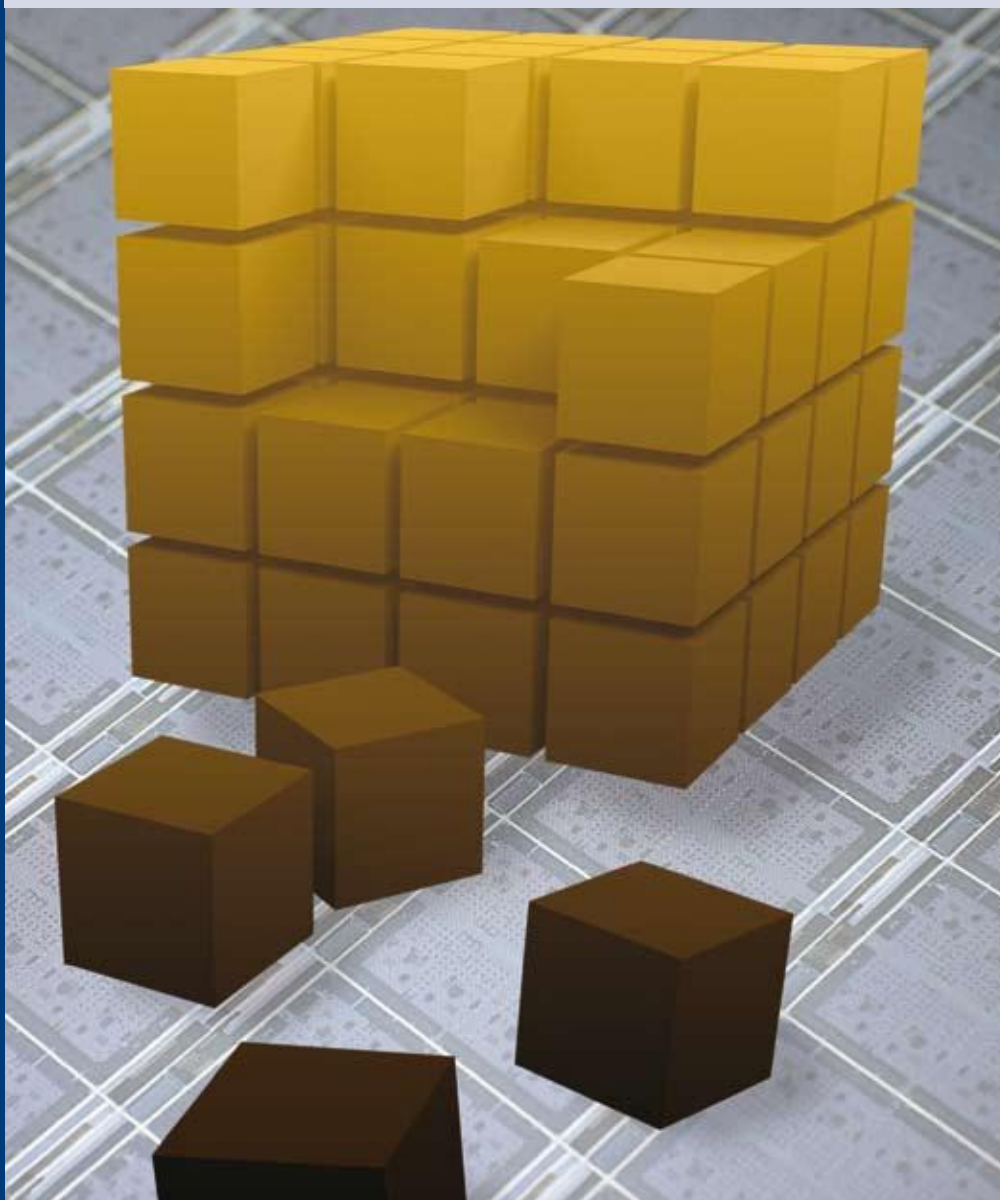


COMPUTER UND ARBEIT

4
2011



Vernetztes Wissen für Betriebs- und Personalräte



Überwachungsdruck

Bei permanenter Videoüberwachung können Beschäftigte jetzt eine Entschädigung von ihrem Arbeitgeber verlangen **Seite 12**

Privates Surfen

Der Abschluss einer Betriebs-/Dienstvereinbarung über die private Nutzung von Internet und E-Mail nutzt beiden Seiten..... **Seite 14**

Beschäftigtendaten

Bei Einführung von Cloud Computing besteht zu Datenschutz und Mitbestimmung ein hoher Verhandlungs- und Regelungsbedarf **Seite 32**

Schwerpunkt: Virtualisierung erkennen, bewerten und regeln

In Zusammenarbeit mit:

- Arbeitsrecht im Betrieb
- Der Personalrat

Virtualisierung in der Arbeitswelt sicher im Griff

Anja Stass und Mattias Ruchhöft // BTQ Kassel

HIER LESEN SIE:

- einen Überblick über die verschiedenen Virtualisierungsvarianten und deren Vor- und Nachteile
- wie Belegschaftsvertretungen die Virtualisierungstendenzen in Unternehmen bewerten können
- die wesentlichen Regelungspunkte für eine Betriebsvereinbarung zur Desktop-Virtualisierung



Virtualisierung ist momentan ein beherrschendes Thema in der IT-Welt. Stichworte wie Desktop-, Anwendungs- oder Server-Virtualisierung tauchen mittlerweile regelmäßig auf. Dieser Schwerpunkt gibt einen Überblick über technische Entwicklungen, Vor- und Nachteile sowie Bewertungsansätze für Interessenvertretungen. Bereits die CuA-Ausgabe 3/2010 hat die Desktop-Virtualisierung aufgegriffen. Vorliegend nähern sich die Autoren dem Thema Virtualisierung globaler und beschreiben kurz Ansätze sowie Varianten der Virtualisierung und streifen das durch diese Technik ermöglichte Cloud Computing. Der Fokus liegt neben der Klärung häufiger Begrifflichkeiten im Zusammenhang mit der Virtualisierung auf der Einschätzung von unternehmerischen Chancen und Risiken. Arbeitnehmervertretungen werden Fragestellungen und Überlegungen an die Hand gegeben, wie sie Virtualisierungstendenzen im Unternehmen bewerten können. Sie münden im Vorschlag einer Muster-Betriebsvereinbarung zum Thema Desktop-Virtualisierung.

Am Anfang steht bei diesem Thema immer noch die entscheidende Frage: Was ist eigentlich Virtualisierung?

Eine einheitliche Definition der Virtualisierung fällt angesichts der vielen Anwendungsmöglichkeiten allerdings schwer. Als virtuell wird ein softwaretechnisch nachgebildeter Rechner bezeichnet, der – in abgeschotteter Umgebung – auf einer realen Maschine (einem Rechner mit ► CPU, Speicher usw.) läuft.

Unter Virtualisierung versteht man die Aufteilung der Ressourcen eines Rechner-

systems, die von mehreren Betriebssystemen genutzt werden können. Diese verhält sich wie ein vollwertiger Computer, auf der ein Betriebssystem mit Applikationen, genau wie auf einem realen Computer, installiert werden kann.¹ Somit koppelt die Virtualisierung Betriebssysteme und Applikationen von der Hardware ab und eröffnet viele Anwendungsmöglichkeiten.

Zwei Anwendungsbeispiele sollen an dieser Stelle genannt werden:

Durch die Virtualisierung – also Anwendungen getrennt von den Anforderungen

der physischen Maschine laufen zu lassen – ergibt sich die Möglichkeit, ältere Varianten einer Software (gerade eine Eigenentwicklung oder Spezialsoftware) auf modernen Betriebssystemen (z.B. Windows 7) zu verwenden.

Weiteres Beispiel ist eine Variante zur Einbindung von mobilen Fremdgeräten (z.B. dem Tablet-Computer iPad des amerikanischen Herstellers Apple) in Firmennetzwerke, wo ein virtueller Desktop auf dem mobilen Endgerät und eine Arbeitsumgebung erzeugt wird.

Software, die auf virtuellen Maschinen läuft, verhält sich nicht anders, als würde sie auf realen Rechnern laufen. Die Anforderungen der Anwendung werden von der Virtualisierungssoftware abgefangen und umgesetzt.

Neu sind diese Ansätze nicht. Bereits bei den Röhren-Großrechnern in den 1950er Jahren wurden Ansätze zur Aufteilung der CPU-Zeit entwickelt und die Eingabe von der eigentlichen Rechnerleistung mit Hilfe von Lochkarten abgekoppelt.² Auf sogenannten Mainframes – Großrechnern, die aufgrund ihrer redundanten Bauart, äußerst robust und für Störungen kaum anfällig sowie auf einen hohen Datendurchsatz ausgelegt sind – ist die Virtualisierung ein seit Jahrzehnten etablierter Standard.

Ansätze der Virtualisierung

Das Thema ist somit nicht neu, hat aber in der breiteren IT-Öffentlichkeit größeren Raum eingenommen, seitdem die Klasse der x86-basierten Server Erweiterungen und Fortschritte hinsichtlich der Virtualisierung erfahren hat.

Wir beschreiben im Folgenden einige Ansätze der Virtualisierung (die sich in realen Anwendungen allerdings überschneiden können):

Emulation

Bei der Emulation handelt es sich um eine Software, die ein Modell eines Computersystems auf Hardware anderen Typs implementiert. Ein relativ bekanntes Beispiel aus dem Consumerbereich ist „Parallels“, das Windows-Applikationen auf einem Apple-Rechner laufen lässt.

Hardwaregestützte Virtualisierung

In diesem Fall handelt es sich um eine Emulation mit gleicher CPU-Architektur (z. B. Linux), die die Devices und die Bootumgebung virtualisiert. Das bringt einige Einschränkungen gegenüber der reinen Emulation mit sich, führt jedoch zu verbesserter Leistung, da nicht mehr verschiedene Prozessoren emuliert werden müssen. Der hardwaregestützten Virtualisierung gehört nach Einschätzung von Fachleuten in weiten Teilen die Zukunft.

Paravirtualisierung

Bei der Paravirtualisierung wird eine Softwareschicht zwischen Hardware des Hosts und den Gast-Systemen geschoben, die die Hardware-Ressourcen über spezielle Schnittstellen den Gast-Systemen verfügbar machen.

Resource Container

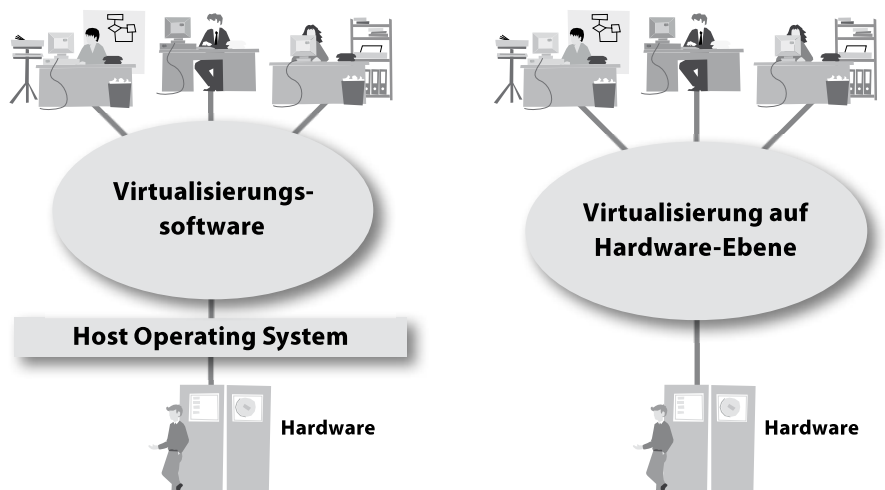
Eine weitere Möglichkeit, virtualisierte Systeme aufzusetzen, sind Resource Container, die auf einem laufenden Betriebssystemkernel – also dem Kern des Betriebssystems – mehrere Container parallel erzeugen. Inhalt dieser Container sind laufende Prozesse, das Dateisystem mit installierter Software und der Platz für eigene Dateien,

sehr flexibel einsetzbar und Resource Container zwar eingeschränkt flexibel, jedoch mit einer hohen Leistungsfähigkeit ausgestattet. Somit hängt letztlich die Wahl der Technologie der Virtualisierung vom Anwendungsfall ab.

Viele Anbieter im Virtualisierungsmarkt (beispielsweise VMware, Citrix, Microsoft) setzen auf eine hardwaregestützte Virtualisierung. Damit können sie sich als Plattform anbieten, die getrennt von Gast-Systemen gemanaged wird.

An dieser Stelle ist noch der Hypervisor oder Virtual Machine Monitor als Variante der Virtualisierungssoftware zu nennen (siehe Abbildung). Diese Software schafft eine Umgebung für virtuelle Maschinen.

Zwei Arten der Virtualisierung



Es werden zwei Arten von Hypervisoren unterschieden: der eine (als Typ 1 bezeichnet) setzt als Software direkt auf der Hardware auf, der andere (Typ 2) setzt auf einem vollwertigen Betriebssystem der physischen Maschine auf...

auf die dann Anwendungen Zugriff auf ihr jeweiliges Dateisystem haben.

Anwendungsvirtualisierung

Eine weitere relativ neue Variante ist die Anwendungsvirtualisierung. Diese trennt einzelne Anwendungen durch eine Virtualisierungsschicht vom Hardwaresystem. Damit wird für die jeweilige Anwendung eine passende Umgebung zur Verfügung gestellt, die in der Hostumgebung nicht zur Verfügung steht.

Betrachtet man die verschiedenen Konzepte der Virtualisierung hinsichtlich Leistung und Flexibilität, so ist die Emulation

Varianten der Virtualisierung

Wir betrachten daher zur Vorbereitung einer Einschätzung von Chancen und Risiken der Virtualisierung verschiedene Anwendungsvarianten:

Desktop-Virtualisierung

Da dieses Thema ausführlich in der Ausgabe 3/2010 dieser Zeitschrift behandelt wurde, genügt an dieser Stelle eine kürzere Zusammenfassung.³ Desktop-Virtualisierung ist die virtuelle Verwaltung des Arbeitsplatzes für den Anwender auf einem physischen

Server, wobei hier auch mehrere Desktop-Systeme betrieben werden können. Vorteile sind die zentrale und daher einfachere Verwaltung sowie die Reduzierung des Aufwands bei den Arbeitsplatzsystemen, da nur noch ein reduziertes PC-System (so genannter Thin Client) gebraucht wird.

Betriebssystem-Virtualisierung

Bei der Betriebssystem-Virtualisierung wird den Anwendungen ein in sich geschlossener Container als Laufzeitumgebung zur Verfügung gestellt. Nach außen treten diese Container wie gewöhnliche eigenständige Systeme auf. Es wird kein zusätzliches Betriebssystem gestartet. Die in dieser Umgebung laufenden IT-Anwendungen haben daher nur Zugriff auf die Prozesse und Daten ihrer Umgebung, obwohl alle Anwendungen auf einer physischen Maschine laufen.

Vorteile bietet die gute Integration, da nur ein Betriebssystem genutzt wird und damit auch eine gute Performance. Nachteil ist die geringe Flexibilität.

Server-Virtualisierung

Die Virtualisierung von Servern ermöglicht die Zuteilung von Rechenleistung für verschiedene Applikationen unter verschiedenen Betriebssystemen. Es können mit Hilfe

KLEINER EXKURS: CLOUD COMPUTING

Die unterschiedlichen Virtualisierungsvarianten können nicht losgelöst vom Thema „Cloud Computing“ betrachtet werden. Dabei steht Cloud Computing im Zusammenhang mit der Bereitstellung von Infrastruktur. Eine mögliche Definition lautet, dass Cloud Computing Virtualisierung und moderne Web-Services nutzt, um Ressourcen verschiedener Art als elektronisch verfügbare Dienste dynamisch bereitzustellen.¹

Der Begriff Wolke (Cloud) ist im Zusammenhang mit IT etwas unglücklich gewählt, da der Eindruck erweckt wird, es handele sich um eine ungeordnete Struktur von IT-Angeboten. Folgende „Wolken“-Arten werden unter anderem unterschieden:

- Software as a Service (z. B. Microsoft Office als webbasierter Service)
- Platform as a Service (z. B. Google App Service)
- Infrastrukture as a Service/IT as a Service (z. B. Amazon EC 2)

Sogenannte „Public Clouds“ beschreiben IT-Services über einen externen Anbieter, wohingegen „Private Clouds“ den Aufbau und Betrieb webbasierter Dienste im eigenen Unternehmen bezeichnen.

Fußnote

¹ siehe: Sinn, Cloud Computing – ein „Wetterbericht“, in: CuA 12/2010, 5 ff.

der Virtualisierungssoftware viele einzelne virtuelle Server gebildet werden. Somit ist es möglich, sich als Unternehmen ganze Server-Landschaften extern virtuell anlegen zu lassen oder Serverleistung als Service einzukaufen.

Unter Server-Virtualisierung versteht man das Betreiben einer oder mehrerer Betriebssysteme auf einem einzigen Rechner, die jeweils als virtuelle Maschine bezeichnet werden. Diese Maschine verhält sich genauso wie ein Betriebssystem, das direkt

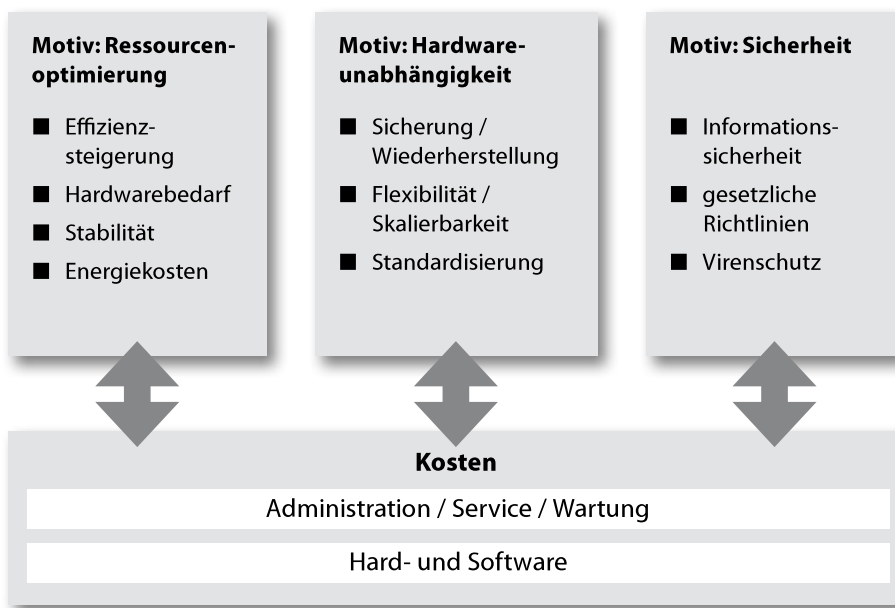
auf der Hardware läuft. Diese Hardware wird als Virtualisierungsserver bezeichnet. Mehrere solcher Server können zu einem virtuellen Rechenzentrum zusammengefasst werden. In einem solchen Rechenzentrum können die Virtualisierungsserver selbst und die auf ihnen betriebenen virtuellen IT-Systeme gemeinsam verwaltet werden.

Eine Möglichkeit der Server-Virtualisierung ist das sogenannte Partitionierungsverfahren, das innerhalb eines Betriebssystems mehrere virtuelle Kontexte einrichtet, die gegeneinander getrennt sind. Diese Lösung funktioniert dann gut, wenn das selbe Betriebssystem in vielen Instanzen benötigt wird.

Für die Virtualisierung von Servern werden im Folgenden zwei weitere Möglichkeiten erläutert: Einmal gibt es die Möglichkeit (in Anlehnung an die Virtualisierung von Desktops) die virtuellen Server auf das Betriebssystem „aufzusetzen“, zum zweiten die Server an sich komplett zu virtualisieren und diese gegebenenfalls in einer Cloud zu hosten.

Bei der ersten Variante erzeugt man auf einem physischen Server mehrere virtualisierte Server, was die Wartung der Komponenten und Anwendungen erleichtert. Dies wird durch eine strikte Trennung der unterschiedlichen Systeme durch Abstraktion der verschiedenen Systemressourcen (Prozessor, Speicher, Netzwerkressourcen) ermöglicht.

Motive für den Einsatz von Virtualisierungs-Lösungen



Quelle: Tim van Wasen, Virtualisierung von Desktops vs. Terminalserver

Die hier in ihren Wechselwirkungen dargestellten Virtualisierungsmotive werden im Kasten auf Seite 8 näher erläutert ...

DIE EINZELNEN VIRTUALISIERUNGSMOTIVE IM ÜBERBLICK

Stichwort: Ressourcenoptimierung

Virtualisierung ermöglicht die Erleichterung des Managements einzelner PCs vor Ort. Die Implementierung neuer Desktops und das Aufspielen neuer ► Patches sollen durch die virtualisierten Anwendungen und Hardware erleichtert werden.

Weitere Motive für eine Virtualisierungsstrategie sind die bessere Ausnutzung vorhandener Hardware. Da die Zahl physischer Server minimiert werden kann, vereinfacht sich die Administration.

Stichwort: Hardwareunabhängigkeit

Die Anwender an ihren PCs erhalten die Option, mehrere Betriebssysteme auf ihren Rechnern laufen zu lassen. Außerdem können sie von jedem Rechner innerhalb des Firmennetzwerks ihr persönliches Image aufrufen, das auf einem zentralen Server gespeichert ist. In diesem Modell ist ein Arbeiten im Offline-Modus allerdings nicht möglich.

Durch virtualisierte Lösungen können neue Infrastrukturen einfacher bereitgestellt werden. Die gesamte virtuelle Anwendungsumgebung kann in einer Datei zusammengefasst werden. Dadurch können solche Umgebungen ohne größeren Aufwand vervielfältigt werden.

Das ermöglicht eine erhöhte Flexibilisierung und die Bereitstellung genau der Umgebung, die der jeweilige Nutzer benötigt. Auch bestimmte Zustandsmomente einer virtuellen Maschine können zu späteren Zeitpunkten wiederhergestellt werden – das minimiert das Risiko von Anwendungsfehlern.

Mit den Ansätzen der Virtualisierung können nun neben Anwendungen auch IT-Infrastrukturen (Server, Netzwerke, Software) in entsprechend der Nachfrage anpassbaren Mengen jedem Unternehmen verfügbar gemacht werden.

Stichwort: Gesteigerte Sicherheit

An dieser Stelle betrachten wir den Sicherheitsgedanken als Motiv zum Einsatz der Virtualisierung. Die komplette Kapselung virtuell betriebener Anwendungen ist dabei einer der wichtigsten Argumente für eine Virtualisierungslösung.

Da beim Betrieb von virtuellen Desktops lokal keine Daten mehr vorgehalten werden müssen, reduziert sich das Risiko von Datenverlusten. Überhaupt wird die zentrale Verwaltung von IT-Systemen als Argument für eine gesteigerte Sicherheit herangezogen, da Anti-Virenprogramme, Patches oder Updates direkt aufgespielt und allen Nutzern zur Verfügung gestellt werden können.

Immer wieder auftretende Diskussionen in der Fachöffentlichkeit zu Sicherheitsbedenken im Zusammenhang mit der Virtualisierung greifen wir weiter unten in einem eigenen Punkt auf.

Stichwort: Kosten

Die Zusammenfassung mehrerer virtueller Betriebssysteme auf einem physischen Server reduziert sowohl Anschaffungs- als auch Energiekosten. Die Betriebskosten lassen sich beispielsweise reduzieren, weil den Anwendern ihre Arbeitsplätze als virtuelle Desktops zur Verfügung gestellt werden können, wodurch statt kompletter PCs geringer ausgestattete sogenannte Thin Clients – also Rechner ohne Laufwerke und andere bewegliche Teile – zum Einsatz kommen.

Durch die Server-Virtualisierung können Rechnerzentren effizienter eingerichtet werden, da mehrere Anwendungen virtuell auf einem Server laufen. Diese Effizienzsteigerungen machen sich im Stromverbrauch deutlich bemerkbar, wenn beispielsweise viele Server in einer sogenannten Serverfarm betrieben werden.

Die andere Möglichkeit ist, ganze Infrastrukturen zu virtualisieren und dann in einer sogenannten Cloud (siehe Kasten auf Seite 7) bereitzustellen und sie zentral zu managen. Dieser Service wird auch unter dem Begriff „IT as a Service“ (ITaaS) angeboten. Dieser Service kann sehr flexibel auf sich ändernde Anforderungen angepasst werden. Zudem ist die Verwaltung solcher gleichartiger Rechenzentren einfacher.

Risiken der Virtualisierung

Die Komplexität virtueller IT-Architektur nimmt aus Sicht des Systemmanagements zu. Das liegt an der Erhöhung der Zahl virtueller Maschinen, die mit nur einem Mausklick initialisiert ist. Diese virtuellen Maschinen müssen jedoch ähnlich physischen Systemen verwaltet, gewartet und gepflegt werden. Einen Nachteil kann auch eine uneinheitliche Plattformlandschaft aus Systemen, Komponenten und Treibern darstellen, da sie einer einfachen Installation, Wartung und Pflege im Wege steht.

Ein weiterer Aspekt virtueller Server ist der Schutz gegen Systemausfälle. Denn je mehr virtuelle Server auf einer physischen Maschine implementiert sind, desto höher ist der Schaden, wenn die reale Maschine ausfällt. Stichwort zur Sicherung vor diesem Risiko ist die Hochverfügbarkeit der Hardware.

Dazu werden in der Fachliteratur zwei Lösungsoptionen erläutert: Hochverfügbarkeit über eine Hardwarelösung durch einen fehlertoleranten Server, der komplett redundant aufgebaut ist. Die Softwarelösung der Hochverfügbarkeit ist nicht so aufwendig, da sie auf x86-Standard-Servern aufsetzt. Zwei dieser Standardserver werden über die Software zu einer Einheit verbunden. Gerade für kleinere und mittlere Unternehmen bietet sich die Softwarelösung an.

Sicherheit

In Fachkreisen wird immer wieder über Sicherheitsbedenken zu virtuellen Umgebungen berichtet bzw. diskutiert. Wenn viele unterschiedliche Server eines Unternehmens virtuell auf einem physischen Server laufen, kommt der Verfügbarkeit

dieses physischen Servers eine große Bedeutung zu. Daher müssen diese wenigen physischen Server entsprechend gegen Abstürze und Angriffe abgesichert werden.

In einem Artikel der Fachzeitschrift CIO wird über eine Studie zum Thema Sicherheit bei Virtualisierungsprojekten berichtet.⁴ Die Hauptgefahren sind demnach die unkontrollierte Datenverbreitung (Data Sprawl) und weitreichende Hypervisor-Privilegien.

Dagegen hilft die sogenannte Data Loss Prevention (DLP), der technische Schutz unerwünschter Datenabflüsse und einer unkontrollierten Datenverarbeitung. Dies ist gerade bei vielen virtuellen Systemen auf einer physischen Maschine wichtig.

Eine weitere Gefahr sind zu weitreichende Privilegien und Zugriffsrechte des Hypervisors. Dadurch kann es zu Fehlern oder Missbrauch durch berechtigte Nutzer des Hypervisors kommen. Der Hypervisor führt eine weitere Schicht zum Betrieb der Virtualisierungsumgebung ein, die eine Angriffsfläche bietet.

Der Schutz gegen diese Angriffsmöglichkeiten bzw. Lücken hängt laut der Umfrage häufig von manuellen Prozessen ab, die durch keine Technik unterstützt wird. Das kann zu einer Beeinträchtigung der Unternehmenssicherheit führen. Zudem müssen die unterschiedlichen Sicherheitsaufgaben klar getrennt werden, denn die dazu nötigen Privilegien sollten auf viele unterschiedliche User verteilt werden.

Dramatisch wird ein Angriff dann, wenn die Virtualisierungssoftware selbst aus einem der Gast-Systeme heraus angegriffen wird. Damit kann es schlimmsten Fall zu einem Schadsoftware-Befall aller anderen Gäste des gleichen Hosts führen. Sicherheitstechnisch sehr relevant ist daher die Trennung der virtuellen Maschinen auf dem gemeinsamen Host, sprich der virtuellen Anwendungen auf der physischen Maschine.

Datenschutz

„53 Prozent der Befragten gehen beim Einsatz von Virtualisierung von einer erhöhten Anfälligkeit aus, die durch gestiegene Komplexität verursacht wird“, so eine aktuelle Studie.⁵ Die Kontrolle der aufgespielten und entstehenden Daten liegt damit

auf der Hand. Aber nicht nur Anlage und Betrieb einer virtualisierten Umgebung sind sicherheitstechnisch relevant, sondern auch die Abschaltung und die sichere Ablage bzw. Löschung der Daten auf den dann abzuschaltenden Systemen.⁶ Daher sollte schon bei der Planung der gesamte Lebenszyklus der Virtualisierungslösung betrachtet werden. Das heißt von der Spezifizierung bis zur Abschaltung und der Sicherung der Daten.

„Insbesondere Befürchtungen aus der Belegschaft, dass sie nun durch virtuell hinterlegte Systeme und durch eine zentrale Datenerhaltung komplett gläsern sind, gilt es ernst zu nehmen.“

Zudem muss in einem stärkeren Maß als bei der Einführung physischer Systeme bei virtualisierten Umgebungen auf die Daten der Applikation, Applikationsnutzer, privilegierte Benutzerdaten sowie Nutzerverhaltensdaten geachtet werden. Gerade die Dynamik einer virtuellen Umgebung durch eine vereinfachte Einrichtung, Duplizierung und Veränderbarkeit der virtuellen Anwendungen und Systeme gebietet den Einsatz von Informationssicherheitssystemen und prozessualen Festlegungen in der IT-Organisation.

Einsatzszenarien für eine Virtualisierungslösung

Betrachten wir nun noch einige Einsatzszenarien für virtuelle Lösungen zum besseren Verständnis, wie die mittlerweile erweiterten Möglichkeiten der Virtualisierung genutzt werden können:

IT-Schulungslösungen

Vorteile bieten sich durch eine schnellere Bereitstellung der Systeme für die Schulung; darüber hinaus ist keine Neuinstallation physischer Rechner nötig. Zudem können virtuell mehrere Schulungssysteme z.B. für unterschiedliche Anwendungen usw. parallel erzeugt werden.

Anwendungsintegration

Hierbei können vorhandene Anwendungen in virtuellen Umgebungen betrieben werden, die möglicherweise nicht für alle Plattformen oder Betriebssysteme verfü-

bar sind. Das ist angesichts eventuell hoher Lizenzierungskosten bei einem Upgrade des Betriebssystems (z.B. auf Windows 7) von Bedeutung.

Softwareentwicklung und -test

Im Bereich der Softwareentwicklung bietet der Betrieb von virtuellen Umgebungen für verschiedene Szenarien Vorteile. Es ist möglich, in einer einfach einzurichtenden, getrennten und gesicherten Umgebung,

gezielt Fehlverhalten zu testen. Einheitliche Testumgebungen können bereitgestellt werden.

Systemkonsolidierung

Damit ist die Zusammenfassung vorhandener Systeme in eine virtuelle Systemumgebung gemeint. Vorteile ergeben sich schon aus der möglichen Reduzierung physisch vorhandener Serverstrukturen.⁷

Bewertungsmöglichkeiten der Belegschaftsvertretung

Was ist von der Virtualisierung von Betriebssystemen, Anwendungen oder Servern aus Sicht von Arbeitnehmervertretungen zu halten? Was ist der zentrale Unterschied bei der Bewertung von Virtualisierungslösungen im Unterschied zu physischen Systemen?

Durch die Virtualisierung ändert sich grundsätzlich die Flexibilität und Anpassbarkeit von IT-Ressourcen. Als Folge daraus sollten bei der Bewertung und Begleitung solcher Projekte durch die Mitarbeitervertretung nicht nur die Funktionen, Datenflüsse, Schnittstellen sowie Berechtigungen betrachtet werden. Vielmehr gilt es bei Virtualisierungsprojekten auch die Einrichtung, den Betrieb, die IT-Ressourcen-Umgebung und das Abschalten solcher Lösungen zu betrachten und gegebenenfalls zu regeln.

Insbesondere Befürchtungen aus der Belegschaft, dass sie nun durch virtuell hinterlegte Systeme und durch eine zentrale

REGELUNGSPUNKTE EINER BETRIEBS-/DIENSTVEREINBARUNG ZUM THEMA DESKTOP-VIRTUALISIERUNG

<p><i>Gegenstand</i></p>	<ul style="list-style-type: none"> ■ Was ist der Regelungsgegenstand? <i>Regelungsgegenstand der Betriebsvereinbarung ist Einführung, Anwendung und Weiterentwicklung der zum Einsatz kommenden Desktop-Virtualisierungslösung, deren Aufbau in der Systembeschreibung geregelt wird.</i> ■ Was soll der Einsatz bewirken? <i>Der Einsatz soll z. B. die virtuelle Verwaltung des Arbeitsplatzes für den Anwender auf einem physischen Server bewirken.</i> 	<p><i>Qualifizierung/Schulung</i></p>	<ul style="list-style-type: none"> ■ In welchem Umfang bedarf es der Qualifizierung/Schulung der Anwender?
<p><i>Ziel und Zweck</i></p>	<ul style="list-style-type: none"> ■ Was ist Ziel und Zweck der Vereinbarung? <i>Ziel und Zweck kann z. B. der Umgang mit der geplanten Virtualisierungslösung sowie deren Weiterentwicklung und der Schutz vor Leistungs- und Verhaltenskontrolle sein.</i> 	<p><i>Schutz vor Leistungs- und Verhaltenskontrolle</i></p>	<ul style="list-style-type: none"> ■ Welche personenbezogenen/-beziehbaren Auswertungen dürfen erstellt werden? <i>Für die Gewährleistung der Sicherheit des Systems und zur Fehleranalyse ist es zumeist notwendig, dass hierzu berechtigte Administratoren Einblick in bestimmte technische Daten nehmen können, die bei einer Anwendersitzung entstehen. Dies bedarf der konkreten Regelung.</i>
<p><i>Systembeschreibung</i></p>	<ul style="list-style-type: none"> ■ Welche Virtualisierungslösung kommt zum Einsatz? ■ Wie ist diese aufgebaut? ■ Wie erfolgt der Zugriff vom Arbeitsplatz-PC auf die Server (z. B. Thin-Client oder Web-Anwendung)? ■ Welche Programme werden mit Hilfe der Virtualisierungslösung dem Anwender zur Verfügung gestellt? ■ Wo befindet sich das Serversystem örtlich und wer betreibt es? 	<p><i>Zu widerhandlungen</i></p>	<ul style="list-style-type: none"> ■ Was soll bei Zu widerhandlungen gegen die vereinbarten Regelungen erfolgen? <i>Hier können Verhinderungsmöglichkeiten und gegebenenfalls das Abschalten der Lösung geregelt werden.</i>
<p><i>Reports und Auswertungsmöglichkeiten</i></p>	<ul style="list-style-type: none"> ■ Welche Auswertungsmöglichkeiten stellt die zum Einsatz kommende Lösung zur Verfügung? ■ Welche Auswertungen dürfen vorgenommen werden und zu welchem Zweck dürfen diese erstellt werden (z. B. Fehleranalyse)? 	<p><i>Datenhaltung, Datenschutz und Datensicherheit</i></p>	<ul style="list-style-type: none"> ■ Wo liegen die Daten – außerhalb des Unternehmens oder sogar im Ausland? ■ Wie ist das Datenschutzkonzept im Zusammenhang mit der zum Einsatz kommenden Virtualisierungslösung aufgebaut? ■ Wie ist die Übertragung der Daten vom Desktop zum Serversystem abgesichert? ■ Wie ist das Datenschutzkonzept bei einem externen Provider aufgebaut? ■ Wer/welche Personengruppe übernimmt bei einem externen Provider die Administration? ■ Ist dieser Personenkreis auf die Einhaltung der getroffenen Regelungen verpflichtet worden?
<p><i>Änderungen und Erweiterungen</i></p>	<ul style="list-style-type: none"> ■ Wann will die Interessenvertretung über Änderungen (z. B. neue Funktionen) informiert werden und in welcher Art und Weise soll hierüber die Information vom Arbeitgeber erfolgen, damit der Betriebs-/Personalrat anhand der Informationen entscheiden kann, ob die Änderung/Erweiterung seiner Mitbestimmung bedarf? 	<p><i>Berechtigungskonzept</i></p>	<ul style="list-style-type: none"> ■ Wer hat Zugriff auf das System und in welcher Ausprägung (Breite und Tiefe der Berechtigung)? ■ Wer/welche Personengruppen hat/haben Administratorenrechte? Handelt es sich hierbei um betriebsinterne Personen oder um einen externen Anbieter?
<p><i>Veränderung von Arbeitsabläufen und Rationalisierung</i></p>	<ul style="list-style-type: none"> ■ Verändern sich durch den Einsatz der Virtualisierungslösung die Geschäftsprozesse/Arbeitsabläufe? ■ Kann dies möglicherweise zu Kündigungen führen? ■ Besteht die Gefahr der Rationalisierung? <i>Hier ist an einen Ausschluss von Kündigungen aufgrund der Einführung und Nutzung der Virtualisierungslösung zu denken.</i> 	<p><i>Kontrollrechte der Belegschaftsvertretung</i></p>	<ul style="list-style-type: none"> ■ Wo kann bzw. sollte Kontrolle erfolgen? <i>Die Ausübung des Kontrollrechts ist auch bei Dritten (z. B. externen Dienstleistern) abzusichern.</i>
		<p><i>Schlussbestimmungen</i></p>	<p>Hier werden die klassischen Punkte geregelt, wie z. B. Inkrafttreten, Kündigungsfrist usw.</p>

Hinweis: Die aufgeführten Fragen und Anmerkungen sowie Hinweise dienen lediglich als Anregung für die Erstellung einer Betriebs-/Dienstvereinbarung zum Thema Desktop-Virtualisierung und bedürfen der Anpassung auf den konkreten Einzelfall. Wenden Sie sich bei entsprechenden Fragen gerne an die Autoren.

Datenhaltung komplett gläsern sind, gilt es ernst zu nehmen.

Angesichts der Datenskandale und Überwachungsvorfälle der jüngsten Zeit (beispielsweise bei der Telekom, beim AWD oder der Deutschen Bahn) sollten auch Projektverantwortliche und der Arbeitgeber diese Bedenken nicht unterschätzen. Gerade bei diesem Aspekt kommt der Interessenvertretung eine besondere Bedeutung zu.

Die gesteigerte Flexibilität hat eine Menge Anwendungsfelder eröffnet, die komplette extern abgewickelte IT-Komplettlösungen ermöglicht. Eine weitere zentrale Frage ist die Organisation und der

Datencontainer auf einem externen Server liegt.

Mitarbeitervertretungen sollten sich angesichts der Dynamik virtueller Lösungen sowohl im Desktop- als auch Anwendungsbereich überlegen, wie sie mit dem Arbeitgeber sinnvolle Rahmenvereinbarungen für Einrichtung, Betrieb und Sicherheit der virtuellen Lösungen vereinbaren. Dabei ist von Seiten der IT-Abteilung auf eine gewisse Planbarkeit und festgeschriebene Prozesse zu achten, da wie oben bereits beschrieben die Komplexität zunimmt.

Ein weiterer Schwerpunkt der Betrachtungen ist die Veränderung von Arbeits-

„... sollte darauf geachtet werden, die Datenhaltung einer extern gehosteten Virtualisierungslösung möglichst in Deutschland wegen des strengen Datenschutzrechts zu realisieren.“

Ort der eigentlichen Datenhaltung. Soll das Unternehmen die Daten aus dem Haus geben?

Und wenn die Serverlandschaft etwa über eine Cloud-Lösung und damit auch die Anwendungs- und Nutzerdaten außerhalb des eigenen Unternehmens liegen. Weitere Fragestellung ist dann, in welchem Land die Daten liegen und welches Datenschutzrecht angewendet wird. Um sich in dieser Frage zu schützen, sollte darauf geachtet werden, die Datenhaltung einer extern gehosteten Virtualisierungslösung möglichst in Deutschland wegen des strengen Datenschutzrechts zu realisieren.

Die folgenden Fragen sollen Ihnen eine Hilfe bei der Einschätzung entsprechender Virtualisierungsplanungen in Ihrem Unternehmen sein und drängen sich äquivalent zur Einführung neuer Softwaresysteme auf:

Welche Auswertungsmöglichkeiten der Nutzerdaten gibt es in der virtuellen Landschaft und wie können diese in einem Berechtigungssystem (beispielsweise durch Trennung der einzelnen Anwendungen oder Beschränkung des Zugriffs der Administratortools auf bestimmte Bereiche) eingeschränkt und kontrollierbar gemacht werden? Besonders interessant wird diese Frage, wenn beispielsweise das gesamte Desktop-System des Anwenders in einem

ablaufen in der IT durch die Virtualisierung oder den Einsatz von Cloud Computing. Welche Anforderungen werden zukünftig an die Mitarbeiter gestellt? Welcher Schulungsbedarf ergibt sich hieraus?

Zudem kann die Frage nach dem Wegfall von Arbeitsplätzen in der IT-Abteilung und weiterer mit IT-Services befasster Stellen durch eine Vergabe an externe Anbieter oder die Nutzung einer externen virtuellen Software-Lösung aufgeworfen werden.⁸

Autoren

Anja Stass und **Mattias Ruchhöft** arbeiten als Technologieberater bei der BTQ Kassel, die arbeitnehmerorientierte Beratung, Qualifizierung und Seminare rund um neue Techniken anbietet; BTQ Kassel, Angersbachstraße 2-4, 34127 Kassel, fon 0561 77 60 04, info@btq-kassel.de, www.btg-kassel.de

Weiterführendes

Folgende Literatur liegt neben der zitierten diesem Beitrag zugrunde:

IT-Administrator Sonderheft II/2009: Virtualisierung – Aufbau und Betrieb virtuelle IT-Infrastrukturen vom Rechenzentrum bis zum Client

Braun/Kunze/Nimis/Tai: Cloud Computing / Webbaasierte dynamische IT-Services, 2010

Christian Baun: Vorlesungsunterlagen der Universität Mannheim / Fakultät für Informatik, Institut für Robotik, 2008

Zudem wurden neben der CuA folgende Fachblätter genutzt:

Datakontext: IT-Sicherheit (www.datakontext.com)

IDG Business Media: CIO, Computerwoche, Tec Channel (www.idg.de)

Heise: c't Magazin, iX Magazin usw. (www.heise.de)

Lexikon:

CPU ► (englisch: central processing unit) Hauptprozessor als zentrale Rechen- und Steuereinheit eines Computers

Patch ► (englisch: Flicken) Korrekturauslieferung für Software oder Daten aus Endanwendersicht, um etwa Sicherheitslücken zu schließen, Fehler zu beheben oder bislang nicht vorhandene Funktionalitäten nachzurüsten (aus: Wikipedia)

x86 ► Abkürzung einer Prozessorarchitektur für Personal Computer

Fußnoten

- 1 Siehe hierzu anschaulich Meier, Virtualisierung – so funktioniert's im Detail, in: CuA 3/2010, 10 ff.
- 2 Tim van Wasen, Virtualisierung von Desktops versus Terminalserver, 2010
- 3 Sinn, Desktop-Virtualisierung, in: CuA 3/2010, 5 ff.
- 4 Gefährliche Virtualisierung – Unkontrollierte Datenverbreitung als Sicherheitsrisiko, CIO vom 27.12.2010, www.cio.de/dynamicit/management_strategie/2259229/index.html
- 5 IDC-Studie, IT Security – Trends und Anwenderpräferenzen, Juli 2010
- 6 Siehe zu diesem Themenkomplex auch den Schwerpunkt „Sicherheitskonzepte in Zeiten des Cloud Computing“, in: CuA 3/2011, 4 ff.
- 7 Fabian Thorns (Hrsg.), Das Virtualisierungs-Buch – Konzepte, Techniken und Lösungen, 2. Auflage, 2008
- 8 Sinn, Cloud Computing – dunkle Wolken über der IT-Abteilung, in: CuA 10/2009, 5 ff. (7)