IT-Sicherheit im Handwerk

Virtualisierung

Dozentenhandbuch

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Das diesem Buch zugrundeliegende Verbundvorhaben "IT-Sicherheitsbotschafter im Handwerk - qualifizierte, neutrale Botschafter für IT-Sicherheit im Handwerk finden, schulen und Awarenesskonzepte erproben (ISiK)" wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie (BMWi) im Rahmen der Task Force "IT-Sicherheit in der Wirtschaft" gefördert und durch den Projektträger im Deutschen Zentrum für Luft- und Raumfahrt (PT-DLR) betreut.

Die Task Force "IT-Sicherheit in der Wirtschaft" ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task Force und ihren Angeboten sind unter: *www.it-sicherheit-in-der-wirtschaft.de* abrufbar.

Herausgeber: Institut für Technik der Betriebsführung (itb) im
Deutschen Handwerksinstitut (DHI) e.V.
Kriegsstraße 103a • 76135 Karlsruhe (Konsortialführer)

Kompetenzzentrum IT-Sicherheit
und Qualifizierte Digitale Signatur (KOMZET) der
Handwerkskammer Rheinhessen
Dagobertstraße 2 • 55116 Mainz (fachliche Leitung)

Westfälische Hochschule
Institut für Internet-Sicherheit – if(is)
Neidenburger Straße 43 • 45877 Gelsenkirchen
(Kooperationspartner)

Interessengemeinschaft des Heinz-Piest-Instituts für Handwerkstechnik (HPI) an der Leibniz-Universität Hannover
Wilhelm-Busch-Straße 18 • 30167 Hannover
(Kooperationspartner)

Das Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung und des Nachdrucks, bleiben, auch bei nur auszugsweiser Verwertung vorbehalten. Kein Teil des Werkes darf in irgendeiner Form (Druck, Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung der Herausgeber reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Text, Abbildung und Programme wurden mit größter Sorgfalt erarbeitet. Die Autorinnen und Autoren können jedoch für eventuell verbleibende fehlerhafte Angaben und deren Folgen weder eine juristische noch irgendeine andere Haftung übernehmen.

ISBN **978-3-944916-xx-x**

Verlag: Handwerkskammer Rheinhessen
Dagobertstraße 2 • 55116 Mainz
www.hwk.de

© 2015 Projekt ISiK, 1. Auflage

Autorenteam

Falk Gaentzsch

Bachelor of Science und wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen. Projektleiter für das Projekt „IT-Sicherheit im Handwerk“.

Schwerpunkte:
IT-Sicherheit & Awareness
Cloud-Computing
Virtualisierung

Prof. Norbert Pohlmann

Informatikprofessor für Verteilte Systeme und Informations-sicherheit sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit - if(is) an der Westfälischen Hochschule in Gelsenkirchen.

Einleitung

Dieses Handbuch vermittelt Ihnen ein Grundverständnis über das Thema Virtualisierung mit vielen Handlungsanweisungen für mehr IT-Sicherheit.
Die Virtualisierung von Computern ist kein Thema das neu ist, wie beispielsweise der Begriff des Cloud-Computings. Werden diese beiden Begriffe, also Cloud-Computing und Virtualisierung miteinander verglichen, so kann festgehalten werden, dass die Virtualisierung ein großer Bestandteil von Cloud-Computing ist. Es ist eine Methode um den Einsatz von Ressourcen, im Allgemeinen Rechenleistung und Speicherkapazitäten, besser auslasten und damit effektiver nutzen zu können. In den Anfängen der Computerisierung stand ein Rechner für ein unabhängiges System, auf dem Befehle eines Nutzers durch das Betriebssystem verarbeitet wurden.
Dies bedeutet, dass ein Computer nur arbeitet, wenn es etwas zu verarbeiten gibt. Die Schlussfolgerung daraus ist, dass ein System häufig nicht ausreichend ausgelastet wird und auf neue Eingaben wartet.
Mit der Virtualisierung konnte eine Technologie entwickelt werde, die es ermöglicht mehrere so genannte virtuelle Maschinen auf einer physischen Maschine auszuführen. Dies ermöglicht eine deutliche effizientere Nutzung der vorhandenen Ressourcen wie beispielsweise des Arbeitsspeichers und des Prozessors.
Im Zeitalter des Cloud-Computing, ist die Technologie der Virtualisierung zu einem effektiven Werkzeug für eine optimale Nutzung von verfügbaren Computersystemen geworden.
Erst durch Virtualisierung kann die Cloud so flexibel genutzt werden, wie es heute der Fall ist. Wird beispielsweise mehr Rechenkraft für einen Server in der Cloud benötigt, weil die Ansprüche durch neue Aufgaben gestiegen sind, kann nun sehr einfach ein neuer virtueller Prozessor oder mehr virtueller Arbeitsspeicher zum System hinzugebucht werden. Dies zeigt sehr einprägsam, welche Möglichkeiten die Virtualisierung von Computer-Systemen bietet.

Anmerkung zu den Beispielen in diesem Handbuch

Die Betriebe, Angriffsszenarien und Schadensbeispiele in diesem Handbuch sind frei erfunden und sollen die möglichen Auswirkungen von Fehlern und Angriffen verdeutlichen.

Seminarziele

Das Ziel dieses Handbuches ist es, ein Grundverständnis für die Vor- und Nachteile von Virtualisierung in Bezug auf die IT-Sicherheit eines Unternehmens zu vermitteln. Die Erkenntnisse in diesem Handbuch basieren auf dem aktuellen Wissensstand rund um das Thema Virtualisierung.

Am Ende dieses Seminars sind Sie in der Lage

- Grundlagen über das Thema Virtualisierung vermitteln zu können.
- Vorteile und Risiken von Virtualisierung darzustellen.
- Bei der Entscheidungsfindung rund um das Thema Virtualisierung zu unterstützen.
- Geeignete Virtualisierungstechniken zu identifizieren und von unpassenden Angeboten abzuraten.
- Sicherheitsempfehlungen bei der Nutzung von Virtualisierung auszusprechen.

Inhaltsverzeichnis

AUTORENTEAM **4**

EINLEITUNG **5**

SEMINARZIELE **5**

INHALTSVERZEICHNIS **6**

1. Grundlagen der Virtualisierung **8**
1.1 Die gängige Vorstellung eines Computers 8
1.2 Was ist eine virtuelle Maschine? 9
1.3 Begriffserklärung 10
1.3.1 Host 10
1.3.2 Kernel 10
1.3.3 Monolithischer Kernel 11
1.3.4 Mikrokernel 12
1.3.5 Hybridkernel 13
1.3.6 Virtualisierungsgrundlagen der x86-Architektur 13
1.3.7 Hypervisor 17
1.3.8 Vollvirtualisierung (Komplettvirtualisierung) 18
1.3.9 Paravirtualisierung 20
1.3.10 Paravirtualisierung mit Hardwareunterstützung 21
1.3.11 Betriebssystemvirtualisierung 23
1.3.12 Emulation 24
1.3.13 KVM - Kernel-based Virtual Machine 25
1.4 Vorteile durch Virtualisierung 26
1.5 Nachteile durch Virtualisierung 28
1.6 Aufsetzten oder Mieten? 30
1.7 Zusammenfassung 30

2. Risiken **32**
2.1 Problematische Voraussetzungen auf dem Host 32
2.2 Fehlkonfiguration des Hosts 33
2.3 Schlechte Passwortsicherheit 34
2.4 Fehlende Redundanz 35
2.5 Mögliche Fehler im Hypervisor 36
2.6 Unzureichender Support bei Virtualisierung 37
2.7 Zusammenfassung 37

3. Basisschutz **39**
3.1 Vorabplanung für Virtualisierung 39
3.2 Separation der Netze 39
3.3 Verantwortlichkeiten und Rollen 41
3.4 Firewalls 42
3.5 VPN Verschlüsselung der Datenübertragung 43
3.6 Optimierte Host- und VM-Konfiguration 45
3.7 Redundanz 46
3.8 Backup 47
3.9 Image 47

3.10 Snapshot 48
3.11 Snapshot ohne Abbild des Arbeitsspeichers 49
3.12 SAN 50
3.13 Sichere Passwörter 50
3.14 Zusammenfassung 51

4. Praxistipps 52
4.1 Anwendungsmöglichkeiten der Virtualisierung in Handwerksbetrieben 52
4.1.1 Virtuelle Maschinen aus existierenden Servern erzeugen 52
4.1.2 Beispiel für Virtualisierung im Handwerk 57
4.2 Vorteile der Serverkonsolidierung nutzen 58
4.3 Anforderung an Host 59
4.4 Sicherheit in der Virtualisierung 59
4.5 Sicherheitsvorkehrungen für den Gast 60
4.6 Datensicherung 61
4.7 Raid 63
4.8 Virtualisierung in der Cloud 63

5. Weblinks 65

6. Literaturverzeichnis 66

7. Stichwortverzeichnis 67

8. Abbildungsverzeichnis 70

1. Grundlagen der Virtualisierung

In diesem Kapitel werden Ihnen Grundlagen und Basisbegriffe zum Thema Virtualisierung vermittelt. Mit verschiedenen Beispielen zu Virtualisierungstechniken wird Ihnen aufgezeigt, welche Vor- und Nachteile diese virtualisierten Systeme aufzeigen können.

1.1 Die gängige Vorstellung eines Computers

In der Abbildung 1 wird sehr grob dargestellt, wie das Innenleben eines normalen Computers aussieht. Er besteht aus der Hardware, mit Prozessoren, Arbeitsspeicher, Festplatten, Netzwerkkarten und weiteren grundlegenden Komponenten.

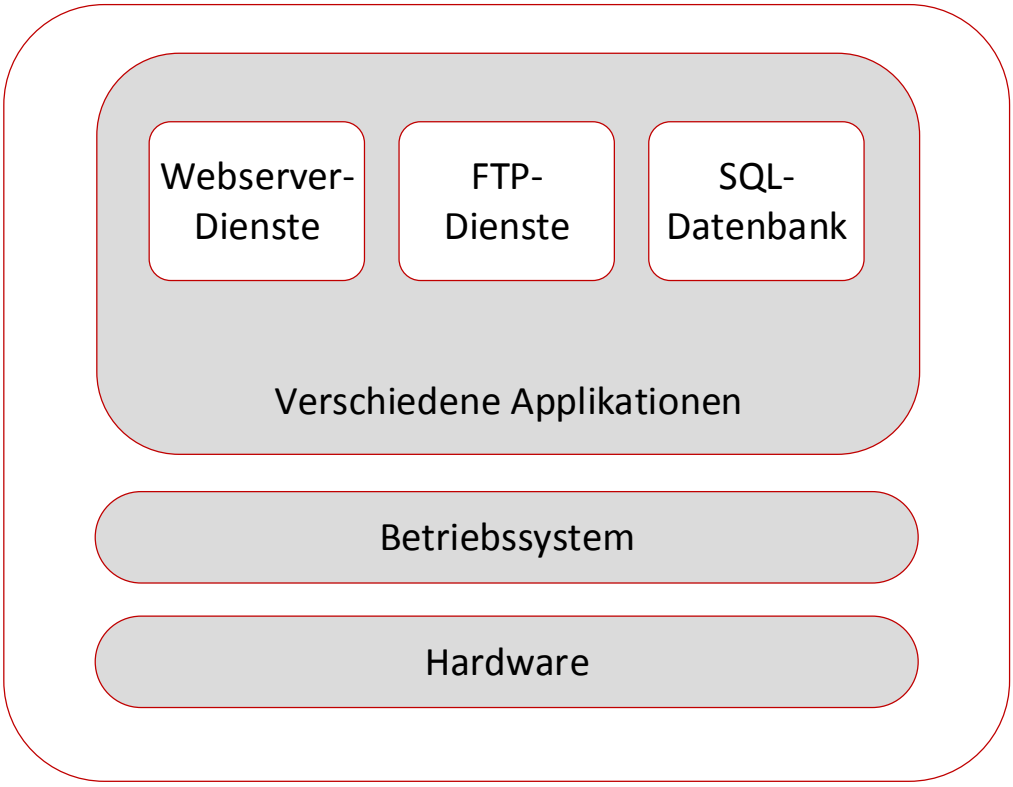


Abbildung 1: Der gängige Computer

Auf der Festplatte ist ein Betriebssystem installiert. Dies kann beispielsweise ein Linux-[1], Windows-[2] oder Mac OS[3]-basiertes System sein. Ein wichtiger Unterschied zu virtualisierten Servern oder Computern ist, dass immer nur ein Betriebssystem

[1] *Linux ist ein freies Betriebssystem mit vielen kostenlosen Programmen.*
[2] *Windows ist ein von Microsoft entwickeltes kommerzielles Softwareprodukt.*
[3] *Mac OS wurde von Apple entwickelt und darf aus Lizenzgründen nur auf Apple Produkten ausgeführt werden*

gleichzeitig ausgeführt werden kann. Die logische Konsequenz ist, dass alle Hardwarekomponenten nur von diesem einen Betriebssystem ausgelastet und genutzt werden kann. Mit Virtualisierung kommt ein Mechanismus zum Einsatz, der genau diese gängige Vorstellung eines Computers verändert. Virtualisierung erlaubt es, gleichzeitig mehrere Betriebssysteme parallel auf einem Computer auszuführen. Ermöglicht wird dies durch raffinierte Technologien, die bereits seit vielen Jahren Stand der Technik sind (siehe Kapitel 1.3.6).
Ein so genannter Hypervisor (s. Kapitel 1.3.7) verwaltet dabei die Ressourcen der im Computer verbauten Hardware und verteilt sie auf mehrere parallel installierte virtuelle Maschinen. Es ist so möglich viele Betriebssysteme gleichzeitig auszuführen, was einige Vorteile bietet (siehe Kapitel 1.4).

1.2 Was ist eine virtuelle Maschine?

Ein virtuelle Maschine (kurz VM) ist vergleichbar mit einem eigenständigen Computer, mit dem Unterschied, dass dieser über keine eigene Hardware verfügt sondern mittels eines Hypervisors verwaltet wird.
Der Hypervisor ist eine Softwarekomponente, die auf einem Computer oder Server (Host-System), innerhalb eines vorhandenen Betriebssystems, ausgeführt wird. Der Hypervisor, auch als Virtual Machine Monitor (VMM) bezeichnet, hat dabei die Aufgabe die Ressourcen des Computers, wie beispielsweise Prozessoren, den Arbeitsspeicher, den Festplattenspeicher, die Netzwerkverbindungen und vieles mehr, an eine oder mehrere virtuelle Maschinen zu verteilen und den Zugriff darauf zu verwalten. Der Hypervisor hat somit eine vermittelnde Funktion zwischen virtuellen Maschinen (Gast-System) und dem Virtualisierungsserver (Host-System).

Somit kann eine virtuelle Maschine ein Betriebssystem, unabhängig vom installierten Host-Betriebssystem beheimaten.

Beispiel:
Ein Windows-PC kann ein oder mehrere virtualisierte Linux-Betriebssysteme bereitstellen. Ebenso kann auch ein Computer mit einem Linux-Betriebssystem als Host für ein Windows-Betriebssystem bereitstehen. Die Kombinationsmöglichkeiten sind vielfältig und werden nur durch die verfügbaren Ressourcen eingeschränkt.

Das virtualisierte System kann all die Aufgaben erledigen, die auch direkt auf einem alleinstehenden Computer möglich sind, sofern ihm genügend Ressourcen zugeordnet werden. Es ist so beispielsweise möglich einen externen WLAN-USB-Adapter einer einzelnen virtuellen Maschine zuzuordnen. Für diesen Zeitraum ist der Adapter jedoch nicht für das Host-System verfügbar. Ebenso können auch USB-Sticks oder ganze Festplatten einer einzelnen virtuellen Maschine zugeteilt werden.
Speichermedien können auch unterteilt werden und somit von mehr als einer virtuellen Maschine verwendet werden.

1.3 Begriffserklärung

Der Begriff der Virtualisierung stammt aus den 1970er Jahren, in denen IBM[4] die VM/370, einem Betriebssystem für virtuelle Maschinen, vorstellte.
In der Virtualisierung gibt es heute verschiedene Ansätze, die in den folgenden Kapiteln erläutern werden. In den nächsten Absätzen werden diesbezüglich auch einige wichtige Begriffe rund um das Thema Virtualisierung erläutert. Dieses Wissen ist notwendig, um die Funktionsweise von Virtualisierung und die unterschiedlichen Virtualisierungsansätze verstehen zu können.

1.3.1 Host

Ein Server oder Computer auf dem virtuelle Maschinen betrieben werden, wird Host oder Virtualierungs-Host genannt.

Unter dem Begriff „Host“ (englisch für Wirt, Gastgeber, Veranstalter) ist allgemein ein Computer zu verstehen, auf dem Virtualisierung zum Einsatz kommt. Generell wird im Bereich der Virtualisierung zwischen Desktop- und Server-Virtualisierung unterschieden. Hierbei handelt es sich nicht im Speziellen um unterschiedliche Technologien, sondern mehr um das Umfeld in der die Virtualisierungsmethode zum Einsatz kommt. So wird bei der Desktop-Virtualisierung ein Gast-System lediglich auf einem gewöhnlichen Desktop-PC ausgeführt. Bei der Server-Virtualisierung verhält es sich analog, es sind jedoch üblicherweise deutlich mehr Ressourcen vorhanden die den virtuellen Maschinen zugeteilt werden können. Im Folgenden wird diese Unterscheidung nur verwendet, wenn diese explizit notwendig ist.

1.3.2 Kernel

Ein Kernel der zentrale Bestanteil eines jeden Betriebssystems.

Der Kernel ist eine grundlegende Softwarekomponente eines jeden Betriebssystems und bildet die Verbindung zwischen der Hardware und der Anwendungsverwaltung auf einem Computer. Die Aufgabe des Kernels ist es unter anderem Funktionen für die Anwendungssoftware bereitzustellen, damit diese auf die Ressourcen wie den Prozessor, den Speicher und andere Hardwarekomponenten zugreifen kann. Um die Kommunikation von Programmen zur Hardware gewährleisten zu können, muss der Kernel mit dem Systemstart, also während des Bootvorgangs, direkt in den Arbeitsspeicher geladen werden. Dieser bietet dann in unterschiedlichen Abstraktionsschichten Schnittstellen für die Anwendersoftware an. Ergänzend ist zu betonen, dass es unterschiedliche Kernel-Varianten gibt, die in den folgenden Absätzen dargestellt werden. Damit der Kernel mit der Hardware kommunizieren kann, benötigt dieser bestimmte Gerätetreiber die von Produkt zu Produkt unterschiedlich sind. Grundsätzlich unterscheiden wir hier drei Kernel-Architekturen, die jeweils unterschiedliche Merkmale aufweisen.

- Monolithische Kernel
- Mikrokernel
- Hybridkernel

[4] http://www.ibm.com/de/ *International Business Machines Corporation (IBM) – US-Amerikanisches IT- und Beratungsunternehmen*

1.3.3 Monolithischer Kernel

Ein monolithischer Kernel hat im ursprünglichen Sinn alle Funktionen und Treiber fest in sich integriert.

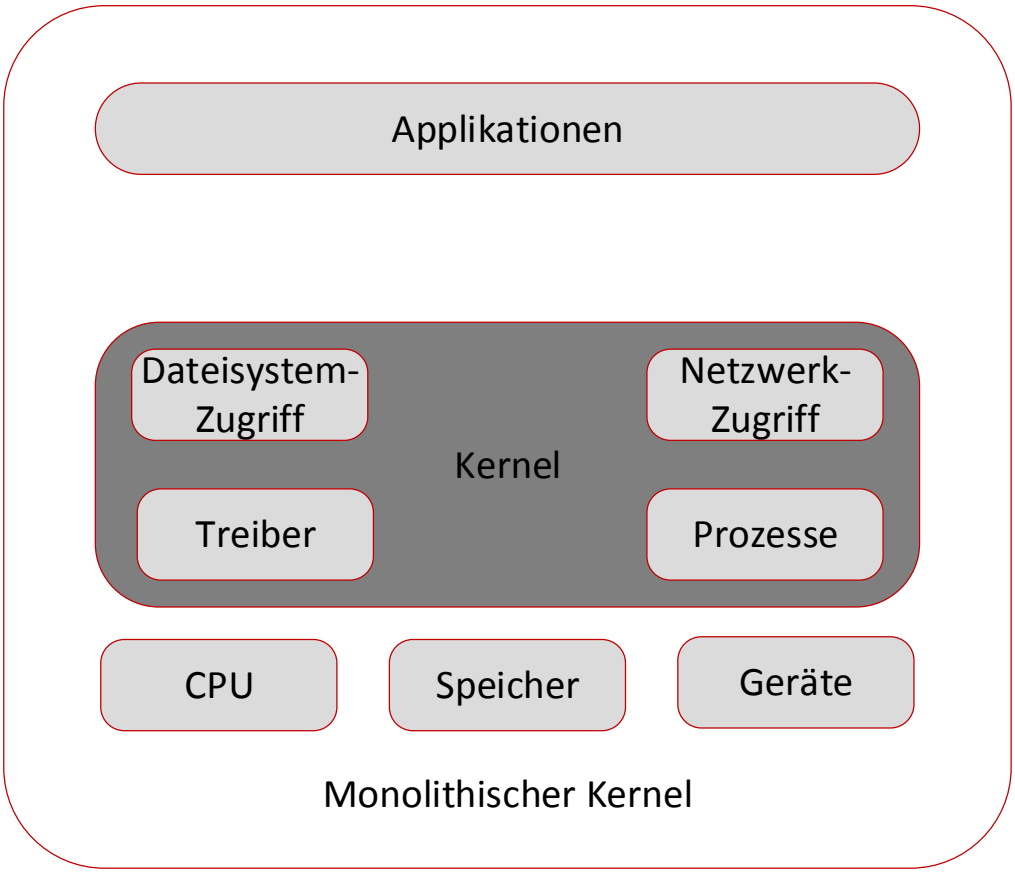


Abbildung 2: Monolithischer Kernel

Dies hat auf der einen Seite einen Geschwindigkeitsvorteil, auf der anderen Seite aber auch einen entschiedenen Nachteil. Wenn ein Gerätetreiber einen Fehler hat und abstürzt kann dieser nicht neu geladen werden. In diesem Fall ist immer ein Neustart des Kernels und somit des gesamten Betriebssystems notwendig, es entsteht ein Problem bei der Verfügbarkeit. Moderne Kernel, wie sie beispielsweise in GNU/Linux[5], BSD/OS[6], MS-DOS[7] und Windows 95/98/ME zum Einsatz kommen, zählen zwar noch zu den monolithischen Kerneln, verfügen aber über dynamisch neustartende Komponenten. Sie ermöglichen die Auslagerung von Software-Komponenten, wie Gerätetreibern in separate Module, die dann zur Laufzeit geladen oder neugestartet werden können. Ein Neustart einzelner Module ist somit bei dieser Art monolithischer Kernel verfügbar, dies ermöglicht eine höhere Verfügbarkeit.

[5] http://de.wikipedia.org/wiki/GNU/Linux *GNU/Linux ist ein freies und quelloffenes Betriebssystem*
[6] http://de.wikipedia.org/wiki/BSD/OS *BSD/OS ist ein kommerzielles Unix-Betriebssystem*
[7] http://de.wikipedia.org/wiki/MS-DOS *MS-DOS Microsofts erstes Betriebssystem für x86-PC's*

1.3.4 Mikrokernel

Der Mikrokernel beinhaltet nur die notwendigsten Funktionen zur Prozess- und Speicherverwaltung. Alle anderen Treiber und Funktionen befinden sich außerhalb des Kernels und laufen auf der Benutzerebene (s. Kapitel 1.3.6).

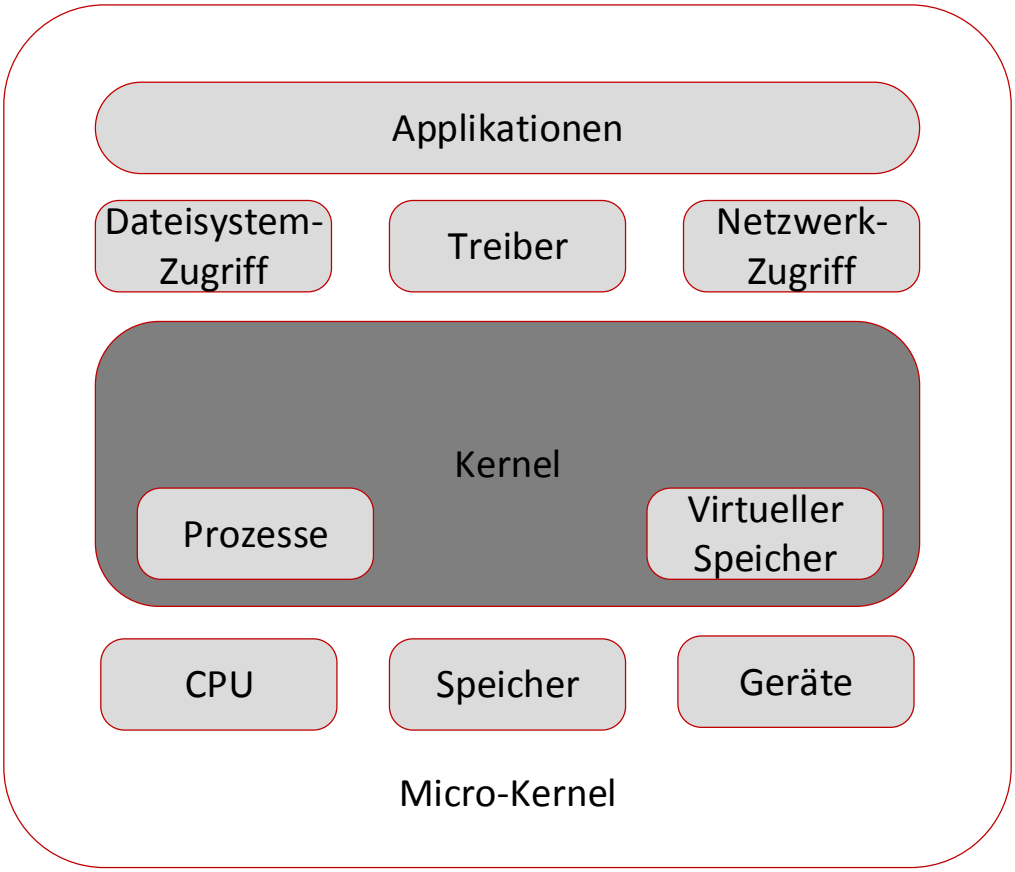


Abbildung 3: Microkernel

Dies ermöglicht eine hohe Stabilität und mehr Sicherheit. Die Struktur des Kernels macht jedoch einen kontinuierlichen Kontextwechsel[8] notwendig, da für die Ausführung der Treibersoftware immer zwischen Kernel- und Benutzerebene hin und her gewechselt wird und erzeugt so einen höheren Datenaufwand. Folglich haben Microkernel eine vergleichbar schlechtere Performance, obwohl das Design im Vergleich zu Monolithischen Kernel schlanker ist. Betriebssysteme, die diese Art Kernel verwenden, sind beispielsweise die noch bekannteren Betriebssysteme wie AmigaOS[9] und Symbian OS[10] aber auch unbekanntere wie Minix[11] und ChorusOS[12]. Mikrokernel werden oft auch im Bereich der eingebetteten-Systeme und Spezial-Hardware bevorzugt eingesetzt, beispielsweise in der Flug und Fahrzeugen.

[8] *Ein Kontextwechsel ist ein Vorgang in einem Betriebssystem zwischen zwei oder mehreren Prozessen und bringt einen höheren Arbeitsaufwand mit sich (vgl. http://de.wikipedia.org/wiki/Kontextwechsel)*
[9] *http://de.wikipedia.org/wiki/AmigaOS AmigaOS wurde für den Commodore Amiga entwickelt.*
[10] *http://de.wikipedia.org/wiki/Symbian_OS Symbian OS wurde von Nokia entwickelt.*
[11] *http://de.wikipedia.org/wiki/Minix_(Betriebssystem) Zu Lehrzwecken entwickeltes Betriebssystem.*
[12] *http://de.wikipedia.org/wiki/ChorusOS ChorusOS ist ein Betriebssystem für Echtzeitsysteme.*

1.3.5 Hybridkernel

Der Hybridkernel, auch bekannt als Makrokernel, stellt den Kompromiss zwischen dem monolithischen Kernel und Mikrokernel dar.

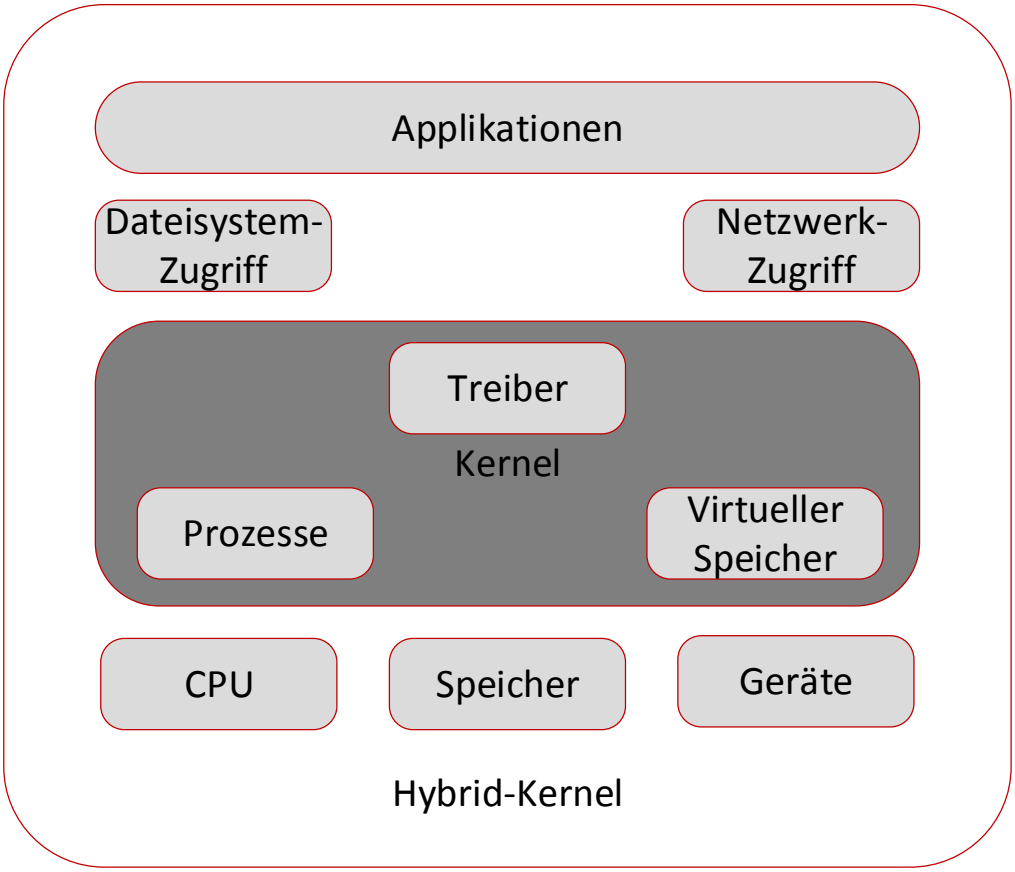


Abbildung 4: Hybridkernel

Der Hybridkernel basiert im Allgemeinen auf den Vorteilen des Micro und des Monolithischen Kernels. Die beim Micro-Kernel vorhandenen Vorteile durch eine hohe Stabilität wurden durch die Integration von Treibermodulen im Kernel erreicht, diese führen bei einem Treiberfehler nicht mehr zum Systemabsturz. Die Treiber werden nur in einem privilegierten Modus ausgeführt (siehe Abbildung 5: Ring-Schema bei Prozessoren). Die Geschwindigkeitsvorteile des Monolithischen Kernel wurden durch eine Minimierung der Kontextwechsel erreicht. Da nicht festgelegt ist welche Komponenten zusätzlich im Kernel integriert werden müssen, kann jedes Unternehmen, das sich an der Herstellung von Kernel-Komponenten beteiligt, eine individuelle Konfiguration erstellen. Soll eine höhere Grafikleistung erreicht werden, können beispielsweise spezielle Grafiktreiber in den Kernel integriert werden. Der Nachteil bei diesem Vorgehen ist jedoch, dass bei fehlerhaften Grafiktreibern das System im schlimmsten Fall abstürzt. Betriebssysteme, die diese Art Kernel verwenden sind unter anderem Windows 2000,2003, Server 2008, Windows XP, Windows Vista sowie Windows 7 und 8.

1.3.6 Virtualisierungsgrundlagen der x86-Architektur

Zum besseren Verständnis der unterschiedlichen Virtualisierungskonzepte werden einige Hintergrundinformationen benötigt, die in den folgenden Abschnitten genauer

dargelegt werden. Um den Umfang der Virtualisierungsgrundlagen zu reduzieren beschränken sich die folgenden Informationen nur auf die x86-Architektur von modernen Prozessoren. Die x86-Architektur kommt in den meisten Desktop- und Server-Systemen zum Einsatz und weist daher eine sehr hohe Verbreitung auf:
Aus Gründen der Sicherheit und Stabilität, ist ein Betriebssystem in zwei logische Komponenten aufgeteilt, der Kernelschicht und der Anwendungsschicht. Diese Aufteilung wird auch durch die x86-Architektur unterstützt, bei der die Kernkomponenten innerhalb eines eigenen Speicherbereichs ausgeführt werden. Hierbei wird vom dem so genannten Kernel-Mode gesprochen, siehe Abbildung 5. Dieser verfügt unter anderem über die Rechte zum Verwalten der Prozesse, des Speichers und weiterer wichtiger Ressourcen eines Systems. Die zweite Komponente ist der User-Mode, der weitaus weniger Rechte für den Zugriff auf Ressourcen besitzt. Diese Aufteilung wurde aus Sicherheits- und Stabilitätsgründen eingeführt. So laufen sämtliche Programme eines Systems, abgesehen vom Kernel, im User-Mode.

Der User-Mode ist eine Funktion, die Betriebssysteme fehler- und ausfallsicherer macht.

Die Idee dahinter ist, dass diese Applikationen nicht direkt auf dem Kernel und die durch diesen verwalteten Ressourcen zugreifen dürfen.
So ist beispielsweise der Hauptspeicher nur vom Kernel direkt nutzbar. Damit auch User-Mode-Applikationen bestimmte Ressourcen nutzen können, bieten alle Kernel verschiedene Schnittstellen an, die aus dem User-Mode heraus angesprochen und genutzt werden können. Auf diesem Weg kann auch indirekt der Speicher durch User-Mode-Applikationen genutzt werden. Die grundlegende Kontrolle darüber bleibt aber in der Zuständigkeit des Kernels selbst. So kann verhindert werden, dass Applikationen kritische Komponenten in einem Betriebssystem beeinflussen oder manipulieren, die für einen reibungslosen Ablauf und die Stabilität von absoluter Notwendigkeit sind. Abbildung 5 veranschaulicht den Aufbau dieser Separierung anhand des sogenannten Ringe-Schemas[13]. Umso höher die Ringnummer, umso weniger Rechte hat die Ausführungsebene. Die Ringe bilden die bereits in der x86-Architektur umgesetzte Hierarchie zur Prozessverwaltung symbolisch ab.

[13] http://de.wikipedia.org/wiki/Ring_(CPU) *Privilegierungs- bzw. Sicherheitsstufen eines Prozesses.*

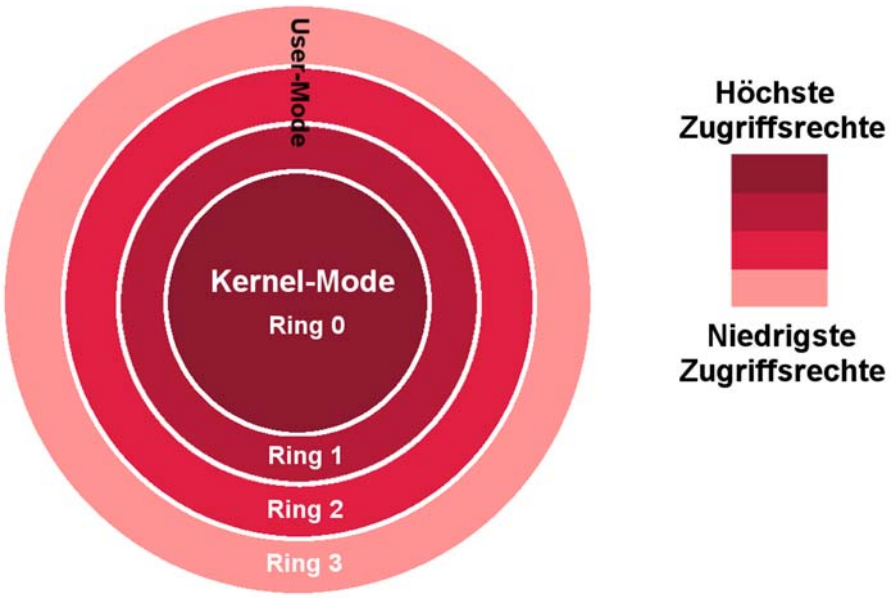


Abbildung 5: Ring-Schema bei Prozessoren

Der Kernel befindet sich in der Regel im Ring 0. Muss nun eine Anwendung beispielsweise direkt den Speicherbereich des Ring 0 beschreiben, tritt eine Speicherzugriffsverletzung auf. Diese Zugriffsverletzung kann dann durch den Kernel verarbeitet werden, was in den meisten Fällen zur sofortigen Beendigung der Applikation führt.

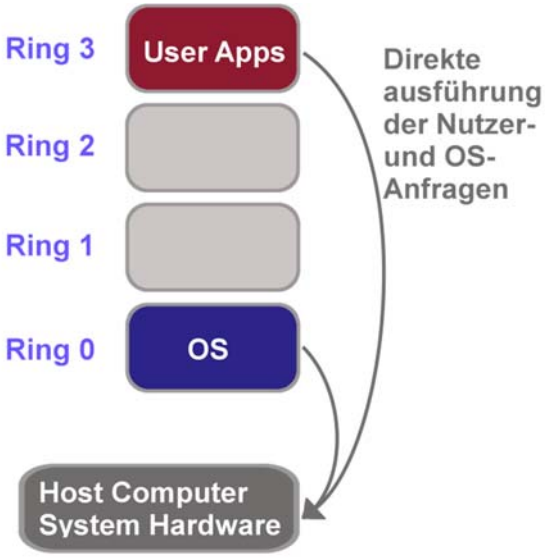


Abbildung 6: Prozessausführung auf nicht virtualisiertem Computer

Diese Einteilung bringt neben den geschilderten Vorteilen aber auch einige Nachteile für die Virtualisierung mit sich: Eine virtuelle Maschine ist in erster Linie nichts anderes als eine User-Mode-Applikation. Dasselbe gilt demzufolge auch für die gestarteten Betriebssysteme innerhalb einer virtuellen Maschine. Ressourcenzugriffe aus dem Gastbetriebssystem heraus können nicht direkt vorgenommen werden. Dies gilt hier ebenfalls für den Kernel des Gastsystems, also der virtuellen Maschine. Einzig der Kernel des Hosts hat die entsprechende Berechtigung direkt auf Ressourcen zuzugreifen und kann diese der virtuellen Maschinen zuteilen.

Durch diese Einschränkung entstanden unterschiedlichen Virtualisierungskonzepte: Die erste mögliche Methode ist, dass der Hypervisor alle kritischen Systemaufrufe kurz vor dem eigentlichen Ressourcenzugriff aus einem Gast-System abfängt, um diese in virtuelle Aufrufe umzuformen und schließlich auszuführen. Bei diesem Verfahren wird von „binary translation“ (siehe Abbildung 7) gesprochen.

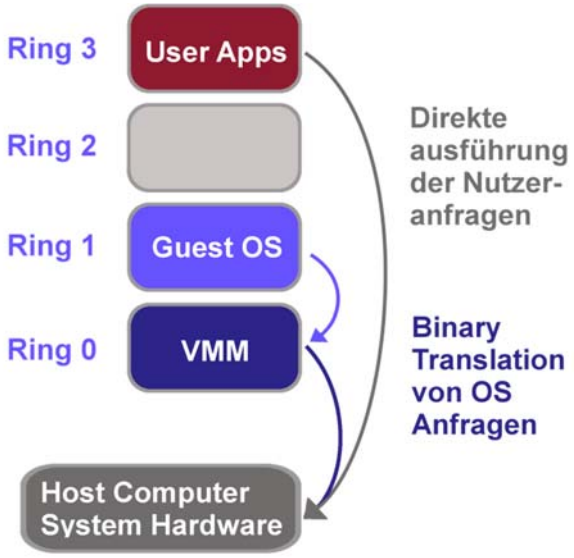


Abbildung 7: Virtualisierung mit binary translation

Diese Methode ist jedoch mit einem höheren Aufwand verbunden und kann zu Performanceverlusten führen. Dieses Verfahren wird zumeist bei Vollvirtualisierung verwendet und ist daher maßgeblich für den Einsatz bei der Desktop-Virtualisierung gedacht.

Der zuvor beschriebene Performanceverlust ist jedoch in vielen Fällen nicht akzeptabel, beispielsweise im Bereich der Servervirtualisierung, wo Prozesse im hohen Maß performant ausgeführt werden müssen. Dem Ringmodel zufolge müsste der Hypervisor in einem privilegierteren Ring laufen, um Ressourcen besser nutzen zu können.
Das Betriebssystem ist in der Regel so aufgebaut, dass die Kernkomponenten, also der Kernel, im Ring 0 laufen. Die Lösung dieses Problems liegt in der Anpassung des Kernelsystems des Hosts, so dass diese nicht in Ring 0 sondern in Ring 1 ausgeführt werden.
Bei diesem Ansatz wird von der so genannten Paravirtualisierung gesprochen. Hierbei wird versucht „binary translation“, also die langsamere Virtualisierungsmethode weitgehend zu vermeiden. Für Paravirtualisierung muss jedoch der Kernel des Gastbetriebssystems soweit modifiziert werden, dass dieser auf Ring 1 laufen kann.
Die Systemaufrufe werden nun über sogenannte Hypercalls realisiert (siehe Kapitel 1.3.9). Alle problematischen Aufrufe des Gast-Systems werden so über den Hypervisor geführt, der wiederum führt entsprechende Systemcalls aus und bedient damit das Gastsystem.
Ein Host-Betriebssystem muss bereits für ein solches Szenario angepasst sein. Wenn ein Betriebssystem nicht angepasst wurde und auch nicht Quelloffen zu Verfügung steht, ist der Einsatz von Paravirtualisierung nicht möglich.

1.3.7 Hypervisor

Der Hypervisor stellt die Schnittstelle des Betriebssystems mit der darunter liegenden Hardware und der virtuellen Maschinen dar. Im Allgemeinen wird zwischen zwei Arten von Hypervisoren unterschieden, diese werden in den folgenden Abschnitten dargestellt:

TYP-I Hypervisor (Bare-Metal-Lösung)

Der Typ-1 Hypervisor läuft sehr Hardware nah und benötigt kein umfangreiches Betriebssystem auf dem dieser betrieben wird. Daher wird der Typ-1 Hypervisor auch als „Bare-Metal“[14]-Lösung bezeichnet. Die meisten Komponenten des Hypervisors werden bei einem Typ-1 Hypervisor selber in einer virtuellen Umgebung ausgeführt, benötig also sehr wenig Ressourcen für die eigene Ausführung. Dieser Typ Hypervisor hat den Vorteil, dass er über eine sehr kompakte Struktur verfügt und daher sehr schnell arbeitet. Aus diesem Grund wird dieser Typ häufig im Bereich der Server-Virtualisierung eingesetzt. Im folgenden Bild sehen Sie beispielhaft den Einsatz einer Bare-Metal-Lösung bei einem Cloud-Service-Provider.

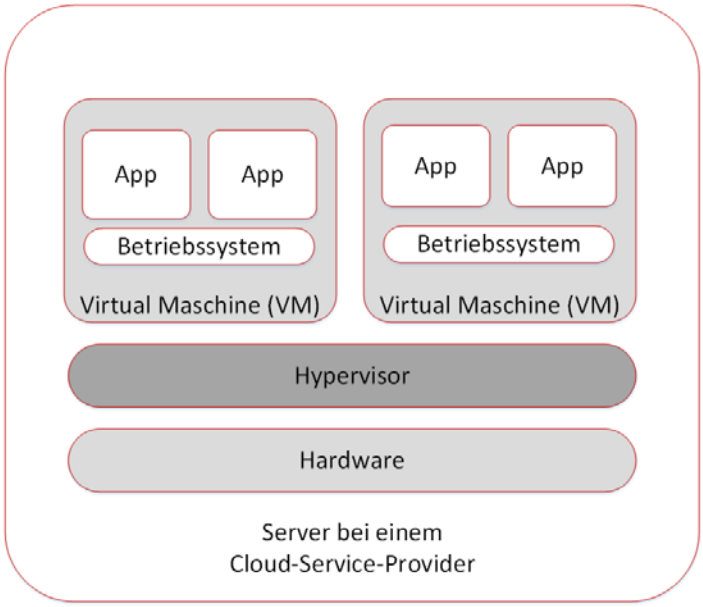


Abbildung 8: Bare-Metal-Lösung mit Hypervisor direkt auf der Hardware

Nachteile dieser Lösung sind die besonderen Hardwareanforderungen. Nicht jeder Treiber von verschiedenen Hardwareherstellern wird durch Bare-Metal-Lösungen unterstützt, was die Vielfalt der verwendbaren Hardware eingrenzt. Es können nur Produkte verwendet werden, für die geeignete Treiber verfügbar sind. Zum Einsatz kommt der Typ-1 Hypervisor beispielsweise in den Virtualisierungslösungen von Xen[15], IBMz/VM und den VMware Server Produkten.

[14] *Sinnbildlich eine Ausführung auf dem blanken Metall (bare metal).*
[15] *http://de.wikipedia.org/wiki/Xen Xen Hypervisor*

TYP-II Hypervisor (Hosted-Lösung)

Anders als der Typ-1 Hypervisor benötigt der Typ-2 Hypervisor ein Basis-Betriebssystem. Er kann im Prinzip mit einem Programm verglichen werden, welches innerhalb eines Betriebssystems installiert und ausgeführt wird. Aus diesem Grund wird der Typ-2 Hypervisor auch als „Hosted"-Lösung bezeichnet. Der Typ-2 Hypervisor kann somit auf vielen gängigen Betriebssystemen (beispielsweise Windows, Linux und MacOSX) installiert und genutzt werden, da dieser keine spezielle Hardware benötigt und Inkompatibilitäten hierbei sehr selten Auftreten. Die Hardware wird bei einem Typ-2 Hypervisor als eine Abstrahierung zur Verfügung gestellt.

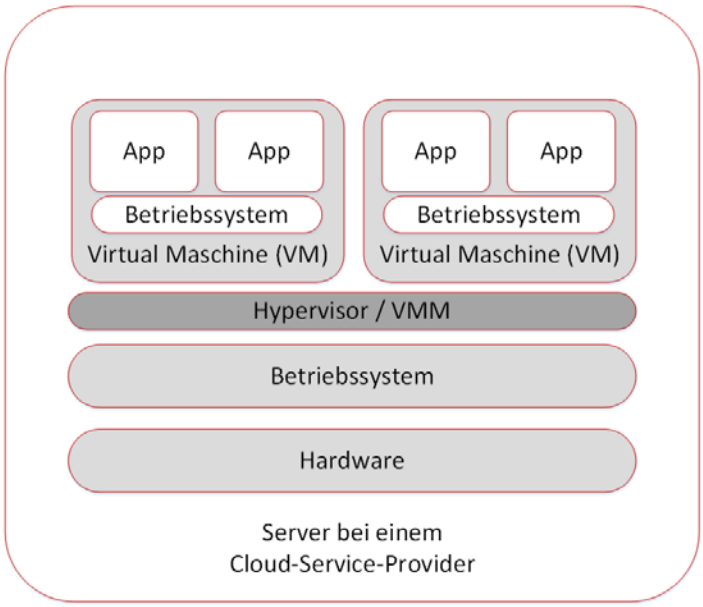


Abbildung 9: Hosted-Lösung auf dem Betriebssystem

Im Vergleich zum Typ-1 Hypervisor hat die Hosted-Lösung einen höheren Ressourcenverbrauch, da bei der Abstrahierung von Schnittstellen und Hardware mehr Rechenleistung, zum Beispiel durch die Verwendung von „binary translation", benötigt wird. Hardwareschnittstellen werden bei einem Typ-2 Hypervisor oft durch Emulation zur Verfügung gestellt, dies bedeutet, dass die innerhalb der virtuellen Maschine verfügbare Hardware – meist in Form von Netzwerk- und Grafikkarten – nicht als reale Hardware vorliegen muss. Diese Komponenten werden durch den Hypervisor emuliert. Die Arbeitsweise eines Typ-2 Hypervisors wird daher als Vollvirtualisierung bezeichnet. Diese Art von Hypervisor wird durch die Vorzüge, wie beispielsweise die Unterstützung und Kompatibilität zu vielen verschiedenen Betriebssystemen, maßgeblich im Bereich der Desktop-Virtualisierung eingesetzt. Typische Beispiele für einen Typ-2 Hypervisor, sind die bekannten Produkte VirtualBox und VMware Workstation.

1.3.8 Vollvirtualisierung (Komplettvirtualisierung)

Vollvirtualisierung ist eine Methode der Virtualisierung, bei der Hardwareressourcen für das Gast-System vollständig durch Virtualisierungssoftware bereitgestellt werden. Diese virtuellen Ressourcen, wie CPU, Arbeitsspeicher, Laufwerke, Netzwerkkarten und sogar ein BIOS werden hierbei den jeweiligen Virtuellen Maschinen zugewiesen und durch den Virtual Machine Monitor verwaltet.
Der „Virtual Machine Monitor" (VMM), auch allgemein als Hypervisor bezeichnet, wird als Anwendung auf dem Host-Betriebssystem ausgeführt und reguliert die Verteilung

der Hardwareressourcen des Host-Systems an die verschiedenen Gast-Systeme. Da diese keinerlei Zugriff auf die Hardware des Hosts haben, muss die Verteilung der Ressourcen wieder über den Hypervisor mit höheren Rechten stattfinden. Hierbei wird die Hardware jeder virtuellen Maschine emuliert, so dass eine hohe Flexibilität und eine optimale Ressourcenauslastung erreicht werden kann. Durch die Emulation können dem Gast-System beispielsweise mehrere unterschiedliche Netzwerkkarten zur Verfügung gestellt werden (siehe Abbildung 10), welche nicht mit der tatsächlich im Gerät verbauten Karte übereinstimmen müssen. So können gerade alte Gast-Systeme, die über keine Unterstützung moderner Hardware verfügen weiterhin genutzt werden.
Hierbei ist jedoch zu beachten, dass alte Betriebssysteme oder veraltete Software oft nicht mehr hinreichend oder wie bei Windows XP gar nicht mehr mit Sicherheitsupdates versorgt werden. Daher ist immer die Verwendung von aktuellen Software- und Betriebssystemen notwendig.

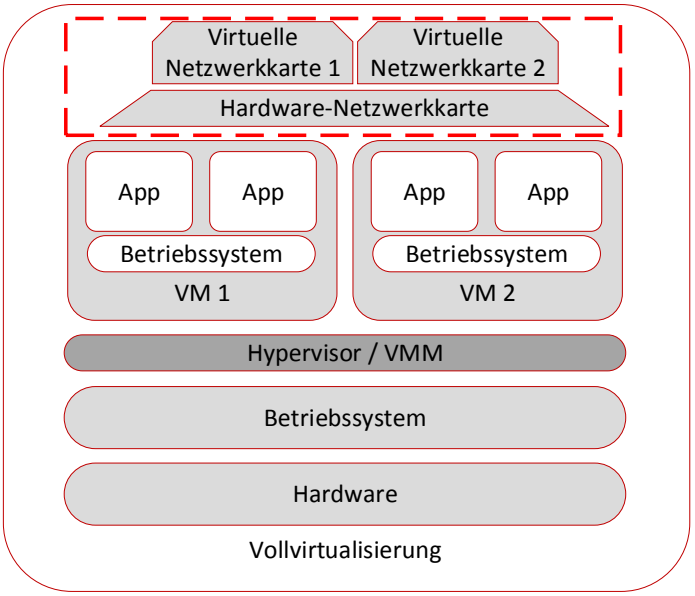


Abbildung 10: Vollvirtualisierung mit virtuellen Netzwerkkarten

Der in der Vollvirtualisierung eingesetzte Hypervisor ist vom TYP-2. Der primäre Einsatzbereich der Vollvirtualisierung ist im Desktop-Bereich angesiedelt und hat daher eine hohe Verbreitung. Aber auch im Bereich der Server-Virtualisierung kann diese Technologie eingesetzt werden, obgleich hier andere Virtualisierungslösungen eine weitaus höhere Performance bieten. Die Vollvirtualisierung wird beispielswiese in den Produkten Parallels Workstation, Parallels Desktop for Mac, VirtualBox, Virtual PC, Hyper-V, VMware Workstation und VMware Server eingesetzt.

Vorteile

- Virtualisierung kann durch die Installation einer Software (z.B. VirtualBox/ VMware Workstation) realisiert werden
- Das Gastsystem muss nicht angepasst werden
- Es sind vom Host und anderen Gästen unabhängige Gastsysteme (Betriebssystem-Typ, -Version) einsetzbar.
- Vielseitige (virtuelle) Gast-Hardware möglich (Netzwerkkarten, Soundkarten)
- Eine flexible Anpassung der Gast-Hardware (teilweise auch während der Laufzeit) ist möglich.

Nachteile

- Ist Vergleichsweise langsam durch „binary translation“.
- Einige Hardwarekomponenten lassen sich im Gastsystem nicht abbilden (etwa Faxkarten).
- virtuelle Hardware wird für jede VM als Prozess abgebildet ("Schwund" / Leistungseinbußen)
  Quelle: (Bertram Wöhrmann, 2012)

Einsatzbereiche

- Eignet sich insbesondere in kleineren Umgebungen mit nur wenigen virtualisierten Maschinen
- Daher besonders für den Einsatz in Handwerksunternehmen geeignet

Quelle : Christian Baun, 2010

1.3.9 Paravirtualisierung

Eine weitere Virtualisierungstechnologie ist die Paravirtualisierung. Hierbei werden anders als bei der Vollvirtualisierung keine Hardwarekomponenten emuliert oder virtualisiert. Bei der Paravirtualisierung wird eine Programmschnittstelle (API[16]- in Abbildung 11 als Virtual-Layer dargestellt) durch den Hypervisor bereitgestellt, die wiederum vom Gast genutzt werden muss. Diese Schnittstelle ermöglicht auch den Zugriff der virtuellen Maschinen auf die Hardwareressourcen des Host-Systems. Der in dieser Technologie eingesetzt Hypervisor ist vom TYP-I.
Die Besonderheit der Paravirtualisierung liegt im Aufbau des Gast-Systems, bei dem der Hypervisor im Ring 0 ausgeführt wird, alle Gast-Systeme befinden sich im Ring 1.

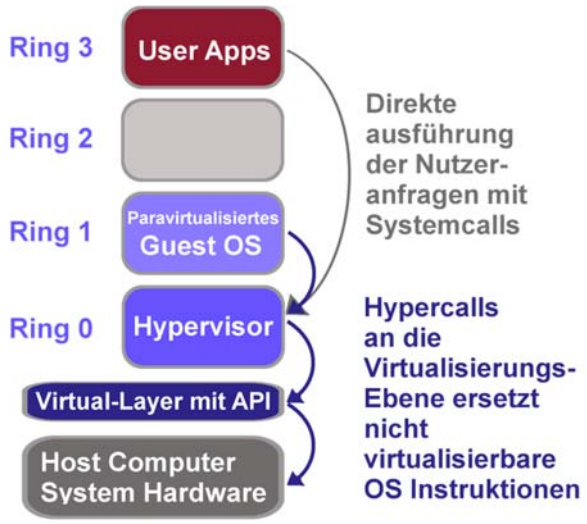


Abbildung 11: Paravirtualisierung

[16] *API, **A**pplication **P**rogramming **I**nterface, auf Deutsch Anwendungsprogrammierschnittstelle*

Der einzige Unterschied zu allen weiteren virtualisierten Gast-Systemen ist, dass die Gast-Komponenten in Ring 1 keinen privilegierten Zugriff auf die Ressourcen erhalten. Dies wird jedoch, wie bereits erwähnt, durch Hypercalls realisiert, die wiederum ein modifiziertes Host-Betriebssystem benötigen. Zum Einsatz kommt dabei ein auf ein Minimum reduziertes Host-Betriebssystem (auch Metabetriebssystem genannt).
Nachteil dieser Technologie ist, dass eine Anpassung des Host-System-Kernels notwendig ist. Im Linux-Kernel ist Paravirtualisierung ab Version 2.6.20 möglich. Der Kernel kann mit Hilfe einer API vom Hypervisors angesprochen werden. Diese Anpassungen des Gast-Kernels umfassen bei einem Linux-Kernel etwa ein, bis zwei Prozent der x86-spezifischen Bestandteile.
Der Umfang notwendiger Anpassungen an einem Linux-Kernel liegt im Bereich von 1-2%, bei einem Windows XP Kernel liegt dieser Anteil bei etwa 0,1 Prozent, wobei diese Werte lediglich auf die Größe des jeweiligen Kernels bezogen sind (Meinel et al., 2011).
Diese Architektur der Virtualisierung kann im Vergleich zur Vollvirtualisierung den Performanceverlust durch Binary-Translation minimieren. Problematisch wird diese aber bei nicht quelloffenen Gast-Systemen, wie beispielsweise Microsoft Windows. Hierbei ist es Dritten nicht möglich die notwendigen Änderungen zur Anpassung an eine Paravirtualisierung durchzuführen. Hier muss der Hersteller des Gast-Systems aktiv werden und diese Anpassungen selber durchführen. So kann nicht sichergestellt werden, dass jedes Betriebssystem als Gast auf Basis einer Paravirtualisierung geeignet ist.
Beispielsoftware mit Paravirtualisierungsunterstützung sind Xen[17] und QEMU[18].

Vorteile

- Kommunikation über eine API deutlich schneller als bei Emulation oder Vollvirtualisierung.
- Kein Performanceverlust durch „binary translation“.

Nachteile

- Der Kern des Betriebssystems muss angepasst werden oder bereits durch einen Hersteller modifiziert sein.

Einsatzbereiche

- Rechenzentren die bewusst auf open source Lösungen setzen, um Lizenzkosten zu sparen.
- Anbieter von Cloud-Computing-Lösungen.

1.3.10 Paravirtualisierung mit Hardwareunterstützung

Eine weitere Möglichkeit ist die Virtualisierung mit Hilfe von Hardwareunterstützung im Prozessor des Host-Computers. Im Jahr 2005 hat Intel eine neue Generation von

[17] http://www.xenproject.org/ *Freier Hypervisor für die Virtualisierung von Betriebssystemen*
[18] http://de.wikipedia.org/wiki/QEMU *QEMU ist eine freie Virtualisierungssoftware*

Prozessoren herausgebracht, die Erweiterungen zur Virtualisierung (VT-x[19]) enthalten. AMD folgte ein Jahr später mit einer vergleichbaren Technologie (AMD-V[20]).
Beide Hersteller setzen dabei auf eine Erweiterung der Ring-Topologie (vgl. Abbildung 5) des Prozessors, wobei beide Lösungen nicht miteinander kompatibel sind.
Die neue Ebene wird als Root-Modus oder root-mode bezeichnet (siehe Abbildung 12).

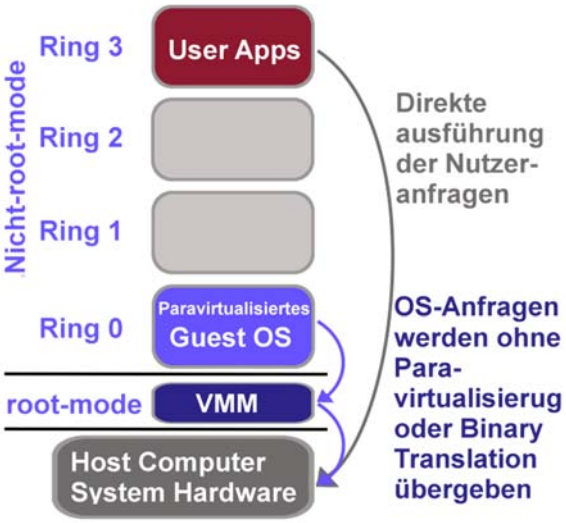


Abbildung 12: Paravirtualisierung mit Hardwareunterstützung

Diese Erweiterung bringt einige wesentliche Vorteile mit sich: So ist es hiermit nicht mehr notwendig den Kernel des Gast-Systems zu modifizieren. Der Hypervisor verschiebt sich so logisch um eine Ebene nach unten, so dass der Kernel des Gast-Systems wieder in Ring 0 operieren kann. Dabei behält die Paravirtualisierung ihre Vorteile gegenüber der Vollvirtualisierung in Bezug auf die Minimalisierung der Binary Translation. Die Hypercalls müssen nicht weiter übersetzt werden sondern können direkt und nativ durch die beschriebenen Virtualisierungstechnologien im Prozessor ausgeführt werden.

Vorteile

- Es sind keine Modifizierungen am Gast-Kernel notwendig, wie es beispielsweise bei Paravirtualisierung der Fall ist.
- Kein Overhead durch binary translation, da der Prozessor Befehle der virtuellen Maschinen direkt übersetzen kann.
  (Christoph Meinel, Christian Willems, Sebastian Roschke, Maxim Schnjakin, 2011)
- Viele aktuelle Prozessoren bieten Hardwareunterstützung für Virtualisierung.

[19] http://de.wikipedia.org/wiki/Intel_Virtualization_Technology *Intel Virtualization Technology*
[20] http://de.wikipedia.org/wiki/AMD-V *AMD Virtualization*

Nachteile

- veraltete Prozessoren ohne Hardwareunterstützung eignen sich nicht für einen Einsatz

Einsatzbereiche

- Rechenzentren mit hohem Datendurchsatz

1.3.11 Betriebssystemvirtualisierung

Ein gänzlich anderer Ansatz im Bereich der Virtualisierungsmethoden ist die Betriebssystemvirtualisierung. Hierbei kommt kein Hypervisor zum Einsatz. Die Gäste sind in sogenannten Jails – auch Container genannt – untergebracht und sind lediglich jeweils eine Teilmenge des Host-Betriebssystems. Die Gäste sind durch die Container, wie bei anderen Virtualisierungstechnologien stark voneinander isoliert. Dabei verwenden Host und alle Gäste denselben Kernel, der auf dem Host-System installiert ist. Dabei verwaltet dieser Kernel alle Ressourcen des Systems und teilt diese unter den Containern auf (siehe Abbildung 13).

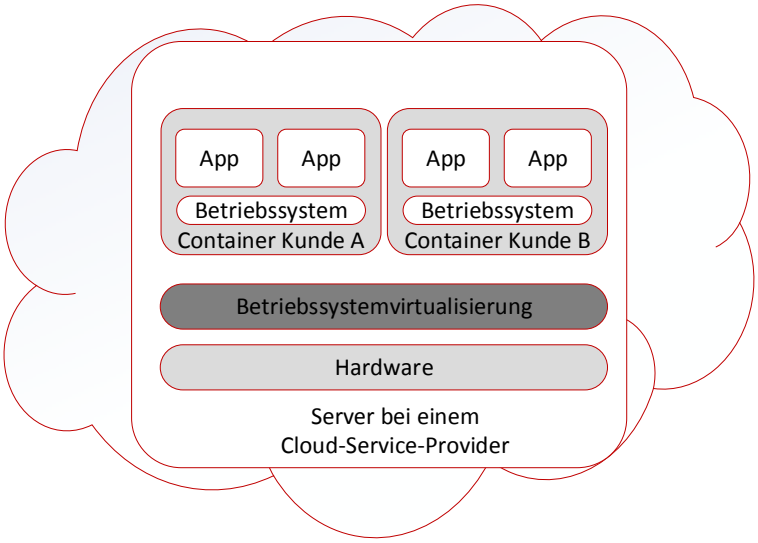


Abbildung 13: Beispielhafte Betriebssystemvirtualisierung

Alle Applikationen innerhalb der Container laufen als Prozess auf dem Host-Kernel. Innerhalb der Container sind jedoch nur die eigenen Ressourcen und Prozesse sichtbar. Alle Ressourcen sind so sicher vor anderen Teilnehmern verborgen.
Die Betriebssystemvirtualisierung nutzt die Hardware-Ressourcen durch die Architektur weitaus besser aus, als alternative Virtualisierungsmethoden und weist eine sehr gute Performance auf.
Dabei ist die Wahl des Gast-Systems vom Kernel des Host-Systems abhängig, da dieses Binärkompatibel, also identisch sein muss. Durch den gemeinsam genutzten Kernel besteht allerdings auch ein höheres Sicherheitsrisiko. Wird ein Gastsystem durch Schadsoftware, oder einen Angreifer übernommen, kann bei einer erfolgreichen Übernahme des Host-Systems das gesamte System, inklusive aller weiteren Container gekapert werden. Die Aktualität des Systems ist somit ein wichtigerer Bestandteil, nicht nur bei der Betriebssystemvirtualisierung.
Diese Virtualisierungsmethode wird sehr häufig für die Realisierung mietbarer V-Server eingesetzt, wobei diese nicht zwingend eine Betriebssystemvirtualisierung nutzen müssen.

Beispiele für Betriebssystemvirtualisierung sind SWSoft Virtuozzo / OpenVZ, Linux vServer, SUN Zones, BSD Jails und LXC (LinuX Containers). Einen aktuellen Ansatz stellt die freie Software Docker[21] zur Verfügung.

Vorteile

- Große Anzahl an Container auf einem Host-System möglich
- Hohe Geschwindigkeit

Nachteile

- Werden Änderungen am Host durchgeführt, müssen auch Gastsysteme angepasst werden. Dies bringt einen Wartungszeitraum mit sich und verringert die Verfügbarkeit.

Einsatzbereiche

- Anbieter von Virtualisierungs-Containern in größeren Rechenzentren.

1.3.12 Emulation

Bisher haben wir nur Verfahren zur Virtualisierung kennengelernt, in der Gast-Prozessor dieselbe Hardware-Architektur aufweist wie das Host-System. Für die bereits erwähnten Methoden zur Virtualisierung ist diese Einschränkung auch zwingend erforderlich, da viele Operationen direkt auf dem Host-Prozessor ausgeführt werden.
Gesetzt den Fall, Sie müssen ein Betriebssystem auf einem Host installieren, der in keiner Weise kompatibel zu ihrer Hardware ist, können keine der bisher beschriebenen Virtualisierungsmethoden verwendet werden.
Emulation bietet hier die Lösung, da die vollständige Hardware, inklusive der CPU durch die Emulationssoftware simuliert werden kann.
Dabei werden alle Instruktionen der emulierten Hardware in die Instruktionen der realen Plattformarchitektur übersetzt und daraufhin ausgeführt. Dieses Vorgehen ist sehr Aufwändig und erfordert sehr viel Rechenleistung des Prozessors, was wiederum zu einem Geschwindigkeitsverlust führen kann. Emulation bietet beispielsweise die Möglichkeit auf einer x86-Plattform Gast-Systeme für eine ARM-Architektur[22] auszuführen. So ist eine Emulation zwar langsamer als andere Virtualisierungstechnologien, aber dennoch sehr flexibel einsetzbar.
Beispiele für bekanntere Emulatoren sind die Programme Windows Virtual PC und QEMU (Kurzform für „Qick Emulation“).

Vorteile

- Ausführen von Betriebssystemen die zur Hardware inkompatibel sind.

[21] https://www.docker.com/ *Freie Virtualisierungssoftware auf dem Container-Prinzip*
[22] http://de.wikipedia.org/wiki/ARM-Architektur *ARM Prozessorarchitektur*

Nachteile

- Ressourcenintensiv, dadurch langsamer als andere gängige Virtualisierungsmethoden.

Einsatzbereiche

- Wird für die Emulation von Computern oder Betriebssystemen eingesetzt, die aus Kostengründen nicht separat angeschafft werden sollen, beispielsweise bei Entwicklungsprozessen.

1.3.13 KVM - Kernel-based Virtual Machine

KVM (Kernel-Based Virtual Machine) ist eine Variante einer Vollvirtualisierung (TYP-II Hypervisor) und fester Bestandteil des Linux Kernels seit der Version 2.6.20.
Die Besonderheit dabei ist, dass der Kernel selbst nach dem Laden der erforderlichen Module als Hypervisor arbeitet. KVM setzt dabei vollständig auf die Hardware-Virtualisierungstechniken von Intel und AMD (VT-x und AMD-V siehe Kapitel 1.3.10) und kann aus diesem Grund eine hohe Performance erreichen. Eine weitere Besonderheit von KVM ist, dass nicht KVM selbst die virtuelle Hardware für die Gäste zur Verfügung stellt. Diese Bereitstellung erledigt eine Emulationssoftware mit dem Namen QEMU, die beispielsweise virtuelle Netzwerkkarten und Grafikadapter simuliert.
Bei Bedarf kann auch das Virtualisierungsframework VirtIO[23] eingesetzt werden, dass den virtuellen Maschinen IO-Schnittstellen für reale Netzwerkkarten, Speicher, Festplatte und so weiter bereitstellt. VirtIO ist bereits ab der Version 2.6.25 im Linux Kernel enthalten und bietet eine noch höhere Performance. VirtIO setzt die Unterstützung im Gast-System voraus, was in Linux bereits fest integriert ist und unter Windows durch spezielle Treiber realisiert werden kann.

IO – steht für Input und Output. Auf Deutsch ist die Eingabe und Ausgabe bei angeschlossenen Geräten gemeint.

Vorteile

- Sehr gute Performance
- Keine Lizenzkosten durch den Einsatz von Open-Source-Software
- Hohe Stabilität durch Integration in Linux Kernel

Nachteile

- Es sind wenige grafische Managementtools verfügbar, daher ist ein hoher Knowhow-Bedarf für Linux-Betriebssysteme notwendig.

Einsatzbereiche

- Rechenzentren
- Bereitstellung von Schulungsräumen
- Unternehmen mit großem Know-how im Bereich Linux-Administration

[23] http://docs.fedoraproject.org/de-DE/Fedora/12/html/Virtualization_Guide/chap-Virtualization_Guide-KVM_Para_virtualized_Drivers.html *(Englisch) KVM paravirtualisierte Treiber*

1.4 Vorteile durch Virtualisierung

Heutige Computer wurden dazu entwickelt ein spezielles Betriebssystem zu besitzen und vielfältige Aufgaben auszuführen. Jedoch sind die meisten Computer, je nach Aufgabe selten optimal ausgelastet.

Durch Virtualisierung kann die Auslastung von Servern verbessert und der Bedarf an Hardware verringert werden.

Das Hauptziel von Virtualisierung ist die Reduzierung von physikalischen Servern sowie der dafür nötigen Hardwarekomponenten. Ein weiteres Ziel ist die Komplexität bei der Verwaltung gering zu halten, um eine zentrale Administration zu gewährleisten. Typischerweise wird bei der Reduzierung von benötigten Servern oder Computern von Serverkonsolidierung oder allgemein Konsolidierung gesprochen.[24]

Serverkonsolidierung

Mittels Virtualisierung ist es demnach möglich mehrere Betriebssysteme und Aufgaben auf einem physikalischen Computer auszuführen. Daraus ergeben sich einige Vorteile die im folgenden Abschnitt näher erläutert werden.

Mehrere Gast-Systeme können auf einem physikalischen Computer erstellt werden. So ist es möglich viele Prozesse mit weniger Hardware gleichzeitig erledigen zu können. Ebenso werden die vorhandenen Ressourcen des Computers oder Servers effizienter auslastet. Hinsichtlich der Hardware haben virtuelle Maschinen immer dieselbe virtuelle Hardware, was bedeutet, dass die Updateprozesse zum Schließen von Sicherheitslücken und beseitigen von Fehlern zentral und überwiegend durch die Virtualisierungssoftware gesteuert werden kann. Dies hält die Komplexität der Systeme niedrig und vereinfacht die Wartbarkeit. Jedoch sollte beachtet werden, dass bei einem Update der Virtualisierungssoftware unter Umständen Änderungen an der virtuellen Hardware durch den Hersteller vorgenommen werden. Dies kann zur Folge haben, dass Anpassungen an der virtuellen Maschine vorgenommen werden müssen. Vor einem Update sollten daher Hersteller-Informationen eingeholt werden, ob Änderungen an den Gastsystemen oder am Host nötig sind. Hersteller kündigen solche umfangreichen Updates oft frühzeitig an, um vor Ausfällen oder Fehlern bei einem Update vorzubeugen.

Einsparung bei Hardwarewartung

Ein weiterer Vorteil durch Virtualisierung ist, dass der Aufwand für die Wartung der Host-Systeme, also den Servern auf der die Virtualisierung stattfindet, deutlich sinkt.

Die Wartungskosten bei Virtualisierung können optimiert werden.

Durch die Serverkonsolidierung läuft beispielsweise nur noch ein Server, wo hingegen ohne Virtualisierung noch drei Server samt Backup und unabhängiger Spannungsversorgung (USV) gewartet werden mussten. Lediglich die Hardware des Host-Systems muss überwacht und bei Ausfällen getauscht werden. Durch diesen Vorteil können Wartungskosten reduziert werden. Der Aufwand für die Update-Pflege eines Betriebssystems, beziehungsweise der darauf laufenden Software, bleibt jedoch gleich. Es gibt Systemprogramme die solche Update-Vorgänge automatisieren können, wie es beispielsweise mit dem VMware vSphere Update Manager[25] möglich

[24] http://openbook.rheinwerk-verlag.de/vmware/01_002.htm *Was ist Serverkonsolidierung?*
[25] http://www.vmware.com/de/products/vsphere/features/update-manager.html

ist. Dabei können Regeln erstellt werden, um alle virtualisierten Betriebssysteme mit wichtigen Sicherheitsupdates zentral versorgen zu können.

Geringere Ausfallzeiten

Da bei dem Einsatz von Virtualisierung durch die Serverkonsolidierung deutlich weniger Hardware zum Einsatz kommt, können mit den richtigen Maßnahmen auch Ausfallzeiten reduziert werden. Dies sind insbesondere Backupmaßnahmen, Maßnahmen zur Sicherung der Stromversorgung (USV) und das Vorhalten von ausfallgefährdeter Hardware. Damit sind insbesondere Netzteile und Festplatten gemeint, die bei einem Defekt zeitnah ersetzt werden müssen.
Auch die Ausfallzeiten bei einem möglichen Systemabsturz eines Betriebssystems in einer virtuellen Maschine, kann über die Nutzung von Snapshots (siehe Kapitel 3.10 und System-Images (siehe Kapitel 3.9) stark verkürzt werden.

Mit Hilfe von Snapshots der virtuellen Maschinen können Ausfall- und Systemwiederherstellungszeiten verringert werden.

Test von kritischen System-Updates

Auch Updateprozesse können mit virtuellen Maschinen sicherer durchgeführt werden, dazu kann eine virtuelle Maschine in eine Testumgebung geklont[26] werden. So kann testweise ein kritisches Update eingespielt und auf die Funktionsweise hin überprüft werden. Diese Vorgehensweise beugt Systemfehlern und Abstürzten nach einem kritischen Update vor.
Einige Hersteller von Virtualisierungssoftware ermöglichen sogar das Kopieren von virtuellen Maschinen samt Arbeitsspeicher auf andere Wirtsysteme, ohne die eigentliche virtuelle Maschine abschalten zu müssen. Mit dieser Methode kann wiederum eine geringere Ausfallzeit gewährleisten werden.

Mit Hilfe von virtualisierten Test-Systemen können kritische-Updates getestet werden, dies beugt Fehlern in den eigentlichen Produktiv-umgebungen vor.

Nutzung von System-Snapshots

Durch den Einsatz von Snapshots (siehe Kapitel 3.10) können virtualisierte Systeme deutlich schneller wiederhergestellt werden als durch System- oder Festplatten-Backups. Ein Snapshot speichert einen festgelegten Systemzustand mit all seinen geöffneten Applikationen sowie dem Inhalt des Arbeitsspeichers. Snapshots können für eine schnelle Wiederherstellung eines Betriebssystems verwendet werden, je nach Umfang des betroffenen Systems kann ein solcher Vorgang wenige Sekunden, bis hin zu mehreren Minuten in Anspruch nehmen. Dies ist aber ein Bruchteil von dem, was eine Neuinstallation oder das Wiedereinspielen von Daten aus einer Bandsicherung in Anspruch nehmen würde.

Snapshots sind ein sehr nützliches Werkzeug zur Sicherung und Wiederherstellung von Systemzuständen.

Ökonomisch und ökologisch effektiver

Aus ökologischer und ökonomischer Sicht kann behauptet werden, dass Virtualisierung Kosten senkt und ebenso die Umwelt schont. Durch die kleinere Dimensionierung von USV's, Klimageräten zur Kühlung und einem geringeren Bedarf an Hardware, können Energiekosten eingespart werden. Darüber hinaus kann durch einen geringeren Energie- und Kostenbedarf Geld gespart werden.

---

[26] *„Klonen" bezeichnet den Vorgang, bei dem ein System eins zu eins kopiert wird.*

Kurze Bereitstellungszeiten

Virtualisierung kann die Bereitstellung von neuen Arbeitsumgebungen deutlich verkürzen.

Der Zeitfaktor bei der Bereitstellung einer neuen virtuellen Maschine spielt ebenso eine tragende Rolle. Wenn ein System für eine neue Aufgabe benötigt wird, kann dies mit Hilfe von Virtualisierung in kürzester Zeit realisiert werden.
Früher hat die Bereitstellung, beispielsweise von einer Testumgebung, mehrere Stunden bis hin zu einigen Tagen in Anspruch genommen. Passende Hardware musste entweder vorhanden sein oder es musste gewartet werden, bis neu bestellte Hardware angeliefert wurde. Daraufhin musste die Hardware auch zusammengebaut und sicher im Serverschrank verbaut werden. Ganz zu schweigen vom Anschließen der Kabel und weiterer Peripherie. Heute genügen wenige Maus-Klicks in der Konfigurationsoberfläche des Hypervisors, um einen virtuellen Server oder einen virtuellen Desktop-PC mit Hilfe eines vorgefertigten Templates, also dem Abbild einer bereits vorkonfigurierten virtuellen Maschine zu erstellen und in Betrieb zu nehmen. Das Gast-System bedient sich einfach an den noch nicht ausgeschöpften Ressourcen des Host-Systems.
Auch das Entfernen von nicht mehr benötigten Servern ging nicht ohne einen gewissen Zeitverlust von statten. Ohne Virtualisierung waren echte Server-Anlagen vorhanden, bei denen erst die Hardware aus einem Rack oder aus dem Serverraum entfernt und zum Schluss entsorgt werden mussten. Virtualisierte Server können in wenigen Schritten sicher über das Konfigurationstool des Hypervisors gelöscht werden. Durch Virtualisierung können ebenfalls alte physikalische Hosts auf denen beispielsweise veraltete Software läuft ersetzt werden (siehe 4.1.1). Der Vorteil liegt auf der Hand, denn oft unterstützen aktuelle Betriebssysteme alte Branchensoftware nicht mehr. In einer virtualisierten Umgebung kann jedoch in einer speziell abgesicherten virtuellen Maschine für mehr Sicherheit gesorgt werden. Diese ist beispielsweise vom Netzwerk getrennt.

Einfacher Test von unbekannter Software oder neuen Betriebssystemen

Neu erworbene Software kann in einer virtuellen Testumgebung ausgiebig geprüft werden, ohne dass Produktiv-Systeme beeinträchtigt werden.

Ein weiterer Vorteil ist das Testen von Betriebssystemen oder neuer Software. Dafür muss keine neue Hardware beziehungsweise ein Test-PC angeschafft werden. Mit den Funktionen von Templates oder Images und dem schnellen bereitstellen der Ressourcen, kann in kürzester Zeit eine virtuelle Maschine erstellt werden. Auf dieser Maschine kann so ausgiebig getestet werden. Kommt es darauf hin zu Fehlern im Betriebssystem oder in der Software, kann bei einem totalen Absturz einer virtuellen Maschine sekundenschnell der Ursprungszustand wiederhergestellt werden. Auch ist ein solcher Absturz nicht kritisch, viel schlimmer wäre es gewesen, wenn dieses Problem in einer Produktivumgebung aufgetaucht wäre.

1.5 Nachteile durch Virtualisierung

Im Folgenden Abschnitt werden einige Nachteile dargestellt, die bei der Planung, der Nutzung und der Wartung einer virtualisierten Umgebung entstehen können.

Hoher Performance-Bedarf

Aus heutiger Sicht bieten Hersteller von Virtualisierungslösungen sehr ausgereifte und performanter Software an. Hypervisoren benötigen jedoch unterschiedliche Mengen an Ressourcen. Dies bedeutet, dass beispielsweise nicht der komplette Arbeitsspeicher eines Host-Systems für Gastsysteme verwendet werden kann.

Unterschiede in der Menge der benötigten Ressourcen ergeben sich unteranderem aus den verwendeten Hypervisoren, gemeint sind also Typ I- und Typ II-Hypervisoren (siehe Kapitel 1.3.7). Zusätzlich müssen auch leichte Einbußen bei der Performance des virtuellen Betriebssystems in Kauf genommen werden. Dies kann sich beispielsweise darin widerspiegeln, dass das Gastbetriebssystem oder die Applikationen minimal langsamer arbeiten, als auf einem nicht virtualisierten Computer. Die Begründung für dieses Phänomen ist sehr einfach zu erklären, die vom Gast benötigten Zugriffe auf Ressourcen müssen über den Hypervisor verwaltet werden und dieser Prozess stellt unter hohen Belastungen einen möglichen Flaschenhals dar.

Ein Virtualisierungs-server benötigt eine dem Einsatzszenario entsprechend hohe Hardware-Performance.

Virtualisierung bedarf einer genauen Planung

Dem Aufbau einer virtuellen Infrastruktur muss eine genaue Planung voraus gehen (siehe Kapitel 3.1), damit es nicht während des Betriebs zu Performanceengpässen und damit zu Ausfällen kommt.
Ein Handwerksunternehmen sollte sich daher gut durch ein zertifiziertes Systemhaus beraten lassen. Dabei sollte erarbeitet werden, welche Virtualisierungstechnologie und welche Virtualisierungssoftware eingesetzt werden sollte, um die Performance sehr hoch und die Kosten sowie den Wartungsaufwand möglichst gering zu halten.
Eine Planung durch ein zertifiziertes Systemhäuser bringt jedoch weitere Kosten und einen Zeitaufwand mit sich, der nicht zu unterschätzen ist. Das Systemhaus sollte auch alle möglichen Lizenzkosten darstellen, die bei kommerzieller Virtualisierungssoftware anfallen können.

Virtualisierung benötigt eine genaue Planung und sollte nur durch geeignetes Fachpersonal ausgeführt werden.

Steigender Speicherbedarf bei hoher Auslastung

Bereits bei der Erstellung von virtuellen Maschinen muss eine optimale Zuteilung hinsichtlich des Arbeitsspeichers stattfinden. Werden beim Betrieb einer virtuellen Maschine Auslastungsgrenzen des Arbeitsspeichers oft oder dauerhaft erreicht, ist möglicherweise beim Erstellungsprozess der virtuellen Maschine nicht genügend Arbeitsspeicher zugeteilt worden. Dies kann jedoch einfach über eine Erhöhung des Arbeitsspeichers der virtuellen Maschine im Managementtool des Hypervisors ausgeglichen werden.
Wenn der gesamte Arbeitsspeicher bereits verschiedenen aktiven virtuellen Maschinen zugeteilt wurde, muss der Virtualisierungsserver mit passendem Arbeitsspeicher nachgerüstet werden. Diese manuelle Wartung führt zu Einbußen bei der Verfügbarkeit des Gesamtsystems, da ein Nachrüsten von Arbeitsspeicher nur im abgeschalteten Zustand möglich ist. Aus diesem Grund ist der zuvor beschriebene Prozess der genauen Planung einer virtualisierten Umgebung äußerst wichtig.

Bei falscher Planung einer virtuellen Umgebung können bei hohem Performancebedarf Ressourcenengpässe entstehen.

Schulung des Personals notwendig

Um in Ausnahmesituationen, beispielsweise bei einem Fehler im Betrieb einer virtualisierten Umgebung möglichst schnell reagieren zu können, sind gut definierte Prozesse und geschultes Personal notwendig.
Zuständige Mitarbeiter sollten sicher und routiniert auf einen Fehler in einem virtualisiertem System reagieren können. Alternativ müssen Servicenummern des zuständigen Systemhauses oder des Wartungsdienstes bereitstehen. Ausnahmesituationen und die dafür notwendigen Sofortmaßnahmen müssen dafür klar definiert werden. Des Weiteren müssen diese Maßnahmen auch korrekt und ohne große Entscheidungsketten umgesetzt werden.

Mitarbeiten müssen im Umgang mit Virtualisierungs-lösungen geschult werden.

Nicht zu vernachlässigende Lizenzkosten

Bei proprietärer Virtualisierungs-software müssen Lizenzkosten eingeplant werden.

Bei der Verwendung von proprietärer Virtualisierungssoftware, kommt es zu Lizenzkosten die nicht zu vernachlässigen sind. Anbieter von lizenzpflichtiger Software sind beispielsweise Microsoft mit seinem Hyper-V und VMware mit seinem vSphere Hypervisor. Die Hypervisoren von Microsoft und VMware werden in einer Basisvariante zunächst kostenfrei angeboten, um jedoch eine wirklich abgesicherte und umfangreiche virtuelle Infrastruktur, beispielsweise mit einem Backup-Management oder zusätzlich mit Hochverfügbarkeitstools auszustatten, müssen Lizenz-Kosten eingeplant werden.
Weitere Betriebssystem-Lizenzkosten entstehen bei der Erstellung von virtuellen Maschinen, beispielsweise mit dem Betriebssystem Windows von Microsoft.

1.6 Aufsetzten oder Mieten?

Die Frage, ob es sinnvoller ist einen Virtualisierungsserver zu Mieten oder selber aufzusetzen, kann im Umfeld von Handwerksunternehmen recht eindeutig beantwortet werden. Wenn die zu erwartenden Kosten eines Wartungsvertrages gering sind und nicht an der Qualität der Dienste sowie am Datenschutz gespart wird, ist das Mieten dem selbstverwalteten Betrieb im eigenen Unternehmen vorzuziehen. Die Wartung und Pflege, insbesondere der Faktor IT-Sicherheit, kann durch ein kompetentes Systemhaus oder einen professionellen Anbieter in einer Cloud, der speziell geschultes Personal einsetzt, deutlich sicherer ausgeführt werden.

Das Nutzen von Virtualisierungs-dienstleistungen bei zertifizierten deutschen Cloud-Anbietern, kann die IT-Sicherheit deutliche erhöhen.

Die Begründung liegt in der Komplexität, die eine umfassende Virtualisierungslösung mit sich bringen kann. Bis sich ein Administrator als wirklicher Fachmann im Bereich der Virtualisierung ausweisen kann, sind viele kostspielige Zertifizierungslehrgänge nötig. Darüber hinaus werden für eine Virtualisierungslösung oft viele einzelne Zertifizierungen angeboten, weil eine fachgerechte Virtualisierung stets viele einzelne Softwarekomponenten benötigt.

Für weitere Hinweise hinsichtlich der Nutzung von Cloud-Computing nutzen Sie bitte das gleichnamige Handbuch. Darin finden Sie auch wichtige Hinweise, die hinsichtlich des Datenschutzes beachtet werden müssen.
Weitere detaillierte Informationen erhalten Sie auch im Handbuch Datenschutz.

1.7 Zusammenfassung

Virtualisierung ist ein seit vielen Jahren erfolgreiches Konzept, welches es Unternehmen ermöglicht, Kosteneinsparungen durch die Reduzierung von Hardware zu erzielen. Zusätzlich können Kosten für Energie und die Wartung von zentralen Servern verringert werden.
Wichtig zu beachten ist jedoch, dass Virtualisierung eine Reduzierung von vielen Servern auf einige wenige Server mit sich bringt. Dabei werden mehrere Systeme auf einem Server vereint, was auch das Angriffspotenzial sowie die Ausfallwahrscheinlichkeit auf ein einzelnes Ziel beschränkt. Aus diesen Gründen müssen Virtualisierungsserver ausreichend durch Sicherheitsmechanismen, wie beispielsweise redundante Speicherung von Daten und der Sicherung der Stromzufuhr über eine unterbrechungsfreie Stromversorgung (USV) abgesichert werden.
Besonders wichtig ist auch eine genaue Planung der virtuellen Infrastruktur, da der Aufbau stets größere Investitionen mit sich bringt. Eine Kosten-Nutzen-Analyse kann vor Fehlinvestitionen schützen. Auch eine fachgerechte Einrichtung durch geschultes Personal ist notwendig, um den sichereren Betrieb der virtuellen Infrastruktur zu

gewährleisten und Fehlkonfigurationen zu vermeiden. Dazu gehört auch ein aktives Patch-Management hinsichtlich der immer wieder aufkommenden Sicherheitsupdates. Fehlende Sicherheitsupdates können insbesondere bei Hypervisoren zu gravierenden IT-Sicherheitsrisiken führen, in dessen Folge die Vertraulichkeit der Daten eines Unternehmens gefährdet werden kann.
Eine detaillierte Planung ist aber auch wichtig, um möglichen Ressourcenengpässen vorzubeugen, die im schlimmsten Fall einen Verlust der Verfügbarkeit mit sich bringen können. Alles in Allem kann jedoch behauptet werden, dass eine gut gewartete und abgesicherte virtuelle Infrastruktur viele Vorteile mit sich bringt.

Notizen

2. Risiken

In diesem Kapitel werden nach den zuvor erwähnten Nachteilen besondere Risiken für die Sicherheit von virtualisierten Systemen dargestellt. Dabei kann es insbesondere zu schweren Sicherheitsrisiken durch mangelhafte Konfigurationen, fehlenden Sicherheitsupdates und nicht existierenden Backup-Routinen auf den Hostsystemen kommen. Diese und weitere Risiken werden in den folgenden Kapiteln dargestellt.

2.1 Problematische Voraussetzungen auf dem Host

Hinter der Überschrift problematische Voraussetzungen auf dem Host, verbergen sich beispielsweise nicht geeignete Hardwarekomponenten und Einsatzszenarien, die eine performante und eine sichere Ausführung einer virtuellen Infrastruktur gefährdet.

Ein Virtualisierungs-server sollte eine 64 Bit Architektur aufweise, damit mehr als 4 GB Arbeits-speicher unterstützt werden.

Nicht kompatible Prozessoren können beispielsweise das Ausführen von 64-Bit Betriebssystemen verhindern, deshalb ist es wichtig vor dem Kauf die Kompatibilität der Hardware zu prüfen. Unternehmen, die Virtualisierungslösungen aus der Cloud nutzen, müssen sich über diese Problematik keine Sorgen machen. Wird jedoch eigene Hardware gekauft und virtualisiert, können auf den Herstellerseiten der Softwareunternehmen besonders empfohlene Hardwarekomponenten vergleichen werden.

Ist eine Virtualisierung von 64 Bit Betriebssysteme nicht unterstützt, kann einer virtuellen Maschine maximal 4 GB, oft sogar auch weniger zugewiesen werden. Dies liegt an der so genannten 4 GB-Grenze[27], die durch die 32 Bit Architektur der Betriebssysteme entsteht.

Weisen Sie bei der Anschaffung von Hardwarekomponenten auf eine Kompatibilität zur Virtualisierungssoftware und einer Unterstützung von 64 Bit Prozessoren hin, um eine Ausführung von mehr als 4 GB Arbeitsspeicher zu gewährleisten.

Nicht benötigte Prozesse und Anwendungen auf dem Host vermeiden

Vermeiden Sie überflüssige Anwendungen auf Ihrer Server-infrastruktur.

Zusätzliche Dienste auf dem Server bergen Risiken, da sie potenzielle Angriffsziele sein können. Daher ist es empfehlenswert auf dem Virtualisierungs-Host ausschließlich Prozesse und Anwendungen auszuführen, die für einen sicheren Betrieb der virtuellen Infrastruktur notwendig sind.

Klären Sie ein Handwerksunternehmen darüber auf, dass nicht benötigte Programme zu Risiken führen können.

[27] http://de.wikipedia.org/wiki/4-GB-Grenze *32 Bit-Betriebssysteme unterstützen nicht mehr als 4 GB Arbeitsspeicher*

Fehlende Planung des Einsatzszenarios

Die Erstellung einer virtualisierten Umgebung beruht auf einer genauen Planung. Ohne diese Planung kann es zu Ressourcenengpässen während des Betriebes kommen. Dies wiederum kann die Verfügbarkeit des Gesamtsystems beeinträchtigen und gefährden. Sehr wichtig ist auch, dass virtuelle Systeme durch geeignete Backup-Maßnahmen geschützt werden.

Eine fehlende Planung kann virtuelle Infrastrukturen gefährden.

Weisen Sie Handwerksunternehmen darauf hin, sich professionell durch geeignete Unternehmen beraten zu lassen.

2.2 Fehlkonfiguration des Hosts

Oft führt eine falsche Konfigurationen oder eine ungenaue Zugriffsregelung eines virtualisierten Systems dazu, dass Risiken für vertrauliche Daten entstehen.
Folgende Risiken können das sichere Ausführen einer virtuellen Infrastruktur gefährden.

Nicht durchgesetzte Isolation virtueller Maschinen

Es muss dafür gesorgt werden, dass die einzelnen virtuellen Systeme unabhängig voneinander arbeiten und nur über bestimmte vorher festgelegte Routen miteinander kommunizieren können. In diesem Fall wird von Isolation gesprochen. Heutige Virtualisierungsumgebungen sind in der Lage dies strikt durchzusetzen.
Im Wesentlichen können auf der Netzwerkebene zwei unterschiedliche Ansätze betrachtet werden, um die Kommunikation zwischen den virtuellen Maschinen zu gewährleisten: Die Erste ist, dass der virtuellen Maschine selbst eine physische Netzwerkschnittstelle des Host-Systems zur Verfügung gestellt stellt wird, um die Kommunikation zu anderen virtuellen Maschinen zu gewährleisten. Jede virtuelle Maschine hat in diesem Fall seine eigene physische Netzwerkkarte.
Ein weiteres Verfahren ist die virtuelle Vernetzung einzelner Gastsysteme. Dabei stellt der Hypervisor einen virtuellen Switch zur Verfügung, über welchen die virtualisierten Systeme miteinander kommunizieren können.
Der bereitgestellte virtuelle Switch kann wiederum so konfiguriert werden, dass dieser einen Zugang zu einer physikalischen Netzwerkschnittstelle erhält und somit Zugang zu allen anderen bestehenden Netzen in einem Unternehmen erhält.

Eine Virtualisierungs-software muss die sichere Isolation von virtuellen Maschinen gewährleisten.

Die sichere Konfiguration von virtuellen oder physischen Netzwerken muss sichergestellt werden. Über die Nutzung von Firewall-Regeln auf den virtuellen Maschinen können weitere Einschränkungen durchgesetzt werden.

Mangelhafte Trennung des Produktiv- und Verwaltungsnetzes

Das Verwaltungsnetz mit Zugängen zu Administrationsoberflächen, beispielsweise eins Datenbankservers, darf nur aus dem internen Netz erreichbar sein. Produktivnetze mit virtuellen Maschinen die beispielsweise einen Webserver bereitstellen, müssen auch aus dem Internet erreichbar sein, um den Besuchern einer Webseite den notwendigen Inhalt bereitstellen zu können. Wichtig ist jedoch, dass ausschließlich authentifizierte Personen Zugriff auf administrative Dienste und schützenswerte Daten erhalten. In der Literatur ist in diesem Zusammenhang von „Separation der Netze“ die Rede. Wird diese Separation nicht konsequent durchgesetzt, führt dies zu Risiken für die gesamte IT-Infrastruktur.

Verwaltungs- und Produktionsnetze müssen sicher voneinander getrennt werden.

Um potenzielle Risiken zu vermeiden, kann wie zuvor beschrieben, eine physische oder eine virtuelle Trennung durchgeführt werden, siehe Kapitel 3.2. Es gilt Verwaltungsnetze besonders zu schützen, da sie einen Zugang zu administrativen Oberflächen bereitstellen. Bei einem unzureichenden Zugriffsschutz könnten diese leicht ein Ziel für Angreifer werden. Dies ist insbesondere der Fall, wenn diese Netze möglicherweise für eine Fernwartung über das Internet erreichbar sind. Ein hohes Risiko sind dazu immer so genannte Brute-Force-Angriffe auf Login-Masken. Bei diesen Angriffen wird versucht über die automatisierte Eingabe von Passwörtern, oft mit Hilfe von Passwortlisten, eine Nutzername-Passwort-Kombination zu erraten.

Die Erstellung von virtuellen und physischen Netzwerken sollte nur durch geschultes Personal erfolgen. Handwerksunternehmen sollten sich durch ein zertifiziertes Systemhaus beraten lassen, welche der dargestellten Lösungen individuell am besten ist.

Ungewollte Freigabe von Dateien

Ungewollte Dateifreigaben können zur Gefahr für die Vertraulichkeit werden.

Die Freigabe von Dateien über die so genannten „shared Folders“ (zu Deutsch geteilte Ordner) kann zu Risiken führen. Dabei muss beachtet werden, dass einzelne Ordner oder Dateien nur freigegeben werden, wenn sie auch dazu geeignet sind. Darüber hinaus ist es wichtig, dass nicht jeder Nutzer wahllos Dateien freigeben darf. Nur ausgewählte Nutzer mit erweiterten Rechten sollte dies gestattet sein.

Die Freigabe von Dateien muss durch ein Rechtemanagement abgesichert sein.

2.3 Schlechte Passwortsicherheit

Wählen Sie ausschließlich sichere und damit starke Passwörter. Ein starkes Passwort ist auf den ersten Blick sinnfrei zusammengesetzt, unterliegt also keiner erkennbaren Systematik. Verwenden Sie mindestens 12 Zeichen, darunter eine Mischung aus Groß- und Kleinbuchstaben, sowie Ziffern und Sonderzeichen.
Mit jedem zusätzlichen Zeichen, das Sie für den Ihr Passwort wählen, steigt der Aufwand zum Knacken des Passwortes für den Angreifer rasant an! Doch das beste Passwort nützt Ihnen nichts, wenn Sie sich später nicht mehr daran erinnern können. Passwortverwaltungssoftware kann dabei helfen (siehe Kapitel 3.13). Es gibt darüber hinaus viele Möglichkeiten sich komplizierte Passwörter mit einer einfachen Eselsbrücke zu merken. Überlegen Sie sich einen Satz, zum Beispiel: „An jedem 1. und 3. Samstag im Monat gehe ich Fußball spielen!“. Wenn Sie nur die Anfangszeichen verwenden, ergibt sich daraus folgendes Passwort: „Aj1.u3.SiMgiFs!“. Eine andere Möglichkeit: Verwenden Sie die Nachbartaste. Aus dem Wort „Urlaubstag“ wird so zum Beispiel die sinnfreie Buchstabenfolge „itösindzsh“. Vergessen Sie nicht dieses noch um Sonderzeichen und Zahlen zu ergänzen!

Verwenden Sie ausschließlich sichere Passwörter mit 12 Zeichen, darunter eine Mischung aus Groß- und Kleinbuchstaben, sowie Ziffern und Sonderzeichen.

Achten Sie darauf, Ihre Passwörter regelmäßig zu ändern. Grundsätzlich geben wir hier keine Empfehlung, wie häufig Sie Ihr Passwort ändern sollten. Das hängt zum einen davon ab, wie häufig Sie ihr Passwort verwenden und zum anderen, wie sensibel Ihre zu schützenden Daten sind (zum Beispiel Passwort für die Administration von Hypervisoren vs. Passwort für eine Newsletter-Anmeldung).

Idealerweise sollten Sie Passwörter für sensible Anwendungen (zum Beispiel Online-Banking) etwa alle drei Monate wechseln. Wenn Sie den Verdacht haben, dass jemand Unbefugtes in den Besitz Ihres Passworts gelangt sein könnte, ändern Sie dieses umgehend. Auch voreingestellte oder von Händlern vorgegebene Passwörter für Software oder Systeme sollten sofort durch ein individuelles Passwort ersetzt werden. Häufig probieren Hacker bei einem Angriff zunächst aus, ob vergessen wurde diese zu individualisieren. Hinweise darauf, ob voreingestellte Passwörter vorhanden sind und wie diese sich gegebenenfalls ändern lassen, finden Sie in den Produkten beiliegenden Handbüchern.

Ändern Sie Ihre Passwörter regelmäßig!

2.4 Fehlende Redundanz

Durch Serverkonsolidierung besteht die Möglichkeit alle einst einzeln betriebenen Systeme auf einem einzigen Host virtualisiert auszuführen. In diesem Fall sind alle Dienste von nur einem Server abhängig. Dies birgt das Risiko, dass der Host aufgrund eines Hardware-Defektes, beispielsweise des Netzteils, der Netzwerkkarte oder anderen gefährdeten Komponenten ausfällt und alle darauf laufenden Gast-Systeme nicht mehr verfügbar sind.
Ein weiteres Risiko ist, wenn die entsprechenden Daten zur Virtualisierung auf der lokalen Festplatte des Hosts gespeichert sind und durch einen Defekt der Festplatte ausfallen. In diesem Fall sind alle auf dem Host ausgeführten virtuellen Maschinen ebenfalls nicht mehr verfügbar.
Fehlen bei den genannten Szenarien geeignete Backupstrategien beispielsweise durch redundant gespeicherte Daten auf verschiedenen Festplatten, kann es zu eklatanten Datenverlusten kommen.
Ist die Wiederherstellung der Daten möglich, können diese oft nur durch professionelle Dienstleister wiederhergestellt werden, was oft zu erheblichen Kosten führt.
Die Beispiele sollen zeigen, dass bereits bei der Planung hohen Anforderungen an die Verfügbarkeit berücksichtigt werden müssen, um eine schnelle Wiederinbetriebnahme im Falle eines gravierenden Fehlers gewährleisten zu können.

Achten Sie auf geeignete Backupmechanismen zum Sichern der Daten auf einem Virtualisierungs-server.

Aber nicht nur der Speicherplatz einer Infrastruktur sollte redundant ausgelegt werden, auch die Stromversorgung kann mittels unterbrechungsfreier Stromversorgung (USV) in Ausnahmesituationen für eine kurze Zeit bis zur Wiederherstellung der Spannungsversorgung oder für ein sicheres Herunterfahren der Datenbanken und Serversysteme genutzt werden. Dies beugt einem Datenverlust bei einem abrupten Stromverlust vor, da die flüchtigen Daten im Arbeitsspeicher vor einem Herunterfahren sicher gespeichert werden können.

Sorgen Sie für eine Aufklärung über die redundante Auslegung von virtualisierten Systemen. Dies sichert die Unternehmensinfrastruktur gegen einen möglichen Datenverlust ab.
In den Kapiteln 4.6 und 4.7 finden Sie diesbezüglich weitere Handlungsanweisungen.

Risiken durch unverschlüsselte Backups

Werden Backups erstellt, muss auch bedacht werden, dass der Zugriff auf diese gesicherten Daten eingeschränkt werden muss. Wenn Datenträger oder Backups entwendet werden, besteht die Möglichkeit diese Daten zu nutzen, um sie auf einem

anderen System wiederzustellen. So könnten abgespeicherte Passwörter ausgelesen und zu einem Angriff auf weitere Dienste, wie beispielsweise Online- beziehungsweise Cloud-Dienste genutzt werden.

Backup-Daten müssen gegen den Zugriff durch unbekannte gesichert werden.

Backup-Daten sollten daher mit einer aktuellen Verschlüsselung versehen werden, alternativ kann auch die Aufbewahrung von Backup-Datenträgern in einem zutrittsbeschränkten Bereich erfolgen.

Wiesen Sie Handwerksunternehmen darauf hin, dass geeignete Maßnahmen zur Sicherung der Backup-Daten getroffen werden müssen. Dies kann mit Hilfe von Verschlüsselung aber auch durch eine sichere Aufbewahrung an einem verschlossenen Ort erfolgen.

2.5 Mögliche Fehler im Hypervisor

Hypervisoren können Sicherheitslücken enthalten, die schnellstmöglich durch Updates geschlossen werden müssen.

Ein Hypervisor ist, wie in diesem Handbuch bereits erläutert wurde, ein Softwareprodukt und kann wie jede andere Software Fehler enthalten. Ein Beispiel hierfür ist, wenn der Hypervisor aufgrund von Fehlern in der Programmlogik kompromittiert werden könnte. Der Super-Gau wäre ein Fehler, durch den es möglich ist in einer virtuellen Maschine einen Zugriff auf den Hypervisor zu erlangen. Hierbei könnte eine Schwachstelle ausgenutzt werden, die es einem Angreifer erlaubt, seine Rechte auf einer virtuellen Maschine so auszuweiten, dass dieser die volle Kontrolle über den Hypervisor erlangt. In Folge dessen hat ein Angreifer Zugriff auf alle virtuellen Maschinen, die der Hypervisor auf dem Host bereitstellt. Vertrauliche Informationen könnten so aus den virtuellen Maschinen entwendet oder ganze Systeme können auf dem Host gelöscht werden. Trotz ausreichender Sicherungen kann dies zu signifikanten Ausfallzeiten und zum Verlust sowie zum Diebstahl von wichtigen Daten führen.

Beachten Sie, dass immer die aktuellste Version des Hypervisors eingesetzt werde muss. Weisen Sie ein Handwerksunternehmen darauf hin, dass Sicherheitslücken im Hypervisor des Virtualisierungsservers zu akuten Sicherheitsproblemen führen können. Sicherheitskritische Updates müssen daher immer zeitnah eingespielt werden.
Hersteller von Virtualisierungssoftware geben dazu so genannte Security-Bulletins, also Informationen über Schwachstellen und deren Sicherheitsupdates heraus.

Nutzen Sie Sicherheitshinweise der Software-hersteller.

VMware:
http://www.vmware.com/de/security/advisories

Microsoft:
https://technet.microsoft.com/de-de/security/bulletin

Auf den Seiten der oben genannten Hersteller kann explizit nach Produkten aus dem Bereich der Virtualisierung gesucht werden.

Weisen Sie Handwerksunternehmen darauf hin, dass stets automatische Updates aktiviert werden müssen.

2.6 Unzureichender Support bei Virtualisierung

Viele Software-Hersteller bieten einen speziellen und oft kostenpflichtigen Support für ihre Anwendungen an. Dies betrifft oft die Virtualisierungssoftware an sich. Da auf virtualisierten Systemen die Lauffähigkeit einer Anwendung vorab geprüft werden muss, sprechen Hersteller oft eine Empfehlung für die Kompatibilität einzelnen Produkten aus. Bei fehlendem Support für ältere Anwendungen, kann zu Risiken für die Stabilität bei der Ausführung kommen.

Fehlender Support von Anwendungen in virtuellen Umgebungen

Der Support der Hersteller für Anwendungen, die auf einem „echten“ Computer ausgeführt und nicht in einer VM betrieben werden, muss oft separat angefragt werden. Generell besteht aber kaum ein Unterschied, ob eine Software auf einem virtualisierten oder nicht virtualisierten Host ausgeführt wird. Dennoch sollte in Betracht gezogen werden, sich über die Kompatibilität hinsichtlich der Ausführung in einer virtualisierten Umgebung zu informieren.

Informieren Sie Handwerksunternehmen darüber, dass sie sich vor dem Kauf von Software für eine virtualisierte Umgebung über die Lauffähigkeit und den Support für diese Anwendung durch den Anbieter bestätigen lassen.

Risiken vor umfangreichen Systemupdates prüfen

Veraltete Anwendungen können nach Systemupdates Fehler produzieren.

Wie in diesen Handbuch bereits erwähnt, sollte die Ausführung von automatischen Updates aktiviert werden. Bei größeren Versionssprüngen ist es jedoch notwendig die Kompatibilität nach einem Versionsupdate zu prüfen. Ein solches größeres Update kann beispielsweise bei einer Aktualisierung von einem durch Langzeitsupport unterstützen Version, zu einer aktuelleren Langzeitsupport-Version vorkommen und muss manuell eingespielt werden.
Hier müssen sich beim Hersteller Informationen über eine Kompatibilität älterer Software-Produkte eingeholt werden. Alternativ kann auch auf Supportseiten oder in den Foren der verschiedenen Hersteller nach möglichen Fehlern oder Problemen bei anderen Kunden recherchiert werden.

Weisen Sie bei der Aktualisierung von Betriebssystemen und großen Systemupdates auf die Prüfung hinsichtlich der Unterstützung zu alten Programmen hin.

2.7 Zusammenfassung

Potenzielle Risiken bietet jede neue Technologie, einige dieser Risiken können über die dargestellten Maßnahmen durch ein Unternehmen selbst reduziert werden. Bei anderen risikobehafteten Punkten, wie beispielsweise bei Schwachstellen in einem Hypervisor selbst, muss auf eine schnelle Reaktion zur Behebung von Sicherheitslücken seitens der Softwarehersteller vertraut werden. Das Einspielen eines Sicherheitsupdates ist wiederum die Aufgabe der Nutzer selber.
Insbesondere fehlende oder fehlerbehaftete Backupmechanismen führen immer wieder zu eklatanten Datenverlusten. Beachten Sie, dass dieses Handbuch nur eine Darstellung von einigen der größten Sicherheitsrisiken behandelt. Handwerksunternehmen haben oft Systemhäuser denen sie die Wartung der

virtuellen Infrastruktur anvertrauen, dies ist auch sehr gut so, denn die Pflege und Verwaltung eines virtuellen Servers ist sehr aufwändig und muss durch gut geschultes Personal überwacht werden.

Notizen

3. Basisschutz

In diesem Kapitel werden Ihnen einige wichtige Mechanismen für einen Basisschutz bei der Virtualisierung von Servern und dem allgemeinen Einsatz von Virtualisierung dargestellt.

3.1 Vorabplanung für Virtualisierung

Handwerks-unternehmen sollten sich durch ein geeignetes Systemhaus bei dem Aufbau einer virtuellen Infrastruktur unterstützen lassen.

Wenn in einem Betrieb Virtualisierung zum Einsatz kommen soll, spielt die Planung eine überaus wichtige Rolle. Es ist mit einem Systemhaus vorab zu klären, welche Virtualisierungssoftware eingesetzt werden soll, da eine Änderung im laufenden Betrieb nur durch einen hohen Aufwand möglich ist. Darüber hinaus muss auch die Ausführung der Virtualisierung unterbrochen werden. Lizenzkosten sind ebenfalls ein wichtiges Auswahlkriterium. Bei einigen Virtualisierungsprodukten müssen für jeden Prozessorsockel[28] weitere Lizenzkosten einkalkuliert werden. Beispielsweise fallen für zwei Dualcore-Prozessoren[29] mehr Kosten an als für einen Quadcore-Prozessor[30], da dieser nur einen Prozessorsockel verwendet. Wenn eine Auswahl bezüglich der Art der Virtualisierung und der passenden Software getroffen wurde, sollte die Hardware, auf der die Virtualisierung stattfindet, alle Mindestvoraussetzungen des Softwareherstellers erfüllen. Zu beachten ist dabei zunächst der Prozessor, dieser sollte Virtualisierungsfunktionen (Intel VT, AMD-V siehe Kapitel 1.3.10) bereitstellen. Des Weiteren sollte dafür gesorgt werden, dass ausreichend Speicherplatz zur Verfügung steht. Der Hypervisor benötigt oft wenig Speicher auf der Festplatte aber das Anlegen von Snapshots oder kompletten Sicherungen in bestimmten Intervallen, also beispielsweise täglich oder wöchentlich, benötigt eine große Menge an Speicher. Dies kann auf Dauer zu einem hohen Datenaufkommen führen und das System an sich sowie alle Backup-Systeme müssen dem entsprechend dimensioniert sein.
Da jedes Handwerksunternehmen seine ganz eigenen Ansprüche und Szenarien für einen Aufbau einer virtuellen Infrastruktur besitzt, werden hier auf die weitere detaillierte Darstellungen einer Planung verzichtet.

Fordern Sie ein Handwerksunternehmen dazu auf sich durch ein qualifiziertes Systemhaus beraten zu lassen. Der Mitarbeiter des Systemhauses sollte dazu eine Zertifizierung für die Virtualisierungstechnologie besitzen, für die er eine Beratung durchführt.

3.2 Separation der Netze

Das Netzwerk gehört sicherlich zu den kritischsten Teilen eines virtualisierten Systems. Es sichert die Erreichbarkeit aller seiner Teilnehmer, daher muss ein besonderes Augenmerk auf die Verfügbarkeit und die Sicherheit gelegt werden. Zwar sind die virtuellen Maschinen auf den Festplatten des Virtualisierungs-Hosts bei aktuellen Virtualisierungslösungen sicher voneinander isoliert und haben somit keinen

[28] *Prozessorsockel – Ist ein Steckplatz für einen Prozessor in einem Computer oder Server*
[29] *Dualcore-Prozessor – Ein Dualcore-Prozessor besitzt zwei Rechenkerne.*
[30] *Quadcore-Prozessor – Ein Quadcore-Prozessor besitzt vier Rechenkerne.*

direkten Zugriff zu den jeweils benachbarten virtuellen Maschinen, dennoch sind diese oft über ein virtuelles Netzwerk miteinander verbunden und können so möglicherweise auf freigegebenen Ressourcen von anderen virtuellen Maschinen oder Netzwerkteilnehmern zugreifen.

Weisen Sie Unternehmen auf eine strenge Reglementierung der Netzwerkressourcen hin.

Bei einer falschen Konfiguration des Netzwerks, können virtuelle Maschinen möglicherweise aus dem Internet erreicht und angegriffen werden.
Eine sehr effiziente Maßnahme ist das Segmentieren von Netzen. Dabei kann zum Beispiel das Risiko für eine Erreichbarkeit aus dem Internet von besonders schützenswerten virtuellen Maschinen, insbesondere mit wichtigen Datenbanken, ausgeschlossen werden. Eine Netzwerkseparation ist daher ein zuverlässiges Mittel, um virtuelle Maschinen zu schützen.
Durch Virtualisierung bietet sich die Möglichkeit, mit so genannten VLAN's[31] zu arbeiten. Diese können oft mit wenigen Mausklicks erstellt und konfiguriert werden und bieten die Möglichkeit Zugriffe zu Netzwerkteilnehmern zu beschränken. Des Weiteren können VLAN's eingerichtet werden, um Gruppen zu erstellen denen ein bestimmter Netzwerkbereich verborgen bleibt. Somit können Daten nur zwischen virtuellen Maschinen ausgetauscht werden, die in der Gruppe von berechtigten virtuellen Maschinen sind.

Weitere Informationen hinsichtlich Subnetze, Segmentierung von Netzwerken und VLAN's erhalten Sie in dem Handbuch Netzwerksicherheit.

Physische Trennung:
Hierbei werden für jede virtuelle Maschine eigene Netzwerkkarten verwendet.

Netzwerkseparierung kann über virtuelle Netzwerke (VLAN) und physische Trennung durch jeweilige Netzwerkkarten-zuordnungen stattfinden.

Vorteile:

- Datenströme werden physisch voneinander getrennt.
- Die Komplexität der Konfiguration ist sehr gering, einer virtuellen Maschine wird lediglich einer Netzwerkkarte zugeordnet.

Nachteile:

- Es werden mehr Hardwarekomponenten benötigt (für jede VM eine eigene Netzwerkkarte).
- Die Fähigkeiten von Virtualisierung werden mit der Nutzung von physischen Netzwerkkomponenten eingeschränkt.

Virtuelle Trennung:
Hierbei wird für jede virtuelle Maschine ein virtualisiertes Netzwerkgerät erstellt und konfiguriert.

[31] *VLAN- Virtual Local Area Network, ein virtuelles Netzwerk mit komfortablen Einstellungsmöglichkeiten.*

Vorteile:

- Die Vorteile der Konsolidierung, also die Reduzierung von Hardware in Form von Netzwerkkarten, kann genutzt werden.
- Die Kosten bei der Wartung und Anschaffung können gering gehalten werden.

Nachteile:

- Die Erstellung von virtuellen Netzwerkkarten und virtuellen Switches bringt einen höheren Konfigurationsaufwand mit sich.
- Die Gefahr von Fehlkonfigurationen steigt mit der Komplexität.

Weisen Sie ein Handwerksunternehmen darauf hin, dass es durch Fehlkonfigurationen in den virtuellen Netzwerken zur Angreifbarkeit der virtuellen Maschinen kommen kann.

3.3 Verantwortlichkeiten und Rollen

Ein weiteres grundsätzliches Thema ist die Zugriffsregelung auf Virtualisierungsservern durch Administratoren und Mitarbeiter. Die meisten Hersteller von Virtualisierungssoftware stellen ein Programm zur Verfügung, in dem Administratoren Einstellungen für VLAN's oder Gastsysteme, beziehungsweise virtuelle Maschinen durchführen können. Oft werden diese Programme als Management-Tool bezeichnet. Doch nicht jeder Nutzer sollte einheitliche oder Administrator-ähnliche Berechtigungen erhalten. Alleine schon, weil ein Host-Administrator nicht zwingend denselben Wissensstand wie ein Netzwerk-Administrator aufweist. Aus diesem Grund sollten verschiedenen Nutzern unterschiedliche Rollen zugewiesen werden.

Teilen Sie Mitarbeitern eine Rolle zu und Prüfen Sie die Zugriffsrechte.

Einige Anbieter von Virtualisierungslösungen bieten die Möglichkeit administrative Aufgaben an Gruppen, beziehungsweise an deren Nutzer zu verteilen. Durch die gezielte Vergabe von Rechten an Administratoren, beispielsweise für das Sichern oder für das Erstellen sowie für das Einrichten von virtuellen Maschinen, kann das Risiko einer zu hohen Machtbefugnis minimiert werden. Auch versehentliche Fehlkonfiguration oder unautorisierte Handlungen an Hypervisoren oder an virtuellen Maschinen können so verhindert werden. Um ein solches Risiko auszuschließen, ist es notwendig, ein Berechtigungsmanagement zu pflegen und zu dokumentieren.

Dokumentieren Sie die Nutzer-Accounts und halten Sie diese Informationen aktuell.

Klären Sie ein Handwerksunternehmen über die genaue Verteilung und Dokumentation von Zugriffsberechtigung auf. Nicht jeder Mitarbeiter sollte das Administratoren-Passwort kennen. Es sollte jedoch immer ein Vertreter des Administrators mit sehr guten Kenntnissen der virtuellen Infrastruktur bestimmt werden, der im Krankheitsfall als Aushilfe fungiert und eine Aufrechterhaltung des Betriebs sicherstellen kann.

Fehlende Zugriffsdokumentation

Account-informationen wie Passwörter dürfen nur von einer Person verwendet werden.

Wenn ein Nutzer-Account, beispielsweise ein Administrator-Account, von mehreren Mitarbeitern genutzt wird, kann nicht mehr nachvollzogen werden, von welchem Nutzer Änderungen an einem System durchgeführt wurden. Darüber hinaus steigt das Risiko, dass es bei Fehlern in der Konfiguration oder bei aktivem Fehlverhalten zu Datenverlusten kommt. Aktives Fehlverhalten kann beispielsweise von Mitarbeitern ausgehen die unzufrieden mit ihrer Jobsituation sind oder die möglicherweise Rache an ihrem alten Arbeitgeber üben wollen. Solche Zwischenfälle hat es in der Vergangenheit immer wieder gegeben. Daher ist es ebenso wichtig gekündigte Mitarbeiter aus dem Nutzerverzeichnis zu löschen. Insbesondere, wenn dies Zugriff auf einen Fernzugang haben.

Weisen sie auf die Nutzung von Administrationswergzeugen hinsichtlich einer Rollenverteilung im Rechtemanagement hin.
Jeder Nutzer muss seinen eigenen Account, mit einer eingeschränkten oder erweiterten Zugriffsberechtigung haben.

3.4 Firewalls

Um das Risiko vor dem Zugriff durch unbekannte Dritte zu minimieren, müssen auch im Umfeld von Virtualisierungen Firewalls genutzt werden. Dabei gibt es verschiedene Lösungen, die im Folgenden dargestellt werden.

Zentrale Firewall-Lösung in der Virtualisierungssoftware

Verwenden Sie eine geeignete Firewall-Lösung zum Schutz der virtuellen Netzwerkinfrastruktur.

Es gibt Firewall-Lösungen die direkt von Hypervisor, also von der Virtualisierungssoftware an sich verwaltet werden. Dabei wird über eine Software die Paketweiterleitung der virtuellen oder Hardware-Netzwerkkarten gesteuert. Es ist wichtig nur Ports für die Dienste zuzulassen, die auch wirklich benötigt werden.
Bei der initialen Einrichtung einer Firewall-Lösung sollten daher zunächst alle Ports gesperrt werden. Daraufhin müssen Ports jener Dienste freigegeben werden, die tatsächlich auf dem Server benötigt werden.
Der Vorteil ist, dass diese Lösung zentral für alle virtuellen Maschinen gesteuert werden kann. Dies ist ressourcensparend, muss jedoch auch durch die Virtualisierungssoftware unterstützt werden. Oft können so genannte Templates oder vordefinierte Regeln genutzt werden, die gegebenen falls angepasst werden müssen.

Viele Anbieter von Virtualisierungssoftware bieten eine implementierte Firewall-Lösung an, die speziell für den Einsatz auf Hypervisoren geeignet ist. Eine Firewall sollte stets aktiviert sein und durch Fachpersonal auf das Einsatzgebiet abgestimmt werden.

Firewall außerhalb der Virtualisierungslösung

Hierbei könnten beispielsweise so genannte „next Gerneration“- also UTM-Firewalls (Unified Threat Management) verwendet werden. Diese Art von Firewall wird zwischen die Internet-Verbindung und das Unternehmensnetzwerk beziehungsweise den Virtualisierungs-Host geschaltet und sorgt für einen weitgehenden Schutz gegen Angriffe von außen. In komplexeren Konfigurationen können diese zumeist kleinen Boxen auch zentral den Datenstrom des gesamten Firmennetzes auf mögliche

Gefährdungen durch Viren oder Trojaner prüfen, sogar der E-Mail-Verkehr könnte auf diese Weise von potenziell schädlichen Anhängen gesäubert werden.

Für weitere Hinweise hinsichtlich der Nutzung von Firewalls nutzen Sie bitte das Handbuch Netzwerksicherheit. Darin finden Sie weitere Szenarien, wie Firewalls im Unternehmen eingesetzt werden können.

Software-Firewall in einer virtuellen Maschine

Eine übliche Software-Firewall kann auch auf einer virtuellen Maschine installiert werden. Firewall-Regeln müssen so auf jeder virtuellen Maschine separat eingestellt werden. Dies hat jedoch den entscheidenden Nachteil, dass diese nicht zentral über den Hypervisor verwaltet werden können.

3.5 VPN Verschlüsselung der Datenübertragung

Wenn durch Mitarbeiter oder Systemhäuser von Extern auf die virtualisierte Infrastruktur zugegriffen werden soll, müssen sichere Lösungen wie beispielsweise ein Zugriff mittels Virtual Private Networks (kurz VPN) genutzt werden.

VPN – Virtual Private Network

Ein virtuelles privates Netzwerk ist ein Netzwerk, welches in einem anderen Netzwerk, beispielsweise dem Internet, gekapselt arbeitet. Als Vergleich kann sich dazu ein Kabelkanal vorstellt werden, in dem unterschiedliche Kabel eingezogen sind. Der Kabelkanal ist das Trägernetz und die Kabel bilden die abgekapselten Tunnel. Heutzutage ist das Internet mit seiner weiten Verbreitung und guten Zugänglichkeit in der Regel das Basisnetzwerk in welchem gekapselt wird.
Um über das Internet ein eigenes privates Netzwerk aufzubauen werden oft VPN-Gateways verwendet.
Diese stellen die Verbindungspunkte zu einem Teil des privaten Netzwerks dar. Die Verwendung von Gateways bietet den Vorteil, dass sowohl Gateways mit dahinter geschaltetem Netzwerk, als auch Clients sich direkt mit diesen verbinden können. Die Verbindung der unterschiedlichen Punkte eines virtuellen Netzwerks wird auch Tunnel genannt. Dies ist darin begründet, dass alle Daten an den jeweiligen Punkten durch die Verwendung eines sicheren VPN-Protokolls ver- und entschlüsselt werden. Dies ist nicht nur sinnbildlich sondern auch wörtlich zu verstehen, denn zwischen verschiedenen VPN kann der Datenstrom komprimiert werden. Das Netzwerk wird durch eine Verschlüsselung des Tunnels privat – von außen kann der Inhalt der getunnelten Kommunikation nicht entschlüsselt werden. In
Abbildung 14 ist exemplarisch dargestellt, wie durch die Verwendung von Gateways ein virtuelles Netz erzeugt werden kann.

Ein Gateway bezeichnet die Verbindung zwischen zwei Netzen oder Teilnetzen, durch das Daten aus dem Internet in ein lokales Netz gelangen. Gateways arbeiten auf Schicht 7 des ISO/OSI-Modells.

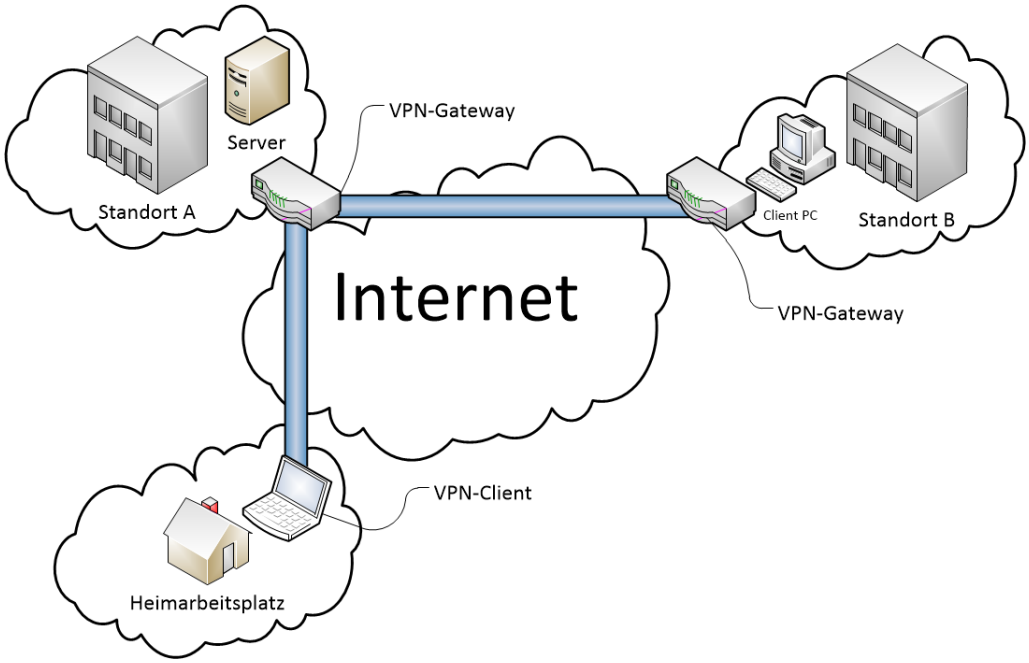


Abbildung 14: Virtual Private Network

Die Abbildung 14 zeigt schematisch, dass am Standort A ein Server in einem Netzwerk vorhanden ist. Dieser soll für die Arbeitsplätze am Standort B und den Heimarbeiter zu erreichen sein. Hierzu wird ein VPN-Gateway genutzt. Da mehrere Arbeitsplätze am Standort B den Zugriff benötigen, bietet es sich an, die Verbindung von einem zentralen Punkt aus zu regeln. Aus diesem Grund wurde hier ein weiteres VPN-Gateway (Standort B) eingerichtet. Für alle Netzteilnehmer am Standort B ist der Server an Standort A nun so zu erreichen, als ob der Server lokal, im eigenen Netzwerk Vorort, angebunden ist. Für den einzelnen Mitarbeiter zu Hause wird ein VPN-Client verwendet, welcher sich mit dem Gateway verbindet und damit am privaten Netzwerk teilnimmt.

Der Einsatz von VPN‘s bietet unter anderem folgende Vorteile:

- VPN‘s sind unabhängig von den Arbeitsplätzen und deren Betriebssystemen (Windows, Linux, Mac OS).
- Gateways bieten Sicherheit in der Kommunikation zwischen Geräten, welche geringe oder keine Sicherheit implementieren.
- In heterogenen Systemen (andere Hardware, Software und so weiter) kann dasselbe Gateway verwendet werden.
- Gateways sind als zentraler Punkt leichter „sicher“ zu realisieren
- Die Sicherheit ist nicht abhängig von anderen Systemkomponenten oder Anwendungen.
- Mit einem VPN-Client können Personen authentifiziert werden.

Für VPNs haben sich zwei Technologien durchgesetzt: IPSec und SSL-VPN.

Für mehr Informationen hinsichtlich dieser VPN-Technologien verwenden Sie bitte das Handbuch Netzwerksicherheit.

3.6 Optimierte Host- und VM-Konfiguration

Die Konfiguration der Host-Systeme und der virtuellen Maschinen ist oft eine komplexe Angelegenheit und sollte ohne ausreichende Schulung nicht durch das Handwerksunternehmen selbst durchgeführt werden.

Weisen Sie Handwerksunternehmen daraufhin, die Konfiguration der virtuellen Systeme durch ein qualifiziertes Systemhaus durchführen zu lassen.

Optimierung der Prozesse auf Host- und virtuellen-Systemen

Bei der Konfiguration von virtuellen Maschinen und den darauf ausgeführten Prozessen ist zu beachten, dass nur Dienste und Anwendungen installiert werden, die auch wirklich eine Verwendung finden. Zum einen spart dies wertvolle Ressourcen, wie beispielsweise Arbeitsspeicher, Festplattenspeicher und Rechenkapazitäten des Prozessors und zum anderen bedeuten mehr Prozesse ein höheres Risiko für mögliche Fehler. Auch die Angreifbarkeit von einem System, ob es jetzt virtualisiert ist oder nicht, steigt mit eine höheren Anzahl von Prozessen.

Vermeiden Sie die Ausführung von nicht benötigten Prozessen.

Weisen Sie ein Handwerksunternehmen darauf hin, nur Prozesse und Dienste auf virtuellen Maschinen oder Host-Systemen zu installieren, die auch wirklich benötigt beziehungsweise empfohlen werden.

Kontinuierliche Überwachung und optimale Zuteilung von Ressourcen

Bei einer akkuraten Planung vor der Installation einer virtuellen Infrastruktur, kann oft sehr gut abgeschätzt werden, wie viele Ressourcen ein Virtualisierungs-Host benötigt. Da virtualisierte Systemumgebungen mit der Zeit wachsen, ist eine kontinuierliche Überwachung der Systemressourcen notwendig. Dabei muss der Virtualisierungsserver an sich, aber auch der System-Status der einzelnen virtuellen Maschinen überwacht werden.
Ausgereifte Virtualisierungssoftware bietet oft eine Zustandsüberwachung über ein Management-Tool an. Darin wird dargestellt, ob Auslastungsgrenzen einzelner virtueller Maschine oder Engpässe im Gesamtsystem erreicht werden.
Auslastungsgrenzen bei einer virtuellen Maschine können oft über die einfache Zuteilung von mehr Arbeitsspeicher oder anderen Ressourcen ausgeglichen werden.

Die Ausführung der virtuellen Infrastruktur muss kontinuierlich auf Ressourcenengpässe überwacht werden.

Weisen Sie ein Handwerksunternehmen darauf hin, den Zustand der virtuellen Maschinen mit Hilfe der Systemprogramme der Virtualisierungssoftware zu überwachen. Dies beugt Ressourcenengpässen vor.
Oft werden solche Zustandsüberwachungen durch ein Systemhaus ausgeführt, die Zuständigkeit für diesen Support sollte jedoch eindeutig abgeklärt sein.

Durch die zuvor dargestellte Überwachung der virtuellen Maschinen, kann auch abgeschätzt werden, wann der Virtualisierungsserver an seine Auslastungsgrenze stößt. Die Wartung eines Virtualisierungsservers bedarf jedoch eines größeren Aufwandes.
Muss in einem Server beispielsweise mehr Arbeitsspeicher-Module eingesetzt werden, ist das sichere Herunterfahren der gesamten virtualisierten Infrastruktur notwendig. Dies bedeutete auch, dass alle virtuellen Maschinen heruntergefahren werden müssen, um einem Verlust von Informationen beispielsweise in Datenbanken vorzubeugen.

Nicht alle Wartungsarbeiten an einem Server können im laufenden Betrieb ausgeführt werden. Ein Server muss sicher herunter gefahren werden, um Datenverlust vorzubeugen.

Weisen Sie Handwerksunternehmen darauf hin, dass Arbeiten am Virtualisierungsserver nur durch professionelle Systemhäuser durchgeführt werden sollten. Bei Wartungsarbeiten, die nicht im laufenden Betrieb durchgeführt werden können, ist immer das sichere Herunterfahren der virtuellen Infrastruktur notwendig, um einem Datenverlust vorzubeugen.

Netzwerk und Netzwerkzugang sichern

Netzwerkressourcen müssen mit Bedacht auf die Datensicherheit freigegeben werden.

Wenn mit virtuellen Maschinen gearbeitet wird, ist es auch möglich Speicherressourcen über das Netzwerk freizugeben. Hierbei ist zu beachten, dass der Zugang zu diesen Ressourcen nur an die virtuellen Maschinen freigegeben wird, die einen Zugriff erlangen dürfen. Dies ist oft über eine einfache Konfigurationskonsole im Hypervisor einstellbar.

Zugriffe auf Ressourcen im Netzwerk müssen eingeschränkt werden.

Auch werden in diesem Zusammenhang oft die Rechte für Lese- und Schreibzugriffe auf diese Netzwerkressourcen definiert. Hierbei ist es wichtig beispielsweise den Schreibzugriff für virtuelle Maschinen auf ein Backuplaufwerk zuzulassen.
Der Zugriff von virtuellen Maschinen untereinander sollte aber generell eingeschränkt werden. Ausschließlich das Teilen von Netzwerkressourcen für einen Dateiaustausch sollte erlaubt werden.

Der externe Zugriff auf ein Unternehmensnetzwerk muss generell untersagt werden. Nur bei bestimmten Mechanismen, wie einer notwendigen Fernwartung sollte dies über den Zugriff per VPN gestattet werden (siehe Kapitel 3.5).

3.7 Redundanz

Bei einem Virtualisierungsserver muss eine hohe Anforderung an die Verfügbarkeit gestellt werden. Dies ergibt sich aus dem Grund, dass viele virtuelle Teilsysteme darauf ausgeführt werden. Bei hochverfügbaren Systemen sind alle Komponenten daher in zweifacher Ausführung vorhanden. Im Handwerk ist dies aus Kostengründen oft nicht so umfangreich realisierbar und kann nur in einem begrenzten Maß erfüllt werden.

Redundante Stromversorgung

Eine redundante Stromversorgung kann vor Datenverlust bei einem Stromausfall schützen.

Eine Unterbrechungsfreie Stromversorgung (USV), kann den übergangsweisen Weiterbetrieb eines Virtualisierungsservers auch bei einem Stromausfall sichern. Die Kapazität sowie die Überbrückungsdauer eines Stromausfalls, muss an die im Unternehmen herrschenden Umstände angepasst werden. Dabei ist es wichtig, dass wichtige Server und Überwachungssysteme sicher heruntergefahren werden können, wenn die Stromzufuhr nicht rechtzeitig wiederhergestellt werden kann. Oft kann jedoch die Stromversorgung im Zeitlimit wiederhergestellt werden, so dass es zu keinen Verfügbarkeitsproblemen kommt.

Informieren Sie Handwerksunternehmen über die Notwendigkeit von Unterbrechungsfreien Stromversorgungen (USV).

Redundante Speichermedien

Die Auslegung von Speichermedien kann auch in einer redundanten Form realisiert werden. Dazu können beispielsweise Techniken, wie das so genannte RAID-System[32] eingesetzt werden (siehe Kapitel 4.7). Dabei werden Daten auf mindestens zwei Festplatten gespiegelt abgespeichert, so dass es zu keinem Datenverlust kommt, wenn eine Festplatte durch einen Hardwaredefekt ausfällt.

Redundant ausgelegte Speichermedien schützen vor Datenverlust bei Hardware- oder Festplattendefekten.

Weisen Sie Handwerksunternehmen darauf hin redundant ausgelegte Speichertechniken zu verwenden.

3.8 Backup

Viele Anbieter von Virtualisierungslösungen bieten in ihren Komplettpaketen auch geeignete Backupmechanismen an. Eine Backup-Lösung aus dem Repertoire von Virtualisierungsanbietern kann oft den Wartungsaufwand, sowie den Zeitaufwand bei der Erstellung und der Wiederherstellung eines Backups reduzieren.
Werden Backups im laufenden Betrieb ausgeführt, schlägt sich dies oft negativ auf die Gesamtperformance des virtualisierten Systems nieder. Daher ist es zu empfehlen ein Backup auszuführen, wenn eine geringe Auslastung stattfindet. Oft sind die Nächte oder frühe Morgenstunden besonders für ein umfangreiches Backup geeignet, zu diesen Zeiten stören sie nicht die Systemressourcen im Tagessgeschäft.

Handwerks-unternehmen müssen ein gut durchdachtes Backupsystem verwenden.

Weisen Sie Handwerksunternehmen darauf hin, geeignete Backuplösungen der Virtualisierungssoftware zu nutzen. Daten müssen immer redundant gesichert werden, um Datenverlust vorzubeugen.

Welche Mechanismen sich besonders für den Einsatz in virtualisierten Umgebungen eignen, erfahren Sie in den folgenden Kapiteln.

3.9 Image

Ein Image im Bereich der Virtualisierung ist eine Datei, in der ein genaues Abbild einer CD/DVD/Blu-ray oder einer Festplatte abgebildet ist.

Images von Betriebssystemen spiegeln die Daten auf einer Festplatte.

Image als Backup

Ein Image kann neben den eigentlichen Dateien, die sich auf dem Medium befinden, auch Informationen über das Dateisystem und dem Startsektor auf einer Festplatte enthalten. Somit ist es möglich das Image für das Wiederherstellen eines Systems zu verwenden. Der Nachteil ist, dass beim Erzeugen eines Images das System nur ein Abbild der eigentlichen Ressourcen auf der Festplatte macht und nicht des gesamten Systems, beziehungsweise den Zustand im Arbeitsspeicher sichert. Somit müssen alle Applikationen oder ähnliches neu gestartet werden, wenn das Image als Backup auf einem Host eingespielt wird.

[32] *RAID* – „Redundant Array of Independent Disks“ *Eine redundante Bereitstellung von Festplatten.*

Image eines alten Servers in eine Virtualisierung überspielen

Ein Image kann auch dazu genutzt werden, um einen alten Server in eine virtuelle Maschine zu konvertieren. Dazu wird mit Tools, wie beispielsweise dem vCenter Converter[33] von VMware, ein Image aus dem Festplatteninhalt eines alten Servers generiert.
Da ein Virtualisierungsserver eine veränderte Hardware für Gastsysteme bereitstellt, ist damit zu rechnen, dass die Treiber auf der virtuellen Maschine angepasst werden müssen. Bei virtualisierten Systemen werden jedoch oft identische Treiber für virtuelle Peripherie eingesetzt, so dass es in diesem Fall seltener zu Treiberproblemen kommt.

Vorteile

- Eins zu eins Abbild der Daten auf der Festplatte.
- Wiederherstellen des Systems hin zum Erzeugungszeitpunkt.
- Kann genutzt werden, um aus einem normalen Server eine virtuelle Maschinen zu generieren.

Nachteile

- Der Zustand des Systems wird ohne den Arbeitsspeicher gespeichert.
- Wiederherstellung nur auf baugleichen Systemen ohne Komplikationen, Treiber müssen nachinstalliert werden.

3.10 Snapshot

In der Virtualisierung ist ein Snapshot eine Methode, um den Zustand von virtuellen Maschinen zu sichern. Snapshots unterscheiden sich in den folgenden Punkten zu einem Image. Bei Snapshots wird nicht nur der Festplatteninhalt in eine Sicherungsdatei geschrieben, sondern auch der gesamte Inhalt des Arbeitsspeichers. Ein Snapshot kann im laufenden Betrieb einer virtuellen Maschine erzeugt werden, ohne dass das System stark beeinträchtigt wird. Somit wird es ermöglicht, das System auf den Zeitpunkt der Erzeugung zurückzusetzen. Dies bedeutet, dass alle Programme die zu diesem Zeitpunkt des Snapshots ausgeführt wurden, auch nach dem Wiederherstellungsprozess laufen.

Mit Snapshots lässt sich der gesicherte Zustand eines virtualisierten Betriebssystems in kürzester Zeit wiederherstellen.

Ein Snapshot wird häufig vor Updateprozeduren erstellt. Schlägt beispielsweise ein Update fehl, kann das System auf den Zeitpunkt vor dem Update wiederhergestellt werden. Auch Änderungen am System, die nicht den gewünschten Effekt erzielen, wie etwa Leistungsabfälle durch fehlerhafte Updates, können so wieder rückgängig gemacht werden. Diese Form der Sicherung bringt jedoch auch Risiken mit sich. Angreifer könnten sich diese Funktion zu Nutze machen, indem sie die Datei in der der Arbeitsspeicherinhalt gespeichert wurde analysieren. Informationen über eine Verschlüsslung der Festplatte könnten so möglicherweise ausgelesen werden, um

[33] http://www.vmware.com/de/products/converter - *konvertiert physische Computer in virtuelle Maschinen.*

etwa den vollen Zugriff zu dem gesamten verschlüsselten Dateisystem zu erhalten. Es gilt also diese Snapshots besonders vor Angreifern zu schützen.

Einige Virtualisierungshersteller bieten eine so genannte „Live Migration“ von virtuellen Maschinen auf andere Host's an. Hierbei wird im Grunde nichts anderes als ein Snapshot erzeugt, welches dann über das Netzwerk auf einen anderen Host kopiert wird. Um sicher zu stellen das Daten nicht während des Kopiervorgangs ausgelesen oder manipuliert wurden, auch wenn diese Informationen nur im eigenen Unternehmensnetzwerk transferiert werden, ist eine verschlüsselte Verbindung empfehlenswert.

Zu beachten ist, dass Snapshots mehr Speicher auf der Festplatte belegen als normale Images da zusätzlich der gesamte Inhalt des Arbeitsspeichers gespeichert wird. Daher sollten immer ausreichend Speicherressourcen zu Verfügung stehen, um in Zukunft eventuelle Engpässe zu vermeiden.

Vorteile

- Erzeugen einer Sicherung im laufenden Betrieb möglich.
- Wiederherstellen des gesamten Systems mit allen gestarteten Applikationen zum Erstellungszeitpunkt.
- Das Wiederherstellen des Systems ist auch auf anderem Host möglich.
- Das System muss bei einer Wiederherstellung nicht neugestartet werden.

Nachteile

- Snapshots wachsen Dynamisch mit der Größe des Gesamtsystems und können sehr schnell große Mengen an Festplattenspeicher belegen.
- Snapshots von verschlüsselten Betriebssystemen können die Vertraulichkeit gefährden.

3.11 Snapshot ohne Abbild des Arbeitsspeichers

Im Grunde ist dies nichts anderes als das Erzeugen eines Snapshots, mit dem Unterschied, das hier kein Abbild des Arbeitsspeichers erzeugt wird. Aus diesem Grund ist nur eine Wiederherstellung des Systems in einem abgeschalteten Zustand möglich. Das virtuelle Betriebssystem muss in diesem Fall erst neu neugestartet werden.

Vorteile

- Wiederherstellen der virtuellen Maschine auf Zustand der Erzeugung.
- Wiederherstellen des Systems auf anderem Host
- Die Erzeugung eines Abbildes ohne den Arbeitsspeicher ist schneller als mit dem Arbeitsspeicher.
- Es können keine vertraulichen Informationen aus dem Arbeitsspeicher ausgelesen werden.

Nachteile

- Der Zustand der virtuellen Maschine ist ohne Arbeitsspeicher gesichert.
- Ein Bootvorgang ist notwendig.

3.12 SAN

Storage Area Networks (SAN) können genutzt werden, um einem Virtualisierungsserver erweiterten Speicher in einem Netzwerk bereitzustellen. In größeren Unternehmen werden oft Glasfaserverbindungen verwendet, um hoch performant Datenspeicher bereit zu stellen. In kleineren Unternehmen wird diese Anbindung aus Kostengründen oft mit normalen Netzwerkverbindungen (bis zu 1 Gbit's) realisiert. Dies ist weitaus günstiger als teure Glasfaser kompatible Hardware zu verwenden. Handwerksunternehmen verzichten oft ganz auf diese Technologie und verwenden nur den verfügbaren Speicherplatz auf den Festplatten eines lokalen Servers.
Speicherkapazitäten des SAN sind für normale Netzwerkteilnehmer nicht sichtbar und werden nur dem Virtualisierungsserver bereitgestellt. Dieser kann Teile des Gesamtspeichers einzelnen virtuellen Maschinen zur Verfügung stellen.

Wenn SANs zum Einsatz kommen, müssen diese Redundant gesichert werden. Dies bedeutet, dass der Zugriff sowie die Stromzufuhr über die bereits beschriebenen Methoden zur Steigerung der Redundanz verwendet werden müssen (s. Kapitel 2.4).

3.13 Sichere Passwörter

Trotz aller Sicherheitsvorkehrungen muss es mindestens einen Administrator geben, der den „vollen Zugriff" auf einen Virtualisierungsserver, beziehungsweise Hypervisor haben muss.
Ein besonderes Augenmerk sollte daher auf gerade dieses Administratoren-Passwort gelegt werden, da es nicht in den Besitz von Nutzern mit eingeschränkten Berechtigungen gelangen darf. Daher sollte unbedingt höhere Anforderungen an die Wahl des Passwortes gelegt werden.

Nutzen Sie sichere Passwörter mit mindestens 12 Zeichen.

Die Wahl von starken Passwörtern ist ein Sicherheitsmerkmal, welches auch potenziellen Angreifern den Zugriff auf ein System verwehrt. Hacker haben die Möglichkeit, einen so genannten Brute-Force-Angriff auf eine Login-Maske. Wenn diese Attacke nicht frühzeitig erkannt wird und der Nutzer ein schlechtes Passwort gewählt hat, könnte ein Passwort mit Begrifflichkeiten aus einer umfangreichen Wortliste erraten werden.

Nutzen Sie sichere Passwörter mit folgenden Kriterien!

- Verwenden Sie mindestens zwölf Zeichen, darunter eine Mischung aus Groß- und Kleinbuchstaben sowie Ziffern und Sonderzeichen in sinnfreiem Zusammenhang.

- Ändern Sie Passwörter regelmäßig.
- Nutzen Sie für jedes Login ein separates Kennwort.
- Bewahren Sie Ihre Passwörter sicher auf. Hierzu eignen sich beispielsweise Passwort-Management-Software wie KeePass(x)[34].

Passwortverwaltungs-software wie KeePass(x) können helfen, Kennwörter sicherer zu Verwalten.

Weitere Informationen zu Keepass(x) erhalten Sie im Handbuch mobiles Arbeiten.

Was unbedingt vermieden werden sollte:

- Nutzen Sie keine zusammenhängenden Wörter, die im Lexikon oder im allgemeinen Sprachgebrauch vorkommen (schlechtes Beispiel: Jahreszeiten, Lieblingsverein, Name).
- Nutzen Sie keine Begriffe, die mit Ihnen in Bezug gebracht werden können – wie den Namen eines Familienmitglieds oder Ihres Lieblingssportvereins.
- Hängen Sie keine Jahreszahlen oder Geburtstage an Kennwörter.

3.14 Zusammenfassung

In diesem Kapitel wurden Ihnen Mechanismen dargestellt, die einen grundlegenden Basisschutz rund um das Thema Virtualisierung ermöglichen. Dies reicht von der Zuordnung der Zuständigkeiten für eine virtuelle Umgebung, über die sichere Datenübertragung mittels VPN, bis hin zur Erstellung von hochwertigen Passwörtern. Der Basisschutz für virtuelle Systeme variiert je nach Einsatzszenario und muss ständig auf einem hohen Niveau gehalten werden, um die Sicherheit der Daten und des gesamten Tagesgeschäfts eines Unternehmens zu sichern.
Der Basisschutz ist ein Zusammenspiel aus vielen verschiedenen Prozessen und erfordert den Einsatz von jedem einzelnen Mitarbeiter im Unternehmen. Wie so oft beschrieben, kann bereits das schwächste Glied einer Kette die gesamte IT-Sicherheit im Unternehmen gefährden.

Notizen

[34] http://keepass.info – *Kostenloser und quelloffener Passwortmanager für Linux und Windows*

4. Praxistipps

Im diesem Kapitel werden Ihnen einige Praxistipps für den Einsatz und die Konfiguration von virtuellen Maschinen und deren Hostsystemen dargestellt.

4.1 Anwendungsmöglichkeiten der Virtualisierung in Handwerksbetrieben

Im den folgenden Abschnitten werde einige Beispiele für Anwendungsmöglichkeiten für Virtualisierung im Handwerk abgebildet.

4.1.1 Virtuelle Maschinen aus existierenden Servern erzeugen

Für die Konvertierung von einem älteren Server in eine virtuelle Maschine sind einige Vorbereitungen notwendig.
Es muss dafür gesorgt werden, dass auf dem Quell-System, in diesem Fall der betroffene Server der konvertiert werden soll, genug Festplattenkapazität zur Verfügung steht. Dies bedeutet, dass mindestens die doppelte Menge des belegten Festplattenspeichers verfügbar sein muss. Vor dem Konvertierungsprozess ist es möglich die Festplatte der Ziel VM so zu reduzieren, dass dies platzsparend auf den zukünftigen Virtualisierungsserver transferiert werden kann.

Ein Beispiel:
Der alte Server hat eine 100 GB große Festplatte. Von diesen 100 GB sind jedoch nur 75 GB mit Daten belegt. Dies bedeutet, dass die erzeugte virtuelle Maschine eine Größe von 75 GB in unkomprimierter Form aufweisen wird. Es muss demnach mindestens 150 GB Festplattenspeicher verfügbar sein, damit ein Image auf der lokalen Festplatte abgelegt werden kann.

Das Softwareprodukt für das folgende Beispiel ist „vCenter Converter“ von VMware. Zum Zeitpunkt dieses Beispiels ist die Software nur in englischer Sprache verfügbar, daher werden einige Begriffe in Englisch ergänzt, siehe Klammern.

Schritt 1:
Zunächst wird der vCenter Converter auf dem Server installiert, aus welchem eine virtuelle Maschine generiert werden soll.

Das Programm vCernter Converter kann virtuelle Maschinen generieren.

Alternative:
Es ist auch möglich, dass eine virtuelle Maschine von einem Computer im Netzwerk erzeugt wird. Dafür muss ein so genannter Agent – ein Tool, das einen Dienst zur Erstellen von Images bereitstellt – auf dem Quell-System installiert werden. Diese Installation eines Agenten kann während der Installation des vCenter Converter ausgewählt werden. Dieser Agent kann über das Netzwerk von dem Virtualisierungs-Host angesteuert und aktiviert werden.
Dies kann beispielsweise dann vorteilhaft sein, wenn nicht genügend Festplattenspeicher auf dem Quell-System verfügbar ist, um das Image für eine virtuelle Maschine abzuspeichern.
Die Daten können so direkt an den Virtualisierungsserver übertragen werden.

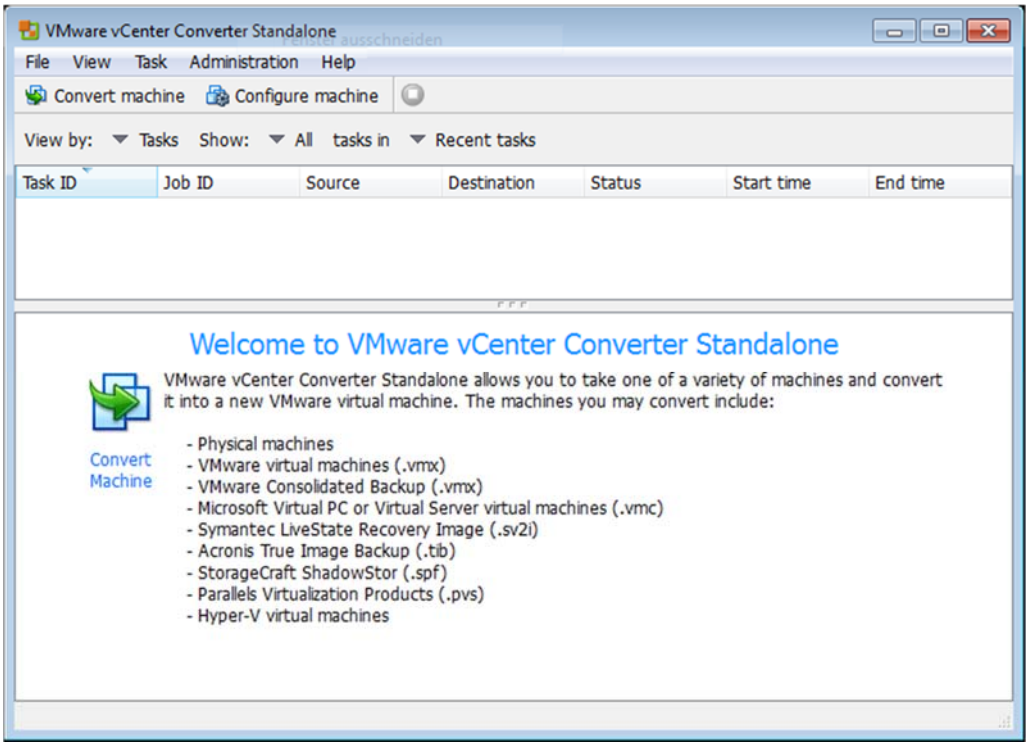


Abbildung 15: VMware vCenter Console

Schritt 2:
Der Prozess zur Konvertierung in eine virtuelle Maschine wird gestartet (convert maschine), siehe Abbildung 15.

Schritt 3:
Die Quelle (select source type) wird ausgewählt, in diesem Fall wird der folgende Parameter verwendet (Powered-on maschine). Es bezeichnet einen Computer, der sich in einem gestarteten, beziehungsweise aktivierten Zustand befindet (siehe Abbildung 16).

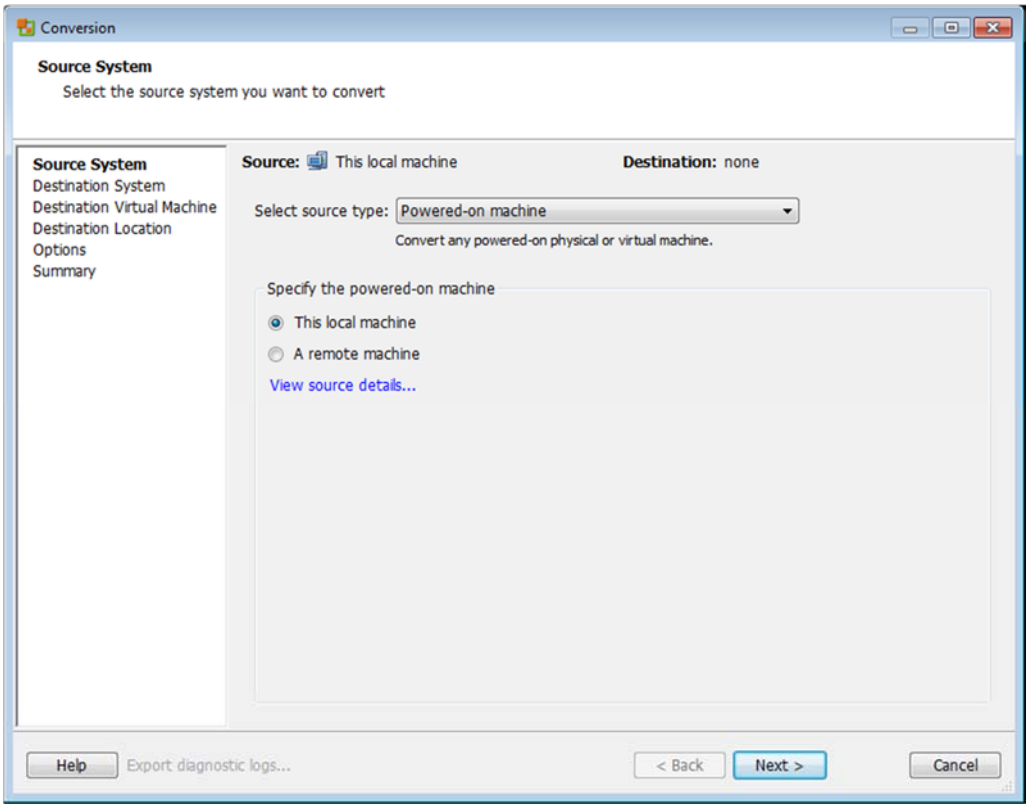


Abbildung 16: VMware vCenter Quell-System

Damit das Konvertierungsprogramm die nötigen Informationen über die Art des zugrundeliegenden Systems erhält, muss (This local maschine) ausgewählt werden, also diese lokale Maschine, siehe Abbildung 16.

Weitere Optionen sind beispielsweise die Konvertierung von bereits existierenden virtuellen Maschinen von Anbietern wie Microsoft Hyper-V, VirtualBox oder anderen virtuellen Maschinen in eine virtuelle Maschine im VMware-Format.

Virtuelle Maschinen können auch direkt über das Netzwerk auf einen Host-Server übertragen werden.

Schritt 4:
Hier muss das Ziel-System (select destination type) ausgewählt werden, siehe Abbildung 17. Dies kann der lokale Computer (VMware Workstation or other VMware virtual machine) oder ein im Netzwerk erreichbarer Virtualisierungsserver (VMware Infrastructure virtual machine) sein.
In diesem Beispiel dient der Server, beziehungsweise der lokale Computer als Ziel, es muss daher VMware Workstation ausgewählt werden (siehe Abbildung 17).

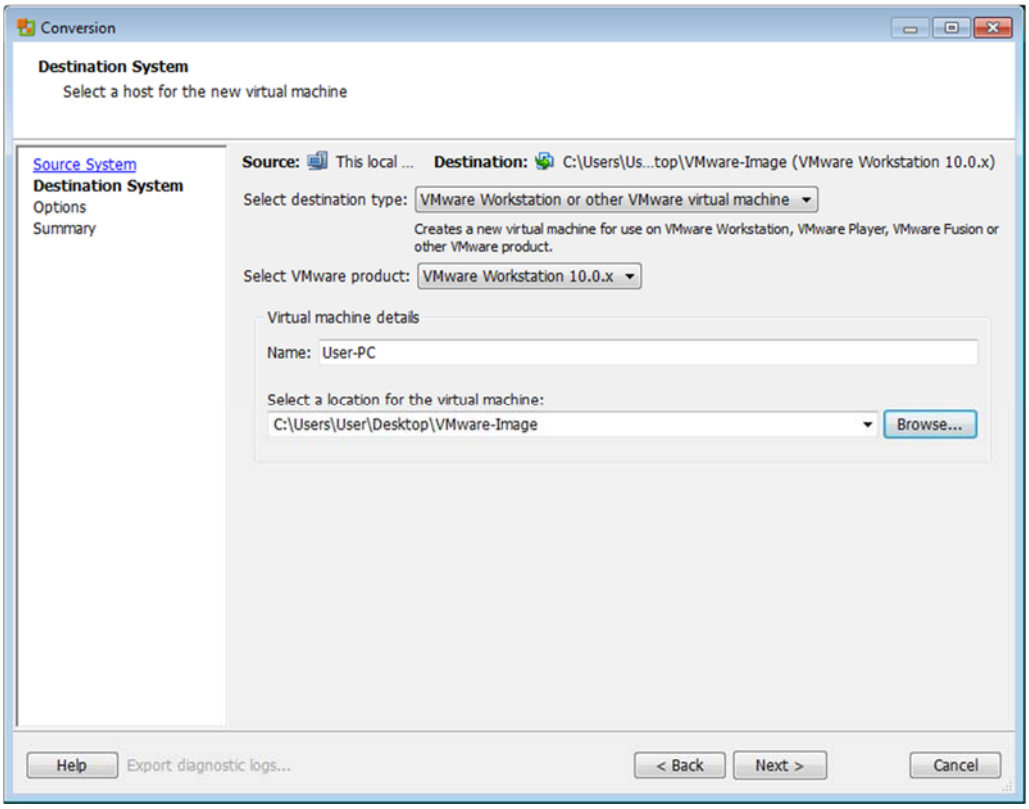


Abbildung 17: VMware vCenter Ziel-System

Es bleibt noch auszuwählen, welcher Zielordner zum Abspeichern der neuen virtuellen Maschine verwendet werden soll.

Schritt 5:

Zuletzt können die Einstellungen der zu erzeugenden virtuellen Maschine überprüft und gegebenenfalls verändert werden. Dies könnten beispielsweise die Größe der Festplatte oder der zugewiesene Arbeitsspeicher sein.

Die Parameter auf einer virtuellen Maschine können während der Konvertierung angepasst werden.

Dieser Parameter können beeinflusst werden:

- Datenträger
- Arbeitsspeicher und Prozessorkerne
- Netzwerkadapter
- Ausgeführte Prozesse

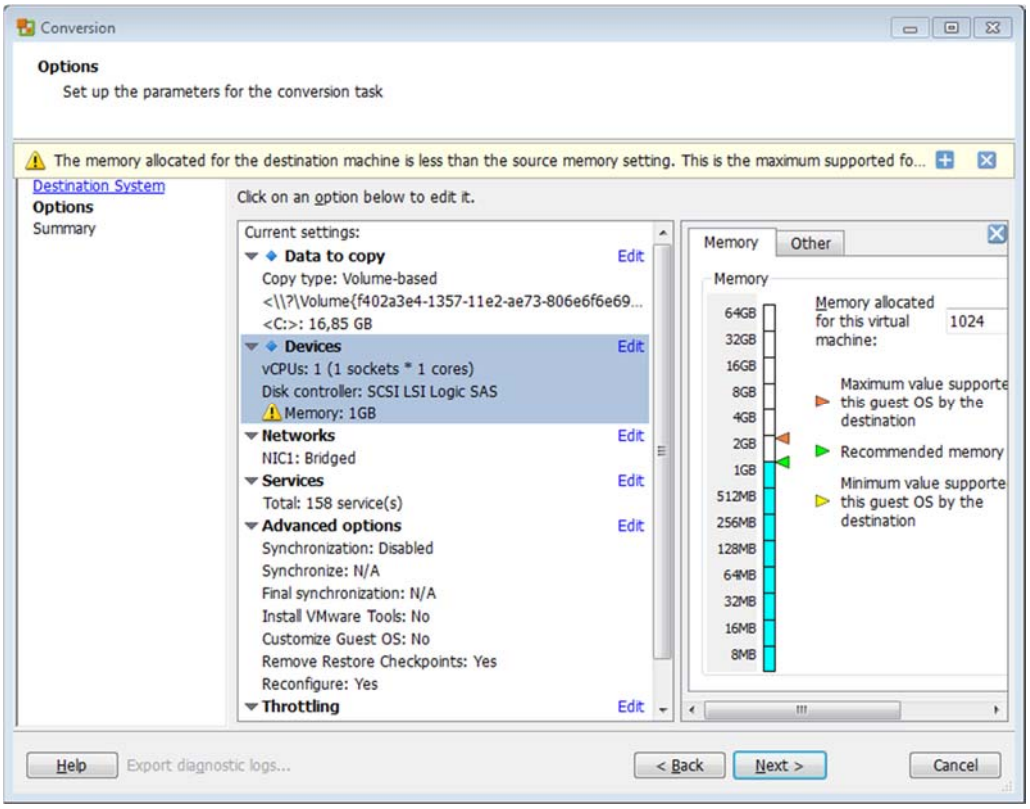


Abbildung 18: VMware vCenter VM-Optionen

In Abbildung 18 ist zu erkennen, dass bei einer Änderung des Arbeitsspeichers ein Untergrenze festgelegt ist. Dies hat den Zweck, dass der virtuellen Maschine nicht weniger Arbeitsspeicher zugewiesen werden kann, als die aktuell ausgeführten Prozesse benötigen.

Schritt 6:
Der letzte Schritt dient als eine Zusammenfassung aller verwendeten Parameter und kann mit (finish) beendet werden. Die virtuelle Maschine wird darauf hin erzeugt, dies kann mehrere Stunden in Anspruch nehmen.

Zusammenfassung:
Die virtuelle Maschine befindet sich nun im dem zuvor ausgewählten Ordner und kann in einer Virtualisierungssoftware auf eine korrekte Lauffähigkeit geprüft werden.
Ist die optimale Ausführbarkeit gewährleistet, kann die virtuelle Maschine in die Infrastruktur des Virtualisierungsservers übertragen werden.

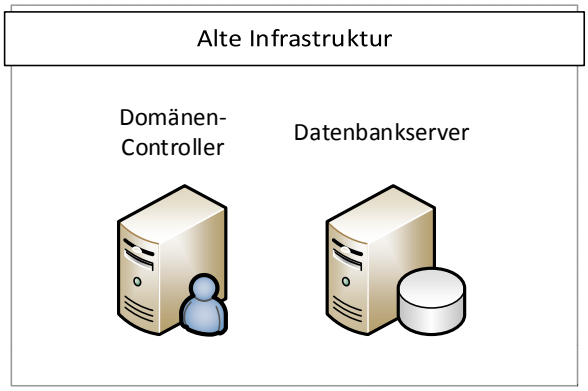
4.1.2 Beispiel für Virtualisierung im Handwerk

Das folgende Beispiel beschreibt ein Szenario, für die Nutzung von Virtualisierung in einem Unternehmen aus dem Elektrohandwerk.

Konsolidierung und Erhaltung von alten Serversystemen in einer virtuellen Umgebung

Einleitung:
Aufgrund der Weiterentwicklungen und den höheren Anforderungen an die Hardware durch Verwaltungsprogramme, hat sich die Geschäftsleitung dazu entschieden in eine neue IT-Infrastruktur zu investieren.

Infrastruktur vor der Virtualisierung:
Die Infrastruktur bestand aus insgesamt zwei Servern, einem Windows Server 2008, der die Domäne (Domänen-Controller) zum Authentifizieren der verschiedenen Mitarbeiter gewährleistet und einem Datenbankserver, dieser wird für die Verwaltungssoftware des Unternehmens verwendet.



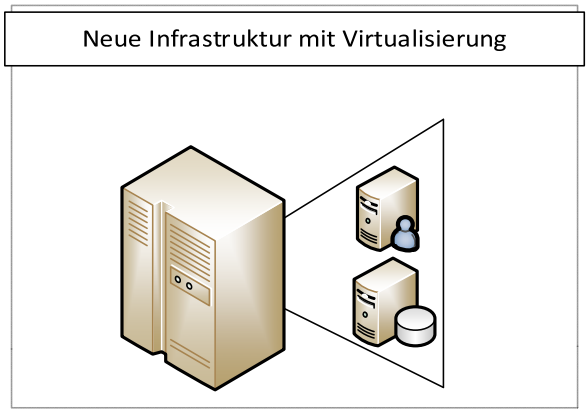
- 2 Netzteile
- 4 Festplatten
- Unabhängiger Arbeitsspeicher
- 2 veraltete Prozessoren

Abbildung 19: Alte Infrastruktur

Schon vor der Virtualisierung der Server wurde eine Sicherung der Daten durch auf einem Bandlaufwerk ausgeführt.

Infrastruktur nach der Virtualisierung:
Für die Virtualisierung wurde ein leistungsstarker Virtualisierungs-Host angeschafft. Dieser besitzt ein Raid-System mit 1000GB Festplattenkapazität. Der Prozessor besteht aus sechs Kernen, mit einer Leistung von jeweils 2.67 GHz. Mit einer üppigen Ausstattung von 26 GB RAM ist bei der Anschaffung des Servers zukunftsorientiert geplant worden. Der Hypervisor, der in diesem Szenario zum Einsatz kommt, ist der kostenloste ESXi Server[35] von VMware.

[35] http://www.vmware.com/de/products/vsphere-hypervisor



- 1 Netzteil
- 2 Festplatten im Raid 1
- 26 GB RAM für alle virtuellen Maschinen verfügbar
- Leistungsfähiger Prozessor mit 6 Kernen, die je nach Bedarf einzelnen Maschinen zugeteilt werden können
- Neue virtuelle Maschinen können je nach Bedarf hinzugefügt werden

Abbildung 20: Virtualisierte Infrastruktur

Überwachung und Wartung der Virtualisierung:
Die Wartung und Überwachung der virtualisierten Infrastruktur wird durch ein zertifiziertes Systemhaus sichergestellt.

4.2 Vorteile der Serverkonsolidierung nutzen

In dem zuvor dargestellten Beispiel wurde gezeigt, wie aus vielen Servern ein zentraler Virtualisierungsserver wurde. Genau dies zeigt sehr deutlich, welches Potenzial in der Konsolidierung von IT-Systemen steckt.

Wie bereits beschrieben, ist die Serverkonsolidierung in heutigen Rechenzentren und kleineren Serverräumen an der Tagesordnung. Es werden nicht mehr viele einzelne Server mit verschiedenen Betriebssystemen aufgesetzt, vielmehr können mit Hilfe von Virtualisierung verschiedenste Betriebssysteme auf einem einzelnen Virtualisierungs-Host bereitgestellt werden.

Zentralisierung der Funktionalitäten

Bei einer Virtualisierungslösung kann eine zentral installierte Software das komplette Backup-Management übernehmen, siehe Kapitel 4.6.
In Kombination mit einer Festplattenspiegelung über RAID und Bandsicherungen werden hier weitere effektive Maßnahmen zum Schutz der Verfügbarkeit bereitgestellt.

Viele wichtige Funktionen können zentral auf einem Hypervisor verwaltet werden.

Weniger Wartungsaufwand

Durch eben diese Zentralisierung einzelner Prozesse, wie beispielsweise Datensicherung, Antivirenlösungen, Firewall-Einstellungen und der Netzwerkverwaltung über VLAN's, kann der Wartungsaufwand für die Systemverwaltung deutlich reduziert werden. Auch die Wartung der Hardware, in Form der Komponenten des Servers, der Unterbrechungsfreien Stromversorgung (USV) und der Anlage zur Kühlung der Systeme, kann kleiner dimensioniert und somit der Wartungsaufwand reduziert werden.

Geringerer Stromverbrauch

Virtualisierung kann ein Unternehmen bei der Reduzierung des Stromverbrauchs unterstützen. Wie bereits in den Kapiteln zuvor dargestellt, können diverse Komponenten in einer virtualisierten Infrastruktur deutlich sparsamer dimensioniert werden.
Einsparungspotenzial bieten vor allem folgende Komponenten:

Virtualisierung bietet Potential für eine Senkung des Stromverbrauchs, sollte aber für jede Planung berechnet werden.

- Server:
  - Netzteile
  - Prozessoren
  - Festplatten
- Serverraum:
  - Klimageräte
  - Netzwerk-Equipment

4.3 Anforderung an Host

Wenn moderne Virtualisierungslösungen, beispielsweise mittels KVM, Xen, VMware oder Microsoft eingesetzt werden, müssen die jeweils gültigen Mindestanforderungen an das Hostsystem erfüllt werden.
Darüber hinaus müssen in einem Server Komponenten verbaut werden, die für die Einsatzumgebung im Umfeld der Virtualisierung geeignet sind. Auf den Herstellerseiten werden dazu ausführliche Listen mit Komponenten dargestellt.

Die Mindest-anforderungen an Server im Bereich der Virtualisierung müssen beachtet werden.

Weisen Sie ein Handwerksunternehmen darauf hin, einen Virtualisierungsserver ausschließlich für die Aufgaben zu verwenden, für die er benötigt wird. Es sollten nur Anwendungen installiert werden, die für eine funktionierende virtuelle Infrastruktur notwendig sind.

4.4 Sicherheit in der Virtualisierung

Wer sich im Handwerk aktuell oder in der Vergangenheit bereits mit dem Thema Virtualisierung beschäftigt hat, hat möglicherweise einen Schritt hin zur Modernisierung der IT-Infrastruktur in einem Unternehmen durchgeführt. Virtualisierung allein ist jedoch kein Garant für umfassende IT-Sicherheit, da auch bei der Konfiguration der Virtualisierung Fehler passieren können.

Die IT-Sicherheit bei Virtualisierung darf nicht vernachlässigt werden!

Basisschutz für Virtualisierung

In Handwerksunternehmen sollte unter keinen Umständen eine Server-Virtualisierung ohne professionelle Hilfe aufgebaut werden.

Für ein Handwerksunternehmen sollten daher Folgende Regeln beachtet werden:

Unterstützung durch zertifizierte Systemhäuser

Weisen Sie ein Unternehmen darauf hin, sich durch ein zertifiziertes Systemhaus unterstützen zu lassen. Systemhäuser sind auch eine erste Anlaufstelle für Informationen über Mechanismen zur Datensicherung, die in ein bestehendes Sicherheitskonzept integriert werden müssen. Wenn noch kein Sicherheitskonzept existiert, besteht ein erhöhter Handlungsbedarf und es muss geprüft werden, ob ein

Mindestmaß an Sicherheitsmechanismen im betroffenen Handwerksunternehmen etabliert ist.

Mehr Informationen zu Sicherheitskonzepten finden Sie im Handbuch Netzwerksicherheit.

Separierung (Netzwerke trennen)

Für eine sichere Trennung von Netzwerken sollten die Möglichkeiten der Virtualisierungssoftware genutzt werden. Oft kann eine einfache Trennung mittels VLAN's etabliert werden.

Firewall-Lösungen aus einer Hand

Firewall-Lösungen sollten aus der Hand des Herstellers einer Virtualisierungslösung gewählt werden. Softwarehersteller haben oft jahrelange Erfahrung auf diesem Gebiet und ihre Lösungen sind oft komfortabel in die Systemlandschaft integrierbar. Dies vereinfacht die Verwaltung und sichert eine gut durchdachte virtuelle Infrastruktur.

Herstellereigene Antiviren- und Firewall-Lösungen sind oft sehr gut in eine virtuelle Infrastruktur integrierbar.

Aktivierung der automatischen Updates

Weisen Sie Handwerksunternehmen darauf hin, dass sich der Hypervisor auf einem aktuellen Softwarestand befinden muss. Die Aktivierung von automatischen Updates im Hypervisor schützt die gesamte virtualisierte Infrastruktur vor den möglichen Gefahren durch Sicherheitslücken.

Beachten Sie darüber hinaus, dass die virtuellen Maschinen ebenfalls auf einem aktuellen Stand mittels automatischer Updates gehalten werden müssen.

Antiviren-Lösung aus einer Hand

Wenn es möglich ist, sollte in einer virtuellen Infrastruktur eine Antivirendistribution integriert werden, die auch von der Virtualisierungslösung an sich unterstützt wird. Antivirensoftware wird daher oft im Paket zusammen mit einer Hypervisor-Lösung angeboten.
Bei kleinen virtuellen Infrastrukturen sind oft gängige Antivirenlösungen ausreichend.

4.5 Sicherheitsvorkehrungen für den Gast

Gastsysteme in einer virtualisierten Umgebung verhalten sich wie normale Netzwerkteilnehmer und müssen gleichermaßen geschützt werden.

Automatische Updates

Dies bedeutet insbesondere, dass virtuelle Maschinen mit wichtigen Updates versorgt werden. Dabei sollten die gängigen Updateroutinen, wie beispielsweise automatische Windows-Updates verwendet werden.

Virtuelle Maschinen müssen mit Updates versorgt werden.

Beachten Sie die Hinweise auf der Checkliste zum Thema Basisschutz.

Für Virtualisierung optimierte Antivirensoftware

Weisen Sie auf die Nutzung einer Antivirenlösung des Virtualisierungsanbieters oder einer gleichwertigen Anwendungen von Drittanbietern hin.
Bei der Verwaltung von vielen virtuellen Maschinen bietet sich eine so genannte agentenlose Antivirus-Lösung an. Der Vorteil dieser Variante ergibt sich aus der performanten Ausführung direkt auf dem Hypervisor. Dieser verwaltet zentral alle Antivirensignaturen, lediglich individuelle regelbasierte Einstellungen werden auf den virtuellen Maschinen an sich vorgenommen.

4.6 Datensicherung

Wie bereits in den vorherigen Kapiteln dargestellt, bietet die Virtualisierung weitere Datensicherungstechnologien, die zusätzlich zur bewährten Bandsicherung eingesetzt werden können.

Daten müssen stets redundant gespeichert werden!

Virtualisierung vereinfacht komplexe Datensicherungen

Vor dem Einsatz von virtualisierten Systemen, mussten alle Server separat gesichert werden. Dies wird durch die Serverkonsolidierung und dem Einsatz von Virtualisierung deutlich vereinfacht. Aktuelle Virtualisierungsprodukte aus dem kommerziellen Bereich, beispielsweise von Microsoft und VMware sowie aus dem Open Source Bereich mit KVM und Citrix Xenserver, bringen umfangreiche Backuplösungen mit sich.
Deutliche Unterschiede werden jedoch schon in der Bedienung sichtbar. Bei den Produkten von Microsoft, VMWare und Citrix wird eine Konfiguration in einer grafischen Oberfläche ermöglicht. Bei KVM hingegen wird sehr viel Erfahrung im Bereich der Programmierung und der Bedienung von Linux in einem Konsolenfester vorausgesetzt.
Bei der Nutzung von kommerzieller Software müssen weitere Lizenzkosten für Datensicherungsanwendungen einkalkuliert werden.

Snapshots sind das neue Backup

Alle Anwendungen, ob kommerziell oder nicht haben eins gemeinsam, Snapshots sind die wichtigsten Hilfsmittel bei der Datensicherung in virtuellen Umgebungen. Sie lassen sich innerhalb von wenigen Minuten anlegen und können erstellt werden, ohne den Betrieb einzelner virtueller Maschinen zu stören. Auch die Verwaltung von Snapshots kann mit diversen Anwendungen optimiert werden. Dabei lassen sich automatisiert, in genau definierten Intervallen, Snapshots erzeugen. Um den oft kostbaren Speicherplatz nicht zu verschwenden, können Snapshots nach definierten Intervallen gelöscht werden, wenn in diesen Zeuträumen keine Datenverluste aufgetreten sind.

Snapshots können die Datensicherung von virtuellen Umgebungen deutlich vereinfachen.

Datenwiederherstellung aus älteren Snapshots

Welche Möglichkeiten zusätzlich zur Wiederherstellung eines kompletten Snapshots existieren, soll folgendes Beispiel demonstrieren:
Stellen Sie sich vor, dass eine spezielle Datei mit wichtigen Kundeninformationen ausversehen auf einer virtualisierten Maschine gelöscht wurde. Zum einen besteht die Möglichkeit, ein altes Snapshot wiederherzustellen, zum anderen bietet Virtualisierung aber auch die Möglichkeit, ausschließlich die einzelne Datei aus einem älteren Snapshot wieder in das aktuell ausgeführte virtuelle System zu überführen. Dies kann eine hohe Zeitersparnis mit sich bringen. Einzelne Dateien können beispielsweise mit

den aktuellen Versionen von Microsoft hyper-v und VMware inklusive dem Zusatzpaket vSphere Data Protection wiederhergestellt werden.

Bandsicherungen sind auch heute noch im Einsatz

Für die Sicherung von gesamten Serversystemen sind immer noch magnetische Bandsicherungen im Einsatz. Dabei werden Informationen auf kassettenähnlichen aufgerollten Streifen gespeichert.
Der Vorteil den die Bandspeicherung bietet ist, dass die Bänder platzsparend verstaut werden können. Ist ein Band gefüllt, wird es durch eine neue Bandkassette ersetzt. Um einen Datenverlust durch ein Feuer vorzubeugen ist es empfehlenswert, die Bänder nicht in den gleichen Räumlichkeiten aufzubewahren, wie der Server, auf dem die Sicherung stattfindet.

Bandsicherungen werden auch heute noch zur Sicherung von Unternehmens-daten verwendet.

Ein deutlicher Nachteil der Bandsicherung ist jedoch, dass eine Datenwiederherstellung über ein Bandlaufwerk oft mehrere Stunden in Anspruch nehmen kann. Dies richtet sich oft nach dem verwendeten Technologiestand der Bandlaufwerke. Neuste Generationen haben eine Übertragungsgeschwindigkeit von bis zu 1180 MB/s beziehungsweise 1,18 GB/s. Auch eine Verschlüsselung mit aktuellen Standards ist bei neueren Bandlaufwerken möglich.

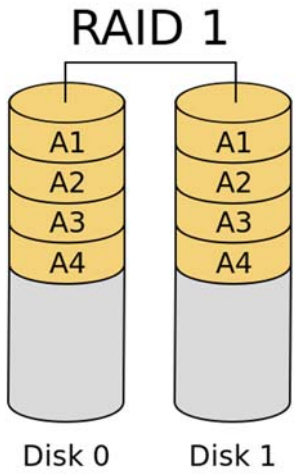
Backupsoftware für virtualisierte Server

Als Backupsoftware ist beispielsweise das Programm Veeam Backup & Replication v8[36] einsetzbar. Diese Software ist auch als kostenlose Testversion verfügbar. In einer Variante für kleine und mittelständische Unternehmen ist diese Software bereits ab 470 € im Jahr zu erhalten.
Die Backup-Software kann gleichermaßen für die Hypervisoren Microsofts V-Server und vSphere von VMware verwendet werden.

[36] http://www.veeam.com/de/vm-backup-recovery-replication-software.html

4.7 Raid

Raid - Redundant Array of Independent Disks ist eine Technologie, die es ermöglicht Daten redundant auf mindestens zwei Festplatten zu speichern. Wird ein Raid 1 verwendet, wird jeder Datenblock auf mindestens einen zweiten Datenträger abgespeichert (siehe Abbildung 21).



RAID ermöglicht eine redundante Speicherung von kritischen Unternehmensdaten.

Abbildung 21: Raid 1 für redundante Datenspeicherung auf zwei Festplatten

Wenn es zu einem Ausfall eines Datenträgers kommt, wird dieser Datenträger durch einen Ersatzdatenträger ausgetauscht. Der Raid-Controller, der sowohl in der Form von Software als auch in Form eines Hardware-Controllers im Server verbaut sein kann, spiegelt daraufhin die Daten auf den Ersatzdatenträger. Unterstützt ein Raid-System das so genannte „Hot-Swapping“ ist das Auswechseln einer defekten Festplatte sogar im laufenden Betrieb möglich.

4.8 Virtualisierung in der Cloud

Da Virtualisierung die Grundlage für das heutige Cloud-Computing ist, werden Lösungen für Virtualisierung auch in der Cloud, beziehungsweise als Dienstleistung im Internet angeboten.

Dies hat für Handwerksunternehmen entscheidende Vorteile aber auch Nachteile, die in den folgenden Abschnitten dargestellt werden.

Vorteile von Virtualisierung in der Cloud

Virtualisierung in der Cloud ist deutlich günstiger als die Verwaltung im eigenen Haus.
Handwerksunternehmen können Infrastructure as a Service einkaufen, dabei werden die Server von einem Unternehmen gepflegt und ständig auf einem aktuellen Stand gehalten. Dies hat insbesondere IT-sicherheitstechnische Vorteile, da die Infrastruktur bei professionellen Cloud-Computing-Lösungen stets mit sehr gut geschultem Personal überwacht wird.
Die Alternative ist, ganz auf Server zu verzichten und nur die jeweiligen Applikationen einzukaufen dies wird Software as a Service (SaaS) genannt.

Nachteile von Virtualisierung in der Cloud

Leider hat die Nutzung von Cloud-Dienstleistungen auch einige Nachteile. Es droht ein Kontrollverlust über die Daten. Dies bedeutet, dass Informationen an Dienstleister weitergegeben werden, dabei muss sich komplett darauf verlassen werden, dass alle Sicherheitsmaßnahmen im Umfeld des Cloud-Dienstes sorgsam eingehalten werden.
Auch wurden in der Vergangenheit Cloud-Dienste in Bezug auf den Datenschutz kritisiert.
Nach den rechtlichen Risiken noch eine schnelle Internetverbindung notwendig, solche Verbindungen sind insbesondere im ländlichen Raum oft noch nicht verfügbar.

Für weitere Hinweise hinsichtlich der Nutzung von Cloud-Computing nutzen Sie bitte das gleichnamige Handbuch. Darin finden Sie auch wichtige Hinweise, die hinsichtlich des Datenschutzes beachtet werden müssen.
Weitere detaillierte Informationen erhalten Sie auch im Handbuch Datenschutz.

5. Weblinks

http://www.it-sicherheit-handwerk.de
https://www.internet-sicherheit.de
http://www.heise.de/thema/Virtualisierung
http://www.kernelthread.com/publications/virtualization/
https://de.wikipedia.org/wiki/Serverpartitionierung#Virtualisierung
https://de.wikipedia.org/wiki/Virtuelle_Maschine
https://de.wikipedia.org/wiki/Hypervisor
http://openbook.rheinwerk-verlag.de/vmware/
https://technet.microsoft.com/de-de/virtualization/
http://www.vmware.com/de/virtualization
http://www.itwissen.info/definition/lexikon/Vollstaendige-Virtualisierung-full-virtualization.html
http://www.itwissen.info/definition/lexikon/Paravirtualisierung-para-virtualization.html
https://www.bsi.bund.de/DE/Themen/CloudComputing/Dossiers/Grundschutz/IT-Grundschutz.html?notFirst=true&docId=4952784
http://www.security-insider.de/themenbereiche/plattformsicherheit/cloudvirtualisierung/
http://www.computerwelt.at/news/hardware/server-appliances/detail/artikel/die-risiken-der-server-virtualisierung-vorsicht-virtualisierung/
http://www.cio.de/topics/virtualisierung,3973
http://www.keepass.info
http://www.vmware.com/de
http://www.microsoft.com/de-de/server-cloud/solutions/virtualization.aspx

6. Literaturverzeichnis

Bertram Wöhrmann (2012): Virtualisierungs-Grundlagen. Varianten und Unterschiede. Hg. v. http://www.tecchannel.de. Online verfügbar unter http://www.tecchannel.de/server/virtualisierung/2029842/faq_alles_ueber_virtualisierung_varianten_und_unterschiede/, zuletzt aktualisiert am 25.06.2014, zuletzt geprüft am 25.06.2014.

Christian Baun (2010): Vorlesung Cluster-, Grid- und Cloud-Computing Hochschule Mannheim. Karlsruher Institut f˙ur Technologie Steinbuch Centre for Computing. Online verfügbar unter http://baun-vorlesungen.appspot.com/CGC1011/Skript/folien_cgc_vorlesung_12_WS1011.pdf, zuletzt aktualisiert am 25.06.2014, zuletzt geprüft am 25.06.2014.

Christoph Meinel, Christian Willems, Sebastian Roschke, Maxim Schnjakin (2011): Virtualisierung und Cloud Computing : Konzepte, Technologiestudie, Marktübersicht (Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam ; 44), zuletzt geprüft am 23.09.2014.

Meinel, Christoph; Roschke, Sebastian; Schnjakin, Maxim; Willems, Christian (2011): Virtualisierung und Cloud Computing. Konzepte, Technologiestudie, Marktübersicht. Potsdam: Univ.-Verl. Potsdam (Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam, 44).

7. Stichwortverzeichnis

4

4 GB-Grenze 32

A

AMD-V 25

B

Backup 6, 26, 30, 32, 33, 36, 39, 47, 58, 61, 62
Backupsoftware 62
Bandsicherung 27, 61, 62
Bare-Metal 17
Basisschutz 6, 39, 51, 59, 60
Betriebssystemvirtualisierung 24
binary translation 16, 18
Brute-Force-Angriff 50

C

Cloud-Computing 63
Container 23

D

Datenaufkommen 39
Desktop-Virtualisierung 18

E

Emulation 19

F

Fehlkonfiguration 6, 33, 41
Firewall 33, 42, 43

H

Host 6, 7, 9, 10, 16, 18, 19, 20, 21, 23, 24, 26, 28, 32, 33, 35, 36, 37, 41, 42, 45, 47, 49, 57, 58, 59
Hot-Swapping 63
Hybridkernel 13
Hypercalls 16, 22
Hypervisor 33, 36

I

Image 6, 47, 48, 52
IPSec 44
ISO/OSI-Modell 43
Isolation 33
IT-Sicherheitsrisiken 31

J

Jails 23

K

Kernel 6, 10, 11, 12, 13, 14, 15, 16, 21, 22, 23, 25
Kernel-Based Virtual Machine
  KVM 25

L

Lizenzkosten 21, 25, 29, 30, 39, 61

M

Managementtool 29
Microsoft 8, 21, 30, 36, 54, 59, 61, 62
Mikrokernel 12
Monolithischer Kernel 11

N

Nutzer-Account 41

P

Paravirtualisierung 6, 16, 20, 21, 22, 65
Passwörter 50, 51
Passwortsicherheit 6, 34
Prozessorsockel 39

Q

Qick Emulation
  QEMU 24

R

Raid 7, 57, 63
Redundanz 46
Ressourcen 5, 9, 10, 14, 15, 16, 17, 18, 19, 21, 23, 26, 28, 29, 40, 45, 46, 47
Ressourcenengpässe 31
Ring 0 15
Risiken 5, 6, 32, 33, 34, 35, 37, 48
root-mode 22

S

SAN 50
Serverkonsolidierung 26, 58
shared Folders 34
Snapshot 7, 27, 39, 48, 49, 61
Stromverbrauch 59
Systemcalls 16
Systemupdates 37

T

Trojaner 43
Typ-1 Hypervisor 17
Typ-2 Hypervisor 18

U

unabhängiger Spannungsversorgung
  USV 26

Unzureichender Support 6, 37
User-Mode-Applikationen 14
USV 26, 27, 30, 35, 46, 58

V

vCenter Converter 52
VirtIO 25
Virtual Machine Monitor
  VMM 9, 18
Virtual Private Network 43
VirtualBox 18, 19, 54
virtuelle Maschine
  VM 6, 9, 15, 27, 28, 33, 40, 48, 52, 53, 54, 56
VLAN 40, 41, 58, 60
VMware 17, 18, 19, 26, 30, 36, 48, 52, 53, 54, 55, 56, 57, 59, 61, 62
Vollvirtualisierung 19
VPN 43, 44
VPN-Gateway 43, 44
VT-x 25

W

Wartung 26, 28, 29, 30, 37, 41, 45, 58
Windows Virtual PC 24

X

x86-Architektur 13, 14
x86-Plattform 24

Z

Zugriffsdokumentation 42

8. Abbildungsverzeichnis

Abbildung 1: Der gängige Computer 8
Abbildung 2: Monolithischer Kernel 11
Abbildung 3: Microkernel 12
Abbildung 4: Hybridkernel 13
Abbildung 5: Ring-Schema bei Prozessoren 15
Abbildung 6: Prozessausführung auf nicht virtualisiertem Computer 15
Abbildung 7: Virtualisierung mit binary translation 16
Abbildung 8: Bare-Metal-Lösung mit Hypervisor direkt auf der Hardware 17
Abbildung 9: Hosted-Lösung auf dem Betriebssystem 18
Abbildung 10: Vollvirtualisierung mit virtuellen Netzwerkkarten 19
Abbildung 11: Paravirtualisierung 20
Abbildung 12: Paravirtualisierung mit Hardwareunterstützung 22
Abbildung 13: Beispielhafte Betriebssystemvirtualisierung 23
Abbildung 14: Virtual Private Network 44
Abbildung 15: VMware vCenter Console 53
Abbildung 16: VMware vCenter Quell-System 54
Abbildung 17: VMware vCenter Ziel-System 55
Abbildung 18: VMware vCenter VM-Optionen 56
Abbildung 19: Alte Infrastruktur 57
Abbildung 20: Virtualisierte Infrastruktur 58
Abbildung 21: Raid 1 für redundante Datenspeicherung auf zwei Festplatten 63