Virtualisierung ganzer Netze

Überprüfung der eigenen Infrastruktur

Kai-Oliver Detken

Die Virtualisierung schreitet immer weiter voran und macht auch vor den Netzen nicht halt. War es früher normal, verschiedene Betriebssysteme zu virtualisieren, um unterschiedliche OS-Plattformen unterstützen zu können, kann heute auch eine gesamte IT-Infrastruktur simuliert werden. Das Forschungsprojekt VISA will dies nutzen, um den Unternehmen Simulationsmöglichkeiten an die Hand zu geben, damit sie im Vorfeld ihre Infrastruktur überprüfen oder erweitern können, um Design- und Konfigurationsfehler auszuschließen. Dabei will man neben einer höheren Verfügbarkeit auch einen höheren IT-Sicherheitsgrad erreichen.

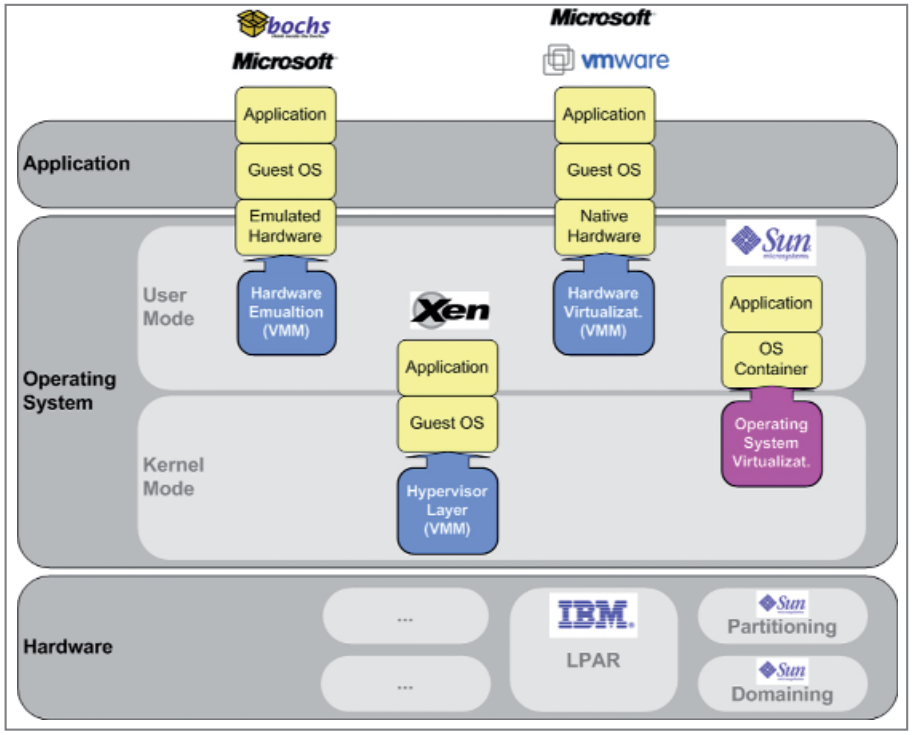

Bild 1: Virtualisierungstechniken zur Schaffung virtueller Betriebsumgebungen [2]

Komplexe IT-Infrastrukturen vereinfachen

IT-Infrastrukturen sind mittlerweile auch schon in kleinen und mittelgroßen Unternehmen (KMU) sehr komplex. Neben den verschiedenen Typen von Rechnern (Desktop-Computer, Laptops, Server u.a.), Peripherie (z.B. Multifunktionsdrucker) und funktionalen Netzkomponenten (Router, Switches u.a.) wächst die Komplexität durch unterschiedliche Sicherheitskomponenten (Firewall, Intrusion Detection System, Proxy u.a.). Die Auswirkungen von Änderungen an diesen IT-Infrastrukturen sind oftmals erst im Echtbetrieb zu erkennen und die Integration neuer Sicherheitskomponenten erfordert dementsprechend die Integration neuer Hardware und den Umbau der Netztopologie. Dies wird meistens ohne genaue Kenntnis über die Auswirkung in KMU umgesetzt.

Darüber hinaus ist das Absichern von Einzelkomponenten – insbesondere im Verbund mit anderen Komponenten, für die Integration in der Unternehmenstopologie nach BSI IT-Grundschutz sowie ISO 27001 – nach denen ein ISMS (Informations-Sicherheits-Management-System) aufgebaut und betrieben werden kann, kein einfaches Unterfangen. Dies ist auch für Conformance und Compliance für Regulierungsanforderungen wie z.B. Basel II essentiell. Da immer mehr KMU ein profundes IT-Risikomanagement vorweisen müssen, muss nachweisbar sein, dass die IT-Infrastruktur über ausreichende Schutzmechanismen (Virenabwehr, Zugangssteuerung, Schutz von Daten über Zugriffsrechte, IT-Notfallplanung und -regelung) verfügt.

Vor diesem Hintergrund muss für KMU der Umgang mit IT-Infrastrukturen vereinfacht werden, da diese wenig Personalressourcen und Know-

Prof. Dr.-Ing. Kai-Oliver Detken ist Dozent an der Hochschule Bremen im Fachbereich Informatik sowie Geschäftsführer der Decoit GmbH

how für das operative IT-Management vorhalten können. Das ist durch den Einsatz von Virtualisierung und Simulation von IT-Infrastrukturen einerseits und durch die Realisierung KMU-gerechter Darstellung und Bedienbarkeit der resultierenden Sicherheitsfunktionalität anderseits zu gewährleisten.

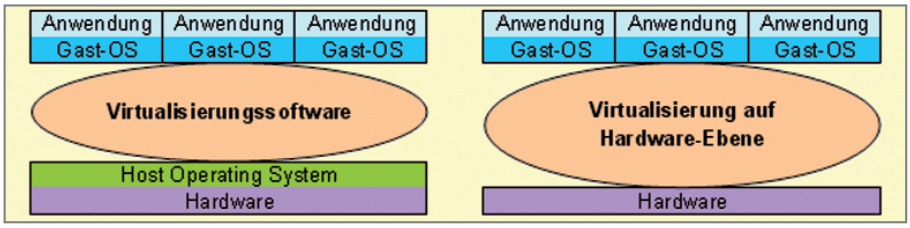

Bild 2: Vergleich unterschiedlicher Virtualisierungstechniken [2]

Virtualisierungsmöglichkeiten

Die Virtualisierung von Betriebssystemen hat sich heute etabliert und hat den wesentlichen Vorteil, dass prototypische Implementierungen und Tests von Soft- und Hardware viel schneller und kostengünstiger realisiert werden können. Hinzu kommt, dass auch die Kontrolle und Überwachung einzelner Komponenten wie auch eine dynamische Veränderung der Netztopologie im laufenden Betrieb möglich ist. Darüber hinaus ermöglichen Virtualisierungstools wie VMware, Xen Source und KVM (Kernel-based Virtual Machine) die Simulation/Emulation von IT-Komponenten und sogar komplexen IT-Infrastrukturen (Subnetze, Router, Switches, Firewalls, DMZ u.a.). Mittlerweile ist sogar die Emulation von Kabeln – beispielsweise mit VDE (Virtual Distributed Ethernet) – möglich. Diese Techniken und Lösungen lassen sich im Prinzip zur Konzeption und Provisionierung von IT-Sicherheitsarchitekturen und Infrastrukturen nutzen, denn einzelne virtualisierte Sicherheitskomponenten wie Firewalls, Authentisierungsserver, IDS-System u.a. könnten mit KVM und VDE flexibel und modular zu komplexen und autarken Systemen zusammengefasst werden. Damit können nicht nur einzelne virtuelle Einheiten, sondern letztendlich auch die gesamte IT-Infrastruktur eines Unternehmens abgebildet werden.

Unterschieden werden muss zwischen den folgenden Virtualisierungstechniken bzw. -definitionen:

- Servervirtualisierung;
- Desktopvirtualisierung;
- Vollvirtualisierung;
- Hardware-basierte Virtualisierung;
- Hardware-/System-basierte Emulation.

Bei der Servervirtualisierung werden mehrere Instanzen eines oder verschiedener Betriebssysteme auf einem einzigen Rechner gleichzeitig nebeneinander betrieben. Die einzelnen Instanzen werden als virtuelle Maschinen (VM) oder Gast bezeichnet und verhalten sich in der virtuellen Umgebung identisch zum herkömmlichen Betrieb direkt auf der Hardware. Zwei weitere Bereiche der Systemvirtualisierung sind Applikationsvirtualisierung und Desktopvirtualisierung.

Bei der Desktopvirtualisierung geht es um die Virtualisierung von Arbeitsplatzrechnern. Anwendern soll ihre individuelle Systemumgebung in Form von virtuellen Maschinen zur Verfügung gestellt werden. Es werden hierbei zwei Ausprägungen unterschieden: Client-basierte Desktopvirtualisierung, bei dem auf dem Arbeitsplatzrechner parallel weitere unabhängige Betriebssysteme in Form von VM betrieben werden, sowie serverbasierte Desktopvirtualisierung (Virtual Desktop Infrastructure – VDI), bei der das virtuelle Desktopbetriebssystem zentral im Rechenzentrum bereitgestellt wird. Gerade die letztere Virtualisierungsvariante nimmt gegenwärtig immer mehr Fahrt auf, da hiermit sowohl der Parallelbetrieb von unterschiedlichen (auch älteren, aktuelle Hardware nicht unterstützenden) Betriebssystem-Varianten als auch die Mitnahme des eigenen Desktops auf beliebige Rechner möglich wird. Hinzu kommt, dass die Treiberprobleme sich verringern und man eine bessere zentrale Administration schaffen kann.

Bei dem Verfahren der Vollvirtualisierung, welches man auch als „echte" Virtualisierung bezeichnen kann, wird die Hardware des Hostsystems in mehrere virtuelle Maschinen aufgeteilt. Die Gastsysteme innerhalb der virtuellen Maschinen entsprechen weitestgehend der Architektur des Hostsystems und laufen getrennt voneinander, jeweils mit ihrem eigenen Betriebssystem. Die Vollvirtualisierung lässt sich noch in die Verfahren Para-Virtualisierung und Hardware-basierte Vollvirtualisierung unterteilen. Beispiele für diese Art der Virtualisierung sind VMware Server, VMware ESX/ESXi, Microsoft Virtual Server und Microsoft Hyper-V [1].

Das Verfahren der Hardware-basierten Virtualisierung kombiniert Techniken der Voll- und Para-Virtualisierung, wobei die Virtualisierungsfunktionalität in die Prozessorhardware integriert wird. Man bezeichnet es auch als Hardware Virtual Machine (HVM) und native Virtualisierung. Ziel der Hardware-basierten Virtualisierung ist es, die Vorteile der Vollvirtualisierung zu erreichen und gleichzeitig deren Performance-Nachteile zu eliminieren.

Durch die immer stärkere Verbreitung der x86-Architektur in den vergangenen zwanzig Jahren, traten die Schwächen in Bezug auf Virtualisierbarkeit in den Vordergrund. Der allgemeine Trend zur Virtualisierung brachte die Hardwarehersteller dazu, ihre neuen x86-Prozessoren um Virtualisierungsfunktionen zu erweitern. Die Grundfunktionalität dieser Erweiterungen besteht darin, zu erkennen, wann kritische Operationen von virtuellen Maschinen ausgeführt werden und diese gesondert zu behandeln. Diese modernen Prozessoren unterstützen die Interaktion zwischen den virtuellen Maschinen und den Hypervisoren. Die ersten Prozessoren mit Virtualisierungserweiterungen kamen im Jahr 2005 auf den Markt (Intel VT, AMD-V). Die Implementierungsansätze sind prinzipiell ähnlich, doch sie sind nicht zueinander kompatibel. Virtualisierungssoftware muss eine getrennte Unterstützung sowohl für Intel VT als auch für AMD-V anbieten.

Das Verfahren der Hardware-basierten Virtualisierung unterscheidet sich

prinzipiell nicht von dem der Vollvirtualisierung. Ein entscheidender Unterschied liegt darin, dass das Privilegiensystem der neuen Prozessoren erweitert wurde, die Gastsysteme müssen nicht mehr in nicht-privilegierten Ringen betrieben werden, sondern deren Kernel kann direkt in Ring 0 gestartet werden. Die Gastsysteme können somit unangepasst bleiben, da sie sich in ihrer gewohnten Umgebung befinden. Virtualisierungslösungen, die das Verfahren der Hardware-basierten Virtualisierung einsetzen, sind beispielsweise Xen oder KVM.
Der Hypervisor ist nach wie vor für die Verwaltung und Kontrolle der virtuellen Maschinen zuständig, verhält sich aber im Gegensatz zur Vollvirtualisierung rein passiv. Durch die neuen zur Verfügung stehenden Befehlssätze können privilegierte Instruktionen regulär und somit sicher ablaufen. Ein Kontextwechsel zum Hypervisor ist nicht jedes Mal notwendig. Der Virtualisierungsprozess wird nicht gestört und der Virtualisierungs-Overhead wird sehr stark reduziert. Bei dem Verfahren der hardware-basierten Virtualisierung laufen virtuelle Maschinen auf Grund der erwähnten Vorteile des Verfahrens äußerst leistungsstark [3].
Unter einem Emulator versteht man eine Software, die ein komplettes Computersystem nachahmt, bzw. simuliert. Bei der Hardware-Emulation wird die komplette Hardware eines Computers simuliert. Es wird u.a. der komplette Befehlssatz des Gastprozessors nachgebildet. Das Verfahren ermöglicht es, beliebige Betriebssysteme, die von der Architektur des Hostsystems abweichen können, zu betreiben. Das emulierte System läuft in einer vom Host vollkommen losgelösten Umgebung. Emulatoren kommen meist dann zum Einsatz, wenn auf einer Plattform gearbeitet werden muss, die aus unterschiedlichen Gründen nicht verfügbar ist. Ihr Einsatzzweck stellt die Kompatibilitätssicherung dar. Man möchte Anwendungen ausführen, die für eine alte Architektur geschrieben wurden, welche nicht mehr hergestellt wird. Weiterhin kommen Emulatoren auch bei der Prototypentwicklung zum Einsatz. Google veröffentlichte beispielsweise schon vor der Markeinführung ihrer neuen Handy-Generation einen Emulator für das Android-Betriebssystem. Auf Grundlage dieses Emulators wurde bereits eine Vielzahl von Applikationen entwickelt, obwohl die Hardware noch nicht verfügbar war. Ein bekannter Vertreter von Hardware- bzw. System-Emulatoren im Bereich Cisco Router und Switches ist Dynamips [4].

Das VISA-Projekt

Durch die starke Heterogenität von IT-Infrastrukturen, der relativ begrenzten Ressourcen sowie des relativ geringen Know-hows muss in Zukunft die Zielgruppe KMU bessere und geeignete Methoden zur Konfektionierung ihrer IT-Infrastruktur bekommen. Das ist gerade auf die IT-Sicherheit bezogen wichtig. Der IT-Sicherheitsmarkt adressiert aber bislang zu wenig diese Zielgruppe, so dass meistens keine bedarfsgerechten und dem Budget angepassten Lösungen vorhanden sind. Um eine höhere Autonomie in der Konfiguration sowie im Betrieb ihrer IT-Infrastruktur zu erhalten, sind modulare und erprobte Lösungen und Systeme essentiell. Die höhere Flexibilität kann und wird mittlerweile durch Virtualisierung von Rechnern und Diensten erreicht. Jedoch existieren keine Lösungen, die auch Netze und Infrastrukturen für Unternehmen virtualisiert abbilden. Auch existieren nur Virtual Appliances, die nur punktuell bestimmte Anwendungen oder Dienste bereitstellen wie z.B. Mail-Security-Dienste, Firewall-Dienste u.a. Eine Kombination von verschiedenen Sicherheitsfunktionen und Diensten wird nicht angeboten. Das möchte das VISA-Projekt durch die Entwicklung von Virtual Security Appliances (VSA) ändern.
Nicht nur vor dem Hintergrund der Flexibilität, sondern auch aus Kostengründen (Investition in Hard- und Software) sind VSA auf Basis von Open-Source-Bausteinen (sowohl die Anwendungen als auch die Betriebssysteme) von Bedeutung. Außerdem würde der Einsatz in Unternehmen kein größeres Know-how erfordern, da erprobte State-of-the-Art-Technologien als integrierbare Lösung in die IT von KMU eingebunden werden können. Ein weiterer essentieller Aspekt ist die bessere Überprüfbarkeit im Sinne von Compliance. Der Aufwand zur Überprüfung von Sicherheitskomponenten bzw. der gesamten IT-Sicherheitsinfrastruktur wird erheblich reduziert, da Security Assessment und Compliance-Tests für Virtual Security Appliances (VSA) bereits vorliegen können. Durch die steigende Komplexität wird die Überprüfung der Konformität vereinfacht.
Vor diesem Hintergrund nahm das BMBF-geförderte Forschungsprojekt VISA (**www.visa-project.de**) am 1. August 2011 seine Arbeit auf. VISA wird die Möglichkeiten zur Modellierung von IT-Infrastrukturen von KMU für Virtualisierung erarbeiten und auf Basis dessen bedarfsgerechte Virtual Security Appliances (VSA) konzeptionieren, die als integraler Bestandteil von KMU eingesetzt werden sollen. Dies soll durch Simulation und Emulation von komplexen Netzwerk- und Dienste-Topologien erreicht werden. Um einen bedarfsgerechten Einsatz für KMU zu ermöglichen, soll eine grafische Oberfläche zur Unterstützung der Modellierung sowie zur Visualisierung und Bedienung der Virtuellen Security Appliances (VSA) entwickelt werden.
Es ist daher das Ziel des Projektes VISA, durch Nutzung von Virtualisierungstechnologien das Management von IT-Infrastrukturen, insbesondere der Sicherheitskomponenten, zu erleichtern und zu unterstützen. Diese Unterstützung basiert auf zwei Kernmerkmalen:

- Simulation und Evaluierung der gesamten IT-Infrastruktur in virtuellen Umgebungen;
- Realisierung von Sicherheitsanwendungen als virtuelle Komponenten, sog. Virtual Security Appliances (VSA).

Durch das VISA-Rahmenwerk wird der passgenaue und vereinfachte Einsatz von Sicherheitsanwendungen auf Basis von Virtual Security Appliances (VSA) ermöglicht. Durch die umfassende Emulation der IT-Infrastrukturen können die betriebsrelevanten Para-

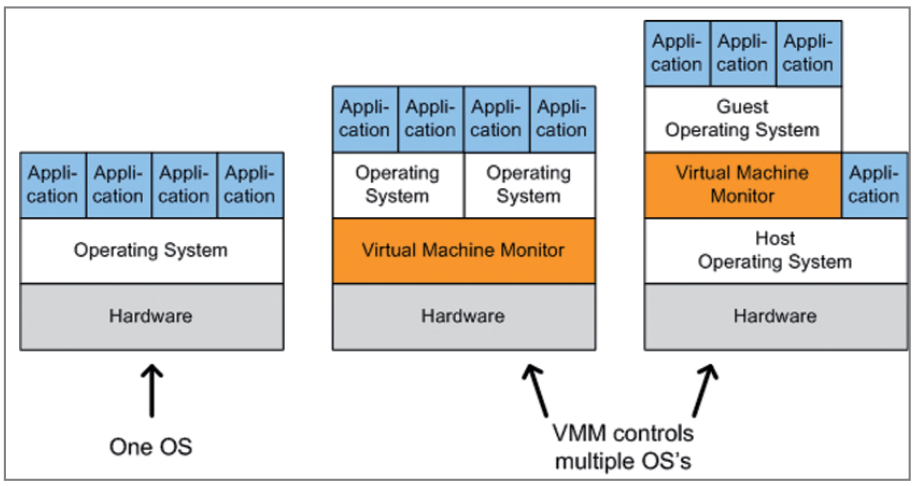

Bild 3: Ansatz der Systemvirtualisierung zur Schaffung virtueller Betriebsumgebungen [2]

meter und die Integrationspunkte der VSA bereits in der virtuellen Umgebung identifiziert und der Einsatz erprobt werden. Erfolgreich getestete VSA kann man dann direkt, ohne Änderung, in der existierenden Infrastruktur, zum Einsatz bringen. Durch die Kombination der Modellierung und formalen Beschreibung von Infrastrukturen auf der einen Seite sowie der Evaluation der Infrastrukturen in virtuellen Umgebungen anhand verschiedener, definierter Kriterien auf der anderen Seite wird es KMU ermöglicht, Kosten und Eigenschaften der jeweiligen IT-Investition besser abzuschätzen und Sicherheitsrisiken geringer zu halten.

VISA erstellt ein Rahmenwerk, das das Erproben von VSA in nachgebildeten, praxisorientierten Szenarien erlaubt. Hierfür sieht das Konsortium folgende technischen Herausforderungen bzw. Ziele:

- Entwicklung und Packetierung verschiedener VSA-Module, die unterschiedliche Bereiche der IT-Sicherheit abdecken;
- eine automatisierte und dynamische Umgebung schaffen, die eine experimentelle Erprobung verschiedener Netztopologien und den Einsatz von VSA erlaubt;
- Modelle entwickeln, die die Simulation der Netztopologien steuern;
- Jede VSA muss am Ende als virtuelles Image vorliegen und durch das Deployment-System entsprechend dem zugrunde liegenden Modell konfiguriert werden können;
- es wird ein Modell bzw. Ausdrucksystem benötigt, um das Deployment zu steuern.
- es wird eine Bibliothek von virtuellen Images benötigt, um die möglichen Wirkszenarien zu bauen.

Fazit

Die Virtualisierungstechniken schreiten immer weiter voran und ermöglichen heute nicht nur mehr den reinen Parallelbetrieb unterschiedlicher Betriebssysteme auf einer Hardware. Längst hat die Virtualisierung auch die Produktivumgebung erreicht, da die Server-Hardware-Systeme immer leistungsstärker und ausfallsicherer werden. Nachdem die Serverdomäne erobert wurde, fängt man im nächsten Schritt an, die Desktop-Systeme zu erschließen. Damit kann letztendlich die gesamte IT-Infrastruktur nachgebildet werden, also auch das Netz zwischen Client und Server. Zukünftig wird vielleicht noch nicht mal mehr die IT-Administration wissen, wo sich das jeweilige Rechnersystem eigentlich befindet. Die Übersichtlichkeit geht durch diverse Virtualisierungsmöglichkeiten verloren. Dadurch können Fehler und Sicherheitslücken entstehen. Dies ist gerade bei KMU problematisch, da hier oftmals das entsprechende Wissen fehlt, um fehlerfrei komplexe IT-Infrastrukturen aufsetzen zu können.

Das Projekt VISA hat sich daher einerseits zum Ziel gesetzt die Komplexität virtueller Umgebungen zu verringern, indem die Handhabung solcher Lösungen verbessert werden soll. Andererseits will man aber auch eine Möglichkeit schaffen, bestehende IT-Infrastrukturen vorab simulieren zu können, um Fehlkonfigurationen zu vermeiden. Das ist nicht nur aus Sicherheitsgründen wichtig, sondern auch aus Sicht der Verfügbarkeit relevant. Nach der erfolgreichen Simulation können zukünftig zwei Möglichkeiten gewählt werden:

- Übernahme der Konfiguration in die bestehende IT-Infrastruktur;
- Überführung der Simulation in das Produktivnetz.

Beide Szenarien sollen im VISA-Projekt untersucht und bewertet werden. Aktuell werden gerade die entsprechenden Szenarien definiert, die für die Entwicklung im Projekt relevant sind. Wenn alle Ziele des Projektes umgesetzt werden können, wird es in Zukunft in jedem Fall einfacher werden Server, Clients und Netze zu virtualisieren und sicher in die Unternehmensstruktur einzubetten.

Literatur

[1] Thorns, F.: Das Virtualisierungs-Buch. 2008. Ausgabe 2. C&L Computer und Literaturverlag

[2] Hirschbach, D.: Vergleich von Virtualisierungstechnologien. Diplomarbeit an der Universität Trier. Trier 2006

[3] Fischer, M.: Xen – Das umfassende Handbuch. 2009. Galileo Press

[4] Davoli, R.: VDE: Virtual Distributed Ethernet. Technical Report UBLCS-2004-12. Department of Computer Science. University of Bologna. June 2004