

Virtualisierung und Cloud Computing: Konzepte, Technologiestudie, Marktübersicht

Christoph Meinel, Christian Willems,
Sebastian Roschke, Maxim Schnjakin

Technische Berichte Nr. 44

des Hasso-Plattner-Instituts für
Softwaresystemtechnik
an der Universität Potsdam



Technische Berichte des Hasso-Plattner-Instituts für
Softwaresystemtechnik an der Universität Potsdam

Christoph Meinel | Christian Willems
Sebastian Roschke | Maxim Schnjakin

Virtualisierung und Cloud Computing

Konzepte, Technologiestudie, Marktübersicht

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Universitätsverlag Potsdam 2011

<http://info.ub.uni-potsdam.de/verlag.htm>

Am Neuen Palais 10, 14469 Potsdam
Tel.: +49 (0)331 977 4623 / Fax: 3474
E-Mail: verlag@uni-potsdam.de

Die Schriftenreihe **Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam** wird herausgegeben von den Professoren des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam.

ISSN (print) 1613-5652
ISSN (online) 2191-1665

Das Manuskript ist urheberrechtlich geschützt.

Online veröffentlicht auf dem Publikationsserver der Universität Potsdam
URL <http://pub.ub.uni-potsdam.de/volltexte/2011/4970/>
URN <urn:nbn:de:kobv:517-opus-49708>
<http://nbn-resolving.org/urn:nbn:de:kobv:517-opus-49708>

Zugleich gedruckt erschienen im Universitätsverlag Potsdam:
ISBN 978-3-86956-113-4

Inhaltsverzeichnis

Abbildungsverzeichnis	5
1 Einführung	8
2 Technologievarianten	10
2.1 Hardwarevirtualisierung	13
2.1.1 Technologievarianten	13
2.1.2 Servervirtualisierung	18
2.1.3 Clientvirtualisierung	20
2.2 Präsentationsvirtualisierung	22
2.3 Applikationsvirtualisierung	24
2.4 Management virtualisierter Umgebungen	26
3 Cloud Computing	28
3.1 Architekturvarianten des Cloud Computing	30
3.1.1 IaaS - Infrastructure-as-a-Service	30
3.1.2 PaaS - Platform-as-a-Service	32
3.1.3 SaaS - Software-as-a-Services	34
3.2 Aspekte des Cloud Computing	35
3.3 Bedenken	39
3.4 Zusammenfassung – Cloud Computing	44
4 Marktübersicht: Virtualisierungstechnologie	45
4.1 Citrix	46
4.2 Microsoft	49
4.3 VMware	53
4.4 Weitere Anbieter	58
4.5 Open Source Projekte	59
4.5.1 Open Source Cloud Computing Plattformen	59

4.6 Zusammenfassung – Marktübersicht	63
5 Zusammenfassung und Fazit	64
Literaturverzeichnis	67

Abbildungsverzeichnis

2.1	System ohne Virtualisierung	10
2.2	Hardwarevirtualisierung	10
2.3	Präsentationsvirtualisierung	11
2.4	Applikationsvirtualisierung	11
2.5	Unterschiedliche Positionen für den Virtual Machine Monitor bzw. Hypervisor	14
2.6	Speicherschutz für x86-Prozessoren (Ringmodell)	15
2.7	Hypervisor bei Paravirtualisierung	16
2.8	Betriebssystemvirtualisierung	17
2.9	Hardware-gestützte Desktopvirtualisierung	21
2.10	Infrastruktur mit Applikationsvirtualisierung in der Microsoft-Welt	24
2.11	VMware Server Console (Beispiel für lokales Virtual Machine Management)	26
3.1	Nutzer und Anbieter des Cloud Computing	29
3.2	Cloud Computing Architektur	31
3.3	„Überversorgung“ mit IT-Kapazitäten	37
3.4	„Unterversorgung“ mit IT-Kapazitäten	38
3.5	Wirtschaftlichkeit der Nutzung von Cloud-Ressourcen	39
4.1	Virtual Desktop Infrastructure mit XenDesktop	47
4.2	Enterprise Desktop Virtualization (MED-V)	51
4.3	Komponenten der VMware vSphere Infrastruktur	55
4.4	Komplexe Virtual Desktop Infrastructure mit VMware	57
4.5	Cloud Computing mit Eucalyptus	60

Virtualisierung und Cloud Computing gehören derzeit zu den wichtigsten Schlagworten für Betreiber von IT Infrastrukturen. Es gibt eine Vielzahl unterschiedlicher Technologien, Produkte und Geschäftsmodelle für vollkommen verschiedene Anwendungsszenarien. Die vorliegende Studie gibt zunächst einen detaillierten Überblick über aktuelle Entwicklungen in Konzepten und Technologien der Virtualisierungstechnologie – von klassischer *Servervirtualisierung* über Infrastrukturen für *virtuelle Arbeitsplätze* bis zur *Anwendungsvirtualisierung* und macht den Versuch einer Klassifikation der Virtualisierungsvarianten.

Bei der Betrachtung des *Cloud Computing*-Konzepts werden deren Grundzüge sowie verschiedene Architekturvarianten und Anwendungsfälle eingeführt. Die ausführliche Untersuchung von Vorteilen des Cloud Computing sowie möglicher Bedenken, die bei der Nutzung von Cloud-Ressourcen im Unternehmen beachtet werden müssen, zeigt, dass Cloud Computing zwar große Chancen bietet, aber nicht für jede Anwendung und nicht für jeden rechtlichen und wirtschaftlichen Rahmen in Frage kommt..

Die anschließende Marktübersicht für Virtualisierungstechnologie zeigt, dass die großen Hersteller – *Citrix*, *Microsoft* und *VMware* – jeweils Produkte für fast alle Virtualisierungsvarianten anbieten und hebt entscheidende Unterschiede bzw. die Stärken der jeweiligen Anbieter heraus. So ist beispielsweise die Lösung von Citrix für *Virtual Desktop Infrastructures* sehr ausgereift, während Microsoft hier nur auf Standardtechnologie zurückgreifen kann. VMware hat als Marktführer die größte Verbreitung in Rechenzentren gefunden und bietet als einziger Hersteller echte *Fehlertoleranz*. Microsoft hingegen punktet mit der nahtlosen Integration ihrer Virtualisierungsprodukte in bestehende Windows-Infrastrukturen.

Im Bereich der Cloud Computing-Systeme zeigen sich einige quelloffene Softwareprojekte, die durchaus für den produktiven Betrieb von sogenannten privaten Clouds geeignet sind.

1 Einführung

Virtualisierung ist in der Informatik ein altbekanntes und verbreitetes Konzept. Bereits in den 1960er Jahren führte IBM das Prinzip der Servervirtualisierung für Großrechner ein: Mehrbenutzerbetrieb auf einem Mainframe wurde ermöglicht, indem mehrere Instanzen des Einzelbenutzerbetriebssystems in *virtuellen Maschinen* (siehe 2.1) gestartet wurden. Damals war das Ziel eine bessere Auslastung der vorhandenen (sehr knappen) Ressourcen, Mainframe-Computer waren selten und sehr teuer.

Heute ist die Verfügbarkeit von Computern mit ausreichend Rechenleistung nur noch im Ausnahmefall ein limitierender Faktor, tatsächlich haben aktuelle Office PCs deutlich mehr Leistung als die damaligen Großrechner. Dennoch ist das Konzept der Virtualisierung und dessen Anwendungsmöglichkeiten zu einem zentralen Innovationsmotor in vielen Bereichen der IT Industrie geworden. Neben der klassischen Hardwarevirtualisierung, die vor allem im Serverbereich Einsatz findet, sind auch Präsentationsvirtualisierung (auch bekannt als Terminal Computing), Applikationsvirtualisierung und das Management virtualisierter IT Infrastruktur wichtige Technologiebereiche geworden. Abschnitt 2 der vorliegenden Studie stellt die unterschiedlichen Technologievarianten aus dem Bereich der Virtualisierung vor und grenzt diese voneinander ab.

Das Potential des Einsatzes von Virtualisierungstechnologie hängt stark vom jeweiligen Szenario und der Technologievariante ab. Ein klassisches Einsatzfeld ist bspw. die Virtualisierung von Servern zur Konsolidierung von physikalischer Hardware, wenn die Dienste, die dort betrieben werden die Rechenleistung nicht effizient genug ausnutzen. Dann können in der Regel auf einem einzigen Computer mehrere Dienste innerhalb virtueller Maschinen laufen, ohne dass sich die Performance oder Wartbarkeit der einzelnen Dienste signifikant verschlechtert. Das gilt aber nicht für jeden Server. So werden z.B. Datenbankserver eher aus Gründen der Erhöhung der Zuverlässigkeit virtualisiert, nicht etwa aus Performancegründen. Möglichkeiten und Grenzen im praktischen Einsatz werden ebenfalls im folgenden Abschnitt dargelegt.

Weiterhin stellt die Studie in Abschnitt 4 Produkte und Hersteller-spezifische Technologien der Marktführer im Virtualisierungsbereich vor – insbesondere Citrix, Microsoft und VMware, ordnet diese den vorher eingeführten Virtualisierungsvarianten zu und zeigt

eventuelle Produkt-spezifische Einschränkungen oder Alleinstellungsmerkmale auf.

Cloud Computing – behandelt Kapitel 3 – beruht in der Praxis für gewöhnlich nicht nur auf dem massiven Einsatz verschiedener Virtualisierungstechnologien, sondern ist auch eine Anwendung des Abstraktionskonzepts: hierbei wird – je nach Architekturvariante – Software, Bereitstellungsplattformen oder ganze Hardwareinfrastrukturen virtuell zur Verfügung gestellt. Der Abschnitt der Studie stellt die allgemeinen Konzepte und verschiedenen Cloud Computing-Varianten (Software-as-a-Service, Platform-as-a-Service sowie Infrastructure-as-a-Service) vor und geht außerdem auf Vor- und Nachteile, die mit dem Einsatz von Cloud-basierten Infrastrukturkomponenten im eigenen Unternehmen verbunden sind. Zudem werden in Abschnitt 4.5.1 einige Cloud Computing-Projekte aus der Open Source-Welt vorgestellt.

2 Technologievarianten

In der Informatik bzw. Informationstechnologie taucht der Begriff Virtualisierung als Konzept in vielen sehr unterschiedlichen Technologiedomänen auf. Prinzipiell meint man damit immer die Abstraktion einer (physikalischen) Ressource, z.B. Prozessoren, Speicher, Bildschirme, etc. mit einem Stück Software. Demnach ist eine virtuelle Maschine („virtueller Computer“) eine Software, die einen „echten“ Computer nachbildet und für ein Betriebssystem, das in dieser virtuellen Maschine installiert wird, auch so aussieht, wie ein „echter Computer“.

Aktuelle Virtualisierungstechnologie setzt auf sehr unterschiedlichen Schichten heutiger, komplexer Computersysteme an. Dies wird beim Vergleich der Abbildungen in diesem Abschnitt deutlich. Abbildung 2.1 zeigt den Normalfall eines nicht-virtualisierten Systems. Das Betriebssystem verfügt exklusiv über die Hardware, Applikationen benutzen Schnittstellen und Bibliotheken (*Shared Libraries*) des Betriebssystems. Die Benutzerschnittstellen (*User Interface, UI*) sind fest an die Applikationen gebunden und werden auf dem Monitor des physikalischen Rechners angezeigt.

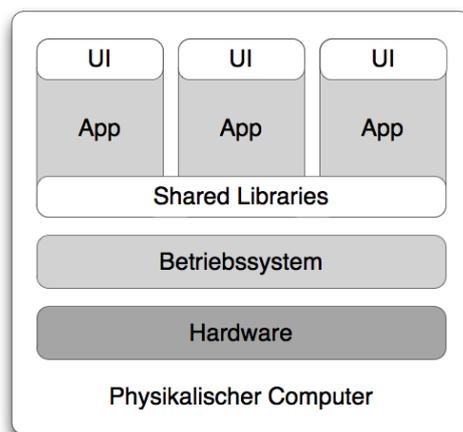


Abbildung 2.1: System ohne Virtualisierung

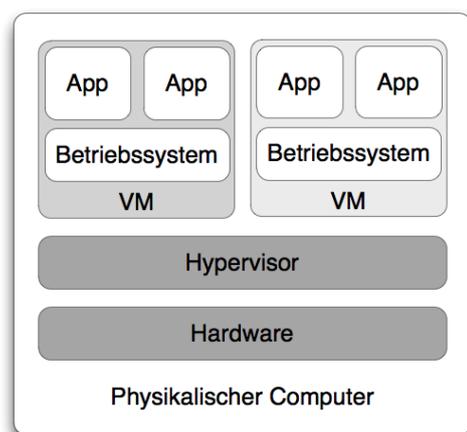


Abbildung 2.2: Hardwarevirtualisierung

Bei der *Hardwarevirtualisierung* (siehe Abschnitt 2.1) wird die Architektur um einen *Hypervisor* oder *Virtual Machine Monitor* erweitert. Dieser besteht aus der Software zur Abstraktion der Hardware – also den eigentlichen virtuellen Maschinen (VM) – und Tools und Programmen zur Verwaltung der VMs, also Anlegen, Starten, Stoppen, oder Zuweisen von (physikalischen) Ressourcen. Bei der Hardwarevirtualisierung unterscheidet man zum einen verschiedene Technologievarianten (z.B. *Hardware-Emulation*, *Paravirtualisierung* oder *Betriebssystemvirtualisierung*) und die Anwendungsbereiche Server- und Desktopvirtualisierung.

Die als *Terminal Computing* bekannte *Präsentationsvirtualisierung* basiert auf der Entkopplung der Darstellung einer Applikation (also des User Interfaces) von der eigentlichen Programmlogik (siehe Abbildung 2.3). Damit ist es bspw. möglich, ein Programm auf einem leistungsfähigen Server auszuführen, während der Benutzer die Applikation auf einem Rechner bedienen kann, der eigentlich zu schwach wäre. Auf diesem muss lediglich eine Software zur Darstellung des entfernten User Interfaces (*Remote Desktop* oder *Terminal Client*) laufen. Ein bekannter Sonderfall der Präsentationsvirtualisierung ist der *Remote Desktop Access* – hierbei wird die komplette Benutzeroberfläche des Betriebssystems entkoppelt und der ganze Rechner „ferngesteuert“.

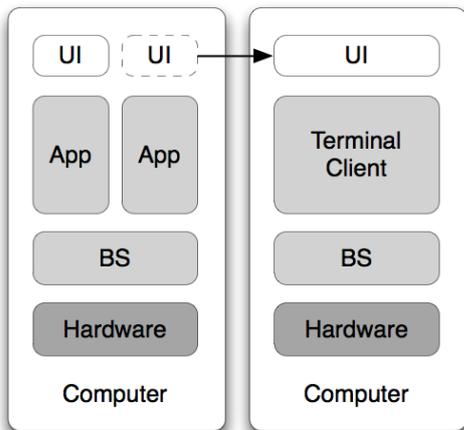


Abbildung 2.3: Präsentationsvirtualisierung

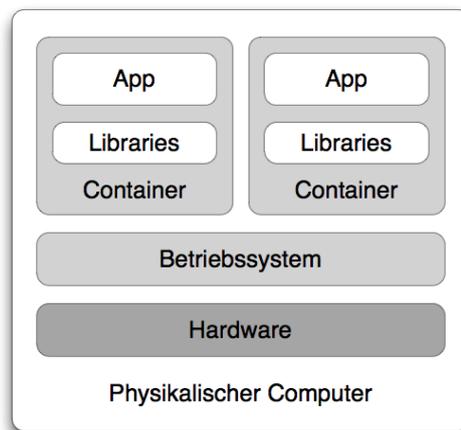


Abbildung 2.4: Applikationsvirtualisierung

Ein verhältnismäßig neues Konzept stellt die *Applikationsvirtualisierung* dar (siehe Abschnitt 2.3). In diesem Fall wird die sogenannte Laufzeitumgebung für einzelne Anwendungen vom tatsächlichen Betriebssystem abstrahiert. Die Applikationen können zum Beispiel nicht mehr nur auf Bibliotheken zugreifen, die das Betriebssystem anbietet. In-

nerhalb eines Virtualisierungscontainers können verschiedenen Anwendungen verschiedene Bibliotheken zugewiesen werden, ohne dass die Anwendungen dafür verändert werden müssten.

Insbesondere die Kombination aus Hardwarevirtualisierung und Präsentationsvirtualisierung hat sich in der Praxis als erfolgreich erwiesen und mündet im Konzept der *Virtual Desktop Infrastructure*.

Der Vollständigkeit halber sollen hier auch kurz noch *Speichervirtualisierung* (logisch abstrakte Sicht auf physikalische Speichermedien, z.B. *Network Storage*, *Storage Area Networks*, etc.) und *Netzwerkvirtualisierung* (im Wesentlichen *Virtual Private Networks*, *VPNs*) genannt, aber nicht weiter berücksichtigt werden.

2.1 Hardwarevirtualisierung

Wenn man in der Informationstechnologie von Virtualisierung im Allgemeinen spricht, meint man tatsächlich meist die Hardwarevirtualisierung. Physikalische Computer werden zu virtuellen Maschinen abstrahiert. Eine virtuelle Maschine (VM) wird aus Software-Komponenten gebildet, die z.B. einen Prozessor nachbilden, Zugriff auf virtuellen Speicher oder eine virtuelle Festplatte ermöglichen, etc. Auf einem „echten“ Rechner können mehrere virtuelle Maschinen gleichzeitig laufen, die sich die physikalischen Ressourcen teilen müssen – ein bewährtes Konzept, das auch alle Multitasking-fähigen Betriebssysteme umsetzen (z.B. Windows, Linux, ...).

Ein Betriebssystem, das in einer VM ausgeführt wird, ist sich dessen in der Regel nicht bewusst und muss auch nicht angepasst werden – es „glaubt“ also, die Hardware des Computers exklusiv nutzen zu können. Ein so genannter *Virtual Machine Monitor* oder *Hypervisor* koordiniert dabei die unterschiedlichen virtuellen Maschinen und regelt deren Zugriff auf die Hardware des Computers.

Diese Virtual Machine Monitors und virtuelle Maschinen an sich werden in verschiedenen Produkten sehr unterschiedlich umgesetzt und haben damit verbundene Vor- und Nachteile.

2.1.1 Technologievarianten

Zwei geeignete Kriterien zur Unterscheidung von Virtualisierungstechnologien in diesem Bereich sind zum Einen die Position des Virtual Machine Monitors bzw. Hypervisors in der Systemarchitektur und zum Anderen der *Grad der Virtualisierung*.

Bei der Position des Virtual Machine Monitors (VMM) unterscheidet man sogenannte *Hosted* Lösungen, bei denen der VMM als Applikation innerhalb eines Betriebssystems laufen muss und *Bare Metal* Lösungen (siehe Abbildung 2.5). Bei der zweiten Variante läuft der Virtual Machine Monitor direkt auf der Hardware (also ohne zusätzliches Betriebssystem) und heißt dann in der Regel *Hypervisor*.

Solche Bare Metal Lösungen haben gegenüber Hosted Lösungen klar den Vorteil, dass sie performanter sind: die Ressourcen, die das Host-Betriebssystem in Variante b) bei jeder Rechenoperation benötigt, fallen bei einer Hypervisor-basierten Lösung weg. Dafür bringen Produkte, die direkt auf der Hardware laufen, häufig starke Anforderungen an eben diese mit: nicht jeder Hersteller wird unterstützt, nicht für jedes Peripheriegerät bringen die Bare Metal Hypervisor passende Treiber mit. Dies gilt insbesondere für besonders aktuelle Hardware, die nicht im professionellen Server-Bereich angesiedelt ist.

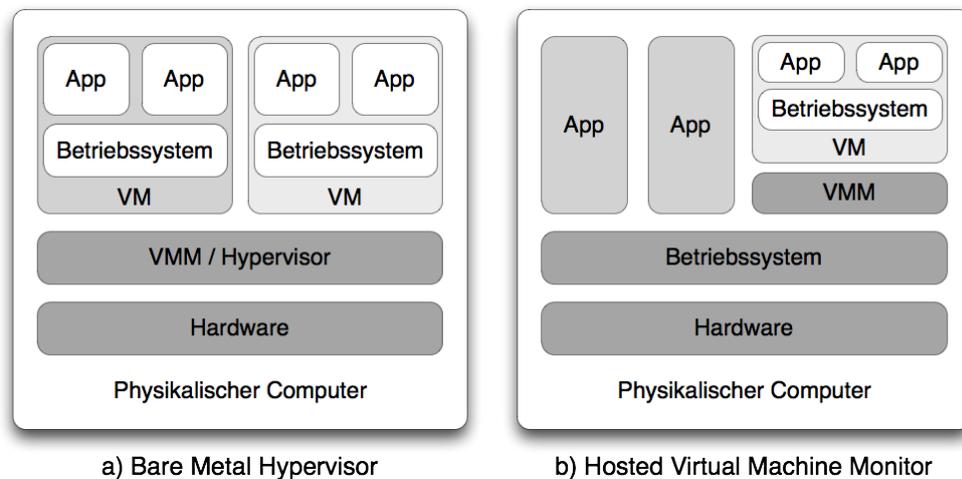


Abbildung 2.5: Unterschiedliche Positionen für den Virtual Machine Monitor bzw. Hypervisor

Die Vorteile der Hosted-Variante liegen vor allem in der größeren Flexibilität: derartige Virtualisierungsprodukte können auf fast jedem Computer installiert werden und unterstützen nahezu jegliche Hardware, die an das Host-System angeschlossen ist. Damit sind Hosted VMMs insbesondere im Bereich der *Desktopvirtualisierung* stark verbreitet.

Um die Unterschiede der verschiedenen Grade der Virtualisierung besser verdeutlichen zu können, muss zunächst die zentrale Schwierigkeit beim Betrieb von Systemen innerhalb virtueller Maschinen kurz erläutert werden – der Schutz bestimmter Speicherbereiche vor dem Zugriff durch Anwendungen. Anschließend werden beispielhaft die unterschiedlichen Konzepte *vollständige Virtualisierung*, *Paravirtualisierung* und *Betriebssystemvirtualisierung* vorgestellt sowie Vor- und Nachteile hervorgehoben.

Aus Gründen der Systemsicherheit und Stabilität dürfen Anwendungen nicht direkt auf bestimmte Bereiche des Hauptspeichers zugreifen, sondern müssen den Umweg über eine Anfrage an den Betriebssystem-Kern (*Kernel*) machen. Das können bspw. Speicherbereiche für den Zugriff auf Ein-/Ausgabegeräte sein, oder Stellen, die das Betriebssystem für den Basisbetrieb benötigt und die nicht überschrieben werden dürfen. Der Kernel darf immer auf den gesamten Speicher zugreifen und entscheidet, ob die jeweilige Anwendung diese Anfrage stellen darf und liefert den Inhalt des angefragten Speicherbereichs aus oder schreibt diesen neu.

In der Intel x86 Architektur wird der Speicher anhand sogenannter Ringe eingeteilt (siehe Abb. 2.6). Prozesse, die in einem bestimmten Ring laufen, können nicht auf Speicherbereiche zugreifen, die in Ringen mit niedrigerer Nummer liegen. In Ring 0 gelten die

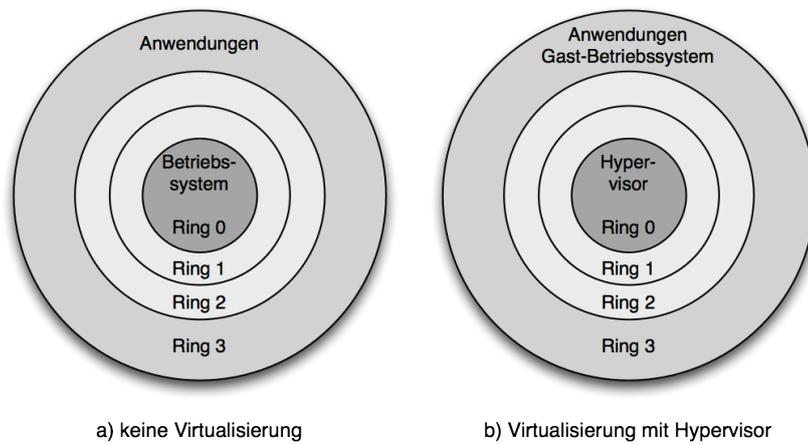


Abbildung 2.6: Speicherschutz für x86-Prozessoren (Ringmodell)

höchsten Privilegien, also Vollzugriff auf den gesamten Speicher. Hier läuft in Systemen ohne Virtualisierung der Betriebssystem-Kern (daher heißt Ring 0 auch *Kernel-Space*). Die Ringe 1 und 2 werden (außer bei OS/2¹ und manchen *Paravirtualisierern*, siehe unten) in der Regel nicht genutzt. In Ring 3 – dem sogenannten *User-Space* – laufen die Anwendungen.

Will eine Anwendung nun direkt auf einen Speicherbereich zugreifen, der für den Kernel reserviert ist, tritt eine Speicherschutzverletzung auf, der Zugriff wird abgelehnt und das Programm stürzt (meistens) ab. In virtualisierten Umgebungen gilt nun per se, dass die virtuellen Maschinen in Ring 3 laufen – unabhängig davon, ob es sich um eine Lösung mit Hypervisor handelt (siehe Abb. 2.6b) oder eine mit Hosted VMM. In jedem Fall sind die virtuellen Maschinen Anwendungen und nicht Teil des Betriebssystems mit Zugriffsrechten auf Ring 0. Dies gilt natürlich auch für die Systeme, die in den virtuellen Maschinen gestartet werden: die Kerne dieser Gast-Betriebssysteme laufen nicht in Ring 0, sondern in Ring 3. Bei einem direkten Zugriff auf privilegierte Speicherstellen oder CPU-Befehle wird wieder eine Schutzverletzung ausgelöst, was zum Absturz des gesamten Systems in der VM führt.

In der Behandlung dieser direkten Systemaufrufe liegt der Unterschied der einzelnen Virtualisierungsvarianten. In der flexibelsten Variante, der *vollständigen Virtualisierung* bzw. *vollständigen Emulation* fängt der Hypervisor alle kritischen Systemaufrufe aus einer VM ab, merkt sich die Quelle des Aufrufs, passt den Befehl so an, dass der Hyper-

¹Historisches graphisches Betriebssystem von IBM, siehe z.B. <http://de.wikipedia.org/wiki/OS/2>

visor selbst die entsprechende Speicheroperation ausführt und besorgt nach dem Aufruf eine entsprechende Rückübersetzung und Rückgabe an die aufrufende virtuelle Maschine. Dieses Vorgehen heißt *binary translation* und muss sehr häufig durchgeführt werden, da solche Systemaufrufe aus Anwendungen heraus keine Seltenheit sind und für virtuelle Maschinen ja auch die Aufrufe des Gast-Betriebssystems übersetzt werden müssen. Offensichtlich bedeutet die *binary translation* also einen Overhead, der signifikante Leistungseinbußen zur Folge hat. Implementierungen mit vollständiger Virtualisierung können zwar jedes unmodifizierte Betriebssystem in virtuellen Maschinen betreiben, ohne dafür spezielle Hardware zu benötigen, leiden aber selbst im besten Fall unter Performanceverlusten von bis zu 25% alleine durch die Virtualisierung [24].

Mit dem Ansatz der *Paravirtualisierung* wird versucht, die Notwendigkeit der *binary translation* weitgehend zu vermeiden, indem die Kerne der Gast-Betriebssysteme so modifiziert werden, dass diese in Ring 1 laufen können (siehe Abb. 2.7).

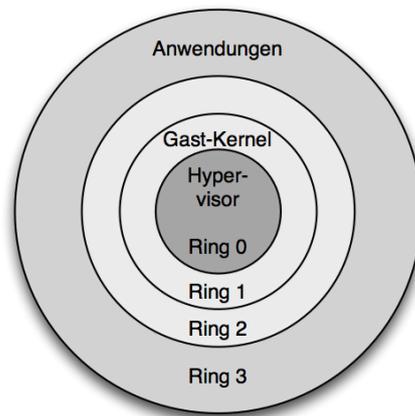


Abbildung 2.7: Hypervisor bei Paravirtualisierung

Diese Anpassung muss an allen Stellen des Gast-Kernels vorgenommen werden, an denen ein direkter Speicherzugriff nicht möglich ist – also eigentlich eine *binary translation* stattfinden sollte. Aus Systemaufrufen (*System Calls*) werden nun *Hypercalls*: problematische Systemaufrufe werden von den modifizierten Systemen nicht mehr direkt an die Hardware gestellt (z.B. Speicherzugriff), sondern an den Hypervisor. Der wiederum führt den entsprechenden System Call aus und bedient die aufrufende virtuelle Maschine.

Der Performanceverlust bei paravirtualisierten Systemen ist im Vergleich deutlich niedriger als bei *binary translation*. Die Entwickler des bekanntesten Vertreters mit Paravirtualisierung – *Xen* – geben einen Leistungsverlust im Bereich von 3-5% in einem vir-

tualisierten Linux-System mit angepasstem Kernel an [5]. Der Umfang notwendiger Anpassungen an einem Linux-Kernel liegt im Bereich von 1-2% des x86-spezifischen Anteil des Kerns, für Windows XP sind es lediglich 0,1%. Ein zentrales Problem dieses Ansatzes ist aber offensichtlich, dass die Hersteller nicht-quelloffener Betriebssysteme (z.B. Microsoft) diese Modifikationen selbst implementieren müssten, damit das entsprechende System ohne hardware-gestützte Virtualisierungstechniken in einer paravirtualisierten virtuellen Maschine funktionieren kann. Ein weiterer Nachteil, der aus der Modifikation des Gast-Kernels resultiert, ist die Einschränkung bei der Abbildung physischer Systeme in eine virtualisierte Umgebung. Dies ist in der Praxis ein häufiger Anwendungsfall, insbesondere für Testumgebungen. Durch die unterschiedlichen Kernel-Versionen (und damit verbundenen Abhängigkeiten für andere Softwarepakete) sinkt die Vergleichbarkeit des Systemverhaltens und damit die Aussagekraft solcher Tests aber deutlich.

Ein dritter interessanter und sehr unterschiedlicher Ansatz ist die *Betriebssystemvirtualisierung*, die Variante mit dem niedrigsten Virtualisierungsgrad. Hier wird auch nicht mehr von "virtuellen Maschinen" gesprochen, sondern von *Containern* oder *Jails*.

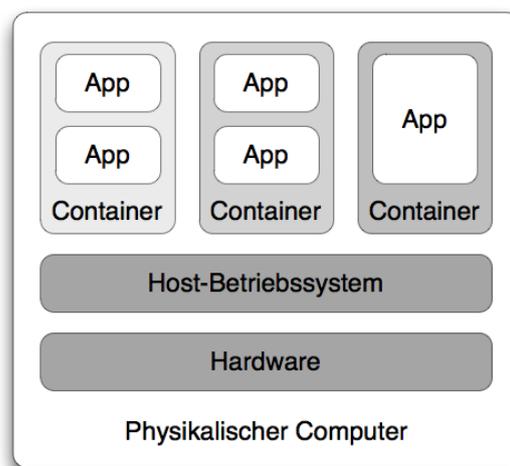


Abbildung 2.8: Betriebssystemvirtualisierung

Diese Container sind lediglich voneinander abgetrennte Laufzeitumgebungen für die Anwendungen. Applikationen, die in einem Container laufen, wissen nichts von den anderen Containern oder von deren Ressourcen. Dabei teilen sich aber alle Container den gleichen Betriebssystemkern samt Laufzeitbibliotheken.

Aus diesem Grund können die so auf einem physischen Host virtualisierten Systeme

nur sehr homogen sein. Dafür lassen sich aber vergleichsweise sehr viele Instanzen dieser gleichartigen Systeme auf einer Hardwareplattform betreiben. Haupteinsatzbereich für diese Lösungen ist der Betrieb von virtuellen Serverfarmen in den Rechenzentren der großen Internet Service Provider. Die dort angebotenen virtuellen *Root-Server* werden jeweils identisch konfiguriert und benötigen in der Regel auch nur recht wenig Hardwareressourcen. Eine weitere sinnvolle Einsatzmöglichkeit kann der zentrale Betrieb von gleichartigen Client-Systemen in einer Virtual Desktop Infrastructure sein. Hierbei laufen die Client-Betriebssysteme in Containern auf dem Server und werden von *Thin Clients* an den Arbeitsplätzen mittels Präsentationsvirtualisierung zugegriffen.

Ein weiterer wichtiger Aspekt, der sich durch die vorgestellten Technologievarianten zieht, ist die Hardwareunterstützung für Hypervisor, z.B. mittels *Intel VT²* oder *AMD-v³*. Beide Hersteller implementieren eine Erweiterung des Prozessor-Befehlssatzes, der es den virtuellen Maschinen erlaubt, System Calls nativ auszuführen, die eigentlich vom Hypervisor abgefangen werden müssten. Hiermit kann der Overhead, der durch die *binary translation* entstehen würde, vermieden werden. Es ist außerdem nicht mehr notwendig, die Kerne der Gastbetriebssysteme zu modifizieren, wie dies bei der Paravirtualisierung der Fall ist.

Neben der Performanceverbesserung bei CPU-Zugriffen durch die virtuellen Maschinen kann mit der hardwareunterstützten Virtualisierung auch eine bessere Trennung der VMs auf einem physikalischen Host erreicht werden.

Heute unterstützen nahezu alle verbreiteten Hypervisor und alle noch vertriebenen Prozessoren (zumindest im Server-Bereich) Virtualisierung mittels erweitertem Befehlssatz.

2.1.2 Servervirtualisierung

Der Grund für die Wiedergeburt der Virtualisierungstechnologie der 1960er Jahre ist im Wesentlichen das sogenannte *Moore'sche Gesetz*[10]. Moore prognostizierte, dass sich die Anzahl der Transistoren in integrierten Schaltungen (also Chips, z.B. Prozessoren) jährlich verdoppelt. Dies resultiert in einem exponentiellen Wachstum der Rechenleistung bei sinkenden Kosten.

Damit wird heute für Systemintegratoren und Administratoren die Frage nach der Auslastung der Rechner immer zentraler. Strom, Platz und Kühlkapazitäten sind wichtige Kostenfaktoren und werden immer wichtiger. *GreenIT* hat den Status eines Trends

²<http://www.intel.com/technology/virtualization/>

³http://www.amd.com/de-de/Processors/ProductInformation/0,,30_118_8796_14287,00.html

längst hinter sich gelassen, Energieeffizienz ist ein wichtiger Innovationsvorsprung geworden. Die Notwendigkeit zur Verbesserung der Energieeffizienz besteht insbesondere für den Serverbetrieb: aktuelle Studien [18, 12] zeigen, dass die durchschnittliche Serverauslastung in Rechenzentren zwischen 5% und 20% liegt. Dies lässt sofort auf ein enormes Einsparpotential schließen. Hardwarevirtualisierung ist genau die Technologie, die die Erschließung dieser Potentiale verspricht.

Ein weiterer Sektor, in dem die Virtualisierung von Computersystemen und die dadurch ermöglichte Konsolidierung von Hardware enorme Kostenersparnis verspricht, ist der Bereich der hochverfügbaren Systeme. Für unternehmens- bzw. verfahrenskritische Systeme muss in der Regel ein bestimmtes Maß an Verfügbarkeit garantiert werden, sprich: die Ausfallzeit des Systems über ein Jahr gesehen muss unter einem strengen Limit liegen. So gilt bspw. ein Computersystem als *hochverfügbar* (Verfügbarkeitsklasse AEC-2), wenn es zu mindestens 99,999% der Zeit funktioniert. Das bedeutet eine maximale Ausfallzeit von ca. 5 Minuten pro Jahr (kumuliert). Eine Erhöhung der Verfügbarkeit erreicht man für gewöhnlich durch Redundanz: insbesondere Verschleißteile wie Netzteil, Lüfter, Festplatten, etc. werden mehrfach verbaut, beim Ausfall eines Bauteils übernimmt das redundante Ersatzteil ohne Betriebsunterbrechung die Funktion. In Rechenzentren werden außerdem ganze Computersysteme redundant betrieben. Fällt ein Computer aus, übernimmt ein zweiter, identischer Rechner mit möglichst geringer Verzögerung den laufenden Betrieb. Eine solche Installation heißt (*Hot*) *Failover Cluster*. Hochverfügbare Systeme mit schlechter Auslastung auf eine gemeinsame Hardwareplattform zusammenzufassen, verringert die Kosten für Hardwarebeschaffung und Energie also überproportional.

Bei der ausfalltoleranten Installation von Servern als Failover Cluster sind die virtualisierten Umgebungen auch wegen der Eigenschaften *virtueller Festplatten*, die in den VMs zum Einsatz kommen, einer rein physikalischen Umgebung im Vorteil: die virtuellen Festplatten sind im Grunde lediglich Dateien, die vom Hypervisor verändert werden. Insbesondere, wenn diese virtuellen Festplatten auf einem redundanten, externen Speichergerät abgelegt werden, ist es offensichtlich leicht, diese virtuellen Maschinen bei Serverausfall im Hypervisor eines anderen physikalischen Systems neu zu starten. Bei einem physikalischen Failover Cluster ist die Spiegelung der Daten komplizierter. Generell ermöglicht diese Besonderheit virtualisierter Serversysteme einfachere und schnellere *Disaster Recovery* Verfahren.

Des Weiteren bieten weitgehend virtualisierte Serverlandschaften umfangreiche Möglichkeiten zur dynamischen Ressourcenzuteilung und flexiblen Bereitstellung zusätzlicher

Systeme (*Capacity on Demand*). Ein Szenario zur Verdeutlichung dieser flexiblen Ressourcennutzung sind Systeme mit großem Anteil an Stapelverarbeitung – rechenaufwändige Verfahren fallen nur zu bestimmten Zeiten an, benötigen dann aber viel Leistung. Auf solchen Systemen ist die durchschnittliche Auslastung meist schlecht, da die Rechenleistung außerhalb der Stapelverarbeitung kaum genutzt wird. In einer virtualisierten Umgebung könnten diese Maschinen nur für die Zeit der Stapelverarbeitung auf einen rechenstarken physikalischen Server geschoben werden und exklusiven Zugriff auf ganze CPUs erhalten, während es in der übrigen Zeit auf einem Server neben vielen anderen virtuellen Maschinen laufen kann.

Die konsequente Weiterentwicklung und Umsetzung des Capacity on Demand Konzepts kennt man heute als Cloud Computing (siehe Abschnitt 3).

2.1.3 Clientvirtualisierung

Unter dem Begriff *Clientvirtualisierung* (auch *Desktopvirtualisierung*) versteht man in Gegenüberstellung zur Servervirtualisierung den Einsatz von virtuellen Maschinen auf Arbeitsplatzrechnern, also Desktop-PCs. Es gibt eine Reihe von Produkten aller großen Hersteller, die speziell für diesen Bereich vorgesehen sind. Generell unterscheiden sich die Anforderungen an Hypervisor für Client-Systeme deutlich von denen für Server. Während bei letzteren in erster Linie ein möglichst geringer Overhead bei der CPU-Nutzung und schnelle Zugriffe auf E/A-Geräte wichtig sind, ist auf Client-Rechnern bspw. die 2D/3D-Grafikleistung oder die Unterstützung viele Peripheriegeräte entscheidend.

Der Haupteinsatzgrund für solche Lösungen ist heute der Betrieb zusätzlicher Betriebssysteme am Arbeitsplatz, weil beispielsweise die Notwendigkeit besteht, eine einzelne Windows-Anwendung auf einem Apple-Computer zu nutzen. Auch speziell konfigurierte Systeme z.B. für sicherheitskritische Anwendungsfälle können so auf einem Desktop zur Verfügung gestellt werden.

Potential bietet die Clientvirtualisierung aber auch in der Konsolidierung von Client-Systemen: richtig eingesetzt minimiert die Technologie den Aufwand für das Desktop-Management (siehe Abschnitt 2.4) und eröffnet den Benutzern zugleich neue, flexible Zugriffsmöglichkeiten. Bis zum Jahr 2013 – so schätzen die Analysten von Gartner – dürften bereits 40 Prozent aller Business-Desktops virtualisiert über zentrale Unternehmensserver bereitgestellt werden [13].

Auch im Zusammenhang mit Green IT ist der Bereich der Desktopvirtualisierung vielversprechend: beim kombinierten Einsatz der Technologie mit schlanken Endgeräten (Thin Clients) kann nach einer Studie des Fraunhofer-Instituts für Umwelt-, Sicherheits-

und Energietechnik (UMSICHT) ein Unternehmen, das 225 Arbeitsplätze auf Thin Clients umstellt, seinen CO₂-Ausstoß um über 148 Tonnen reduzieren und dabei die Energiekosten erheblich senken.

Aktuell zeichnet sich auch im Client-Bereich zudem eine immer tiefere Durchdringung der Hardware mit Virtualisierungstechnologie ab. Auf der CeBit 2009 wurde von Citrix und Intel ein erster Prototyp eines Laptops mit integriertem Hypervisor (hier: XenClient, siehe Abschnitt 4.1) vorgestellt [6].

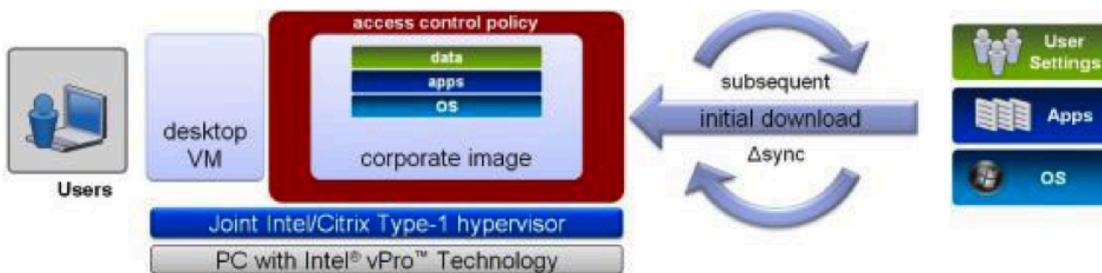


Abbildung 2.9: Hardware-gestützte Desktopvirtualisierung, Quelle: [6]

Derartige Laptops erlauben insbesondere in Verbindung mit einer durchgängig genutzten virtuellen Umgebung nicht nur den sicheren Betrieb personalisierter Arbeitsplätze auf beliebiger, häufig wechselnder Hardware. Zudem wird auch das Deployment und Lifecycle Management von Systemen auf Laptops und anderen mobilen Endgeräten deutlich einfacher.

Das in Unternehmen gerade aufkommende Konzept *BYOC* – *Bring Your Own Computer* – wird mit einem derartigen Ansatz ebenfalls deutlich interessanter: Laptops mit integriertem Hypervisor implementieren eine *Secure Virtual Machine* und erlauben die strikte Trennung zwischen dem (virtuellen) Enterprise-Desktop und dem eigenen System des Mitarbeiters. So können auch kritische und sensible Vorgänge auf privaten Laptops sicher ausgeführt werden.

Marktreife Produkte sind allerdings zum heutigen Stand der Dinge noch nicht verfügbar, werden aber im Laufe des Jahres 2010 erwartet.

2.2 Präsentationsvirtualisierung

Software, die zur Benutzung durch Anwender entwickelt wird, trennt in der Regel nicht die Ausführung der Programmlogik von der Darstellung der (graphischen) Benutzerschnittstelle (= Präsentation). Office-Pakete oder Branchenlösungen sind dafür klassische Beispiele, solche Anwendungen müssen auf dem Computer installiert werden, auf dem sie auch genutzt werden sollen.

Dies führt insbesondere in großen Enterprise-Infrastrukturen zu Problemen: es ist bspw. kaum zu vermeiden, dass in solchen Umgebungen sensible Daten auf leicht zu erreichbaren Arbeitsplatzrechnern liegen – auch beim Einsatz zentraler Fileserver. Das intuitive Benutzerverhalten führt meist dazu, dass zentrale Netzlaufwerke wie eine Datenablage genutzt werden. Die Dateien, mit denen aktiv gearbeitet wird, werden meist auf den Arbeitsplatzrechnern vorgehalten (und mit Glück regelmäßig auf das Netzlaufwerk gesichert). Außerdem muss verhältnismäßig viel Administrationsaufwand betrieben werden, um die auf den Clients verteilten Anwendungen zu pflegen.

Das Prinzip der Präsentationsvirtualisierung erlaubt den Betrieb von *virtuellen Benutzersitzungen (Sessions)*, bei denen entweder eine einzelne Applikation oder ein ganzer Desktop eines entfernten Rechners (Server) auf dem lokalen Arbeitsplatz wiedergegeben wird. Die gesamte Anwendung sowie die Daten liegen dabei auf dem Server, der lokale Computer dient lediglich zur Anzeige des Desktops oder Fensters sowie für die Benutzereingaben (Maus, Tastatur, etc). Natürlich können mehrere Benutzer gleichzeitig Anwendungen auf einem Server zugreifen.

Dieses als *Terminal Computing* bekannte Setup hat einige offensichtliche Vorteile:

- Daten können zentral gehalten werden. Dieses Vorgehen vereinfacht Zugriffskontrolle und Backupverfahren, führt somit zu erhöhter Sicherheit und Datenintegrität und geringeren Anforderungen bei Datenreplikation bzw. -reinigung.
- Die Kosten für das Lifecycle Management von Applikationen können drastisch reduziert werden: lediglich die zentralen Terminalserver müssen gewartet werden.
- Terminal Computing erlaubt eine deutlich effizientere Durchsetzung von Sicherheitspolicies in Unternehmen. Der Einsatz von Thin Clients an den Arbeitsplätzen führt nicht nur zu Kostenersparnis, sondern die funktionale Reduktion der Arbeitsplatzrechner auf Benutzereingabe und Ausgabe am Bildschirm verkleinert die Angriffsfläche am Arbeitsplatz signifikant. Angesichtes der Tatsache, dass 80%

der Angriffe mit signifikanten Folgen für ein Unternehmen durch eigene Mitarbeiter verübt werden, ist dies ein nicht zu unterschätzender Vorteil.

- Inkompatibilitäten zwischen Desktop-Betriebssystem und spezifischen Anwendungen sind in einer Terminal-Umgebung nicht mehr relevant. Die verbreiteten Betriebssysteme mit graphischem Desktop (Windows, Linux, Mac OS) können jeweils Terminal Sessions zu allen anderen Systemen anbieten.
- Bei Client-/Server-Anwendungen, bei denen der Client während des Betriebs große Datenmengen vom Server anfordern muss, kann es zu extremen Spitzen in der Netzlast kommen. Dies wird vor allem bei verteilten Standorten problematisch. Man benötigt in solchen Fällen entweder eine sehr breitbandige Leitung, deren Kapazität nur selten ausgeschöpft wird oder es kommt zu Situationen mit langen Wartezeiten für den Benutzer. Terminal Computing kann hier Abhilfe schaffen: Client (in diesem Fall der Terminal Server) und Anwendungsserver liegen im gleichen lokalen Netzwerk. Von den entfernten Standorten aus wird via Präsentationsvirtualisierung zugegriffen: so ist die Netzauslastung sehr konstant.

Der inhärente Nachteil beim Terminal Service Computing ist natürlich die absolute Abhängigkeit von der Netzanbindung. Geht die Verbindung verloren, ist ein Weiterarbeiten nicht möglich – wenn auch kein Datenverlust entsteht, falls lediglich die Leitung ausfällt und nicht der Server. Im Gegensatz zu regulären Client-/Server-Anwendungen kann beim Terminal Computing nicht auf der Clientseite zwischengespeichert werden. Die Anwendungen sowie die Daten liegen lediglich auf dem Server vor und werden nicht auf den Client repliziert. Für Unternehmens- bzw. Verfahrenskritische Einsatzszenarien ist eine redundante Netzanbindung also unabdingbar.

Wie schon erwähnt, setzt sich die Kombination aus Clientvirtualisierung und Präsentationsvirtualisierung als eigenständiges Konzept durch: die *Virtual Desktop Infrastructure (VDI)*. Hierbei werden auf einem Server für jeden Benutzer individuelle virtuelle Maschinen betrieben, auf die diese dann via Remote Desktop-Verbindung von einem beliebigen Arbeitsplatz zugreifen können. Die Anforderungen an die Desktop-PCs (bezüglich Leistung oder vorausgesetztes Betriebssystem) sind dabei minimal, alle Clientsysteme können zentral gewartet werden und dynamisch auf physikalische Server verteilt werden – je nach tagesaktuellem Ressourcenbedarf.

2.3 Applikationsvirtualisierung

Das wesentliche Ziel von Applikationsvirtualisierung besteht darin, Anwendungen von ihrer Umgebung zu isolieren, so dass Konflikte mit anderen Programmen oder dem Betriebssystem vermieden werden. Dadurch soll sich das Systemmanagement vereinfachen und die Sicherheit erhöhen.

Auch mit Desktop- und Server-Virtualisierung kann man einzelne Applikationen vom Betriebssystem auf den Arbeitsplatz-Computern entkoppeln. Im Unterschied dazu wird bei Applikationsvirtualisierung nicht die Hardware virtualisiert, sondern nur eine Abstraktionsschicht zwischen einzelnen Anwendungen und das Betriebssystem gesetzt. Geteilte Ressourcen des Betriebssystems (wie z.B. *shared libraries*), deren unterschiedliche Versionen Konflikte hervorrufen können, werden in einem Container um die eigentliche Anwendung herum untergebracht und von dort auch aufgerufen (siehe Abbildung 2.4).

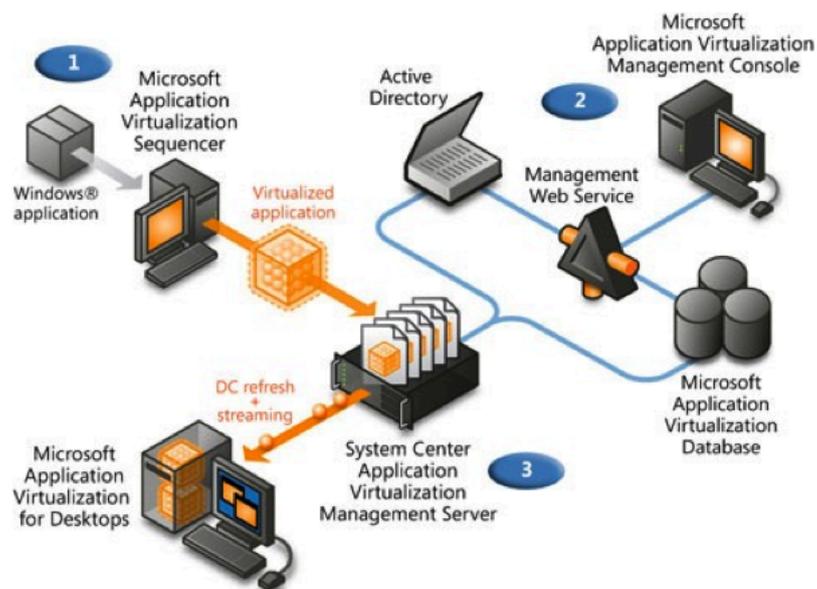


Abbildung 2.10: Infrastruktur mit Applikationsvirtualisierung in der Microsoft-Welt, Quelle: [8]

Im Gegensatz zum gewöhnlichen Desktop entfällt in derart virtualisierten Infrastrukturen die Installation von Programmen. Applikationen werden nicht mehr auf den Arbeitsplätzen direkt deployed, sondern werden in Container-Umgebungen auf einem *Ap-*

plication Streaming Server installiert. Von dort müssen die *virtualisierten Anwendungen* lediglich bei Bedarf auf einen Client-PC kopiert werden. Dort können diese selbstverständlich auch in einem Cache zwischengespeichert werden.

Beim klassischen *Application Provisioning (Applikationsverteilung)* mittels Terminal Services kann eine gestreamte Anwendung auch im Offline-Betrieb genutzt werden.

Bei Microsoft ist der Dienst für das Application Streaming ein Teil des System Centers, der System Center Application Virtualization Management Server. Caching und Lifetime-Check erledigt die Client-Komponente *Microsoft Application Virtualization for Desktops*.

Die Vorteile, die eine solche Infrastruktur bietet, liegen klar auf der Hand:

- Softwareverteilung wird deutlich einfacher, Applikationen können durch einfaches Löschen des Applikationscontainers entfernt werden
- Applikationen können problemlos in mehreren Versionen gleichzeitig auf einem System genutzt werden
- aufwändiges Integrations-Testing wird deutlich vereinfacht, es muss i.d.R. lediglich die Kompatibilität der Applikation mit dem Virtualisierungscontainer getestet werden

Zudem bringen die meisten auf dem Markt erhältlichen Lösungen Software zum Lizenzmanagement mit. Der Streaming Server weiß, wie viele Lizenzen gerade in Benutzung sind und teilt neuen Applikationsinstanzen automatisch Lizenzen aus einem Pool zu.

2.4 Management virtualisierter Umgebungen

Bei der Abwägung über den Einsatz jeglicher Virtualisierungstechnologie ist die Verwaltbarkeit der gewählten Produkte ein entscheidender Faktor. In der Regel bilden die Personalkosten den größten Anteil des finanziellen Aufwands für eine IT-Infrastruktur. Wenn nun der Einsatz von Virtualisierungstechnologie zu besserer Ressourcenausnutzung für Hardware führt, darf diese Einsparung natürlich nicht durch höheren Verwaltungsaufwand überstiegen werden.

Generell gilt, dass mit der Einführung von Virtualisierung die Abstraktion und damit auch die Komplexität des Gesamtsystems steigt. Insbesondere in großen, verteilten Infrastrukturen muss die Virtualisierungslösung in bestehende Software-Suites für Systemadministration und *Data Center Monitoring* integriert werden können.

Das ist nicht nur wichtig, um flexibles Deployment oder dynamische Umverteilung von Hardware-Ressourcen erst effektiv zu ermöglichen. Auch das integrierte Monitoring der virtuellen Maschinen im Rechenzentrum ist von großer Bedeutung. Werden mehrere unternehmenskritische Systeme auf eine gemeinsame Hardware-Plattform gezogen, wird die Verfügbarkeit des Systems umso wichtiger. Eine schlecht gemanagete virtuelle Umgebung kann an diesem Punkt zu weniger Zuverlässigkeit führen und damit in Ausfallsituationen teurer werden, als das nicht-virtualisierte Pendant.

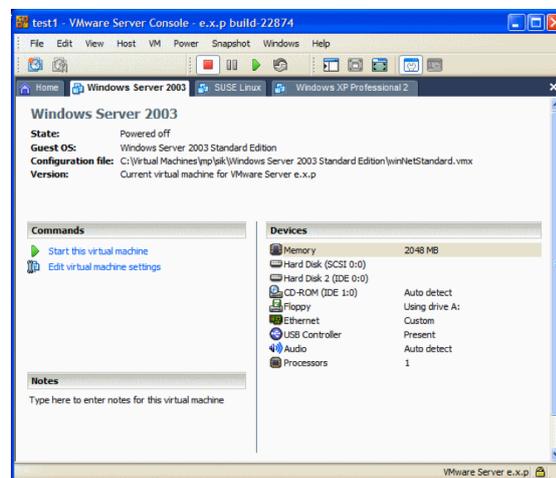


Abbildung 2.11: VMware Server Console (Beispiel für lokales Virtual Machine Management)

In der Regel bringen die Virtualisierungs-Produkte nicht nur den eigentlichen Hypervisor sondern auch ausgefeilte Management-Software (z.B. *VMware Server Console*) mit.

Diese kann meist sowohl lokal als auch über Netzwerk genutzt werden und erlaubt Konfiguration, Deployment und Monitoring der virtuellen Maschinen auf einem oder mehreren physikalischen Hosts mit der gleichen Virtualisierungs-Suite.

In großen Rechenzentrumsinfrastrukturen gibt es normalerweise bereits Management- und Monitoringsysteme für die vorhandene physikalische Umgebung, z.B. das *Microsoft System Center*. Virtualisierungs-Suites für den Enterprise-Betrieb bringen idealerweise auch Erweiterungen für diese Systeme mit, so dass sich die virtuellen Maschinen bzgl. Management und Monitoring so verhalten, wie physikalische Systeme. Zusätzlich sollten jedoch auch die VM-spezifischen Funktionalitäten (z.B. Verschieben auf andere physikalische Hosts, Workload-Begrenzung, etc.) in dieser integrierten Management-Umgebung möglich sein.

Insbesondere wenn mehrere unterschiedliche Virtualisierungstechnologien (z.B. Server-, Präsentations-, und Anwendungsvirtualisierung) bzw. Produkte unterschiedlicher Hersteller in einer gemeinsamen Umgebung eingesetzt werden, ist die Integration aller Lösungen mit einem zentralen Management-System unabdingbar. Werden beispielsweise zwei Hypervisor unterschiedlicher Hersteller eingesetzt, sollte zudem (falls möglich) auf die Interoperabilität der virtuellen Maschinen geachtet werden. Die großen Hersteller (z.B. Microsoft, VMware, Citrix, Dell, HP, etc.) haben dazu als Distributed Management Task Force (DMTF) ein offenes Format für virtuelle Maschinen entworfen und zur Standardisierung eingereicht: das *Open Virtualization Format (OVF)*⁴. Die Idee ist, dass jeder Hypervisor, der OVF unterstützt, virtuelle Maschinen aus anderen Hypervisor aufnehmen und ausführen kann. Bei Kaufentscheidungen sollte schon heute auf die Unterstützung des Standards durch das gewählte Produkt geachtet werden.

⁴Open Virtualization Format Spezifikation 1.0.0 (vorläufiger Standard) abrufbar unter http://www.dmtf.org/standards/published_documents/DSP0243_1.0.0.pdf

3 Cloud Computing

Eine breit akzeptierte Definition des Begriffs Cloud Computing gibt es bis heute nicht. Allerdings können die grundlegenden Eigenschaften wie folgt zusammengefasst werden: Cloud Computing nutzt Virtualisierung und das Internet zur dynamischen Bereitstellung von IT-Ressourcen. Dabei kann es sich um IT-Infrastruktur, Plattformen oder Anwendungen aller Art handeln. Cloud Computing bezeichnet also sowohl Anwendungen, welche als Dienste über das Internet angeboten werden, als auch auf die Hard- und Software, die in Rechenzentren zu deren Bereitstellung benötigt werden. Die Abrechnung erfolgt dabei stets nach Verbrauch.

In der Praxis differenziert man zwischen den Modellen Private Cloud und Public Cloud. Beide unterscheiden sich weniger in der technischen Umsetzung, als vielmehr in der Zugangsform und der Einbettung in die in einem Unternehmen vorhandene IT-Infrastruktur. Wenn Cloud-Dienste öffentlich zugänglich sind, also von beliebigen Personen und Unternehmen im Internet genutzt werden können, dann wird in der Regel von einer Public Cloud gesprochen. Stehen Dienstleistungen nur einem eingeschränkten Nutzerkreis zur Verfügung wie z.B. ausschließlich Anwendern in einem bestimmten Unternehmen, so werden solche Angebote als Private Clouds bezeichnet. Üblicherweise erfolgt der Zugang zu solchen Diensten über ein Intranet beziehungsweise ein Virtual Private Network (VPN). Private Clouds verfügen zwar nicht über die Vielfalt der öffentlichen Angebote, sie weisen jedoch einige Vorteile im Bezug auf die verfügbare Netzbandbreite und Sicherheit auf. Dies ist damit zu erklären, dass bei einer Private Cloud Anbieter und Benutzer der gleichen Organisation angehören. Eine dritte und letzte Kategorie bildet die Kombination aus den beiden Ansätzen. Diese Variation wird als Hybrid Cloud bezeichnet. Der Regelbetrieb erfolgt dabei über die traditionelle IT-Infrastruktur und private Ressourcen, wobei für bestimmte Funktionen auch öffentliche Dienste bezogen werden.

Die Gründe für Cloud Computing liegen auf der Hand: Es entfallen die Kosten für Anschaffung, Betrieb und Wartung eigener Hardware. Die Benutzer können auf praktisch unbegrenzt verfügbare Ressourcen zugreifen ohne sich um die Installation und Pflege von Hard- und Softwareware kümmern zu müssen.

Im täglichen Betrieb bleibt dabei für Endnutzer alles unverändert. Er kann seine Diens-

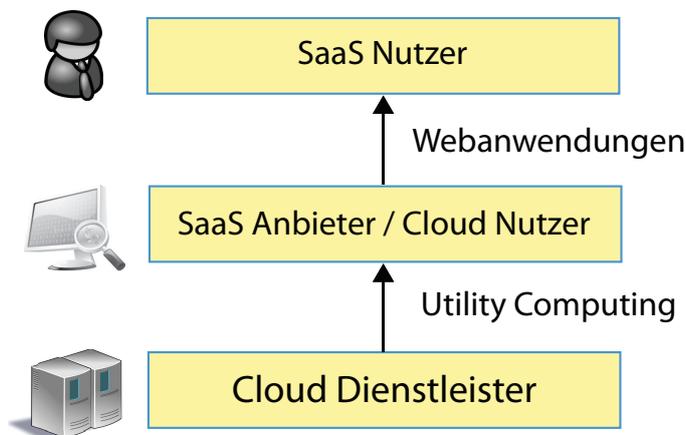


Abbildung 3.1: Nutzer und Anbieter des Cloud Computing

te bzw. Software weiterhin von überall und jederzeit nutzen und braucht sich idealerweise nicht um die dahinter stehende Technologie zu kümmern. Folglich lässt sich Cloud Computing auch als Weiterentwicklung des Software as a Service (SaaS) Konzepts begreifen (siehe Abbildung 3.1). Ein Beispiel hierfür ist das Unternehmen Cloudize Inc.¹, das eine Internet-basierte Kollaborationsplattform für kleine und mittlere Unternehmen anbietet, mit der sich, unter anderem, Daten in der Cloud verwalten lassen. Die Speicher-Plattform dahinter wird von der Firma Nirvanix² bereitgestellt, einem spezialisierten Cloud Speicher-Dienstleister.

Aus technischer Perspektive sind es im Wesentlichen drei Aspekte, die Cloud Computing von bisherigen IT-Modellen unterscheiden:

Das ist zum Einen die Vorstellung unendlicher Rechenressourcen, die völlig frei an den aktuellen Bedarf angepasst werden können. Wenn eine Anwendung zusätzliche Rechenressourcen benötigt, können diese direkt verfügbar gemacht werden. In der herkömmlichen IT müssen zur Bereitstellung eines neuen Dienstes dagegen erst die technischen und organisatorischen Voraussetzungen geschaffen werden (Einkauf, Installation und Wartung von Hardware und Infrastruktur).

Beim Cloud Computing entfallen die Kosten zur Beschaffung neuer Hardware zur Bereitstellung zusätzlicher IT-Dienste. Das Modell bietet vor allem kleineren Unternehmen eine preiswerte Möglichkeit, mit neuen Diensten zu experimentieren und sich auf das

¹<http://cloudize.net/>

²<http://www.nirvanix.com/>

eigentliche Kerngeschäft zu fokussieren.

Cloud-Anbieter rechnen ihre Leistungen in der Regel nach den tatsächlich genutzten Ressourcen ab, beispielsweise nach CPU-Stunden, übertragener Datenmenge oder Speichervolumen pro Tag. Somit wird immer nur die aktuell benötigte Menge an Ressourcen bereitgestellt und bezahlt. Ältere Abrechnungsmodelle für Hosting-Dienste sehen in der Regel einen fixen Geldbetrag pro Server oder eine monatliche Gebühr vor.

Die existierenden Cloud-Ansätze unterscheiden sich hinsichtlich ihrer Zielsetzung, Architektur sowie der Funktionalität, die sie dem Benutzer bieten. Die grundsätzlichen Cloud-Kategorien abstrahieren unterschiedlich stark von der darunterliegenden Hardware und werden im nächsten Kapitel vorgestellt. Was allerdings alle Ansätze gemein haben, ist, dass IT-Ressourcen ihren Nutzern als abstrakte Web-Dienste bereitgestellt werden. Speicher, Rechenzeit oder komplexere Dienste können über festgelegte Schnittstellen angefordert werden. Aktuell sind jedoch alle kommerziellen Angebote zugunsten eines Wettbewerbsvorteils proprietär. Es gibt bisher keine weitreichenden Standards, wodurch ein Wechsel des Anbieters nicht ohne Weiteres möglich ist. Auf diese und weitere Nachteile der Cloud-Dienste wird in Abschnitt 3.3 genauer eingegangen.

3.1 Architekturvarianten des Cloud Computing

In diesem Kapitel wird auf die Architektur und die Darstellungsform des Cloud-Modells eingegangen. Die Landschaft verfügbarer Cloud Dienste ist äußerst vielfältig. Die grundlegende Architektur verfügbarer Angebote lässt sich jedoch in drei Ebenen aufteilen und in einer Pyramidenform darstellen. Dabei nutzen die höheren, abstrakteren Schichten die Dienste der tieferen, konkreteren Kategorien. Allgemein gilt: Nutzer von Cloud-Ressourcen können ihrerseits eigene Angebote als Dienste im Internet anbieten. Dabei werden die Vorteile des bereits etablierten Software-as-a-Service Bereitstellungsmodells (SaaS) auf die tieferliegenden Schichten der IT-Architektur übertragen (vergleiche Abbildung 3.2).

3.1.1 IaaS - Infrastructure-as-a-Service

Die unterste Schicht bildet die Infrastruktur-Schicht. Diese Schicht stellt Mittel bereit, mit denen Basisspeicher und Rechenleistung als standardisierte Services über das Netzwerk angeboten werden können. Hierzu werden Server, Speicher, Router und weitere Systeme zusammengeschaltet, um verschiedene Arten von Arbeitslast zu bewältigen.

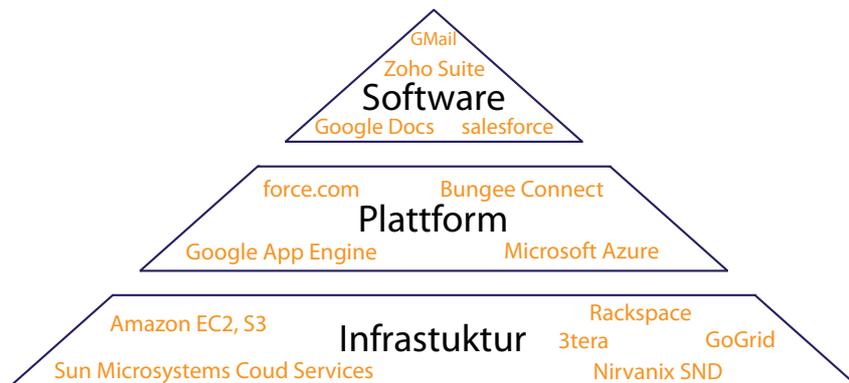


Abbildung 3.2: Cloud Computing Architektur

Das Angebot von Amazon Web Services zählt zu den prominentesten Vertretern des IaaS Models. Amazon Elastic Compute Cloud (EC2) bietet die Möglichkeit, virtuelle Maschinen in der Cloud zu konfigurieren und zu starten. Dies erfolgt über so genannte Amazon Maschine Images (AMIs). Aus Nutzerperspektive sieht die angebotene Infrastruktur wie physische Hardware aus. Zur Verwaltung der Infrastruktur werden spezielle Webservices zur Verfügung gestellt. Innerhalb nur weniger Minuten können beliebig viele Instanzen (virtuelle Server) gestartet und wieder entfernt werden. Nutzer können die Images entweder selbst erstellen oder auf die von Amazon bereitgestellte Sammlung zurückgreifen.

Einzelne EC2-Instanzen können dabei in verschiedenen Regionen und Verfügbarkeitszonen platziert werden. Regionen sind über verschiedene geographische Bereiche bzw. Länder verteilt. Verfügbarkeitszonen sind verschiedene Standorte innerhalb einer Region. Dabei ist die Infrastruktur so realisiert, dass die Zonen untereinander isoliert sind. Dadurch können mögliche Fehler in einzelnen Bereichen nicht den Betrieb in anderen Verfügbarkeitszonen beeinflussen. Darüber hinaus kann das Starten von Instanzen in separaten Regionen auch rechtlichen Anforderungen gerecht werden.

Amazon bietet auch eine Reihe weiterer Services an. Diese können zum Teil auch von externen Anwendungen verwendet werden. Zur Datenspeicherung stehen beispielsweise folgende Dienste zur Verfügung: S3, Elastic Block Store (EBS) und SimpleDB.

- Mit Amazons S3 kann eine beliebige Datenmenge in sogenannten Buckets abgelegt und über eine Webservice-Schnittstelle verwaltet werden. Die gelagerten Objekte können allerdings nicht hierarchisch geschachtelt werden. Jedes Datenobjekt

ist über seine Bucket-Bezeichnung und über seinen eigenen Namen identifizierbar. Amazon S3 ist daher kein herkömmliches Dateisystem.

- Bei SimpleDB handelt es sich um eine sehr einfache, verteilte und nicht-relationale Datenbank, in der Daten zwar strukturiert, aber ohne explizites Schema abgelegt werden können. Die gespeicherten Daten liegen in so genannten Domains in Form von Attribut-Wert-Paaren vor (ähnlich wie in einer Tabelle). Allerdings können einem Attribut mehrere Werte zugewiesen werden, wobei jedes Objekt auch über andere Attribute verfügen kann.
- EBS ist ein persistenter Low-Level Storage-Mechanismus für EC2-Instanzen. EBS erlaubt somit einen blockbasierten Zugriff auf ein Speichermedium. Dadurch können EBS-Devices mit beliebigen File-Systemen formatiert oder auch als Datenbank-Devices verwenden werden. Aus Sicht einer EC2-Instanz lässt sich EBS wie eine externe Festplatte benutzen. Die gleichzeitige Nutzung eines EBS-Volumes durch mehrere EC2-Instanzen ist jedoch nicht möglich.

EC2-Nutzer können das gesamte Betriebssystem sowie die darauf laufende Software kontrollieren. Es gibt keine Einschränkungen im Bezug auf Anwendungen, die von den Systemen gehostet werden können. Der Nachteil dieser Virtualisierungsvariante liegt darin, dass eine automatische Skalierung der Recheninstanzen nur schwer umgesetzt werden kann. Amazon bietet zwar einige Instrumente wie Amazon CloudWatch oder Elastic Load Balancing Service zur automatischen Anpassung der Rechenleistung an den aktuellen Bedarf, allerdings liegt es in der Verantwortung der Nutzer selbst, sich um die Konfiguration dieser Services zu kümmern.

Mit Elastic Load Balancing steht ein Dienst zur Verfügung, mit dem eingehender Anwendungsverkehr gleichmäßig über mehrere EC2-Instanzen innerhalb einer festgelegten Arbeitsgruppe verteilt werden kann. Bei Amazon CloudWatch handelt es sich um einen Dienst zur kontinuierlichen Überwachung und Kontrolle von EC2 sowie Elastic Load Balancing Instanzen. Darüber hinaus kann CloudWatch so konfiguriert werden, dass im Falle einer Überschreitung eines vorher definierten Grenzwertes, automatisch weitere EC2-Instanzen gestartet und in die Arbeitsgruppe aufgenommen werden können.

3.1.2 PaaS - Platform-as-a-Service

Die mittlere Schicht, die Platform-as-a-Service (PaaS)-Schicht bietet Funktionen für die Bereitstellung von Entwicklungsumgebungen und Anwendungen als Dienste. Bekannte

Beispiele sind dafür die Google App Engine³ und Force.com⁴. Im Gegensatz zu EC2 bietet Google App Engine eine vollautomatische Skalierung der Rechenleistung. Entwickler müssen sich nicht selbst um die Einrichtung und Wartung der Infrastruktur kümmern. Die Plattform ist in erster Linie für das Entwickeln und Betreiben von Webanwendungen geeignet. Es gibt eine klare Trennung zwischen der Verarbeitungsschicht und der Speicherebene. Jede Google App Anwendung läuft in einer abgeschirmten Umgebung (Sandbox) und orientiert sich am seitenbasierten HTML-Modell: dabei erfolgt der Datenabruf ausschließlich auf Anfrage-/Antwortbasis. Die eingehenden Browser-Anfragen werden bei Bedarf automatisch auf mehrere Server verteilt, welche nach Datenaufkommen von der Plattform gestartet oder gestoppt werden.

Bei dieser Virtualisierungsvariante ist die gesamte Infrastruktur stark abstrahiert: Skripte der Anwendungen (und damit auch Nutzer) haben keinen Zugriff auf das darunter liegende Betriebssystem. Es gibt keine Auskunft darüber, auf welchen Servern die Anwendungen laufen. Der physische Ort der betreffenden Server ist nicht bekannt. Darüber hinaus gibt es weitere Einschränkungen: Webanwendungen haben keine Schreibrechte auf das Dateisystem. Es dürfen nur Daten gelesen werden, die der Anwender zuvor zusammen mit der Anwendung auf den Server geladen hat. Für eine dauerhafte Datenaufbewahrung muss auf einen internen Datenspeicherdienst zurückgegriffen werden. Diese Datenbank basiert auf dem verteilten Dateisystem Google File System (GFS) und dem hauseigenen Speichersystem BigTable. Die nichtrelationale Struktur der proprietären Datenbanklösung erschwert zusätzlich eine potentielle Migration auf eine andere Cloudplattform. Des Weiteren schränkt die Plattform die Größe der Applikationen sowie Prozessor- bzw. Ausführungszeiten der Skripte ein: jedes Skript darf maximal ein Megabyte groß sein und muss in wenigen Sekunden ausgeführt werden. Dauert die Bearbeitung länger als 30 Sekunden wird der Prozess (mit einer entsprechenden Fehlermeldung) abgebrochen, um eine Überlastung der Webserver von Google zu verhindern. Auch bei anderen PaaS-Anbietern gibt es ähnliche Einschränkungen. Force.com ist eine komplette Entwicklungs- und Betriebsplattform für die Implementierung von SaaS-Geschäftsanwendungen von dem Anbieter salesforce.com. Für die dauerhafte Konservierung von Daten müssen die Anwendungen allerdings auf die exklusiv von salesforce.com bereitgestellte Datenbank zurückgreifen. Plattformbereitstellung nimmt Entwicklern und Anbietern von Anwendungen eine Menge Detailarbeit ab. Allerdings erschweren die proprietären Dienste wie z.B. der jeweilige Datastore die Migration von Anwendungen zu anderen Anbietern wo-

³<http://code.google.com/intl/de-DE/appengine/>

⁴<http://www.salesforce.com/platform/>

durch Nutzer an eine Plattform gebunden werden.

3.1.3 SaaS - Software-as-a-Services

Die höchste Schicht des Modells bildet die Anwendungsschicht, die so genannte Software-as-a-Service Schicht. Sie unterstützt das Angebot, komplette Anwendungen als Dienste auf Anfrage anzubieten. Der Ansatz sieht vor, dass einzelne Softwarekomponenten bei einem Dienstleister betrieben werden, der allein für die gesamte Administration der Software verantwortlich ist, also Hardware und Software, Wartung und Betrieb. Dies betrifft auch die interne Ressourcenanpassung zur performanten Bereitstellung der Dienste. Der Zugriff auf Anwendungen erfolgt über standardisierte Schnittstellen, wobei beim Endnutzer nur eine minimale EDV-Infrastruktur vorausgesetzt wird. Dieses Prinzip funktioniert für einzelne Funktionen wie beispielsweise einen Adressencheck ebenso wie für komplette Applikationen. SaaS-Produkte variieren einerseits aufgrund der Programmierung der Software und andererseits aufgrund der Voraussetzungen an die Infrastruktur der Nutzer. Bei SaaS-Angeboten wird in der Regel zwischen Web- und Terminalanwendungen unterschieden. Bei letzteren handelt es sich um Software, die auf einem entfernten System als Client-Anwendung installiert werden kann (siehe Abschnitt 2.2). Webanwendungen setzen auf einen Webbrowser. Ein bekanntes Beispiel für eine Anwendung dieser Schicht ist die Google App Engine mit Applikationen wie Google Docs. Der Anbieter salesforce.com hat sich auf Customer-Relationship-Management (CRM) Lösungen spezialisiert und ist zu einer Plattform für zahlreiche Cloud-Dienste gewachsen.

Im Zusammenhang mit SaaS-Anwendungen stehen vor allem die Probleme der Migration sowie der Integration mit anderen Softwarelösungen. Die Kommunikation mit den SaaS-Anwendungen erfolgt zwar über beschriebene Schnittstellen, der Anwender hat aber in der Regel keine Kontrolle über die Syntax sowie die Semantik der Daten, in denen die Datensätze von den Anwendungen angelegt werden. Das betrifft sowohl traditionelle Desktop-Softwarelösungen als auch SaaS-Anwendungen. Auch im Falle einer vorhandenen ausführlichen Datenbeschreibung müssen die extrahierten Inhalte an neue Dienste angepasst werden. Üblicherweise wird dazu der ETL-Prozess eingesetzt⁵. Es besteht allerdings immer das Risiko, dass sich nicht alle Informationen aus den extrahierten Dokumentvorlagen korrekt und vollständig übernehmen lassen.

So stellt sich beispielsweise die Frage, wie Informationen über Kunden aus einem haus-eigenen ERP-System mit einer Anwendung wie salesforce.com zu verbinden sind. Je mehr

⁵Das Verfahren beschreibt den Prozess zur Vereinigung von Daten aus mehreren ggf. unterschiedlich strukturierten Datenquellen in einer Zieldatenbank.

SaaS-Systeme unterschiedlicher Hersteller eingesetzt werden, desto komplexer gestaltet sich diese Herausforderung.

Es kann für ein Unternehmen genauso schwer sein, Daten aus einer SaaS-Lösung wieder herauszubekommen wie sie hineinzubringen. Viele Provider bieten keine Werkzeuge für Massensexport von Daten, weder für Daten in Datenbanken noch für Dokumente oder E-Mails. Wenn ein Service-Nutzer viele Informationen, wie beispielsweise über seine Kunden, in einem bestimmten System hat, ist er dadurch de facto auch an den SaaS-Anbieter gebunden. Das Defizit solcher Bindung mag bei Lösungen wie SAP Business By Design noch zu vertreten sein, weil eine Entscheidung für derartige Systeme einen strategischen Charakter hat und in der Regel auch eine langfristige Bindung vorsieht. Mit jeder solcher Abhängigkeit verringert sich jedoch die Flexibilität der Unternehmen bei den IT-Entscheidungen.

3.2 Aspekte des Cloud Computing

Mit Cloud Computing können Unternehmen Kapitalkosten in laufende Kosten überführen. Vor allem kleine Unternehmen und Start-Ups profitieren von dem neuen Ansatz. Es fallen keine Kosten für IT an, für die im Voraus Kapital aufgebracht werden muss. Aber auch für Mittelständler bewirkt die Anwendung des Cloud Computing Modells nachhaltige Effizienzsteigerungen. Mit Hilfe von Cloud Computing entfällt eine zeitintensive und teure Administration eigener, zum Teil sehr komplexer IT-Infrastruktur. Damit können sich Unternehmen verstärkt auf ihr Kerngeschäft konzentrieren. Signifikante Kostenersparnisse sind vor allem aufgrund der flexiblen Bereitstellung der Ressourcen möglich. Damit müssen Unternehmen sich nicht mehr um die voraussichtliche Planung der erforderlichen IT-Ressourcen kümmern. Eine mögliche Fehleinschätzung führt entweder zu Überversorgung oder zu Unterversorgung in der verfügbaren Kapazität. In beiden Fällen haben Unternehmen finanziellen Einbußen. Dieses Risiko übernimmt der Cloud-Dienstleister.

Elastische Skalierbarkeit Mit Cloud Computing können Ressourcen feinkörniger eingerichtet und wieder freigegeben werden als mit bisherigen Ansätzen in der Informationstechnologie. Zusätzliche Infrastruktur kann jetzt in wenigen Minuten und nicht in Wochen oder Monaten eingerichtet werden. Damit ist es möglich, die verfügbare Kapazität dem aktuellen Bedarf akkurat anzupassen. In der Regel liegt die physische Serverauslastung eines Rechenzentrums zwischen 5% und 20% [12]. Dies mag auf den ersten Blick überraschend erscheinen, es lässt sich jedoch damit erklären, dass die Systemauslastung zu Spit-

zenzeiten die durchschnittlichen Werte bis um das Zehnfache überschreiten kann. Um die Spitzenlast abzufangen, entscheiden sich Unternehmen bewusst dafür, mehr Ressourcen als notwendig bereitzustellen (auch wenn die meisten von ihnen ungenutzt bleiben). Für eine vorsorgliche Einrichtung von IT-Ressourcen spricht außerdem die Tatsache, dass die Bestellung und Integration des zusätzlichen Equipments in die bestehende Infrastruktur von einigen Tagen bis hin zu mehreren Wochen in Anspruch nehmen kann.

Je größer die Diskrepanz zwischen der reservierten Kapazität und der Durchschnittslast, desto größer ist die Menge ungenutzter Ressourcen. Dieses Verhalten führt nicht nur zu höheren Kosten, sondern auch zu einer überflüssigen Belastung der Umwelt.

In der herkömmlichen IT wird dieses Problem mit exakterer Kapazitätsplanung angegangen. Eine genaue Einschätzung der Nachfrage nach Rechenleistung oder Speicherplatz ist allerdings schwierig zu gewährleisten. Außerdem kann eine gute Kapazitätsplanung bestenfalls nur bei der Vorhersage helfen, wann eine bestimmte Anwendung über die Leistung der vorhandenen Server hinauswächst. Aber: selbst wenn die Nachfrage korrekt eingeschätzt wird, verliert das Unternehmen Geld. Der Vorteil einer verbrauchsabhängigen Abrechnung gegenüber dem Erwerb der Hardware lässt sich anhand eines einfachen Beispiels verdeutlichen:

Wir nehmen an, dass ein exemplarischer Anbieter X zur Bereitstellung seiner Leistungen voraussichtlich 400 Server benötigt. Dabei wird diese Spitzenlast nur jeweils mittags erwartet. Nachts nimmt der Dienst nur 100 Server in Anspruch (siehe Abbildung 3.3). Damit liegt die durchschnittliche Auslastung der Infrastruktur bei 250 Servern. Über den Tag verteilt werden $250 \times 24 = 6000$ Server-Stunden verbraucht. Um die tägliche Spitzenlast zu bewältigen, werden allerdings $400 \times 24 = 9600$ Server-Stunden bereitgestellt. Es werden also 1.6 mal mehr Ressourcen bereitgestellt als benötigt. Verwendung von Cloud-Ressourcen bietet somit eine direkte Kostenersparnis, sofern die Kosten pro Server-Stunde sich auf weniger als das 1.6-fache gegenüber dem Erwerb und Betrieb der Hardware belaufen.

In Wirklichkeit bietet ein verbrauchsabhängiges Abrechnungsmodell sogar ein noch größeres Einsparungspotential: außer täglichen Schwankungen gibt es außerdem saisonbedingte Veränderungen in der Dienstanfrage. Im elektronischen Geschäftsverkehr ist dieses Verhalten zum Jahreswechsel bzw. zur Weihnachtszeit zu beobachten. Auch unvorhersehbare Ereignisse wie z.B. Berichterstattungen in frequentierten Medien können einen unerwarteten Anstieg in der Nachfrage verursachen. Schwankungen in der Nachfrage zwingen somit Dienstbetreiber zur Bereitstellung größerer Rechenleistung.

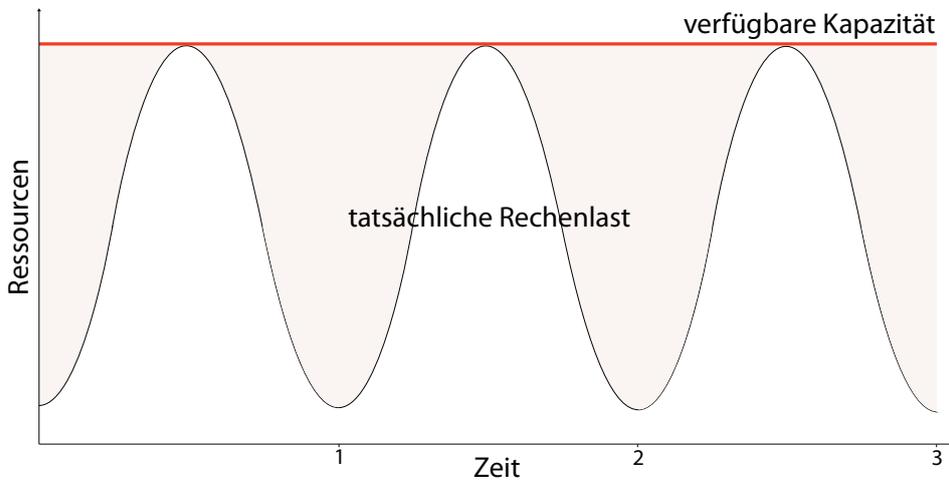


Abbildung 3.3: „Übersorgung“ mit IT-Kapazitäten

Bisher wurde nur der Fall untersucht, in dem die Nachfrage nach dem Dienst „überschätzt“ wurde. Der andere Fall, bei dem die verfügbare Kapazität zur Beantwortung der Anfragen nicht mehr ausreicht, ist wesentlich gefährlicher für Unternehmen. Finanzielle Auswirkungen einer Leistungs-Übersorgung können sehr leicht wie im obigen Beispiel ausgerechnet werden. Bei einer Unterschätzung der Dienst-Nachfrage ist das nicht mehr der Fall. Auslastung der Infrastruktur kann zu längeren Bearbeitungszeiten oder im schlimmsten Fall sogar zum Totalausfall betroffener Dienste führen. Es besteht die Gefahr, dass Kunden aufgrund der schlechten Erfahrung den entsprechenden Dienst in Zukunft nicht mehr in Anspruch nehmen werden.

Ein rasanter Anstieg in der Nachfrage nach einem Dienst ist gar nicht so unwahrscheinlich. Als der Anbieter Animoto seinen Dienst 2008 über Facebook verfügbar machte, musste die Infrastruktur innerhalb von drei Tagen von 50 auf beinahe 3500 Server erweitert werden [14]. Innerhalb von 72 Stunden verzeichnete der Dienst 750.000 neue Nutzer. Am Gipfel der Auslastung wurden bis zu 40 neue Instanzen pro Minute konfiguriert und hochgefahren. Ein derartiger Erfolg konnte kaum vorhergesehen werden. Der Anbieter benötigte diese zusätzlichen Server nur für einen kurzen Zeitraum. Die Bereitstellung des Dienstes über AWS versetzte das Animoto in die Lage, die überschüssigen Instanzen (dem jeweiligen Bedarf entsprechend) ohne weitere Kosten wieder herunterzufahren.

Abbildung 3.4 fasst die im Zusammenhang mit der Kapazitätsplanung stehenden Probleme noch einmal zusammen und verdeutlicht den Vorteil einer elastischen Skalierbarkeit

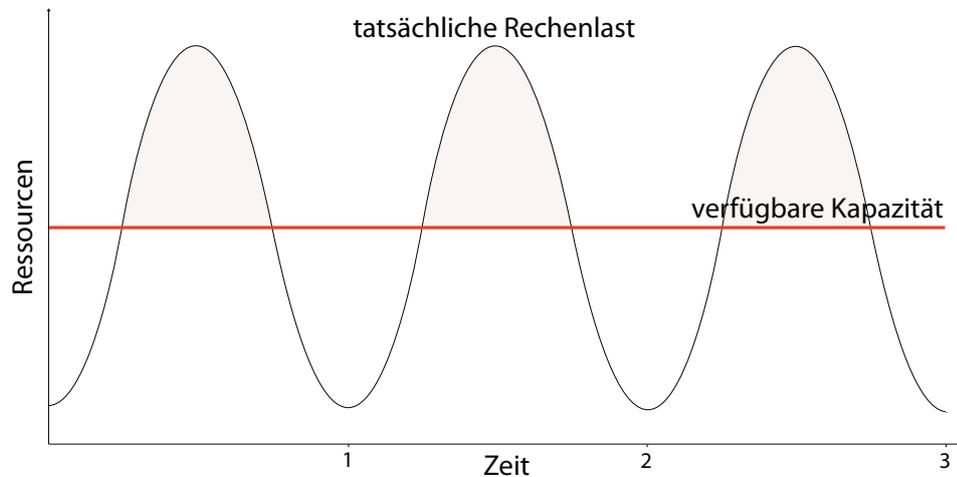


Abbildung 3.4: „Unterversorgung“ mit IT-Kapazitäten

aus der Nutzerperspektive.

Materielle Wertverluste Außer einer flexiblen und dynamischen Anpassung von IT-Ressourcen bietet Cloud Computing zwei weitere Vorteile für den Nutzer. Innerhalb von 3 Jahren verliert Computerhardware mehr als 50% ihres Anschaffungspreises. Mit Cloud Computing können solche Wertverluste vermieden werden. Der Wertverfall der Hardware ist zum Teil darauf zurückzuführen, dass immer neue und leistungsfähigere Geräte auf den Markt kommen. Cloud-Dienstleister profitieren von Vorteilen der Massenproduktion und sind daher in der Lage, neue Trends in der Hard- und Softwareentwicklung (zur Kosteneinsparung) in der eigenen Infrastruktur sehr schnell umzusetzen. Cloud Computing ist ein wettbewerbsintensiver Markt. Immer mehr Anbieter drängen sich auf den Markt und kämpfen um die Gunst der Nutzer. Daher kann davon ausgegangen werden, dass ein Teil der Ersparnisse, die die neuen Technologien bieten, an den Endnutzer weitergereicht wird. In den letzten vier Jahren konnte bei Amazon eine deutliche Reduktion der Kosten für die Benutzung der Web Dienste beobachtet werden (Tabelle). So werden heute für 50 Terabyte Speicher im EU-Raum nur noch 15 (Dollar-) Cent pro Monat [17] berechnet. In 2007 waren es noch 18 (Dollar-)Cent [16]. Auch die Kosten für die Datenübermittlung wurden um drei Cent pro Gigabyte gesenkt.

$$\text{Nutzung}_{\text{Cloud}} \times (\text{Einnahmen} - \text{Kosten}_{\text{Cloud}}) \leq \frac{\text{Nutzung}_{\text{RZ}} \times (\text{Einnahmen} - \text{Kosten}_{\text{RZ}})}{\text{Auslastung}_{\text{RZ}}}$$

Abbildung 3.5: Wirtschaftlichkeit der Nutzung von Cloud-Ressourcen

Höhere Wirtschaftlichkeit Viele Unternehmen setzen bereits Cloud-Anwendungen im Produktivbetrieb ein. Andere bewerten derzeit den Kostenaufwand und Nutzen einer Umstellung der gesamten IT-Infrastruktur auf Cloud-Computing. Die Formel aus Abbildung 3.5 kann bei der Kalkulation aus rein ökonomischer Perspektive helfen:

Auf der linken Seite der Gleichung ergeben sich die Kosten aus der Multiplikation der Nettoeinnahmen mit der tatsächlichen Beanspruchung der IT-Ressourcen. Auf der rechten Seite wird die selbe Berechnung unter Berücksichtigung der tatsächlichen Auslastung der Infrastruktur durchgeführt. Die Gleichung gilt unter der Annahme, dass Cloud-Dienstleister über stundengenaue Abrechnungsmodelle verfügen. Die Seite mit dem größeren Ertrag deutet auf bessere Gewinnmöglichkeiten. Wenn die ständige Auslastung der Infrastruktur bei 100 Prozent liegt, sehen beide Seiten der Gleichung absolut identisch aus. Allerdings besagt der Grundsatz der Bedienungstheorie, dass bei maximaler Auslastung die System-Reaktionszeit gegen Unendlichkeit wächst [4, 9]. Außerdem liegt die tatsächlich nutzbare Kapazität eines Rechenzentrums in der Regel nur zwischen 60 und 80 Prozent [11]. D.h. wenn ein Unternehmen einen 100 Mbit/s Internetzugang mietet, kann die Ressource in der Praxis mit großer Sicherheit nur zwischen 60 und 80 Mbit/s genutzt werden.

3.3 Bedenken

Trotz wirtschaftlicher Vorteile gibt es vor allem für größere Unternehmen mit gewachsenen IT-Strukturen ein Reihe von Bedenken, wenn sie Cloud Computing betreiben wollen.

Fehlende Standards Auf das Problem der fehlenden Standardisierung, das sich in der mangelnden Portabilität und Interoperabilität der Dienste äußert, wurde bereits bei der Vorstellung einzelner Cloud Computing-Konzepte eingegangen. Die Problematik äußert sich unterschiedlich in den verschiedenen Schichten des vorgestellten Modells.

Interoperabilität und Portabilität auf der Infrastrukturebene (IaaS) wirft zwei wichtige Probleme auf. Es betrifft das Format der Images virtueller Maschinen sowie die Konfiguration entsprechender virtueller Ressourcen.

In der Regel wird das Format eines Images von der darunter eingesetzten Virtualisierungslösung bestimmt. Trotz bereits existierenden Standards wie das Open Virtualization Format (OVF) haben Cloud-Anbieter aus verschiedenen Gründen ihre eigenen Formate entwickelt (wie z.B. das bereits erwähnte Amazon Machine Image). Ein Ansatz zur Gewährleistung der Portabilität auf der Infrastrukturebene liegt in der Formatumwandlung. Allerdings ist das eine sehr rechenintensive Operation. Aus diesem Grund akzeptieren einige Service Provider inzwischen mehrere Formate.

Die zweite wichtige Herausforderung besteht in der Inkompatibilität der Management-Schnittstellen. Diese sind für das Hoch- und Herunterladen, die Überwachung und Konfiguration virtueller Maschinen sowie verschiedene andere Aufgaben verantwortlich. Jeder Anbieter hat seine eigenen Schnittstellen, die Orchestrierungs-Anwendungen daran hindern, mit mehreren Dienstanbietern zusammenzuarbeiten. Für dieses Problem gibt es mehrere Lösungsansätze.

So gibt es zum Beispiel interessante Initiativen aus dem Open-Source-Bereich. So implementiert z.B. Eucalyptus Systems⁶ die Amazon-EC2-Schnittstellen als einheitliche API für mehrere Hypervisor um damit den Wechsel von der Amazon-Plattform hin zu einer Open Source-Lösung zu ermöglichen (siehe 4.5.1). Andere Gruppen wie das Open Grid Forum (OGF)⁷ versuchen, mit dem Open Cloud Computing Interface (OCCI)⁸ einen neuen Standard zu definieren. Des Weiteren gibt es noch das Unified Cloud Interface Project⁹, das sich ebenfalls zum Ziel gesetzt hat, eine einheitliche Schnittstelle für diverse Lösungen zu entwickeln.

Für Platform-as-a-Service (PaaS) wiederum stellt Portabilität und Interoperabilität eine größere Herausforderung dar, denn Plattform-Dienste können naturgemäß sehr verschiedene Anwendungsformate umfassen. Windows Azure beispielsweise bietet Datenbank-Dienste und Anwendungs-Container basierend auf der hauseigenen .NET-Plattform. Die Applikationen und Daten in Azure sind somit nicht kompatibel zur Google AppEngine. Die einzige Möglichkeit, eine Abhängigkeit auf Plattformebene zu verhindern ist, ein Framework zu wählen, das von mehreren Providern unterstützt wird. Außerdem sollte auf anbieterspezifische Erweiterungen, wie die von Python, in AppEngine verzichtet werden.

Die größten Interoperabilitätsprobleme gibt es im SaaS-Modell. Dies ist vor allem auf die vorhandene Dienst- und Datenvielfalt zurückzuführen. Auf die damit verbundenen Probleme wurde bereits in Kapitel 3.1.3 eingegangen.

⁶<http://www.eucalyptus.com>

⁷<http://www.gridforum.org>

⁸<http://www.occi-wg.org/doku.php>

⁹<http://code.google.com/p/unifiedcloud>

Anbieter Lock-In Als Lock-In-Effekt werden Kosten bezeichnet, die eine Änderung der aktuellen gebuchten Clouddienstleistungen unwirtschaftlich machen. Das Problem tritt vor allem bei längerer Nutzung der selben Dienste auf. Hier spielt auch die Problematik der fehlenden Standardisierung mit ein. Die Abhängigkeit eines Nutzers wächst mit dem Umfang der Daten, die an einen externen Dienstleister übertragen werden. Dieses Verhalten ist darauf zurückzuführen, dass auch der Datentransfer zum Dienstleister mit Kosten verbunden ist. Sollte ein Dienstanbieter von heute auf morgen seine Preispolitik ändern, können Kunden nicht ohne Weiteres zu einem anderen Anbieter wechseln. Auf der einen Seite ist ein Wechsel des Anbieters mit enormen Kosten allein für die Übertragung der Daten verbunden. Auf der anderen Seite verfügt jeder Anbieter über seine eigenen proprietären Schnittstellen, d.h. bestehende Anwendungen müssten an die APIs des neuen Anbieters angepasst werden. Darüber hinaus gibt es auch keine Garantie, dass der neue Anbieter seine Preisstruktur dauerhaft beibehält.

Sicherheit Mit Cloud Computing wird Unternehmen eine ganze IT-Infrastruktur oder Teile davon als Dienstleistung zur Verfügung gestellt. Die Nutzung solcher Dienste bedingt natürlich auch die Übertragung von Unternehmensdaten zu einem externen Dienstleister über das Internet. Das betrifft auch vertrauliche Daten wie Kundeninformationen, Projektplanung, Buchhaltung, Geschäftsideen, Betriebsgeheimnisse oder juristische Dokumente.

Bevor Informationen dieser Art jenseits der Unternehmensgrenzen gespeichert werden, muss geklärt werden wie potentielle Dienstleister die ihnen anvertrauten Daten schützen. Oft ist dabei noch nicht einmal bekannt (wie z.B. im Falle von Google App Engine), auf welchem Server die Daten der Anwender liegen bzw. an welchem physischen Ort dieser Server steht.

Ein Verlust physischer Kontrolle über die Datenbestände setzt zudem viele herkömmliche Einschränkungen und Schutzmechanismen außer Kraft. Physische Server werden im Cloud-Modell durch virtuelle Instanzen ersetzt. Ein Cloud-Anbieter muss daher in der Lage sein, sowohl die physische als auch die virtuelle Infrastruktur zu schützen. Hierbei spielt die Gewährleistung der Isolation virtueller Instanzen eine besondere Rolle, da die Infrastruktur der Cloud-Anbieter von verschiedenen Prozessen, Anwendungen und Unternehmen gemeinsam genutzt wird.

Große Cloud-Dienstleister veröffentlichen zwar ihre Sicherheitsrichtlinien in denen sie auf die verwendeten Methoden der verteilten Datenspeicherung (für mehr Ausfallsicherheit), Vergabe von Zugangsrechten-, Datenreplikation und Monitoring eingehen. Aller-

dings schliessen sie für gewöhnlich die Möglichkeit eines Besuchs vor Ort aus, bei dem Kunden sich selbst von der Gewährleistung der Informationssicherheit überzeugen können. Die Sicherheit im Cloud Computing ist somit nicht nur eine Frage der Technologie, sondern auch des Vertrauens. Denn selbst, wenn davon ausgegangen werden kann, dass Cloud-Anbieter in der Lage sind, Daten ihrer Kunden vor Zugriffen unberechtigter Dritter zu schützen, müssen Dienst-Nutzer darauf vertrauen, dass ihre Informationsbestände von Cloud-Anbietern nicht für eigene Zwecke missbraucht werden.

Rechtliche Aspekte Neben dem nachvollziehbaren eigenen Interesse der Unternehmen, ihre Informationen zu schützen gibt es bei bestimmten Informationsbeständen klare gesetzliche Vorschriften, wie diese behandelt und gespeichert werden. Branchenstandards und Richtlinien wie HIPPA¹⁰, Payment Card Industry Data Security Standard [19] oder Statement on Auditing Standards 70 [15] legen eindeutige und messbare Sicherheitsbestimmungen fest, mit denen Unternehmen nachweisen müssen, wie Daten verarbeitet und gelagert werden. Im Falle einer so genannten Auftragsverarbeitung muss ebenfalls festgelegt werden, wo und von wem die Daten verarbeitet werden. Dabei muss auch die lastabhängige Verteilung berücksichtigt werden, denn eine grenzüberschreitende Datenverarbeitung kann durchaus nicht zulässig sein. Bei Regelverstößen bleibt der Auftraggeber, also der Dienst-Nutzer als „Herr der Daten“ gesetzlich verantwortlich.

So hat beispielsweise das deutsche Datenschutzrecht den Schutz personenbezogener Daten zum Gegenstand. Dieses gilt für jeden in Deutschland stattfindenden Vorgang der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten. Da die Datenschutzrichtlinien innerhalb der EU weitgehend vereinheitlicht sind, gelten bei einem Datentransfer innerhalb deren Grenzen grundsätzlich keine Besonderheiten gegenüber einer rein innerdeutschen Speicherung. Anders ist dies, wenn Daten in Länder außerhalb der EU übermittelt werden.

Cloud-Anbieter versuchen, eine sichere Umgebung zu liefern, doch die Verantwortung für den sicheren Umgang mit Daten liegt bei den Unternehmen, die den Dienst nutzen. Amazon weist beispielsweise jegliche Garantie für die Sicherheit der in der Cloud gespeicherten Daten von sich und betont diesen Punkt in den Kundenvereinbarungen für seine Dienste. Damit steht das Unternehmen nicht allein da. Die meisten Cloud-Anbieter schließen die Gewährleistung der Sicherheit aus, die über die Überprüfung des Sicherheitspersonals und die Sicherstellung der Basis-Perimetersicherheit der IT-Landschaft hinaus geht.

¹⁰Health Insurance Portability and Accountability

Zuverlässigkeit und Verfügbarkeit IT-Systeme, die zentrale Unternehmensprozesse unterstützen, müssen sicher, zuverlässig und hochverfügbar sein. Dabei ist Zuverlässigkeit eine der wichtigsten Vorteile des Cloud-Computing-Modells. Denn beim Cloud Computing werden Netzwerk-, Verarbeitungs- und Speicherfunktionen auf eine sehr große Basis physischer und virtueller Ressourcen verteilt. Theoretisch soll dadurch eine wesentlich höhere Toleranz gegenüber einzelnen Hardware-Ausfällen erreicht werden. In der Vergangenheit kam es allerdings immer wieder zu Aufsehen erregenden Ausfällen diverser Cloud-Computing Dienste, so zum Beispiel im Februar 2008 bei Amazons S3. Hier kam es zu einem zweistündigen Ausfall des kompletten Speicherdienstes [20]. Wenige Monate später gab es einen weiteren Störfall, dieses Mal war der S3-Dienst über acht Stunden nicht erreichbar [23]. Aber auch andere Anbieter sind von solchen Vorfällen nicht verschont geblieben. Anfang Oktober 2009 kam es bei dem Mobiltelefon-Service Sidekick (T-Mobile USA) zu einem Zwischenfall, bei dem Sidekick-Telefonkunden ihre persönlichen Daten einschließlich Kontaktnamen, Telefonnummern und digitale Fotos verloren haben.

Die meisten Cloud-Angebote handeln auf der Basis des „Best Effort“. Vorfälle solcher Art zeigen deutlich, dass Hochverfügbarkeit eine große Herausforderung an Cloud Computing-Systeme darstellt. Unternehmen können zwar im Vorfeld ihre Erwartungen an die Dienstgüte (wie z.B. Verfügbarkeit oder Erreichbarkeit) in Service Level Agreements (SLA) vereinbaren, diese genügen aber in der Regel nicht den Geschäftsanforderungen. Im Falle von Störungen oder Ausfällen gibt es meist nur eine entsprechende Gutschrift. Strafen oder Schadensersatz für Ausfälle sind nicht vorgesehen.

So definiert beispielsweise Amazon in den SLA für seine EC2 und S3 Dienste, dass ein Kunde 10 Prozent der Gebühren für die letzten 365 Tage zurückerstattet bekommt, wenn die Verfügbarkeit unter 99,95 Prozent fällt¹¹. Dabei wird die Zurückerstattung ausschliesslich für zukünftige Gebühren gut geschrieben.

Eine Möglichkeit, die Zuverlässigkeit der Datenverarbeitung zu erhöhen, besteht in der Verteilung der Anwendungen auf mehrere Dienst-Anbieter. Einige Anwendungsfälle – etwa Datenspeicher – können sich für einen solchen verteilten Ansatz gut eignen, während andere wiederum sich nur schwer verteilen lassen.

Jedes Unternehmen sollte sich daher vor der Auslagerung der Daten an einen externen Anbieter darüber bewusst werden, was passiert, wenn die Verbindung zum Dienstleister plötzlich abbricht und die Mitarbeiter keinen Zugriff auf die Daten bzw. Services haben.

¹¹Eine Verfügbarkeit von 99,95% entspricht einer Ausfallzeit von ca. 4,38 Stunden pro Jahr

3.4 Zusammenfassung – Cloud Computing

Die Frage nach dem besseren Modell ist nicht einfach zu beantworten und hängt stark vom jeweiligen Anwendungsszenario ab. Die Unterschiede in den Ansätzen lassen sich anhand eines Vergleichs zwischen Maschinensprachen, höheren Programmiersprachen und Web-Frameworks veranschaulichen. Maschinensprachen wie Assembler ermöglichen eine sehr hardware-nahe Softwareentwicklung. Andere Programmiersprachen wie Java bieten ein höheres Maß an Abstraktion und erlauben insgesamt mehr Logik mit weniger Text auszudrücken. Entwicklung moderner Webanwendungen kann eine weitere Abstraktionsstufe erfordern. Denn der Umgang mit Sockets¹², das Abfertigen von Datenbankabfragen usw. selbst mit guten Bibliotheken kann sehr umständlich sein. In bestimmten Anwendungsfällen können Frameworks wie Spring die Programmierung vereinfachen, indem sie Entwickler von technischen Details befreien.

Wer also die vollständige Kontrolle über einen Mikroprozessor anstrebt, muss auf Maschinen- oder Assemblersprachen zurückgreifen. Web-Frameworks sind nur dann wirklich hilfreich, wenn eine hohe web-orientierte Abstraktion gefragt ist. Die Überlegenheit von Java gegenüber solchen Frameworks bei bestimmten Programmieraufgaben ist unbestreitbar, das gilt umgekehrt genauso.

Beim Transfer dieser Analogie aus der Welt der Programmiersprachen zurück auf die unterschiedlichen Modelle des Cloud-Computing, wird deutlich, dass unterschiedliche Problemstellungen und Anforderungen seitens der Anwender auch unterschiedliche Lösungen seitens der Cloud-Dienstleister begünstigen.

Der Ansatz von Amazon bietet eine sehr hohe Flexibilität allerdings liegt es in der Verantwortung der Nutzer, sich um die Skalierung eigener Anwendungen zu kümmern. Bei Google App Engine werden keine virtuellen Images verwaltet, sondern Web-Anwendungen. Bei steigender Nachfrage erhöht die Plattform die Anzahl der Prozesse der eigenen Anwendung dynamisch. Der Entwickler braucht sich um die Skalierung nicht zu kümmern. Das Angebot von Google ist somit nicht so individuell gestaltbar wie das von Amazon, es erfordert aber deutlich weniger Administrationsaufwand. Welches Konzept für das eigene Unternehmen am besten geeignet ist, kann nur den internen Anforderungen entsprechend entschieden werden.

¹²Ein Socket ist eine bidirektionale Software-Schnittstelle zur Interprozess- oder Netzwerk-Kommunikation

4 Marktübersicht: Virtualisierungstechnologie

Im Folgenden werden einige Produkte und Lösungen zu den im Abschnitt 2 eingeführten Virtualisierungstechnologien der wesentlichen Hersteller aufgeführt. Hierbei handelt es sich insbesondere um die Produktfamilien von Citrix, Microsoft und VMware, die jeweils für alle Virtualisierungsvarianten eine Lösung anbieten. Zudem werden kurz einige weitere Produkte anderer Anbieter aufgeführt, die einen speziellen Fokus haben. Abschließend werden einige bewährte Open Source-Projekte aufgeführt, die teilweise eng mit den kommerziellen Produkten zusammenhängen (bspw. im Fall von Citrix und Xen).

4.1 Citrix

Ursprünglich ist Citrix in erster Linie mit Applikations- und Terminalserver-Produkten bekannt geworden, das Unternehmen hat also große Expertise im Bereich der Präsentationsvirtualisierung. Das hat zur Folge, dass mittlerweile oftmals der Name der Firma Citrix bzw. die frühere Bezeichnung des Presentation Servers – Citrix Metaframe – als Synonym für eine solche Anwendung verwendet wird. In den letzten Jahren hat Citrix jedoch sein Produktportfolio durch eine Virtual Desktop Infrastructure Lösung (*XenDesktop*) erweitert und mit dem Zukauf von XenSource auch den Schritt auf den Markt für Servervirtualisierung gemacht. Die zentralen Produkte aus dem Bereich der Virtualisierung von Citrix sind demnach *XenApp*, *XenDesktop* und *XenServer*.

XenApp Mit XenApp realisiert Citrix nicht nur die Präsentations- und Applikationsvirtualisierung, sondern auch Verteilung und den Zugriff auf die Anwendungen von beliebigen (virtuellen) Anwender-Desktops.

Die Marktführerschaft von Citrix im Bereich Terminal Computing lag insbesondere am selbstentwickelten ICA-Protokoll (*Independent Computing Architecture*). Dieses Kommunikationsprotokoll regelt den Austausch zwischen Client und Applikationsserver und ist dabei sehr effizient: im Gegensatz zu anderen Remote Desktop-Protokollen wie Microsofts RDA, X11 oder das freie VNC (Virtual Network Computing) benötigt ICA sehr wenig Bandbreite bei der Nutzung entfernter Anwendungen und kann selbst über eine GPRS-Verbindung von mobilen Endgeräten oder Laptops performant genutzt werden.

Heute liegt die Stärke von XenApp in der Flexibilität. Anwendungen aus dem zentral gepflegten Application Repository können sowohl von Thin Clients auf dem Server genutzt (klassische Anwendungsverteilung), als auch gestreamt werden. Anwendungen, die per Application Streaming verteilt werden, können auch ohne permanente Netzwerkverbindung genutzt oder dynamisch in virtuellen Desktops verfügbar gemacht werden.

XenDesktop und XenClient Für den Betrieb von Virtual Desktop Infrastructures hat Citrix *XenDesktop* im Programm. Das Konzept von XenDesktop trennt Betriebssystem, Anwendungen und Benutzereinstellungen (Profile, siehe Abbildung 4.1). Dieses Konzept ermöglicht es, beliebig viele virtuelle Desktops von einem Standard-Desktop-Image zu booten. Erst im zweiten Schritt werden die Applikationen mit Hilfe der Applikationsvirtualisierung den jeweiligen Benutzer-Desktops bereitgestellt. Gleichzeitig lädt der virtuelle Desktop die ebenfalls separat vorgehaltenen persönlichen Benutzereinstellungen.

So wird für den Benutzer bei der Anwendung on Demand eine individuelle Desktop-Umgebung generiert. Die Anwender können bei jedem Start einen “frisch aufgesetzten” IT-Arbeitsplatz nutzen, während die Administratoren nur noch eine geringe Anzahl von Standard-Desktop-Images managen müssen. Dieses Verfahren senkt den Wartungsaufwand und den Storage-Bedarf im Rechenzentrum erheblich, verglichen mit einer Lösung, die jeweils Desktop-Images für jeden Benutzer verwalten würde.

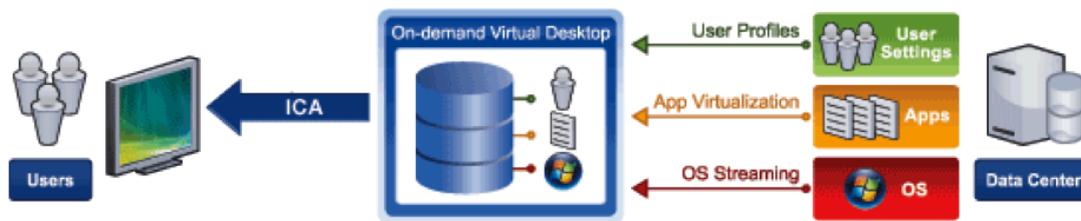


Abbildung 4.1: Virtual Desktop Infrastructure mit XenDesktop, Quelle: [22]

Arbeitsplätze, die mit XenDesktop verteilt werden, lassen sich zur Zeit allerdings nur mittels Remote Desktop Client nutzen – also nur mit vorhandener Netzwerkverbindung. Der Offline-Betrieb virtueller Desktops wird erst mit der Einführung von XenClient möglich: diese Clientsoftware ermöglicht das Streaming virtueller XenDesktops auf physikalische Computer und damit auch den Offline-Betrieb. Citrix kündigte *XenClient* bereits 2009 als “erste und einzige Client-Virtualisierung mit 100% Separation der virtuellen Maschinen voneinander” [21, vgl.] an.

XenServer, Citrix Essentials und XenServer MP Zur Servervirtualisierung bietet Citrix neben *XenServer* das Management-Tool *Citrix Essentials* an. XenServer ist aus dem Open Source-Paravirtualisierer *Xen* entstanden und wird auch heute von Citrix zum kostenlosen Download¹ angeboten.

Xen implementiert – wie alle modernen Hypervisor – die Funktionen der Hardware-gestützten Virtualisierung (Intel VT bzw. AMD-v) und kann damit jegliches Betriebssystem als Gast in virtuellen Maschinen aufnehmen. Linux-Systeme mit paravirtualisierten Kernen können zur Performanzverbesserung auch direkt mit dem Hypervisor interagieren. Citrix Essentials ist das korrespondierende Management Tool, das den Betrieb komplexer virtualisierter Server-Infrastrukturen erst sinnvoll ermöglicht. Mit Essentials

¹<http://www.citrix.com/xenserver/download/>

können alle vorhandenen physikalischen Xen-Server zentral administriert werden. Dazu gehören unter anderem

die dynamische Zuweisung von Ressourcen (Storage, Speicher, CPUs), also auch die Migration von laufenden Systemen zwischen verschiedenen Xen-Servern,

Unterstützung beim *Stage Management*, dem dynamischen Integrieren, Testen und Verteilen neuer Anwendungen (bzw. Versionen) in laufende Systeme,

flexibles, teil-automatisiertes *Lab Management* zum Betrieb von Test- und Entwicklungsinfrastrukturen,

oder rudimentäre Hochverfügbarkeitsunterstützung, die automatisiert virtuelle Maschinen auf einem ausgefallenen physikalischen Host auf einem anderen Xen-Server neu startet.

Essentials ist nicht nur für den XenServer verfügbar, sondern kann auch virtuelle Maschinen verwalten, die in Microsofts Hyper-V laufen.

Zudem gibt es mit *XenServer MP (Xen Management Pack for Microsoft System Center Operations Manager)* eine passende Erweiterung für ein eventuell vorhandenes Microsoft System Center und damit die Integration in bewährte (ITIL²-basierte) Prozesse im Rechenzentrum.

²ITIL – IT Infrastructure Library, Sammlung von bewährten Praktiken zur Umsetzung von IT-Service-Management

4.2 Microsoft

In den letzten Jahren hat auch Microsoft durch Entwicklungsentscheidungen und strategische Einkäufe immer wieder die wachsende Bedeutung der Virtualisierungstechnologie unterstrichen. Der Desktop-Virtual Machine Monitor *Virtual PC* stammt aus der Akquisition von Connectix, Microsofts Lösung für die Applikationsvirtualisierung *App-V* (vormals SoftGrid) und wurde 2006 mit der Firma Softricity eingekauft. Der Hypervisor für den Serverbetrieb – *Hyper-V* – ist seit Windows Server 2008 essentieller Bestandteil des Betriebssystems.

Die bekannten Lösungen zur Präsentationsvirtualisierung von Microsoft – *Windows Terminal Services* bzw. *Remote Desktop Access* – werden hier nicht weiter ausführlich betrachtet.

Hyper-V und Windows Server 2008 Microsofts aktuelle Hypervisor-Lösung ist im Gegensatz zum Vorgänger – Microsoft Virtual Server 2005 – ein Bare-Metal Hypervisor, läuft also direkt auf der Hardware und nicht innerhalb eines Host-Betriebssystems. In der Standard-Installation von Windows Server 2008 läuft das Betriebssystem immer in einer sogenannten Partition, einem Container für virtuelle Maschinen – auch dann, wenn man nur eine einzelne Instanz des Windows Servers auf der Maschine nutzt und die Virtualisierung nicht nötig wäre. Die erste Instanz eines Betriebssystems auf einem Windows Server heißt *Parent Partition*. In dieser werden Tools installiert, mit der weitere virtuelle Maschinen angelegt und verwaltet werden können. Für den Betrieb in Rechenzentren kann Windows Server 2008 auch in einer *Server Core* Variante installiert werden. Hier gibt es keine Parent Partition, und kein graphisches Benutzerinterface auf dem eigentlichen physikalischen Server. Die virtuellen Maschinen werden entfernt verwaltet, etwa mit den passenden Erweiterungen für das Microsoft System Center, etwa dem Hyper-V Management Paket für *Operations Manager 2007* bzw. *Configuration Manager 2007 R2* oder dem *System Center Virtual Machine Manager 2008*. Der Virtual Machine Manager wird für den Betrieb von Windows Server 2008 im Core Server Modus benötigt und kann auch virtuelle Maschinen auf *VMware ESX* Servern integriert verwalten.

Auch in Hyper-V-Installationen mit mehreren Servern (Cluster-Betrieb) können wie beim XenServer virtuelle Maschinen dynamisch verteilt werden oder neue Ressourcen zugewiesen bekommen. Neben weiteren Instanzen des Windows Server 2008 selbst kann Hyper-V auch verschiedene, zertifizierte Linux-Distributionen (z.B. SuSE Enterprise Linux) als Gastbetriebssystem aufnehmen, mit der Erweiterung um die *Linux Integration Components* können die Linux-VMs auch mit paravirtualisierten Kernen betrieben wer-

den.

Hyper-V zielt klar auf die Virtualisierung von Windows Servern in einer integrierten Microsoft-Infrastruktur mit System Center (Operations Manager) ab und ist hierfür auch eine optimale Lösung. Der Betrieb von Client-Betriebssystemen auf Hyper-V Servern in Virtual Desktop Infrastructures ist kritisch zu prüfen: lediglich für das in Unternehmensumgebungen kaum eingesetzte Windows Vista gibt es derzeit umfassende Unterstützung für Peripheriegeräte und Multimedia. Zudem können lediglich komplette Instanzen dieser Client-Betriebssysteme in einer VM betrieben werden und benötigen jeweils ein komplettes Festplatten-Image – im Gegensatz zu XenDesktop.

Virtual PC 2007 Das Produkt zur Desktop-Virtualisierung von Microsoft, *Virtual PC 2007*, ist ein klassischer Virtual Machine Monitor, läuft also auf einem Desktop Betriebssystem wie Windows Vista oder XP und leidet dementsprechend unter deutlichen Performance-Verlusten. Offiziell werden als Gastssysteme alle 16- und 32-Bit Windows-Varianten und OS/2 Warp unterstützt, aber auch die gängigen Linux-Distributionen laufen in diesen virtuellen Maschinen.

Virtual PC wird für den Betrieb von großen IT-Systemen primär in Verbindung mit den anderen Produkten von Microsoft interessant (siehe *Microsoft Enterprise Desktop Virtualization – MED-V*).

Microsoft Application Virtualization (App-V) Wie schon beschrieben, dient die Applikationsvirtualisierung zur Entkopplung von Anwendungen und Betriebssystem. So sollen Konflikte zwischen unterschiedlichen Anwendungen oder der mehrfachen Installation einer Anwendung in verschiedenen Versionen vermieden werden, die dadurch entstehen, dass gemeinsam genutzte Teile des Betriebssystems nur für jeweils eine Anwendung passen. Microsofts *App-V* erstellt bei der Installation von Software als virtuelle Anwendung einen Container, in den alle gemeinsam genutzten Anteile als Applikations-spezifische Kopie abgelegt werden. Hierbei unterstützt ein *Sequenzier-Tool* den Systemadministrator.

Auf dem Client (oder Terminal Server), auf dem diese virtualisierten Applikationen dann ausgeführt werden, ist ein passender *App-V Client* installiert, der zur Laufzeit den virtuellen Anwendungen die passenden Ressourcen aus dem Container zur Verfügung stellt. Gleichzeitig können auch native Anwendungen konfliktfrei auf dem gleichen Arbeitsplatz genutzt werden.

Virtualisierte Anwendungen werden auf einem *Application Virtualization Management*

Server abgelegt und können im System Center verwaltet werden (integriert auch mit Systems Center Configuration Manager). Dort können auch Zugriffsrechte auf die Anwendungen mit einem existierenden Active Directory verknüpft werden. Von diesem Server werden die Anwendungen auch auf den Client gestreamt (Application Streaming).

Auf dem Client werden solche Anwendungen in einem *App-V Cache* vorgehalten. Bei jedem Start der Anwendung überprüft App-V, ob auf dem Server eine neue Version der Applikation vorliegt und lädt diese gegebenenfalls nach. Anderenfalls wird die Anwendung direkt aus dem Cache gestartet. Auch bei fehlender Netzwerkverbindung wird so vorgegangen, ein Offline-Betrieb der gestreamten Applikation ist also möglich.

Microsoft Enterprise Desktop Virtualization (MED-V) Das Konzept des Application Streaming erweitert Microsoft mit MED-V zu einem Streaming ganzer virtueller Maschinen. Clients, auf denen Virtual PC 2007 installiert ist, können vorkonfigurierte Arbeitsplatz-VMs von einem MED-V Server beziehen. Dieser hält eine Reihe von VM-Images für verschiedene Einsatzzwecke vor.

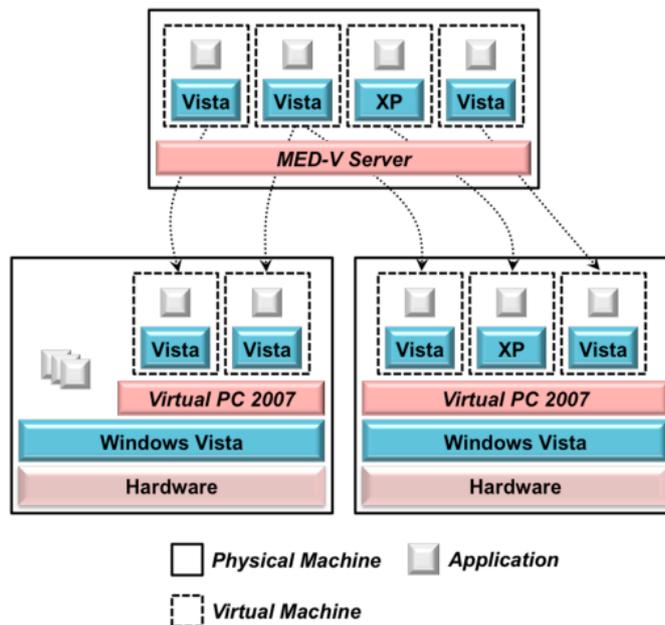


Abbildung 4.2: Enterprise Desktop Virtualization (MED-V), Quelle: [3]

Auf dem Desktop des Benutzers werden diese virtuellen Maschinen transparent (oder “seamless”) betrieben. Das bedeutet, dass die Anwendungen in den VMs, die auf den

Arbeitsplatz gezogen wurden, per Remote Desktop Client zugegriffen werden und für den Anwender auf dem nativen Desktop der Arbeitsstation transparent genutzt werden können. Daneben können auch weitere lokale Anwendungen genutzt werden, ohne dass der Anwender sich über diese Unterscheidung bewusst sein müsste (siehe Abbildung 4.2, unten links). Auch können Anwendungen aus verschiedenen, eigentlich inkompatiblen Betriebssystemen auf dem gleichen Desktop genutzt werden (Abbildung 4.2, rechts).

MED-V stellt damit im Sinne der Virtual Desktop Infrastructure partiellen Desktops zur Verfügung – erst die Kombination aus lokalem System, virtuellen Maschinen und Präsentationsvirtualisierung erzeugt das komplette Client-System. Konsequenterweise können diese partiellen Desktops, die mit den MED-V VMs zur Verfügung gestellt werden, zentral aus dem System Center administriert werden.

4.3 VMware

Der Marktführer im Bereich Servervirtualisierung hat neben einer Reihe an Hypervisor-Produkten (*VMware Server*, *ESX*, *ESXi*) eine große Menge von Produkten für Management, Ausfallsicherheit, Live-Migration und vieles mehr kompiliert als verschiedene Varianten von *Virtual Infrastructure*- und *VMware vSphere*-Editionen. *Virtual Infrastructure* stellt verschiedene Pakete aus Hypervisor- und Management-Software dar, VMware selbst nennt die *vSphere-Suite* das hauseigene Betriebssystem für privates Cloud Computing.

Neben Produkten zur Servervirtualisierung bietet das Unternehmen mit *VMware View* eine VDI-Lösung und hat mit *ThinApp* einen Applikationsvirtualisierer im Angebot.

Des Weiteren gibt es eine Reihe von Produkten, die in erster Linie für den Einsatz im Privatbereich gedacht sind – so etwa *VMware Workstation* oder *VMware Fusion* – die hier nicht näher betrachtet werden sollen.

VMware Server und VMware Server ESX Den Kern der Produktpalette von VMware für den Einsatz im Serverbereich bilden die Hypervisor *VMware Server* (vormals *Server GSX*) und *VMware Server ESX*.

Der kostenlose VMware Server ist als Komplettpaket für Einsteiger oder den semi-professionellen Betrieb gedacht und ist ein Virtual Machine Monitor (verfügbar für die Host-Betriebssysteme Windows und Linux). VMware Server unterstützt alle gängigen Betriebssysteme als Gast (“Volle Virtualisierung”) und kann die CPU-Virtualisierung von Intel und AMD nutzen. Außerdem unterstützt VMware Paravirtualisierung für Linux-Kernels. Der VMware Server bringt eine Web-basierte Management-Oberfläche mit und kann über Webservices verwaltet werden.

Für den Einsatz im Rechenzentrum und im großen Maßstab ist der VMware Server ESX vorgesehen. ESX unterstützt dabei alle Virtualisierungsvarianten, die auch der freie Server bietet. Der ESX Server ist ein Bare Metal-Hypervisor mit einer sehr schlanken und zuverlässigen Architektur. Einen großen Teil der Zuverlässigkeit erreicht VMware, indem die Hardware, die für den ESX Server zertifiziert ist, relativ eingeschränkt ist: der Hypervisor läuft nur auf bestimmten Hardware-Plattformen aus dem professionellen Segment.

Neben der kostenpflichtigen Variante ESX gibt es auch den kostenlosen Bare Metal-Hypervisor ESXi. Die Varianten unterscheiden sich neben den Lizenzmodellen insbesondere in den Management-Features: der ESXi-Server kann ohne *vCenter Server* oder *vSphere Client* nicht im Rechenzentrums-Betrieb genutzt werden.

VMware Virtual Infrastructure *Virtual Infrastructure (VI, vormals Virtual Center)* bezeichnet eine Reihe von Paketen, die jeweils den ESX/ESXi als Hypervisor mitbringen. Zudem kommen je nach Edition noch eine Reihe von Tools für Verwaltung und weitere Funktionalitäten hinzu.

In der Foundation-Version sind zentrales Management (mehrerer ESX/ESXi Server), zentrale Updates und konsolidiertes Backup möglich. In der Standard-Edition kommt zusätzlich das *High Availability*-Paket hinzu. Erst die Enterprise-Variante bringt auch die Pakete (*VMotion* und *Storage VMotion*) zur Live-Migration virtueller Maschinen zwischen verschiedenen ESX Servern und Tools zum automatisierten Ressourcen- und Energiemanagement (*DRS, DPM*) mit. Ein Teil der Funktionalitäten aus diesen Komplettpaketen (Update Management, High Availability, Live Migration) setzt den Einsatz des *vCenter Servers* voraus.

VMware vCenter Unter dem Namen vCenter fasst VMware eine Reihe von Verwaltungstools für die Virtual Infrastructure zusammen. Kernkomponente ist der vCenter Server, der auch für Management und Monitoring mehrerer ESX/ESXi-Server benötigt wird.

vCenter Converter (Assistent zur Konvertierung von physikalischen Systemen zu virtuellen Maschinen)

vCenter Lab Manager (Virtual Lab Management, einfache Verwaltung virtualisierter Test- und Entwicklungsumgebungen)

vCenter Lifecycle Manager (Unterstützung bei Lifecycle-Management für virtuelle Maschinen von Anforderung und Erstellung bis Ausserbetriebnahme)

vCenter Site Recovery Manager (dedizierte Unterstützung bei der Disaster Recovery Planung und Durchführung)

vCenter Orchestrator (automatisierte Workflows in vCenter)

vCenter ConfigControl, vCenter CapacityIQ, vCenter AppSpeed, etc.

VMware bietet also mit der vCenter-Suite ein umfangreiches, konfigurierbares Paket für den Betrieb komplexer virtueller Server-Infrastrukturen. Insbesondere für den Einsatz in Unternehmen mit definierten Workflows oder dynamischen Anforderungen an IT Systeme (wie z.B. Infrastruktur-Provider) ist daher VMware die Servervirtualisierung der Wahl. Zudem integriert der ESX/ESXi-Server in einer Microsoft-Umgebung mit dem *Microsoft System Center Virtual Machine Manager 2008* als zusätzliche Monitoring- und

Management-Schnittstelle. Der vCenter Server kann an zentrale Microsoft-Dienste wie *Active Directory* angebunden werden.

VMware vSphere vSphere ist ebenso wie *Virtual Infrastructure* ein Paket aus Software-Komponenten um die Hypervisor ESX/ESXi und die vCenter Management-Suite (siehe Abbildung 4.3) und als der designierte Nachfolger von VI anzusehen.



Abbildung 4.3: Komponenten der VMware vSphere Infrastruktur, Quelle: [5]

VMware begegnet mit vSphere dem aktuellen Trend des Cloud Computing. Eine vSphere-Infrastruktur kann daher im Gegensatz zu VI virtuelle Maschinen auch über das Internet einbinden und zum Beispiel Ressourcen aus einer externen Cloud (z.B. Public Cloud) einbinden – ohne die Sicherheit der internen virtuellen Maschinen zu gefährden.

Wie die Virtual Infrastructure-Suite gibt es vSphere in einer Reihe von Editionen für kleine und mittlere sowie für große Unternehmen. Ab der Advanced-Edition kommt vSphere mit einer *Fault Tolerance*-Option, und ist damit derzeit die einzige Lösung, die echte *Continuous Availability* ermöglicht. Der Unterschied zur Hochverfügbarkeit ist der, dass HA letztlich nur Garantien über maximale Ausfallzeiten macht, während bei Continuous Availability tatsächlich die permanente Verfügbarkeit des Servers gewährleistet werden kann. Das Fault Tolerance-Paket in vSphere sorgt dafür, dass von Servern,

die auf diese Weise verfügbar sein sollen, jeweils eine Schattenkopie auf einem anderen physikalischen ESX Server vorgehalten wird. Jede Operation auf dem primären virtuellen Server wird gleichzeitig auch in der Schattenkopie nachvollzogen – sowohl für Festplattenaktivitäten als auch für das Speicherabbild. Bei Ausfall des primären Servers übernimmt der Schatten-Server übergangslos.

VMware ThinApp *ThinApp* ist die das VMware-Alternative zur Applikationsvirtualisierung und gehört erst seit 2008 zum Produktportfolio. Vorher wurde die Software als *ThinInstall* von Jitit entwickelt, die von VMware aufgekauft wurden.

Applikationsvirtualisierung funktioniert bei ThinApp im Gegensatz zu den bisher aufgeführten Produkten ohne Client-seitigen Agenten, der die Ausführung der virtualisierten Applikation steuert und überwacht. Stattdessen wird die Anwendung dabei in eine einzelne, in sich geschlossene EXE-Datei (oder MSI) gepackt, welche dann selbständig ausführbar ist. Dadurch ist es möglich, verschiedenste Softwareanwendungen ohne eine örtlich gebundene bzw. umständliche Installation auf Client-PCs oder Servern zu nutzen.

Zudem ist die so virtualisierte Applikation “footprint-free”, d.h. sie hinterlässt keine Einträge in der Registrierungsdatenbank und es werden keine DLL-Dateien auf dem Client erstellt. Alle zur Ausführung erforderlichen Informationen und benötigten Bibliotheken sind in dem virtuellen Container enthalten. Benutzereinstellungen und erstellte Dokumente werden in einer erstellbaren Sandbox gespeichert.

Die von ThinApp erstellte EXE-Datei kann sowohl über ein Netzwerk als auch mit wiederbeschreibbaren Speichermedien z.B. USB-Stick genutzt werden, eine Nutzung auf mehreren unterschiedlichen Rechnern ist so einfach möglich. Die Notwendigkeit für Application Streaming oder Provisioning wie in anderen gemanagten Applikationsinfrastrukturen besteht daher so nicht.

Lizenzmanagement kann mit ThinApp direkt nicht betrieben werden, hierfür benötigt man zusätzlich Software wie z.B. *SoftwareKey Metering for VMware*³.

VMware View *VMware View* (vormals *VMware VDI*) ist die *Virtual Desktop Infrastructure* passend zu *vSphere*. View bietet dabei wie die Konkurrenz zentralisiertes Desktop-Management mit virtuellen Arbeitsplätzen, automatisches Provisioning, komfortable Wartung der zentralen Desktop-Images (es können bspw. Änderungen an einem Master-Image vorgenommen werden, die dann an alle davon abgeleiteten Images und deren laufende Instanzen automatisiert deployed werden), dedizierte Unterstützung von

³<http://www.softwarekey.com/metering-system/>

Thin Clients und enge Integration mit ThinApp.

Insbesondere im Zusammenspiel mit vSphere und ThinApp ist VMware View eine interessante Lösung für den Betrieb von Enterprise Desktops (siehe Abbildung 16).

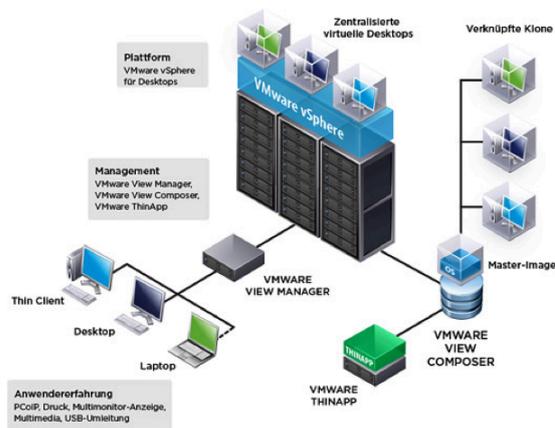


Abbildung 4.4: Komplexe Virtual Desktop Infrastructure mit VMware, Quelle: [7]

Eine wichtige Einschränkung ist allerdings, dass View – genau wie die Microsoft VDI-Lösung – offiziell nur das Provisioning von Online-Desktops leisten kann. Eine Möglichkeit, virtuelle Desktops offline zu betreiben (wie mit XenClient), ist derzeit zwar in der Entwicklung, aber momentan nur experimentell verfügbar und damit für den produktiven Unternehmenseinsatz nicht geeignet.

4.4 Weitere Anbieter

Neben den gerade vorgestellten, großen Anbietern, die ganzheitliche Lösungen für den Betrieb virtueller Infrastrukturen versprechen, gibt es auch eine Reihe von Virtualisierungsprodukten mit speziellen Einsatzbereichen. Einige der bekannteren werden hier nur kurz aufgelistet:

Integrity Virtual Machine (IVM) von Hewlett-Packard, wird in erster Linie zum Partitionieren von HP-Servern mit HP-UX Betriebssystem verwendet

Oracle VM, basiert auf dem Xen-Projekt und ist als Hypervisor für Oracle Enterprise Installationen gedacht

PowerVM, Partitionierung für IBM Power4/5/6 Betriebssysteme

Virtuozzo von Parallels, Betriebssystemvirtualisierung (Container), basiert auf dem quelloffenen OpenVZ-Projekt

z/VM, Hypervisor für die IBM z/Series

Den Einsatz von Plattform-spezifischen Virtualisierungslösungen wie bspw. *IVM* oder *z/VM* kann die Bindung an eben diese speziellen Hardwareplattformen erfordern. Parallels *Virtuozzo* kann eine interessante (da kostengünstige und performante) Alternative für den Betrieb von virtualisierten Clients in einer Virtual Desktop Infrastructure sein.

Ein interessantes Produkt im Bereich Präsentationsvirtualisierung bietet die Firma *NoMachine!* mit dem *NX Server* an. *NX* ist eine Remote Desktop-Technologie, die sowohl mittels Microsoft RDP, als auch mit den Protokollen VNC oder X11 Remote Desktop Sessions zur Verfügung stellen kann und dabei sehr stark komprimiert. *NX*-Desktops können daher auch über schmalbandige Verbindungen (wie GPRS) genutzt werden.

4.5 Open Source Projekte

Weiterhin existiert im Virtualisierungsbereich eine Reihe von Open Source Projekten, die wegen fehlendem Herstellersupport für den produktiven Einsatz im Unternehmen nur bedingt geeignet sind.

Hervorzuheben sind hier zum einen *Xen* (von Citrix kommerziell vertrieben) als Hypervisor mit Paravirtualisierung oder das Paket aus *QEMU*, *KVM* und *libvirt*, die gemeinsam ein Hypervisor-Paket mit voller Virtualisierung sowie VT-Unterstützung anbieten.

Die Open Source Virtualisierungspakete können durchaus in kleinerem Rahmen für Testsysteme oder Nischenanwendungen auch in Rechenzentren genutzt werden, jedoch muss das Know-How für Installation, Konfiguration und Management aus der jeweiligen Projektdokumentation zusammengetragen werden.

4.5.1 Open Source Cloud Computing Plattformen

Einschränkungen in der Standardisierung und Portabilität kommerzieller Angebote für Cloud Computing-Infrastrukturen haben diverse Open Source Initiativen ins Leben gerufen. Im Folgenden werden einige dieser offenen Softwarelösungen für Cloud Computing vorgestellt.

Eucalyptus Bei der *Elastic Utility Computing Architecture for Linking Your Programs To Useful Systems (Eucalyptus)*⁴ handelt es sich um eine Open Source Software zum Aufbau skalierbarer Cloud Computing Infrastrukturen für spezielle Cluster-Systeme oder auch einfachen miteinander verbundenen Arbeitsplatzrechnern. Die Software basiert auf der BSD-Lizenz und wird an der University of California (UCSB) entwickelt.

Die aktuelle Version ist mit den Schnittstellen von Amazon EC2, S3 und EBS kompatibel. In der freien Version unterstützt Eucalyptus alle virtuelle Maschinen, die auf einem Xen Hypervisor oder einer Kernel-based Virtual Machine (KVM) ausgeführt werden. Die Enterprise Edition⁵ unterstützt zusätzlich VMware. Die Anwendung besteht aus drei Hauptkomponenten, die als Webservices realisiert sind. Es handelt sich dabei um Cloud Controller (CLC), Cluster Controller (CC) und Node Controller (NC).

Der Node Controller steuert das Betriebssystem eines jeden Rechners (Node) und den zugehörigen Hypervisor. Das Modul muss auf jeder physikalischen Maschine laufen, auf

⁴<http://www.eucalyptus.com/>

⁵<http://www.eucalyptus.com/products/eee>

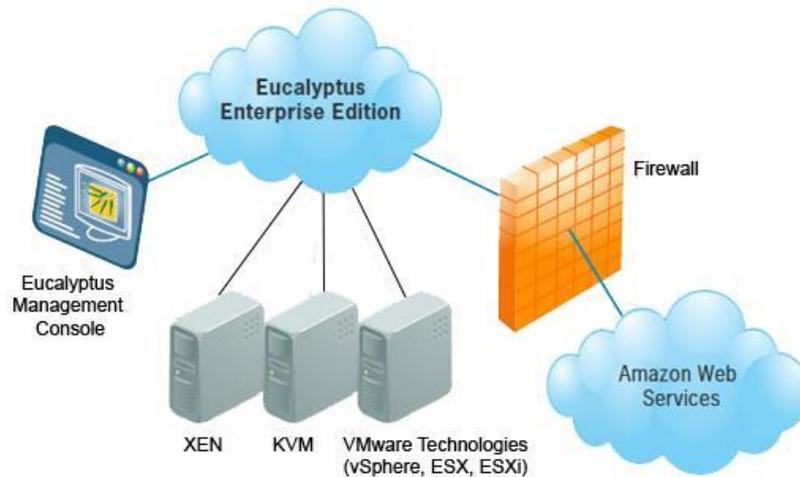


Abbildung 4.5: Cloud Computing mit Eucalyptus, Quelle: [2]

der eine virtuelle Instanz ausgeführt werden soll. Jeder NC überwacht den Zustand seiner eigenen Ressourcen und sendet die Informationen an den Cluster Controller (CC).

Auf Basis der übermittelten Informationen verteilt die CC-Komponente die virtuellen Maschinen auf die verfügbaren Knoten. Somit ist der Cluster Controller innerhalb des Eucalyptus Systems für die Verwaltung des virtuellen Netzwerks zuständig. Jeder CC sendet wiederum Informationen über den aktuellen Zustand der Ressourcen im eigenen Cluster an den Cloud Controller.

Der Cloud Controller verteilt die virtuellen Instanzen zwischen den verbundenen Clustern und stellt damit das Hauptmodul zur Steuerung des Gesamtsystems dar. Die CLC-Komponente ist der zentrale Zugriffspunkt für Administratoren und Anwender eines Eucalyptus-Systems.

Darüber hinaus verfügt das System über zwei weitere Komponenten: Walrus und Storage Controller. Letztere ist für die Verwaltung des Speicherdienstes innerhalb des Eucalyptus-Systems verantwortlich und verfügt über eine Schnittstelle zum S3 Dienst. Des Weiteren wird die Komponente für die Speicherung und den Zugriff auf die Virtual Machines Images, die Kernel Images und die Benutzerdaten verwendet. Walrus ist für die Zugriffsverwaltung auf den Speicherdienst innerhalb des Gesamtsystems verantwortlich.

Eucalyptus ist sehr flexibel und bietet die Möglichkeit alle drei Komponenten auf einem physischen Server zu betreiben. Somit ist die Anwendung auch für Infrastrukturen mit einer geringen Anzahl an physischen Servern geeignet. Mit der Softwarelösung kön-

nen öffentliche Cloud Dienste (auf der Infrastruktur von Amazon basierend) zusammen mit den privaten Clouds im hauseigenen Rechenzentrum erstellt und betrieben werden. Auf Grund dieser Kompatibilität können Anwendungen ohne großen Aufwand von einer Cloud in die andere migriert werden.

OpenNebula OpenNebula ist eine weitere Open Source Lösung mit der sich private, öffentliche oder hybride Clouds auf Basis heterogener Virtualisierungssysteme errichten lassen. Die Software verfügt über ein ähnliches Leistungsspektrum wie das bereits vorgestellte Eucalyptus. So unterstützt die Software alle virtuelle Maschinen die entweder auf Xen Hypervisor, VMware oder KVM ausgeführt werden. Darüber hinaus können weitere Virtualisierer via libvirt angebunden werden.

Mit OpenNebula können virtuelle Infrastrukturen in einem Rechenzentrum oder einem Cluster verwaltet werden. Außerdem kann damit die lokale Infrastruktur mit einer Public Cloud Infrastruktur verbunden und kombiniert werden. Zur Verwaltung virtueller Maschinen, des Speicherplatzes und des Netzwerks in öffentlichen Clouds stellt die Anwendung spezielle Schnittstellen zur Verfügung. Die Verwaltung der Arbeitslast sowie Ressourcenzuweisung kann nach bestimmten Regeln (wie z.B. der aktuellen Auslastung) komplett automatisiert werden.

Allerdings setzt der Betrieb einer OpenNebula-Cloud beträchtliches Know-How voraus. Im Gegensatz zu Eucalyptus ist die Benutzerschnittstelle nicht über ein Web-Frontend, sondern über eine Kommandozeile realisiert. Zur Verwaltung der Lebenszyklen virtueller Maschinen und physikalischer Server stellt OpenNebula zusätzlich eine XML-RPC API zur Verfügung.

OpenQRM OpenQRM ist eine Open Source Software zur Verwaltung von Rechenzentren und Cloud-Computing-Plattformen. Die Lösung unterstützt KVM, Xen, VMware und Linux-VServer als Virtualisierungstechnologien. Zusätzliche Funktionalitäten und Virtualisierungskonzepte werden über so genannte Plugins angeboten, die von Anwendern modular, nach Bedarf zusammengesetzt werden können. Ab der Version 4.6 stehen beispielsweise zwei neue Plugins zur Verfügung, mit denen der Betrieb von nicht Linux-basierten Betriebssystemen, wie z.B. Windows und Solaris unterstützt wird. Mittels Plugins werden auch diverse Speichertechnologien integriert, wie z.B. LVM, NFS, iSCSI, AOE, SAN oder ZFS. Weitere Erweiterungen stehen zur Verwaltung verschiedener Subsysteme und Ressourcen zur Verfügung und lassen sich über einen zentralen Plugin-Manager steuern.

Das System lässt sich außerdem mit Fokus auf Hochverfügbarkeit der Dienste betreiben. Die strikte Trennung der Dienste von den darunter liegenden physikalischen oder virtuellen Ressourcen reduziert die verfügbare Hardware zu einem Dienst-Container, der jederzeit ausgetauscht werden kann. Alle aktiven Dienste werden von OpenQRM automatisch überwacht. Fällt ein Dienst bzw. darunter liegender Container aus, so verschiebt die Managementkomponente die entsprechende Instanz in einen neuen Container. Die Abstraktion der Ressourcen ermöglicht OpenQRM ein n-zu-1-Failover zu unterstützen. Damit kann eine Gruppe von Systemen einen gemeinsamen Reserveserver nutzen.

Die Software bietet die Option, komplette physikalische Systeme in virtuelle Instanzen und umgekehrt zu migrieren. Im Hinblick auf Verfügbarkeit und Ausfallsicherheit kann das System im Fehlerfall einen beliebigen Dienst eines physikalischen Servers automatisch auf eine virtuelle Maschine transferieren.

Dabei integriert OpenQRM öffentliche Cloud-Anbieter und erlaubt bidirektionale Migration von virtuellen System. Dadurch können einerseits interne virtuelle Instanzen in Amazon-, Eucalyptus- oder UEC-Clouds ausgelagert werden; andererseits können auch Systemimages (AMIs) der externen Dienstleister in die lokale Infrastruktur importiert werden. Darüber hinaus unterstützt OpenQRM aktuelle Power Management Technologien wie etwa Wake-on-LAN und IPMI mit denen physikalische Instanzen automatisch an- und ausgeschaltet werden können. Diese Funktionalität ermöglicht die Einsparung von Stromkosten aller passiven Ressourcen (z.B. Reserveserver).

Die Administration der gesamten IT-Landschaft erfolgt in einer übergreifenden zentralen Managementkonsole. Das Ziel von OpenQRM ist die Verwaltung kompletter Rechenzentren innerhalb einer einzigen Anwendung. Daher richtet sich das Produkt primär an Betreiber von Rechenzentren. Die offenen und gut dokumentierten Schnittstellen sowie der modulare Aufbau des Systems ermöglichen einfache Integration existierender und zukünftiger Methoden und Werkzeuge. Aktive Weiterentwicklung zusammen mit kontinuierlicher Funktionserweiterung durch neue Plugins macht OpenQRM zu einer interessanten Alternative zu kommerziellen Datacenter-Management-Lösungen.

4.6 Zusammenfassung – Marktübersicht

Der Markt für Virtualisierungsprodukte jeglicher Ausprägung ist heute hart umkämpft und wird dies auch in den nächsten Jahren sein. Zur Zeit bemüht sich Microsoft die Marktführerschaft von VMware anzugreifen. Durch den entstehenden Wettkampf nähern sich die Produkte in Featureumfang und Performanz immer dichter aneinander an. Dabei wird es allerdings immer schwieriger, die Versprechen der Marketing-Abteilungen von den eigentlichen Kernfeatures der Produkte zu unterscheiden.

So ist es kaum verwunderlich, dass sowohl Citrix als auch Microsoft oder VMware für die meisten denkbaren Szenarios eine passende Lösung bieten. Es lassen sich jedoch jeweils Stärken der einzelnen Anbieter erkennen: Citrix war schon immer stark im Bereich *Terminal Computing* und bietet auch heute die ausgereiftesten Lösungen für *Virtual Desktop Infrastructures*. Insbesondere die Weiterentwicklung und Veröffentlichung von *XenClient* zum sicheren Offline-Betrieb von virtuellen Desktops auch auf fremder Hardware ist aufmerksam zu verfolgen.

Die Stärken von Microsoft liegen klar in der engen Integration mit vorhandenen Infrastrukturen. Für die Virtualisierung von Windows-Serverfarmen ist Hyper-V zusammen mit den Management-Paketen für Microsoft System Center sicherlich eine zu bevorzugende Lösung. Auch die Nutzung von vorhandenem Know-How mit der Administration von Microsoft Systemen im Rechenzentrum ist hier als positiv hervorzuheben. Nachteilig wirkt sich die Fokussierung auf die Virtualisierung von Windows-Servern allerdings in sehr heterogenen Umgebungen aus – nicht jedes Linux oder Unix wird von Hyper-V offiziell unterstützt.

VMware bietet eine sehr ausgereifte Software-Suite für den Betrieb großer virtualisierter Infrastrukturen und wird dort auch schon seit längerem erfolgreich eingesetzt. Viele große Hersteller für Unternehmenssoftware (z.B. SAP) zertifizieren daher primär VMware für die Virtualisierung ihrer Applikationsserver. Mit der Öffnung der Virtual Infrastructure zum Cloud Computing (vSphere) ist VMware auch hier bereits einen Schritt weiter als die Konkurrenz. Besonders hervorzuheben sind die Features für Hochverfügbarkeit und Fehlertoleranz (Continuous Availability). Hier besitzt vSphere ein Alleinstellungsmerkmal.

Es liegt also nahe, dass es bei der Wahl einer zu implementierenden Virtualisierungslösung keine eindeutige Empfehlung geben kann: der Markt ist in Bewegung, die Hersteller nähern sich an. Entscheidungsgrundlage müssen daher neben wirtschaftlichen Zwängen wie der Total Cost of Ownership auch Faktoren wie vorhandenes Know-How sein.

5 Zusammenfassung und Fazit

Die vorliegende Studie zeigt deutlich die Relevanz, die Virtualisierung und Cloud Computing heute und auch in den nächsten Jahren haben wird. Dabei hat die Basistechnologie den Hype-Status durchaus hinter sich und kann als etabliert gelten – zumindest was den Bereich der Servervirtualisierung angeht. Hier gibt es eine Reihe von ausgereiften Produkten nebst passender Management-Software. Eine Schwierigkeit in diesem Bereich ist mittlerweile eher die Verschleierung der tatsächlichen Fähigkeiten der Produkte durch die Marketing-Auslegung geworden.

Sowohl generell, als auch insbesondere für die Servervirtualisierung bleibt aber deutlich festzuhalten, dass Virtualisierungstechnologie kein Wundermittel gegen Kostendruck im Rechenzentrum ist. Es muss darauf geachtet werden, dass der zusätzliche Administrationsaufwand durch die Einführung einer (teil-)virtualisierten Infrastruktur die Einsparung durch Serverkonsolidierung nicht übersteigt (wichtig: ausgereifte Administrationswerkzeuge).

Weiterhin ist der Gedanke, dass Konsolidierung im Sinne der Einsparung physikalischer Hardware der entscheidende Vorteil der Servervirtualisierung ist, zu dominant. Nicht jedes IT-System leidet unter schlechter Auslastung der physikalischen Hardware und ist daher ein offensichtlicher Kandidat für Servervirtualisierung.

Jedoch sollte insbesondere für Systeme, die hohe Verfügbarkeitsanforderungen mit sich bringen, geprüft werden, ob eine Virtualisierung aus Performancegründen ausgeschlossen werden muss. Prinzipiell gilt nämlich, dass virtualisierte Systeme ein deutlich einfacheres Disaster Management sowie zentralisiertes Backup erlauben: Failover-Cluster sind einfacher zu realisieren, Live-Migration beim Austausch von Hardware, die z.B. kurz vor dem Versagen steht, wird in virtualisierten Umgebungen sehr leicht. Dies gilt auch für den regulären Austausch von Server-Computern beim turnusmäßigen Rollout. Die Virtualisierung eines Systems mit hohen Anforderungen an Hardwareressourcen kann also auch sinnvoll sein, wenn sich damit das Disaster Management vereinfachen lässt. Ein Szenario mit Kostenersparnis kann durchaus vorsehen, dass etwa nicht für jedes System ein Failover-Server zur Verfügung stehen muss, sondern dieser aus einem Pool ausgewählt werden kann. Dies kann natürlich nur der Fall sein, wenn es die Verfügbarkeitskriterien

zulassen.

Die Zukunft der Servervirtualisierung läuft auf eine Entwicklung der virtualisierten Infrastrukturen zur privaten Cloud hinaus. Die meisten virtuellen Infrastrukturen haben heute schon Eigenschaften, die dem Cloud Computing zugerechnet werden, wie die dynamische Verteilung der Workloads der virtuellen Maschinen auf physikalische Server.

Auch die Integration externer Cloud-Dienste oder die Migration dorthin wird für viele Unternehmen zu einer interessanten Option. Erlauben Geschäftsmodell sowie rechtlicher Rahmen (Compliance) die Nutzung heutiger Cloud-Angebote, steht die Wirtschaftlichkeit einer solchen Maßnahme fast immer ausser Frage. Dabei sind aber stets die in Abschnitt 3.3 dargelegten Bedenken und Einschränkungen zu beachten.

Der Bereich der Applikationsvirtualisierung bietet besonders Unternehmen mit einer komplexen, heterogenen Applikationslandschaft Chancen zur Vereinfachung der Workflows. Hier werden häufig Probleme durch Inkompatibilitäten zwischen Anwendungen als Gründe für aufwändige Testprozeduren und als Hinderungsgrund für das Deployment auf Terminal Servern aufgeführt. Sowohl XenApp, als auch App-V und ThinApp kommen für eine detaillierte Evaluation bei anstehenden Projekten in Frage. Wie auch bei der Virtualisierung von Servern muss darauf geachtet werden, dass die Virtualisierung von Applikationen in den existierenden Software-Rollout-Workflow integriert werden kann.

Auch die Neuerungen im Bereich der Desktop-Virtualisierung sollten kontinuierlich im Auge behalten werden. Hierbei sind die kommenden technischen Entwicklungen ebenso von Relevanz wie die Veränderungen im Unternehmensalltag durch die fortschreitende Durchdringung aller Vorgänge mit Informationstechnologie (z.B. mobile Clients wie Smartphones). Virtual Desktop Infrastructures bergen ein enormes Einsparpotential, wenn die Anforderungen an die IT-Landschaft es zulassen. Da heute für den Einsatz in vielen Unternehmen ein stetiger Online-Betrieb von Desktops nicht vorausgesetzt werden darf, kommt VDI zur Zeit häufig noch nicht in Frage – lediglich der MED-V Ansatz von Microsoft erlaubt heute bereits einen Offline-Betrieb bei gleichzeitiger zentraler Pflege der Desktop-Images.

Zukünftig wird aber insbesondere die Lösung von Citrix und Intel interessant: die Integration von XenClient als Bare Metal Hypervisor direkt in der Hardware für Laptops erlaubt den isolierten Offline-Betrieb von virtuellen Desktops (diese müssen hierzu verschlüsselt ausgeliefert werden). Diese Möglichkeiten können zukünftig auch den Rollout von Geräten beeinflussen: Rechner müssen nicht mehr an Arbeitsplätze gebunden sein, Mitarbeiter können sich ohne Probleme Laptops teilen oder ihre eigenen Geräte verwenden, wenn diese mit dem entsprechenden Hardware-Hypervisor ausgestattet sind.

Trotzdem haben sie auf diesen privaten oder geteilten Laptops ihren personalisierten Enterprise-Desktop zur Verfügung.

Es ist offensichtlich, dass Virtualisierungstechnologie und die Integration von Cloud Computing-Angeboten in allen Varianten heute und vor allem in Zukunft in komplexen IT-Landschaften kaum mehr wegzudenken sind. Die kommenden Entwicklungen (insbesondere im Sektor VDI) lassen im Unternehmenskontext auf ein noch höheres Einsparpotential hoffen, als beispielsweise die Servervirtualisierung, da hier vor allem der Administrationsaufwand gesenkt werden kann. Gleichzeitig bleibt aber auch festzuhalten, dass die Anforderungen an die zentralen IT-Dienstleistungen immer weiter steigen werden: eine rechtzeitige, nachhaltige Verstärkung des Know-Hows in diesem Bereich und die Schulung von Mitarbeitern im IT-Service sind schon heute wichtig.

Literaturverzeichnis

- [1] Michael Armbrust, Armando Fox, Rean Griffith, Anthony D. Joseph, Randy Katz, Andy Konwinski, Gunho Lee, David Patterson, Ariel Rabkin, Ion Stoica, and Matei Zaharia. Above the clouds: A berkeley view of cloud computing. "*Technical Report UCB/EECS-2009, EECS Department, University of California, Berkeley*", 2009.
- [2] Nicolas Barcet. Cloud-Infrastruktur für Entwickler: Mit Open-Source-Software lokale Server zur privaten Cloud machen. *t3n Magazin*, 18, 2010.
- [3] David Chappell. Virtualization for Windows: a Technology Overview. Technical report, Microsoft Corporation, 2008.
- [4] TU Clausthal. Das Grundmodell der Warteschlangentheorie. Website, 2010. Erreichbar unter <http://www.stochastik.tu-clausthal.de/Presse/Schulen/Grundmodell>; abgerufen am 6.12.2010.
- [5] VMware Deutschland. VMware vSphere: private Cloud mit Virtualisierung im Rechenzentrum. Website, 2010. Erreichbar unter <http://http://www.vmware.com/de/products/vsphere>; abgerufen am 02.11.2010.
- [6] Vishal Ganeriwala. Citrix XenDesktop Developer Network: Project Independence. Website, 2009. Erreichbar unter <http://community.citrix.com/display/xd/independence>; abgerufen am 02.11.2010.
- [7] VMware Inc. VMware View Features: Virtual Desktop Management & Desktop Security. Website, 2010. Erreichbar unter <http://www.vmware.com/products/view/features.html>; abgerufen am 02.11.2010.
- [8] Anthony Kinney. Microsoft TechNet: Getting Started with Microsoft Application Virtualization. Website, 2008. Erreichbar unter <http://technet.microsoft.com/en-us/magazine/2008.10.appv.aspx>; abgerufen am 02.11.2010.
- [9] Teodora Mladenova. *Einsatz der Warteschlangentheorie: Vergleich beider Entscheidungsinstrumente anhand eines Praxisbeispiels*. VDM Verlag, 2009.

-
- [10] Gordon E. Moore. Cramming more components onto integrated circuits. *Electronics*, 29(8), 1965.
- [11] David A. Patterson and John L. Hennessy. *Rechnerorganisation und -entwurf*. Spektrum Akademischer Verlag, 2005.
- [12] K. Ragnar. The cloud wars: \$100+ at stake. Technical report, Merrill Lynch, 2008.
- [13] Gartner Research. Gartner says worldwide hosted virtual desktop market to surpass \$65 billion in 2013. Website, 2009. Erreichbar unter <http://www.gartner.com/it/page.jsp?id=920814>; abgerufen am 02.11.2010.
- [14] Rightscale. Animoto's Facebook scale-up. Website, 2008. Erreichbar unter <http://blog.rightscale.com/2008/04/23/animoto-facebook-scale-up/>; abgerufen am 02.12.2010.
- [15] SAS70.com. SAS 70 Overview. Website, 2010. Erreichbar unter http://sas70.com/sas70_overview.html; abgerufen am 02.11.2010.
- [16] Amazon Web Services. Website, 2007. Erreichbar unter <http://www.amazon.de/gp/press/pr/20071106>; abgerufen am 02.12.2010.
- [17] Amazon Web Services. Amazon Simple Storage Service (Amazon S3). Website, 2010. Erreichbar unter <http://aws.amazon.com/de/s3/>; abgerufen am 02.12.2010.
- [18] Ludwig Siegele. Let it rise – a survey on corporate IT. *The Economist*, 10, 2008.
- [19] Thomas Smedinghoff. *Information Security: The Emerging Standard for Corporate Compliance*. IT Governance Pub., 2008.
- [20] A. Stern. Update From Amazon Regarding Friday's S3 Downtime. Website, 2008. Erreichbar unter <http://www.centernetworks.com/amazon-s3-downtime-update>; abgerufen am 6.12.2010.
- [21] Citrix Systems. XenClient features. Website, 2010. Erreichbar unter <http://www.citrix.com/English/ps2/products/subfeature.asp?contentID=2300446>; abgerufen am 02.11.2010.
- [22] Citrix Systems. Desktop Virtualisierung: Citrix XenDesktop. Website, 2010. Erreichbar unter <http://www.desktop-virtualisierung.com/>; abgerufen am 02.11.2010.

- [23] The Amazon S3 Team. Amazon s3 availability event: July 20, 2008. Website, 2008.
URL <http://status.aws.amazon.com/s3-20080720.html>.
- [24] Dennis Zimmer. Trau, schau, wem – Professionelle Virtualisierungsprodukte: ein Überblick. *iX – Magazin für professionelle Computertechnik*, 8:64–73, 2006.

Aktuelle Technische Berichte des Hasso-Plattner-Instituts

Band	ISBN	Titel	Autoren / Redaktion
43	978-3-86956-110-3	SOA-Security 2010 : Symposium für Sicherheit in Service-orientierten Architekturen ; 28. / 29. Oktober 2010 am Hasso-Plattner-Institut	Christoph Meinel, Ivonne Thomas, Robert Warschofsky et al.
42	978-3-86956-114-1	Proceedings of the Fall 2010 Future SOC Lab Day	Hrsg. von Christoph Meinel, Andreas Polze, Alexander Zeier et al.
41	978-3-86956-108-0	The effect of tangible media on individuals in business process modeling: A controlled experiment	Alexander Lübbe
40	978-3-86956-106-6	Selected Papers of the International Workshop on Smalltalk Technologies (IWST'10)	Hrsg. von Michael Haupt, Robert Hirschfeld
39	978-3-86956-092-2	Dritter Deutscher IPv6 Gipfel 2010	Hrsg. von Christoph Meinel und Harald Sack
38	978-3-86956-081-6	Extracting Structured Information from Wikipedia Articles to Populate Infoboxes	Dustin Lange, Christoph Böhm, Felix Naumann
37	978-3-86956-078-6	Toward Bridging the Gap Between Formal Semantics and Implementation of Triple Graph Grammars	Holger Giese, Stephan Hildebrandt, Leen Lambers
36	978-3-86956-065-6	Pattern Matching for an Object-oriented and Dynamically Typed Programming Language	Felix Geller, Robert Hirschfeld, Gilad Bracha
35	978-3-86956-054-0	Business Process Model Abstraction : Theory and Practice	Sergey Smirnov, Hajo A. Reijers, Thijs Nugteren, Mathias Weske
34	978-3-86956-048-9	Efficient and exact computation of inclusion dependencies for data integration	Jana Bauckmann, Ulf Leser, Felix Naumann
33	978-3-86956-043-4	Proceedings of the 9th Workshop on Aspects, Components, and Patterns for Infrastructure Software (ACP4IS '10)	Hrsg. von Bram Adams, Michael Haupt, Daniel Lohmann
32	978-3-86956-037-3	STG Decomposition: Internal Communication for SI Implementability	Dominic Wist, Mark Schaefer, Walter Vogler, Ralf Wollowski
31	978-3-86956-036-6	Proceedings of the 4th Ph.D. Retreat of the HPI Research School on Service-oriented Systems Engineering	Hrsg. von den Professoren des HPI
30	978-3-86956-009-0	Action Patterns in Business Process Models	Sergey Smirnov, Matthias Weidlich, Jan Mending, Mathias Weske
29	978-3-940793-91-1	Correct Dynamic Service-Oriented Architectures: Modeling and Compositional Verification with Dynamic Collaborations	Basil Becker, Holger Giese, Stefan Neumann
28	978-3-940793-84-3	Efficient Model Synchronization of Large-Scale Models	Holger Giese, Stephan Hildebrandt

ISBN 978-3-86956-113-4
ISSN 1613-5652