Server-Virtualisierung

Teil 3: Sicherheit in virtuellen Umgebungen

Leitfaden

BITKOM

Impressum

Herausgeber: BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner: Holger Skurk
Tel: 030.27576-250
h.skurk@bitkom.org

Redaktion Version 3: Markus Beckhaus, Netlution GmbH
Frank Koch, Microsoft Deutschland GmbH
Holger Skurk, BITKOM e.V.
Peter Stedler, Netlution GmbH
Michael Walther, Netlution GmbH
Patrick Würl, CA Deutschland GmbH

Redaktionsassistenz: Biliana Schönberg

Stand: Oktober 2009, Revision 3

Gestaltung / Layout: Design Bureau kokliko / Anna Müller-Rosenberger (BITKOM)

Der Leitfaden (Version 3) basiert auf der BITKOM-Publikation „Virtualisierung - Überblick und Glossar“ (Redaktion: Frank Beckereit, Dr. Ralph Hintemann, Thomas Harrer, Knut Müller, Bernhard Moritz, Ingolf Wittmann und Dr. Robert Zwickenpflug) von Juli 2006, sowie dem “Leitfaden Server-Virtualisierung„ Version 2“ (Frank Beckereit, Gerd Elzenheimer, Albrecht Frei, Thomas Harrer, Frank Kohler, Nils Meyer, Frank Petersen, Dr. Dietrich Schaupp, Holger Skurk, Peter Stedler, Dr. Jens Timm, Michael Walther, Ralph Wölpert).

Server-Virtualisierung

Teil 3: Sicherheit in virtuellen Umgebungen

Leitfaden

BITKOM

Inhaltsverzeichnis

1 Einleitung

Viele Unternehmen haben in den letzten Jahren die Virtualisierung von IT-Anwendungen und IT-Infrastrukturen vorangetrieben und damit die Grundlage für eine bedarfsgerechte IT geschaffen. Die Server-Virtualisierung spielt dabei eine wichtige Rolle. BITKOM bietet seit 2006 ein Glossar zur Server-Virtualisierung an. Um der wachsenden Bedeutung dieser Technologie gerecht zuwerden, stellt der BITKOM-Arbeitskreis Server- und Betriebskonzepte hiermit einen aktualisierten und erweiterten vierteiligen Leitfaden zur Server-Virtualisierung vor. Die einzelnen Teile widmen sich den folgenden Themen:

Teil 1: Servervirtualisierung - Business Grundlagen

Dieses Dokument gibt Antworten auf die Fragen, welchen Nutzen die Einführung von Virtualisierung bringt und welche monetären Auswirkungen Virtualisierung haben kann. Dieser Teil richtet sich an Entscheider.

Teil 2: Servervirtualisierung - Technologie, Design, Deployment und Betrieb

Dieser Teil beschreibt ausführlich unterschiedliche Ansätze der Virtualisierung und setzt einen Schwerpunkt auf Konzepte für den Betrieb von virtualisierten Umgebungen.

Teil 3: Servervirtualisierung - Sicherheit in virtuellen Umgebungen

Das Dokument betrachtet ausführlich den Aspekt Sicherheit, der in virtualisierten Umgebungen eine besondere Rolle einnimmt.

Teil 4: Servervirtualisierung - Glossar

Das vierte Dokument stellt ein Glossar für konzeptionelle Begriffe der Servervirtualisierung und zu zahlreichen am Markt vorhandenen Technologien dar. Dieser Teil wird Anfang 2010 veröffentlicht werden

Die Teile 2, 3 und 4 richten sich an Verantwortliche für Design und Betrieb der IT.

Sonstige BITKOM-Aktivitäten zur Virtualisierung in der IT

Der BITKOM behandelt neben der Servervirtualisierung weitere Virtualisierungsthemen. Der Arbeitskreis Speichertechnologien befasst sich aktuell mit dem Thema Speichervirtualisierung. Im Arbeitskreis Thin Client & Server Based Computing entsteht ein Dokument zur Desktopvirtualisierung. Arbeitskreisübergreifend entsteht ein Übersichtsmodell der Virtualisierung.

2 Sicherheit in virtuellen Umgebungen

Die Entwicklung der Virtualisierung bietet Unternehmen die Möglichkeit, IT Ressourcen besser zu nutzen und damit osten zu sparen. Weiterhin kann die IT flexibler an die Bedürfnisse von Geschäftsprozessen angepasst werden. Mit der steigenden Bedeutung der Virtualisierung für die Geschäftsprozesse ist das Thema Sicherheitsmanagement immens wichtig geworden. Gleichzeitig wird durch die zusätzliche Technologie berechtigterweise auf zusätzliche Sicherheitsfragen hingewiesen, die es zu klären gilt. Die wichtigsten Aspekte zum Thema Sicherheit in virtuellen Umgebungen werden in diesem Leitfaden behandelt.

2.1 Grundlagen zum IT Sicherheitsrisikomanagement

Das Sicherheitsrisikomanagement ist ein detaillierter Prozess, der dazu dient, die Bedrohungen und Sicherheitslücken zu ermitteln, die die größten potenziellen Auswirkungen auf eine bestimmte Organisation haben. Da Unternehmen sehr unterschiedliche Ansprüche an ihre Geschäftsprozesse stellen, kann man keine universal gültige Liste von Sicherheitslücken angeben, die in jeder Umgebung die gleichen Auswirkungen haben. Sicherheit als Prozess zu betrachten, bietet aber den Security-Verantwortlichen die Möglichkeit, sehr schnell, flexibel und adäquat auf neue Bedrohungspotentiale oder Anforderungen zu reagieren.

Als Basis eines Sicherheitskonzepts dient die Sicherheitsrichtlinie, welche als „High Level Statement“ die Sicherheitsanforderungen definiert und die von dem Sicherheitsverantwortlichen (CSO oder CISO) als Grundlage seines Handelns angewandt werden muss. Diese Richtlinie definiert, welche organisatorischen, administrativen und technischen Maßnahmen implementiert werden müssen, um den gestellten Anforderungen gerecht zu werden. Grundlagen zum Thema Sicherheitskonzept finden Sie in den gängigen Sicherheitsstandards wie ISO 27000 oder BSI, sowie den gängigen IT Betriebsprozessmodellen wie ITIL.

Die Schutzmaßnahmen müssen den steigenden internen und externen (legislativen) Anforderungen hinsichtlich Compliance gerecht werden. D.h. sie müssen flexibel, dynamisch, anpassbar, wiederholbar und sicher sein, um diesem Anspruch gerecht zu werden. Solche Konzepte behalten auch für virtuelle Umgebungen ihre Gültigkeit, müssen jedoch an die zusätzlichen Anforderungen solcher Umgebungen entsprechend erweitert werden.

2.2 Standortbestimmung

Zum Erstellungszeitpunkt dieses Leitfadens (Stand Nov. 2009) ist Virtualisierung zwar eine etablierte, jedoch keinesfalls eine voll ausgebaute Technologie. Wie in vielen neuen IT Bereichen, steht der zusätzliche Nutzen und die Erhöhung der Produktivität zuerst (und mit Recht) im Fokus, andere Aspekte, insbesondere die Sicherheit, müssen sich nachgeordnet positionieren. Hier kann man eine gewisse Analogie zur Einführung des Internets in den Unternehmen Mitte/Ende der 90er Jahre sehen. Zu diesem Zeitpunkt galt es auch, vor allem die zusätzlichen Möglichkeiten zu nutzen. Sicherheitsmechanismen, wie z.B. Firewalls waren damals zwar schon bekannt, fanden aber nur mit Verzögerung Ihren festen Platz in den Infrastrukturen

Eine ähnliche Situation gilt es heute zu meistern. Server-Virtualisierung hat Ihren festen Platz in den Unternehmen, andere Virtualisierungstechniken (Desktop- und Anwendungsvirtualisierung) folgen diesem Trend. Allerdings gibt noch keine gefestigten Erkenntnisse zu Fragen der Risiken sowie zu notwendigen und sinnvollen Sicherheitsmechanismen. Nicht zuletzt aus diesem Grund soll der vorliegende Leitfaden den aktuellen Stand wiedergeben und konkrete Hinweise zum Sicherheitsmanagement virtualisierter Umgebungen geben.

Wie bereits oben ausgeführt bleiben, die grundlegenden Prinzipien der IT-Sicherheit auch in einem virtualisierten Umfeld weitgehend unverändert.

2.3 Risikobetrachtung

Vielfach werden Aspekte der Sicherheit einseitig betrachtet, indem man sich auf bestimmte Bedrohungsszenarien konzentriert und andere aus dem Blickfeld verschwinden. Dies ist auch und vor allem in virtualisierten Umgebungen der Fall, so dass die Risikobewertung nicht ausgeglichen ist.

Aus diesem Grund lohnt ein kurzer Blick auf die klassischen Grundschutzbedürfnisse. Diese sind:

- Vertraulichkeit (Confidentiality)
- Integrität (Integrity)
- Verfügbarkeit (Availbility)

Die übliche Diskussion über IT-Sicherheitsrisiken geht intuitiv in Richtung der beiden erstgenannten Punkte, da die Gefahren überwiegend in einem direkten Angriff durch bestimmte Personen gesehen werden.

Solche Bedrohungen dürfen nicht verharmlost werden, jedoch muss auch festgestellt werden, dass die betriebliche Praxis ein anderes Bild abgibt. Tatsächlich besteht das höchste Risikopotenzial im Bereich der Verfügbarkeit. Dies hat vielfältige Ursachen.

Wenn wir diese Erkenntnis auf die Virtualisierung anwenden, so ergeben sich zum einen definitiv neue Risiken durch zusätzliche Komponenten und höhere Komplexität. Zum anderen jedoch kann die Virtualisierung einen erheblichen Beitrag zur Erhöhung der Verfügbarkeit und sogar insgesamt zu Produktivität der IT beitragen.

Das Ziel muss es demnach sein, die erstgenannten Sicherheitsrisiken durch sorgfältige Planung, Einführung und Betrieb zu beherrschen, um das Potenzial der Virtualisierung voll ausschöpfen zu können.

Zusammenfassend kann man feststellen, dass Virtualisierung die Chance bietet, das Sicherheitsniveau insgesamt zu erhöhen.

2.4 Virtualisierung als Abbild der bestehenden Umgebung

Wird eine bestehende Umgebung virtualisiert, ändert sich an den Sicherheitsanforderungen der virtualisierten Systeme in der Regel nichts.

Alle bestehenden Prozesse und Techniken können und sollten daher zunächst weiter im Einsatz verbleiben. Dies beinhaltet u.a.

- Prozesse und Techniken zur Verwaltung der Zugriffsrechte und Rollenkonzepte innerhalb der virtuellen Systeme
- Datensicherung und Redundanz innerhalb der virtuellen Systeme
- Patchmanagement der virtuellen Systeme
- Virenschutz und Anti-Malware Schutz der virtuellen Systeme
- Schutz gegen Angriffe aus dem Netzwerk

Für die jeweils verwendeten Gastsysteme finden sich hinreichend Literatur und Ratgeber bei den jeweiligen Herstellern oder im Internet. Daher wird hier lediglich noch einmal darauf hingewiesen, dass sich diese Anforderungen an die Sicherheit der Gastsysteme nicht durch den Einsatz von Virtualisierungstechniken gegenüber dem klassischen Betrieb verändern, sondern weiterhin bestehen bleiben.

Analog gilt dies auch für andere Sicherheitsanforderungen, z.B. das Backup oder redundante Systeme. Grundsätzlich kann ein Verfahren, welches in klassischen Umgebungen gut funktioniert hat, auch auf eine virtualisierte Umgebung übertragen werden. Obwohl es durchaus erstrebenswert ist, Funktionen in die virtuelle Umgebung auszulagern, z.B. auf das Hostsystem oder das Management der virtuellen Infrastruktur, ist dies nicht immer

möglich oder sinnvoll. So kann z.B. das alleinige Sichern von virtuellen Umgebungen aus dem Hostsystem heraus dazu führen, dass Dateninkonsistenz im Gastsystem auftritt. Ohne Redundanz im virtuellen System kann es zu Serviceausfällen kommen, sollte das virtuelle System z.B. gebootet werden müssen.

Gleichwohl soll bereits an dieser Stelle darauf hinweisen hingewiesen werden, dass die Virtualisierung hier neue Technologien anbietet und weiter entwickeln wird. Diese können die klassischen Schutzmechanismen und Verfahren ergänzen oder ersetzen. Eine Vertiefung solcher Konzepte finden Sie in den folgenden Kapiteln.

3 Zusätzliche Anforderungen durch die Verwendung von Virtualisierungstechniken

3.1 Sicherheit in virtuellen Umgebungen - Unterschiede und Übereinstimmungen

Es ist offensichtlich, dass sich in virtualisierten Umgebungen einige Fragen zu Sicherheit gänzlich neu stellen. Die Sicherheitsbetrachtungen, die sich im Grundsatz nicht ändern, betreffen überwiegend das Gastsystem und wurden bereits im vorangegangenen Kapitel beschrieben.

Betrachten wir nun die zusätzlichen Bedrohungsszenarien bei einer Virtualisierung. Diese entstehen durch die Einführung neuer Komponenten, nämlich des Hypervisors selbst und eines den Hypervisor umgebenden Host-Betriebssystems. Die Begriffe Host(-Betriebsystem) und Hypervisor sollen im Folgenden synonym verwendet werden, sofern dies im konkreten Fall nicht explizit anders dargestellt wird.

Die Virtualisierungsplattform insgesamt ist eine besonders kritische Komponente, da es den Zugangspunkt zu allen virtuellen Systemen und zu vielen kritischen Diensten und Ressourcen darstellt Sollte diese Virtualisierungsplattform kompromittiert werden, so sind Host-Betriebssystem und die virtuellen Maschinen einem hohen Risiko ausgesetzt. Das einfache Herunterladen eines VM-Images oder das Einfügen einer verfälschten virtuellen Maschine hat dabei gleiche Wertigkeit wie das Einbrechen in ein Rechenzentrum und das Stehlen einer physischen Maschine. Ähnliches gilt für den administrativen Zugriff auf das Hostsystem: Hatte man bisher damit nur Zugriff auf ein Serversystem, hat man nun Zugriff auf alle momentan darauf laufende Gastsysteme.

Ein weiterer Punkt ist, dass sich mehrere virtuelle Maschinen die gleiche Infrastruktur teilen. So ergeben sich neue Herausforderungen, was den Schutz von VLANs, CPU Ressourcen und Systemen angeht. So kann ein kompromittiertes Gastsystem u.U. den kompletten Host auslasten und somit eine Denial-of-Service Attacke gegen alle weiteren Systeme fahren.

Darüber hinaus sei die physikalische Ausfallsicherheit des Hostsystems genannt, die es zu beachten gilt. Da in der Regel mehrere Gastsysteme auf einem Host laufen, sind im Falle eines Hardwareausfalls mehr Systeme betroffen.

Im Einzelnen können bzgl. des Hosts folgende Gefährdungen identifiziert werden:

- Übergriffe von einem Gastsystem auf den Host
- Übergriffe vom Host auf ein Gastsystem
- Angriffe von Außen auf den Host

Die beiden erstgenannten Punkte sind interner Natur und können primär durch den Hersteller der Virtualisierungsplattform adressiert werden. Hierzu muss man anmerken, dass der Hypervisor selbst ein relativ kompaktes System ist. Das hat den positiven Effekt, dass man in einer solchen kleineren Codebasis generell ein höheres Sicherheitsniveau erreichen kann, also in komplexen Betriebssystemen. Die Hersteller arbeiten an entsprechenden Sicherheitszertifizierungen und haben solche auch bereits erreicht. Gleichwohl kann ein Fehler in einer Software niemals ausgeschlossen werden. Insofern ist dieses Risiko, in einem für die jeweilige Umgebung angemessenen Maß, im Sicherheitskonzept zu berücksichtigen.

Die im dritten Punkt angesprochene potenzielle Bedrohung des Hosts selbst kann sowohl durch Softwarefehler, als auch durch Mängel in der Konfiguration oder durch organisatorische Schwächen entstehen. Die entsprechenden Gegenmaßnahmen bestehen primär in einem Update-Management, einer Isolation des Management Segments und einem angemessenen Berechtigungskonzept.

Neben den ausgeführten technischen Übereinstimmungen und Differenzen in Bezug auf die Sicherheitsthematik gibt es noch einige zusätzliche Sicherheitsaspekte in virtuellen Umgebungen zu beachten.

Hier ist als wichtigster Punkt die Organisation zu nennen, der im weiteren Verlauf ein eigener Abschnitt gewidmet ist. Grundsätzlich geht es darum, dass durch die Virtualisierung viele IT-Bereiche miteinander verschmelzen, die vorher getrennt waren. Die Organisation der IT muss sich hier entsprechend anpassen

Ein weiterer Aspekt, der bereits erwähnt wurde, ist die Thematik der Komplexität, welche im Rahmen der Virtualisierung, unter anderem aufgrund der bereitgestellten Funktionalitäten, erheblich ansteigt. Zur Virtualisierung der Server kommt in der Regel die Virtualisierung fast aller anderen Infrastrukturkomponenten hinzu, z.B. das Netzwerk oder der Storage. Auch hier muss rechtzeitig gehandelt und sichergestellt werden, das insbesondere durch geeignete Qualifikationsmaßnahmen für die IT-Mitarbeiter entsprechendes Know-How für einen qualitativ hochwertigen und sicheren Betrieb vorhanden ist.

Beachtenswert ist ebenfalls, dass die Virtualisierung eine zentrale Datenhaltung auf geeigneten Speichersystemen (z.B. SAN/NAS) quasi erzwingt. Diese Technologie ist in manchen Unternehmen noch nicht etabliert. Aber selbst dort, wo ein Speichernetzwerk bereits im erprobten Einsatz ist, kann es neu sein, dass auch Server in sensiblen Sicherheitszonen (z.B. DMZ) auf dieses zugreifen dürfen oder sogar müssen.

3.2 Überlegungen zur Infrastruktur

Absicherung des Host-Systems

Der Virtualisierungshost ist aus Sicherheitsgründen zunächst wie jede normale Systemkomponente der IT-Infrastruktur zu betrachten und genauso in die eigenen Sicherheitsprozesse einzubeziehen. Das bedeutet, dass Prozesse etabliert werden sollten, um das Hostsystem regelmäßig zu aktualisieren. Dies gilt sowohl für die Serverhardware (Bios, Firmware etc.) als auch für die grundlegende Virtualisierungstechnologie (z.B. Hypervisor-Schicht etc.).

Ebenso sollten die Sicherheitsempfehlungen der jeweiligen Hersteller ernstgenommen, implementiert und ständig überwacht werden. Dies kann durch entsprechende Systems-Managementprodukte vereinfacht werden. Ein wichtiger Aspekt hierbei ist, das Hostsystem idealerweise nur als Virtualisierungshost zu verwenden und keine weiteren Serverrollen dort zu betreiben. Zusätzliche Rollen sollten eher in virtuelle Systeme oder auf zusätzliche physische Server verlagert werden.

Haben Sie ein Klassifizierungssystem für Ihre Server eingerichtet, so sollten Sie das Klassifizierungssystem auch auf Ihre Virtualisierungshosts ausdehnen. Der Virtualisierungshost sollte dabei die gleiche Klassifizierung wie die insgesamt höchste Einstufung der auf ihm betriebenen virtuellen Serverinstanzen erhalten. Erleichtert wird dies, indem man gleiche Sicherheitsklassifizierungen der virtuellen Instanzen auf jeweils eigenen Hostgruppen zusammenfasst und Überschneidungen vermeidet.

Virtualisierung und Sicherheit im Netzwerk

Grundsätzlich wird empfohlen, einen Virtualisierungshost mit mehreren Netzwerkkarten, mindestens aber zwei Karten, zu betreiben. Hierbei ist eine Netzwerkkarte reserviert für ein separates Managementnetzwerk direkt vom und zum Host. Virtuelle Maschinen sollten keinen Zugriff auf diese Netzwerkkarte bekommen. So wird verhindert, dass eine Virtuelle Maschine die gesamte Netzwerkbandbreite einnimmt und die Verwaltung des Hosts verhindert.

Diese Trennung sollte durch VLANs oder eigene Netzkreise für das Management-Netzwerk und das Netzwerk für die virtuellen Systeme weiter separiert werden. Der Zugriff

auf das Management-Netzwerk ist auf reine Verwaltungsaufgaben zu beschränken und durch geeignete Mittel wie IPSec, auch in Kombination mit NAP / NAC, zu schützen und zu überwachen.

Virtuelle Maschinen sollten keinen Zugriff auf das Management Netzwerk haben. Für ihre Verwaltung ist bei Bedarf ein eigenes Managementnetzwerk einzurichten. Hier unterscheiden sich die Anforderungen der virtuellen Maschinen nicht von einer physischen Installation, so dass die bekannten Sicherheitsempfehlungen auch weiterhin ihre Gültigkeit behalten:

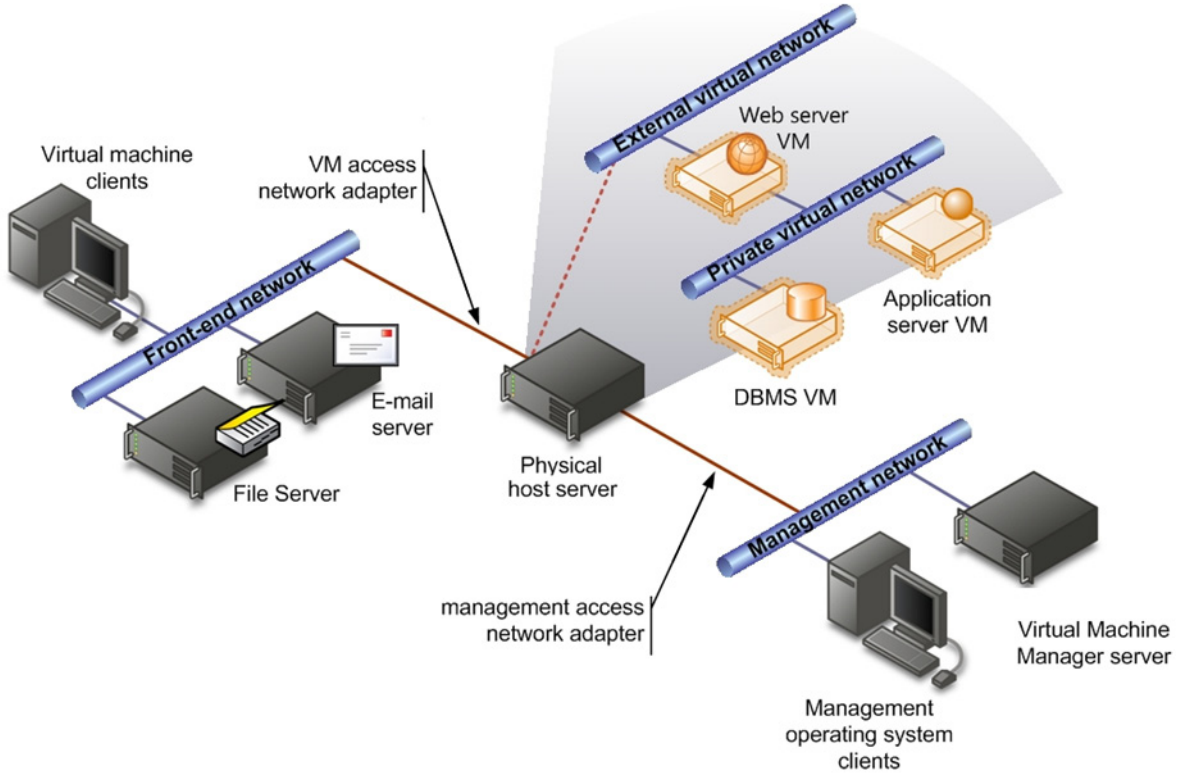
- Je nach Sicherheitsanforderung gehören unterschiedliche Maschinen in separate (V)LANs
- Je nach Sicherheitsanforderung ist ein separates (virtuelles) Managementnetzwerk einzurichten
- Je nach Sicherheitsanforderungen sind die virtuellen Maschinen zu schützen und die Netzwerke zu überwachen.

Je nach Konfiguration oder Funktionalität der verwendeten Virtualisierungstechnologien gilt es hier folgendes zu beachten:

- Aus Skalierungs- und Effizienzgründen werden Hardwareressourcen wie Netzwerkkarten oft zwischen virtuellen Maschinen geteilt, d.h. die gleiche Karte von mehreren Systemen verwendet. Der Zugriff wird über das Hostsystem und / oder die Hypervisorschicht koordiniert, welches entsprechende, vertrauenswürdige Treiber verwenden sollte. Eine End-to-End Überwachung und Sicherung der virtuellen Systeme wie oben erwähnt wird dadurch nicht überflüssig.
- Neueste Netzwerkkarten können bereits selber „virtuelle“ Netzwerkkarten emulieren, die den jeweiligen virtuellen Systemen dediziert zugewiesen werden können. Auch hier ist jedoch die weitere Überwachung und Absicherung der virtuellen Systeme nötig.
- Die gängigen Virtualisierungstechnologien erlauben das Einrichten von virtuellen Switches und, damit verbunden, rein virtuellen VLANs. Hier läuft der komplette Netzwerkverkehr rein virtuell im Speicher des Systems. Externe Netzwerküberwachungsmethoden können auf diesen IP-Traffic nicht zugreifen. Als Abhilfe können Tools verwendet werden, die entweder spezielle Herstellerschnittstellen der Virtualisierungsschicht verwenden oder mit Zusatzkomponenten arbeiten, die in den virtuellen Systemen installiert werden.

Die folgende Abbildung soll noch einmal die unterschiedlichen Netzwerke und deren Bezug zueinander erläutern:

1. Links außen befinden sich die klassischen PCs und Server, die mit einem Front-end Netzwerk verbunden sind und auf physische Serverressourcen wie File- und Emailserver als auch virtuelle Server zugreifen.
2. Die Virtualisierungshosts sind sowohl mit dem Front-end Netzwerk verbunden als auch mit dem dedizierten Management Netzwerk.
3. Im Management Netzwerk befinden sich alle nötigen Ressourcen zum Verwalten der Virtualisierungshosts wie Management Server und Management Workstations
4. Zusätzlich kann es rein virtuelle Netzwerke geben, welche über die Virtualisierungsschicht zur Verfügung gestellt wird. Im Bild sind dies die Netzwerke „External virtual network“ als auch „private virtual network“ im grau hinterlegten Bildausschnitt. Virtuelle Netzwerke erlauben z.B. die Realisierung einer virtuellen DMZ Umgebung wie im vorherigen Text besprochen.



Um die Ausfallsicherheit der Systeme zu erhöhen, kann bei den Netzwerkkarten zusätzlich auf Netzwerkkarten-Teaming gesetzt werden. Hierbei werden 2 Netzwerkkarten parallel betrieben, treten aber für die Systeme als eine einzige Karte auf. Diese Technik ist seit Jahren bekannt und deren Konzepte gelten auch in der virtuellen Welt weiter.

Netzwerkzonen wie DMZ und ähnliche Konstrukte

Viele Anwender haben Server in unterschiedliche Netzwerksicherheitszonen verschoben, um so eine aus ihrer Sicht höhere Netzwerksicherheit zu erreichen. Wie geht man aber damit um, Server aus unterschiedlichen Netzwerksicherheitszonen zu virtualisieren?

Ein einfacher Ansatz ist, nur jeweils Systeme aus einer Sicherheitszone auf einem Virtualisierungshost zu betreiben und so die Netzwerkzonen auf die Hosts zu erweitern. Der Nachteil ist die unflexiblere, und somit oft schlechtere, Ausnutzung der Hostressourcen. Auch muss darauf geachtet werden, dass für das Management-Netzwerk des Hostsystems die gleichen Anforderungen gelten müssen wie für ein Management-Netzwerk anderer physischer Systeme innerhalb dieser Netzwerksicherheitszone. Das gilt auch für gemeinsam genutzte Storagebereiche, auf denen die virtuellen Maschinen platziert sind.

Sollen hingegen Systeme aus unterschiedlichen Netzzonen auf einem Host zusammenbetrieben werden oder Storagesysteme für virtuelle Systeme unterschiedlicher Netzwerkzonen gemeinsam verwendet werden, weicht die Netztrennung automatisch etwas auf. Hier könnten lediglich dedizierte Netzwerkkarten bzw. Storageadapter helfen. Zusätzlich bleibt die Absicherung der virtuellen Maschinen durch Verfahren wie IPSec auch in Kombination mit NAP / NAC; um die Trennung der Netzwerkzonen auch auf Maschinenseite zu forcieren.

Es bleibt jedoch das Risiko, dass eine virtuelle Maschine kompromitiert wird und durch einen Fehler in der Virtualisierungsschicht auf den Host zugreifen kann. In

diesem schlimmsten anzunehmenden Fall könnte über eine virtuelle Maschine direkt auf eine Maschine einer anderen Sicherheitszone zugegriffen werden. Dieser unwahrscheinliche Fall kann nicht zu 100% ausgeschlossen werden und muss bei den eigenen Sicherheitsüberlegungen und –abwägungen entsprechend berücksichtigt werden.

Speichersysteme

Virtuelle Maschinen bestehen in der Regel aus mehreren Dateien, welche auf einem Speichersystem abgelegt werden. Soll die Maschine auf mehreren Virtualisierungshosts zur Verfügung stehen (z.B. für Host-Clustering oder bei Verwendung von Technologien wie „Live Migation"), so müssen diese Speichersysteme an die jeweiligen Hostsysteme angebunden werden. Auch für diese Anbindungen gelten die gleichen Überlegungen wie für die Netzwerksicherheitszonen und das Managementnetzwerk. Ob Maschinen aus unterschiedlichen Sicherheitszonen auf die gleichen Ressourcen zugreifen dürfen oder nicht, ist eine grundsätzliche Entscheidung, die es zu treffen gilt. In der Regel können hier jedoch die ähnlichen Entscheidungskriterien wie aus der realen Systemwelt übernommen werden, ergänzt um den Faktor der Kompromittierung der verwendeten Virtualisierungstechnologie.

In diesem Zusammenhang ist es auch wichtig, die Lage von System-Bibliotheken bzw. Systemklonen zu beachten. Ein Bespiel kann dies verdeutlichen:

Man konfiguriert eine virtuelle Maschine als Server der höchsten Sicherheitsstufe und legt diese als Template in einer Virtualisierungsbibliothek ab. Auf diese Maschine sollten im Anschluss nur Serveradministartoren zugreifen dürfen, die Zugriffsberechtigungen für Systeme der höchsten Sicherheitsstufe haben. Systemkopien bzw. Systemklone dürfen ebenfalls nur auf Speicherbereichen der entsprechenden Sicherheitsstufe angelegt werden. Dieses ist durch geeignete Konfiguration der Virtualisierungshosts und Audits dieser Einstellungen zu erreichen und zu überwachen. Detaillierte Empfehlungen finden sich in den Sicherheitsleitfäden der jeweiligen Hersteller.

Die physische Sicherheit der eigentlichen Speichersysteme ist ebenfalls zu beachten. Während der Diebstahl eines physischen Servers optisch auffällt, ist das Kopieren eines virtuellen Systems auf einen USB Stick kaum bemerkbar. Hier helfen nur zusätzliche Sicherheitstechnologien wie auditierbare Zugriffsberechtigungen auf das Speichersystem sowie zusätzliche Verschlüsselungstechnologien der Festplatten. Letztere helfen gegen unberechtigten Zugriff z.B. bei Entwendung der Platten.

3.3 Systems Management virtueller Systeme

Auch virtuelle Maschinen müssen genau wie physische Serverinstanzen gemanaged werden. Dies umfasst vor allem das Patchen und Sichern der virtuellen Systeme z.B. durch eine Antivirensoftware. Werden virtuelle Systeme nicht ständig betrieben, sondern zwischenzeitlich in den Ruhezustand verschoben oder gar als Template in einer Bibliothek abgelegt, muss auch hier sichergestellt werden, dass diese Systeme nur aktualisiert wieder in das normale Netz zurückkommen. Hierfür gibt es zwei unterschiedliche Ansätze:

Die virtuellen Systeme werden in regelmäßigen Abständen gebootet bzw. gestartet und aktualisiert. Nachdem die neuesten Patches, Service Packs etc. eingespielt wurden, wird die virtuelle Maschinen wieder in ihren Ausgangszustand versetzt. Tools der gängigen Systemsmanagementhersteller automatisieren dieses Verfahren, um eine hohe Prozessqualität zu erlauben.

Beim Starten der virtuellen Systeme werden durch geeignete Maßnahmen wie NAP / NAC die virtuellen Instanzen zunächst vom eigentlichen Netzzugriff isoliert, bis das System die vorgeschriebenen Sicherheitskonfigurationen und Versionsstände aufweist. Im Anschluß erhält das System normalen Zugriff auf das Netz. Auch diese Pro-

zesse können von modernen Systemsmanagementtools unterstützt werden.

Neben Patching ist das Systemmonitoring ein weiterer wichtiger Bereich im Systems Management von virtuellen Maschinen. Auch hier gilt, dass die normalen Prozesse der realen Welt auch in der virtuellen Welt weiterhin ihre Berechtigungen und Notwendigkeiten haben. Daher muss auch eine virtuelle Maschine zunächst ganz normal durch geeignete Tools überwacht werden. Zusätzlich muss jedoch auch ihre Auswirkung auf den Virtualisierungshost beachtet werden: Nutzt eine virtuelle Maschine zu viele Ressourcen des Hosts, muss sie unter Umständen auf einen anderen Host verschoben oder andere virtuelle Maschinen gestoppt / verschoben werden. Idealerweise setzt man hierbei Systems Management Tools ein, die sowohl mit den Virtualisierungshosts als auch den virtuellen Maschinen gemeinsam umgehen können und auch eine Korrelation der beiden Umgebungen erlauben.

3.4 Zusätzliche Möglichkeiten

Neben Netzwerküberwachungstools gibt es neu auch Überlegungen und Ansätze, Antivirensoftware und weitere Sicherheitssoftware (z.B. Firewalls) von den virtuellen Systemen auf das Hostsystem zu verlagern. Hier gilt es abzuwägen, was erreicht werden soll: laufen ähnliche virtuelle Maschinen auf einem Host, könnte der gesamte Netzwerkverkehr an einer Stelle abgesichert werden. Aufgrund der Vielfalt von unterschiedlichen Applikationen und damit verbundenen Scanengines und Sicherheitsregeln kann dies aber auch kontraproduktiv sein. Zudem kann ein Onlinescan nicht regelmäßige Offlinescans ersetzen, um bereits abgelegte bzw. installierte Malware zu finden. Ob die Scanengines dabei in den virtuellen Maschinen installiert werden oder „von außen“ die virtuellen Festplatten scannen, sollte von Fall zu Fall und nach Verfügbarkeit einer entsprechenden Engine entschieden werden.

3.5 Virtuelle Sicherheitssysteme

Es stellt sich die Frage, ob man klassische Sicherheitssysteme einfach virtualisieren kann oder darf. Um dies zu beantworten, muss man die in Frage kommenden Systeme in verschiedene Gruppen unterteilen. Betrachten wir zunächst solche Sicherheitssysteme, die im Wesentlichen auf Anwendungseben laufen, z.B. Proxies oder Gateways auf Anwendungsebene, wie Virenschutzgateways. Diese Systeme können grundsätzlich behandelt werden wie ganz normale Serversysteme und sind daher in der Regel problemlos virtualisierbar. Natürlich muss auch hier ein besonderes Augenmerk auf die Systemlast gelegt werden, die solche Komponenten erzeugen. Auch Systeme, die etwas näher am Netzwerk positioniert sind, z.B. VPN-Gateways oder Load-Balancer, können im Einzelfall noch zu dieser Kategorie gezählt werden und sind daher potenzielle Kandidaten für eine Virtualisierung. Für viele Systeme, die in diese Kategorie fallen, gibt es sogar bereits vorgefertigte virtuelle Appliances vom Hersteller, in einigen Fällen sogar mit entsprechenden Zertifizierungen für bestimmten Virtualisierungsplattformen

Dem gegenüber stehen klassische Netzwerkfirewalls und vergleichbare Komponenten. Im Moment spricht nicht viel dafür, diese Firewalls zu virtualisieren, nicht zuletzt, weil die meisten Produkte dieser Art ohnehin auf einer dedizierten Plattform laufen. Die Hauptgründe dagegen liegen im strukturellen Umfeld. Wie bereits oben angedeutet, werden die bisher klaren Zuständigkeiten durch Virtualisierung aufgeweicht. Für eine Firewall, die unterschiedlichste Sicherheitszonen trennt, ist dies organisatorisch kaum zu verantworten. Auch technisch rücken alle Systeme enger zusammen - eine scharfe Trennung ist kaum mehr möglich. Die Auswirkungen von Fehlern, insbesondere Konfigurationsfehlern, wirken sich ungleich schwerwiegender aus als bisher. Nicht zuletzt gibt es noch keine Erfahrungen über das Performanceverhalten in der Praxis und die potenziellen Auswirkungen auf die Host-Systeme. Insgesamt kann zum jetzigen Zeitpunkt nicht empfohlen werden, klassische Firewalls durch virtuelle Firewalls zu ersetzen.

Gleichwohl gibt es auch ein Einsatzgebiet für virtuelle Firewalls, z.B. wenn es darum geht, verschiedene Sicherheitszonen oder Hosts innerhalb der virtuellen Umgebung zu trennen. Hierfür gibt es spezielle Entwicklungen, die auf die Besonderheiten in einem virtuellen Umfeld angepasst sind. Zwar gelten für diese System grundsätzlich dieselben Bedenken wie für die klassischen Firewalls, jedoch sind hier die Freiheitsgrade in der Entscheidung deutlich größer, da es nicht darum geht, etablierte und unternehmenskritische Systeme abzulösen, sondern zusätzliche Sicherheitsfunktionen einzuführen.

Im Zusammenhang solcher neuen Sicherheitsfunktionalitäten sei hier nochmals auf die kommenden Produktgenerationen von Sicherheitssystemen hingewiesen, die bereits im vorangegangenen Kapitel eingeführt wurden. Solche Systeme, z.B. ein zentralisierter Virenscanner oder IDS-System laufen selbstverständlich auch als virtuelle Systeme.

3.6 Überwachung

Der Zugriff auf Ressourcen innerhalb virtueller Systeme ist genauso zu regeln wie der Zugriff innerhalb physischer Systeme. Hierbei sind die grundlegenden Sicherheitsvorgaben und Herstellerempehlungen in beiden Welten genau gleich zu beachten. Dies betrifft Härten von Systemen gegen Zugriff von außen, Zugriffsberechtigungen und Rollenkonzepte wie Administrator / Root bzw. Anwender inklusive aller nötiger Abstufungen als auch das Überwachen der Systeme und Auditieren von Zugriffen und Aktionen. Zusätzlich ist die Zugriffberechtigung auf das Hostsystem und die administrativen Rechte zur Einrichtung und Konfiguration der virtuellen Systeme zu beachten.

Die Rolle des Virtualisierungshostadministrators nimmt dabei eine Sonderstellung ein. Diese Anwender haben vollen Zugriff auf den Host und können somit alle weiteren Zugriffe konfigurieren bzw. delegieren. Dies umfasst den Zugriff auf die Netzwerke, die Speichersysteme sowie die Zuteilung der Systemressourcen an die virtuellen Maschinen. Auch kann der Hostadministrator in der Regel jede virtuelle Maschine stoppen, starten, löschen oder kopieren. Diese Arbeit verlangt eine hohe Vertrauenswürdigkeit der jeweiligen Mitarbeiter und sollte entsprechend überwacht und auditiert werden. Es ist zu überprüfen, ob die verwendeten Virtualisierungstechnologien einen adäquaten Schutz und die Granularität für das Einhalten der regulativen Anforderungen bieten. Es kann ansonsten nötig sein, unabhängig von der genutzten „Host-Technologie“ eine zusätzliche Schutz-Schicht einzubauen. Diese Access Control Lösungen müssen dann unabhängig auf Kernel-Ebene arbeiten ohne selbst in den Kernel einzugreifen.

Um das allgemeine Sicherheitsrisiko zu minimieren, sollte die Virtualisierungstechnologie neben dem Hostadministrator noch weitere Zugriffsrollen mit entsprechenden Berechtigungen erlauben. Somit können weitere Mitarbeiter berechtigt werden, neue virtuelle Systeme anzulegen. Mitarbeiter sollten dabei nur Zugriff auf die Ressourcen bekommen, die ihrer jeweiligen Sicherheitseinstufung entsprechen. In der Regel kann dies durch entsprechend konfigurierte Templates für virtuelle Systeme ermöglicht werden. In den Templates werden dabei Netzwerke, Hostsysteme und physikalische Systemressourcen wie zugewiesene Speichersysteme und Prozessorauslastungen etc. hinterlegt. Auch diese Tätigkeiten sollten dabei überwachbar und auditierbar sein.

Je nach verwendeter Virtualisierungstechnologie und verlangtem Sicherheitskonzept, kann zusätzlich auch eine Trennung zwischen reiner Hostadministration und virtueller Netzwerkadministration erfolgen. Dies ist besonders interessant für Organisationen, die historisch diese beiden Bereiche getrennt haben.

Ein weiterer Sicherheitsansatz ist es, eine strikte Trennung zwischen Hostadministratoren und (virtuellen) Serveradministratoren so umzusetzen, dass kein Hostadministrator auch Rechte innerhalb der virtuellen Systeme hat. So wird zumindest erschwert, dass ein Hostadministrator

eine neue virtuelle Maschine startet, diese für böswillige Tätigkeiten missbraucht und diese im Anschluss direkt wieder löscht um Spuren zu verwischen.

3.7 Datensicherung

Backup und Recovery gehören zu den Kernaufgaben eines Rechenzentrums. Sie bilden das Rückgrat einer durch geschäftliche Vorgaben und Ziele geprägten Datensicherungsstrategie. Sie trägt dank policy-gesteuerter Prozesse wesentlich zur Umsetzung von Compliance- und Governance-Strategien bei.

Bei der Datensicherung in virtuellen Umgebungen sind zwei grundsätzliche Ziele für die Datensicherung zu unterscheiden. Zum einen muss selbstverständlich die virtuelle Umgebung selbst gesichert werden, zum anderen alle Gastsysteme.

Die Sicherung der virtuellen Umgebung betrifft alle wichtigen Konfigurationsdaten des Systems, insbesondere

- Konfiguration der virtuellem Maschinen
- Benutzer und Berechtigungssystem
- Netzwerkkonfiguration
- Storagekonfiguration

Je nach Aufbau der virtuellen Umgebung umfasst dies mindestens die Sicherung der Hostkonfigurationen oder die Sicherung eines zentralen Managementsystems, wobei letztgenanntes in Umgebungen mit mehreren Hosts der Regelfall sein wird. Wie eine solche Sicherung durchgeführt werden kann, hängt vom eingesetzten Virtualisierungsprodukt ab. Entweder bringt das Produkt ein eigenes Sicherungsmodul mit, oder es gibt entsprechende Agenten die die führenden Datensicherungsprodukte. Möglicherweise genügt aber auch eine ganz klassische Sicherung des Hosts oder des zentralen Konfigurationssystem.

Die Sicherung der Gastsysteme kann auf unterschiedlichste Arten erfolgen. Wie bereits oben erwähnt, können Gastsysteme genauso gesichert werden wie bisher. Dies hat den Vorteil, dass man trotz Virtualisierung die bisherige Datensicherungsstrategie nicht verändern muss, was insbesondere in der Einführungsphase eine gewisse Konstante und Zuverlässigkeit darstellt.

Über die klassische Art der Datensicherung hinaus, drängt sich in virtuellen Umgebungen eine weitere Art der Sicherung auf. Da die Gastsysteme durch einige wenige Dateien repräsentiert werden, kann man diese Dateien sichern, um ein komplettes Bild der Maschine zu erhalten. Im einfachsten Fall funktioniert dies jedoch nur dann sicher, wenn die Maschine zum Zeitpunkt der Sicherung ausgeschaltet oder zumindest in einem Ruhemodus ist. Im anderen Fall ist die Gefahr groß, dass die Maschine in einem inkonsistenten Zustand gesichert wird und nicht oder nicht einwandfrei wieder in Betrieb genommen werden kann. Abhilfe schaffen hier Methoden, die zuerst einen Snapshot des Gastes erstellen und dann diesen Snapshot sichern. Auf diese Weise wird ein konsistentes Abbild der Maschine gespeichert.

Sicherungen mit der Methode ganzer Abbilder haben a priori den Nachteil, dass sie keinen Zugriff auf einzelne Dateien erlauben. Daher ist es nicht immer sinnvoll, ein ganzes System zu sichern. Bei der Rücksicherung ist dies noch weniger der Fall, denn recht häufig werden nur einzelne Dateien zur Wiederherstellung angefordert. Hier gibt es mehrere Lösungsansätze. Zum einen können bei der Sicherung die virtuellen Maschinen bzw. die oben angesprochenen Snapshots als Dateisystem eingebunden werden, so dass ein Backup-System zur Sicherung direkt auf die Dateien zugreifen kann. So entsteht wieder eine Datesicherung klassischer Prägung, die einfach zurück zu sichern ist. Die andere Variante besteht darin, auf ein gesichertes komplettes Abbild der virtuellen Maschine so zuzugreifen, so dass man aus dieser einzelne Dateien wiederherstellen kann.

Eine weitere Herausforderung bei der Sicherung kompletter Maschinen besteht in der großen Datenmenge, die hierbei anfallen kann. Das zu sichernde Gastsystem ist normalerweise deutlich größer als die im System enthaltenen Daten. Außerdem gibt es bei dieser Art

der Sicherung kein einfaches inkrementelles Verfahren. Gegen diese stark wachsenden Mengen an Backup-Daten gibt es Methoden der Deduplizierung, die durch das Backup-System oder ggf. durch den zentralen Storage angeboten werden.

3.8 Organisatorische Rahmenbedingungen

Wie bereits an mehreren Stellen erwähnt wurde, bringt die Virtualisierung neue organisatorische Herausforderungen mit sich. Dies wird deutlich, wenn man betrachtet, welche Funktionen sich innerhalb einer Virtualisierungsumgebung sammeln, die bisher klar getrennt waren – sei es nur durch die Qualifikation der Mitarbeiter oder sogar organisatorisch in verschiedenen Gruppen oder Abteilungen. Die zusammengeführten wesentlichen Funktionen sind:

- Server-Administration
- Netzwerk
- Storage
- Sicherheit
- RZ Betrieb (Gastsysteme statt Hardware)
- Monitoring/Überwachung
- Datensicherung

In einigen der genannten Fälle ist es zwar möglich, die klassische Vorgehensweise beizubehalten (z.B. Datensicherung oder Monitoring), jedoch ist dies nicht immer die sinnvollste Variante, da man hier große Potenziale der Virtualisierung ungenutzt lässt.

Dem Problem, dass die technische Infrastruktur sich entgegen der vorhandenen Organisation konsolidiert, kann man mit verschiedenen Maßnahmen entgegen wirken.

Zum einen kann es technische Lösungen geben, die den spezialisierten Fachabteilungen wieder die Möglichkeiten geben, die sie bisher hatten. Als Beispiel sei hier die Netzwerkintegration genannt, bei der sich Lösungen ankündigen, wo sich das virtuelle Netzwerk voll in das „echte“ Netzwerk integriert und den Spezialisten dieselben Konfigurations- und Überwachungsmöglichkeiten geben wie bisher.

Entscheidender als solche technischen Ansätze ist die frühzeitige Qualifikation und Integration aller betroffenen Mitarbeiter. Es ist nicht sinnvoll, die Virtualisierung allein in irgendeiner Gruppe zu platzieren- üblicherweise bei den Server-Adminstratoren- nur weil es dort am ehesten hineinpasst.

Soweit machbar, sollten bereits während der Planungsphase eines Virtualisierungsprojektes die oben genannten Punkte mitbehandelt werden. Obwohl dies offensichtlich zu sein scheint, ist dies in der Praxis leider nicht der Regelfall.

Da viele verschiedene Mitarbeiter in ein solches Projekt eingebunden sind, sollte bereits frühzeitig über ein geeignetes Berechtigungskonzept nachgedacht werden.

Viele Prozesse und Sicherheitsstrukturen für klassiche physische Systeme sind auch für virtuelle Umgebungen geeignet und weiter anwendbar. Dennoch stellen sich durch die Verwendung von virtueller Infrastruktur neue Herausforderungen, insbesondere bei der Zugriffsrechteverwaltung und der Sicherung der Verfügbarkeit. Durch sorgfältige Planung und entsprechende Anpassung der IT-Organisation können aber die Vorteile der Virtualisierung bei gleichbleibend hohem Sicherheitsstandard genutzt werden.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.300 Unternehmen, davon 950 Direktmitglieder mit etwa 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Anbieter von Software, IT-Services und Telekommunikationsdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien. Der BITKOM setzt sich insbesondere für bessere ordnungspolitische Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein..

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org