind uns alle einig, dass die Virtualisierung etwas Gutes ist und sich durchsetzen wird. Die Sicherheits-Administratoren müssen jedoch gewährleisten, dass sie bezüglich der Risiken auf Ballhöhe bleiben und Überlegungen im Zusammenhang mit virtualisierten Bedrohungs-Vektoren anstellen, bevor die Angreifer ihnen zuvorkommen und den entsprechenden Code schreiben.

Ralf Sydekum

eJournal
1/1 Seite