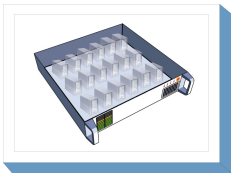
B 3.304 Virtualisierung



Beschreibung

Bei der Virtualisierung von IT-Systemen werden ein oder mehrere virtuelle IT-Systeme auf einem physischen Computer betrieben. Ein solcher physischer Computer wird als Virtualisierungsserver bezeichnet. Mehrere solcher Virtualisierungsserver können häufig zu einer virtuellen Infrastruktur zusammengefasst werden. In einer solchen virtuellen Infrastruktur können die Virtualisierungsserver selbst und die auf ihnen betriebenen virtuellen IT-Systeme gemeinsam verwaltet werden.

Die Virtualisierung von IT-Systemen bietet vielfältige Vorteile für den IT-Betrieb in einem Informationsverbund. Es können Kosten für Hardwarebeschaffung, Strom und Klimatisierung eingespart werden, wenn die Ressourcen der Server effizienter genutzt werden. Durch die damit verbundene Zentralisierung und Konsolidierung sowie die vereinfachte Bereitstellung von IT-Systemen können im Bereich Personal und Administration ebenfalls Kostenvorteile erreicht werden. Die Möglichkeiten der Virtualisierung stellen aber auch gleichzeitig eine neue Herausforderung für den Betrieb des Informationsverbundes dar. Da durch den Einsatz der Virtualisierungstechnik unterschiedliche Bereiche und Arbeitsfelder im Informationsverbund berührt werden, müssen Wissen und Erfahrungen aus den unterschiedlichsten Bereichen zusammengeführt werden.

Der Einsatz von Virtualisierungsservern und virtuellen IT-Systemen muss in der Schutzbedarfsfeststellung für den vorliegenden Informationsverbund berücksichtigt werden. Es ist zu beachten, dass der Schutzbedarf des Virtualisierungsservers durch den Schutzbedarf der auf ihm betriebenen virtuellen IT-Systeme beeinflusst wird. Probleme auf einem Virtualisierungsserver oder einem virtuellen IT-System können sich möglicherweise auch auf alle anderen virtuellen IT-Systeme, die auf dem selben Virtualisierungsserver betrieben werden, auswirken.

In diesem Baustein wird beschrieben, wie die Virtualisierung von IT-Systemen in den Informationsverbund eingeführt werden kann und unter welchen Voraussetzungen virtuelle Infrastrukturen im Informationsverbund sicher betrieben werden können.

Thematische Abgrenzung

In diesem Baustein wird nur die Virtualisierung vollständiger IT-Systeme behandelt, andere Techniken, die teilweise ebenfalls mit dem Wort "Virtualisierung" in Verbindung gebracht werden (Anwendungsvirtualisierung mittels Terminalservern, Storage-Virtualisierung etc.), sind nicht Gegenstand dieses Bausteins. Es werden Virtualisierungsserver und virtuelle IT-Systeme betrachtet, in denen Betriebssysteme ablaufen, die häufig auch direkt auf physischen IT-Systemen zum Einsatz kommen.

Im Bereich der Software-Entwicklung werden die Begriffe Virtuelle Maschine und Virtuelle-Maschinen-Monitor (VMM) manchmal auch für bestimmte Laufzeitumgebungen, beispielsweise beim Einsatz von Java oder Dot-NET (Microsoft .NET), verwendet. Solche Laufzeitumgebungen werden in diesem Baustein ebenfalls nicht betrachtet.

Gefährdungslage

Für den sicheren Betrieb von Virtualisierungsservern und virtuellen IT-Systemen gibt es auf Grund der vielfältigen Funktionen der Virtualisierungsserver und der Manipulationsmöglichkeiten für virtuelle IT-Systeme einige neue organisatorische und technische Gefährdungen. Dies hängt damit zusammen, dass ein neuer Infrastrukturbestandteil, nämlich die Virtualisierungsinfrastruktur für IT-Objekte, entsteht. Auch können virtuelle IT-Systeme neue Zustände einnehmen. So kann sich ein System, das ausgeschaltet wurde, dennoch im Zustand *laufend* befinden, wenn es durch die Virtualisierungssoftware lediglich eingefroren wurde. Zudem werden Lebenszyklen von virtuellen IT-Systemen in der Regel in wesentlich kürzeren Zeitabständen durchlaufen.

In virtuellen Infrastrukturen werden für den IT-Grundschutz die folgenden typischen Gefährdungen angenommen:

Organisatorische Mängel

- G 2.29 *Softwaretest mit Produktionsdaten*
- G 2.32 *Unzureichende Leitungskapazitäten*
- G 2.37 *Unkontrollierter Aufbau von Kommunikationsverbindungen*
- G 2.60 *Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement*
- G 2.148 *Fehlerhafte Planung der Virtualisierung*
- G 2.149 *Nicht ausreichende Speicherkapazität für virtuelle IT-Systeme*
- G 2.150 *Fehlerhafte Integration von Gastwerkzeugen in virtuellen IT-Systemen*
- G 2.151 *Fehlende Herstellerunterstützung von Applikationen für den Einsatz auf virtuellen IT-Systemen*

Menschliche Fehlhandlungen

- G 3.16 *Fehlerhafte Administration von Zugangs- und Zugriffsrechten*
- G 3.28 *Ungeeignete Konfiguration der aktiven Netzkomponenten*
- G 3.36 *Fehlinterpretation von Ereignissen*
- G 3.79 *Fehlerhafte Zuordnung von Ressourcen des SAN*
- G 3.99 *Fehlerhafte Netzanbindungen eines Virtualisierungsservers*
- G 3.100 *Unsachgemäße Verwendung von Snapshots virtueller IT-Systeme*
- G 3.101 *Fehlerhafter Einsatz der Gastwerkzeuge in virtuellen IT-Systemen*
- G 3.102 *Fehlerhafte Zeitsynchronisation bei virtuellen IT-Systemen*

Technisches Versagen

- G 4.74 *Ausfall von IT-Komponenten in einer virtualisierten Umgebung*
- G 4.75 *Störung der Netzinfrastruktur von Virtualisierungsumgebungen*
- G 4.76 *Ausfall von Verwaltungsservern für Virtualisierungssysteme*
- G 4.77 *Ressourcenengpässe durch fehlerhafte Funktion der Gastwerkzeuge in virtuellen Umgebungen*
- G 4.78 *Ausfall von virtuellen Maschinen durch nicht beendete Datensicherungsprozesse*

Vorsätzliche Handlungen

- G 5.29 *Unberechtigtes Kopieren der Datenträger*
- G 5.133 *Unautorisierte Benutzung web-basierter Administrationswerkzeuge*
- G 5.147 *Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes*
- G 5.148 *Missbrauch von Virtualisierungsfunktionen*
- G 5.149 *Missbräuchliche Nutzung von Gastwerkzeugen in virtuellen IT-Systemen*
- G 5.150 *Kompromittierung des Hypervisor virtueller IT-Systeme*

Maßnahmenempfehlungen

Um einen Informationsverbund abzusichern, müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz. Für die Modellierung von Virtualisierungsservern und virtuellen IT-Systemen ist Folgendes zu beachten:

- Der Baustein B 3.304 *Virtualisierung* ist auf jeden Virtualisierungsserver oder jede Gruppe von Virtualisierungsservern anzuwenden. Ein Virtualisierungsserver ist ein physisches IT-System (Client oder Server), auf dem virtuelle IT-Systeme betrieben werden. Neben dem Baustein B 3.304 müssen auch die jeweils relevanten Server- oder Client-Bausteine der Schicht 3 auf die Virtualisierungsserver angewandt werden.
- Neben physischen IT-Systemen und Virtualisierungsservern müssen auch virtuelle IT-Systeme (virtuelle Maschinen, VMs) mit Hilfe der Bausteine aus den IT-Grundschutz-Katalogen modelliert werden. VMs werden grundsätzlich in der gleichen Weise wie physische IT-Systeme modelliert, das heißt, es werden die jeweils relevanten Bausteine der Schichten 3 und 5 herangezogen. Da es in der Praxis oft vorkommt, dass viele VMs eingerichtet werden, ist eine sinnvolle Modellierung der VMs häufig nur durch geeignete Gruppenbildung möglich. Für die Gruppenbildung gelten bei VMs die gleichen Regeln wie für physische IT-Systeme. Prinzipiell können auch solche VMs zu einer Gruppe zusammengefasst werden, die auf verschiedenen physischen IT-Systemen ablaufen. Weitere Hin-

weise zur Modellierung virtueller IT-Systeme finden sich in der Maßnahme M 2.392 *Modellierung von Virtualisierungsservern und virtuellen IT-Systemen*.

Planung und Konzeption

Bei der Planung einer virtuellen IT-Infrastruktur müssen eine Reihe von Rahmenbedingungen bedacht werden. Neben den Fragen nach der zur nutzenden Virtualisierungstechnik und entsprechenden Produkten (siehe M 2.477 *Planung einer virtuellen Infrastruktur*) sowie nach der Eignung der in Frage kommenden Systeme bezüglich der Virtualisierung (M 2.444 *Einsatzplanung für virtuelle IT-Systeme*) ist insbesondere die zukünftige Netzstruktur zu planen (M 5.153 *Planung des Netzes für virtuelle Infrastrukturen*). Weiterhin sind auch eine Reihe von organisatorischen Regelungen anzupassen.

Da sich Virtualisierungsserver besonders für den Aufbau von Test- und Entwicklungsumgebungen eignen, sollten detaillierte Regelungen getroffen werden, wie mit den in diesen Umgebungen verarbeiteten Daten umgegangen werden soll (M 2.82 *Entwicklung eines Testplans für Standardsoftware*).

Beschaffung

Bei der Auswahl der Hardware für Virtualisierungsserver ist darauf zu achten, dass Systeme beschafft werden, die für die gewählte Virtualisierungslösung geeignet sind. Die Systeme müssen leistungsfähig genug sein, um für alle geplanten virtuellen IT-Systeme genügend Performance bereitstellen zu können (M 2.445 *Auswahl geeigneter Hardware für Virtualisierungsumgebungen*).

Umsetzung

Der Aufbau der virtuellen Infrastruktur bzw. die Installation der Virtualisierungsserver selbst kann gemäß der eingeübten Vorgehensweisen der Organisation durchgeführt werden (B 3.101 *Allgemeiner Server*). Der Komplexitätsgrad eines Virtualisierungsprojektes insgesamt sollte jedoch nicht unterschätzt werden, daher sind einige Besonderheiten bei der Konfiguration der Netze (M 5.154 *Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen*) und der Gestaltung des administrativen Zugangs zu den Virtualisierungsservern (M 2.446 *Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern*) zu beachten.

Für die Bereitstellung virtueller IT-Systeme auf den Virtualisierungsservern müssen organisatorische Maßnahmen für die Installation der virtuellen IT-Systeme (M 2.447 *Sicherer Einsatz virtueller IT-Systeme*) durch technische Maßnahmen ergänzt werden (M 4.346 *Sichere Konfiguration virtueller IT-Systeme*), um deren sicheren Betrieb zu gewährleisten.

Auf den eigentlichen Virtualisierungsservern sollten möglichst nur solche Dienste betrieben werden, die zur Virtualisierungstechnik gehören. Andere Dienste sollten in den virtualisierten Instanzen (oder auf Systemen außerhalb der virtuellen Infrastruktur) bereitgestellt werden.

Betrieb

Die Maßnahmen M 2.448 *Überwachung der Funktion und Konfiguration virtueller Infrastrukturen* und M 4.349 *Sicherer Betrieb von virtuellen Infrastrukturen* von virtuellen Infrastrukturen bilden die Grundlage für den sicheren Betrieb sowohl der Virtualisierungsserver als auch der virtuellen IT-Systeme. Weiterhin ist die Maßnahme M 4.348 *Zeitsynchronisation in virtuellen IT-Systemen* zu beachten.

Notfallvorsorge

Bei der Notfallvorsorge für Virtualisierungsserver sollte berücksichtigt werden, dass das potentielle Schadensausmaß umso höher ist, je mehr virtuelle IT-Systeme auf einem Virtualisierungsserver betrieben werden. Daher muss der Schutzbedarf der Gesamtheit der virtuellen IT-Systeme auf den Schutzbedarf der Virtualisierungskomponenten abgebildet werden (M 6.138 *Erstellung eines Notfallplans für den Ausfall von Virtualisierungskomponenten*).

Nachfolgend wird das Maßnahmenbündel für den Baustein "Virtualisierung" vorgestellt.

Planung und Konzeption

- M 2.82 (B) *Entwicklung eines Testplans für Standardsoftware*

- M 2.314 (Z) *Verwendung von hochverfügbaren Architekturen für Server*
- M 2.392 (A) *Modellierung von Virtualisierungsservern und virtuellen IT-Systemen*
- M 2.444 (A) *Einsatzplanung für virtuelle IT-Systeme*
- M 2.477 (A) *Planung einer virtuellen Infrastruktur*
- M 3.70 (W) *Einführung in die Virtualisierung*
- M 3.71 (B) *Schulung der Administratoren virtueller Umgebungen*
- M 5.153 (B) *Planung des Netzes für virtuelle Infrastrukturen*

Beschaffung

- M 2.445 (C) *Auswahl geeigneter Hardware für Virtualisierungsumgebungen*

Umsetzung

- M 2.83 (B) *Testen von Standardsoftware*
- M 2.446 (B) *Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern*
- M 2.447 (A) *Sicherer Einsatz virtueller IT-Systeme*
- M 3.72 (W) *Grundbegriffe der Virtualisierungstechnik*
- M 4.97 (Z) *Ein Dienst pro Server*
- M 4.346 (A) *Sichere Konfiguration virtueller IT-Systeme*
- M 4.347 (Z) *Deaktivierung von Snapshots virtueller IT-Systeme*
- M 5.154 (B) *Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen*

Betrieb

- M 2.448 (B) *Überwachung der Funktion und Konfiguration virtueller Infrastrukturen*
- M 2.449 (Z) *Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme*
- M 4.348 (C) *Zeitsynchronisation in virtuellen IT-Systemen*
- M 4.349 (A) *Sicherer Betrieb von virtuellen Infrastrukturen*

Notfallvorsorge

- M 6.138 (C) *Erstellung eines Notfallplans für den Ausfall von Virtualisierungskomponenten*

Goldene Regeln

Bei der Virtualisierung von IT-Systemen werden ein oder mehrere virtuelle IT-Systeme auf einem physischen Computer betrieben. Ein solcher physischer Computer wird als Virtualisierungsserver bezeichnet. Je nach Produkt können mehrere Virtualisierungsserver zu einer virtuellen Infrastruktur zusammengefasst werden. In einer solchen virtuellen Infrastruktur können die Virtualisierungsserver selbst und die auf ihnen betriebenen virtuellen IT-Systeme gemeinsam verwaltet werden. Betrachtet werden Sicherheitsaspekte der Virtualisierung.

- Aufgrund der hohen Komplexität ist eine detaillierte Planung beim Aufbau einer virtuellen Infrastruktur unerlässlich. Daher sollte schon bei einer konzeptionellen Betrachtung und im Vorfeld einer Projektierung eine genaue Analyse der notwendigen Rahmenbedingungen durchgeführt werden.
- Es ist zu prüfen, ob alle Anwendungen, die auf virtuellen IT-Systemen betrieben werden sollen, durch ihre Hersteller auf der gewählten Virtualisierungsplattform unterstützt werden.
- Bei der Entscheidung, welche virtuellen IT-Systeme gemeinsam auf einem Virtualisierungsserver ausgeführt werden dürfen, muss der Schutzbedarf der einzelnen virtuellen IT-Systeme berücksichtigt werden.
- Die einzusetzende Virtualisierungssoftware muss eine ausreichende Isolation und Kapselung der virtuellen IT-Systeme gewährleisten. Dies bedeutet insbesondere, dass die einzelnen virtuellen IT-Systeme nur über festgelegte Wege miteinander kommunizieren und nur über definierte Kanäle auf die Hard-/Software des Virtualisierungsservers zugreifen können.
- Auf den eigentlichen Virtualisierungsservern, das heißt außerhalb der virtuellen IT-Systeme, sollten möglichst nur solche Dienste betrieben werden, die zur Virtualisierungstechnik gehören.
- Bei der Auswahl der Hardware für Virtualisierungsserver ist darauf zu achten, dass Systeme beschafft werden, die für die gewählte Virtualisierungslösung geeignet sind. Jeder Virtualisierungsserver muss so leistungsfähig sein, dass für alle virtuellen IT-Systeme, die auf diesem Virtualisierungsserver ablaufen sollen, genügend Performance bereitsteht.
- Der Umgang mit Snapshots muss geregelt werden.
- Die Verwaltungsschnittstellen der Virtualisierungsserver sollten in einem eigenen Netz angeschlossen werden. Dieses ist physisch oder logisch von dem Netz zu trennen, in dem die virtuellen IT-Systeme betrieben werden.

- Beim Einsatz von Virtualisierung kann es Probleme mit der Systemzeit geben. Es muss sichergestellt werden, dass die Systemzeit in den virtuellen IT-Systemen stets korrekt ist.
- Viele Hersteller stellen für die virtuellen IT-Systeme so genannte Gastwerkzeuge zur Verfügung, mit denen die virtuellen IT-Systeme auf einfache Weise durch die Virtualisierungssoftware gesteuert werden können. Es sind verbindliche Regelungen zur Konfiguration und zum Einsatz dieser Gastwerkzeuge in virtuellen IT-Systemen zu erstellen.

Die Sicherheitsempfehlungen zum Thema *Virtualisierung* müssen zielgruppengerecht aufbereitet und institutionsweit veröffentlicht werden. Weitere Informationen zum Thema *Virtualisierung* finden sich im Baustein B 3.304 *Virtualisierung* und in weiteren Bereichen der IT-Grundschutz-Kataloge.

G 2.29 Softwaretest mit Produktionsdaten

Vielfach ist zu beobachten, dass Softwaretests mit Produktionsdaten vollzogen werden. Als wesentliche Gründe werden hierfür angeführt, dass nur im direkten Vergleich mit vorhandenen Arbeitsergebnissen eine abschließende Beurteilung über die Funktion und Performance des Produktes möglich ist. Darüber hinaus sind mangelndes Sicherheitsbewusstsein, überzogenes Vertrauen in die zu testende Software und Unkenntnis über mögliche schädliche Auswirkungen ursächlich für diese Vorgehensweise.

Beim Test mit Produktionsdaten kann es zu folgenden Problemen kommen:

- Software wird mit Kopien von Produktionsdaten in isolierter Testumgebung getestet:
  Wenn neue Software mit nicht anonymisierten Daten getestet wird, erhalten evtl. nicht befugte Mitarbeiter, bzw. Dritte, die mit dem Softwaretest beauftragt worden sind, hierbei Einblick in Dateien mit evtl. vertraulichen Informationen.
- Software wird mit Produktionsdaten im Wirkbetrieb getestet:
  Fehlfunktionen von Software während des Testens können über den oben geschilderten Fall hinaus beispielsweise dazu führen, dass neben der Vertraulichkeit der Produktionsdaten auch deren Integrität und Verfügbarkeit beeinträchtigt werden.
  Aufgrund der Inkompatibilität unterschiedlicher Programme können Seiteneffekte auftreten, die bei anderen Systemkomponenten zu nachhaltigen Beeinträchtigungen führen können. Bei vernetzten Systemen kann das von Performanceverlusten bis hin zum Systemabsturz des Netzes reichen.
  Durch fehlerhaftes Verhalten der zu testenden Software oder Bedienfehler können Produktionsdaten ungewollt verändert werden. Möglicherweise wird diese Veränderung nicht festgestellt. Da Datenbestände, um unnötige Redundanz zu vermeiden, zunehmend durch unterschiedliche Programme gemeinsam genutzt werden, können sich diese Fehler auch auf andere IT-Anwendungen auswirken. Im Schadensfall ist nicht nur der Aufwand für die Rekonstruktion der Daten notwendig, darüber hinaus müssen bereits erstellte Arbeitsergebnisse auf ihre Integrität überprüft werden.

G 2.32 Unzureichende Leitungskapazitäten

Bei der Planung von Netzen wird oft der Fehler begangen, die Kapazitätsauslegung ausschließlich anhand des aktuellen Bedarfs vorzunehmen. Dabei wird übersehen, dass die Kapazitätsanforderungen an Netze stetig steigen, z. B. wenn neue IT-Systeme in das Netz integriert werden oder das übertragene Datenvolumen zunimmt.

Wenn die Kapazität des Netzes nicht mehr ausreicht, wird die Übertragungsgeschwindigkeit und gegebenenfalls auch die Erreichbarkeit im Netz für die jeweiligen Benutzer stark eingeschränkt. Beispielsweise werden Dateizugriffe auf entfernte IT-Systemen erheblich verzögert, wenn gleichzeitig das Netz von anderen Benutzern stark in Anspruch genommen wird.

Beispiel:

In einem Gebäude werden zusätzliche PC-Arbeitsplätze geschaffen, indem Räume zu Großraumbüros umgewidmet werden. Der Anschluss der Endgeräte wird durch einfache Hubs und Switches im jeweiligen Büro und durch "fliegende" Verkabelung realisiert. Mit der Einführung neuerer System- und Anwendungssoftware, die stetig Updates aus dem Internet oder von Management-Servern der Institution lädt, kommt es zu gravierenden Störungen normaler Arbeitsabläufe, weil das Datenvolumen der Updates die vorhandene Leitungskapazität überfordert.

G 2.37 Unkontrollierter Aufbau von Kommunikationsverbindungen

Beim Einsatz von Kommunikationskarten innerhalb eines IT-Systems (Fax-, Modem- oder ISDN-Karten) ist für den Benutzer nicht immer offensichtlich, was außer seinen Nutz- und Protokollinformationen zusätzlich übertragen wird. Nach Aktivierung einer Kommunikationskarte ist es grundsätzlich möglich, dass diese, ohne Initiierung durch den Benutzer, Verbindungen zu einer nicht gewünschten Gegenstelle aufbaut oder, über dem Benutzer nicht bekannte Remote-Funktionalitäten, durch Dritte angesprochen wird.

Beispiele:

- Bei der erstmaligen Konfiguration einer Faxkarte wurde der Benutzer vom Installationsprogramm nach der Landesvorwahl von Schweden gefragt. Zu vermuten ist, dass der Kartenhersteller über den Einsatz seines Produkts, eventuell aus Gründen des Produkt-Marketings, informiert werden wollte.
- Eine große Anzahl von Modem-Karten unterstützt den ferngesteuerten Zugriff auf IT-Systeme. Zwar lassen sich diese Zugriffe über teilweise sogar auf den Karten integrierte Mechanismen (Callback-Option und Rufnummernauthentisierung) absichern, voreingestellt ist dies jedoch nicht. Ein so konfiguriertes IT-System lässt sich, über die Modemkarte, von außen vollständig manipulieren.

G 2.60 Fehlende oder unzureichende Strategie für das Netz- und Systemmanagement

Werden für die Bereiche Netzmanagement und/oder Systemmanagement keine organisationsübergreifenden Managementstrategien festgelegt, kann es insbesondere in mittleren und großen Netzen mit mehreren Managementdomänen durch Fehlkoordination der einzelnen Subdomänen zu schwerwiegenden Problemen durch Fehlkonfiguration kommen, die bis hin zu völligem Systemzusammenbruch auf Netzebene führen können.

Aus diesem Grund ist die Festlegung und Durchsetzung einer Managementstrategie zwingend erforderlich. Im folgenden werden einige Beispiele für Probleme durch eine fehlende oder unzureichende Strategie für das Netz- und Systemmanagement gegeben.

Fehlende Bedarfsanalyse vor Festlegung der Managementstrategie

Um eine Netz- und/oder Systemmanagementstrategie festlegen zu können, ist eine vorangehende Bedarfsanalyse durchzuführen. Ohne die Feststellung des Managementbedarfs (etwa: Welche verwaltbaren Netzkoppelelemente existieren? Wie dynamisch ist der zu verwaltende Softwarebestand?) können Anforderungen an die Managementstrategie nicht formuliert werden. Da die Managementstrategie zudem Einfluss auf das zu beschaffende Softwareprodukt hat, kann dies zu Fehlentscheidungen führen.

Wird dann z. B. ein Managementprodukt eingeführt, das einen zu geringen Funktionsumfang besitzt, so kann diese Funktionslücke zusätzlich zu einem Sicherheitsproblem werden, da die nötige Funktion "von Hand" bereitgestellt werden muss. In größeren Systemen kann dies dann leicht zu Fehlkonfigurationen führen.

Beschaffung von nicht managebaren Komponenten

Wird ein Rechnerverbund mit Hilfe eines Netz- und/oder eines Systemmanagementsystems verwaltet, so ist bei der Beschaffung neuer Komponenten darauf zu achten, dass sie in das jeweilige Managementsystem integrierbar sind, damit sie in das Management einbezogen werden können. Ist dies nicht der Fall, so fällt mindestens zusätzlicher Verwaltungsaufwand an, da auch auf den nicht mit dem Managementsystem verwalteten Komponenten die festgelegte Managementstrategie durchgesetzt werden muss. Da jedoch diese Komponenten insbesondere nicht in die automatisierten Verwaltungsabläufe des Managementsystems integriert sind, kann es hier zu Fehlkonfigurationen kommen. Dies birgt durch nicht abgestimmte Konfigurationen ein Sicherheitsrisiko.

Nicht koordiniertes Managen von benachbarten Bereichen (Communities, Domänen)

Existieren in einem durch ein Managementsystem verwalteten Rechnernetz mehrere Verwaltungsbereiche, die jeweils von einem eigenen Systemmanager betreut werden, so sind deren Kompetenzen durch die Managementstrategie eindeutig festzulegen. Ist dies nicht der Fall, kann es durch unkoordiniertes Management einzelner Komponenten zu Sicherheitsproblemen kommen.

Werden z. B. einerseits einzelne Komponenten wie Netzkoppelelemente fälschlicherweise von zwei Verwaltungsbereichen verwaltet (dies kann etwa geschehen, wenn keine unterschiedlichen SNMP-"Passwörter" (Community

Strings) verwendet werden), so führt das unkoordinierte Einstellen von Konfigurationsparametern unter Umständen zu Sicherheitslücken.

Werden andererseits Komponenten (etwa Drucker) gemeinsam von zwei Verwaltungsbereichen genutzt und wurde z. B. die Vertrauensstellung des jeweils anderen Verwaltungsbereiches (z. B. Windows NT Netzwerkfreigaben) nicht korrekt eingerichtet, so kann dies unbeabsichtigt zu Sicherheitsproblemen führen, wenn nun auch unberechtigten Dritten der Zugriff gestattet wird.

Nicht integrierte Verwaltungssoftware

Beim Verwalten von mittleren und großen Systemen kann es vorkommen, dass nach Einführung des Managementsystems neue Komponenten in das System integriert werden sollen, deren Verwaltung Funktionen erfordern, die das eingesetzte Managementsystem nicht unterstützt. Dies gilt insbesondere für den Bereich Applikationsmanagement. Wird zur Verwaltung der neuen Komponente nun eine Verwaltungssoftware eingesetzt, die nicht in das eingesetzte Managementsystem integriert werden kann (z. B. über eine Programmierschnittstelle, oder durch den Einsatz von so genannten Gateways), so ist ein koordiniertes Einbinden in das Managementsystem nicht möglich. Dadurch unterliegt die neue Komponente jedoch nicht dem "automatisierten" Management, was ein Verwalten "von Hand" nötig macht. Die festgelegte Managementstrategie muss nun für zwei Systeme umgesetzt werden, dies kann jedoch zu Fehlkonfigurationen führen, die Sicherheitslücken bedingen können.

G 2.148 Fehlerhafte Planung der Virtualisierung

Die Einführung von Virtualisierungservern in ein Rechenzentrum bedeutet, dass eine neue Klasse von IT-Systemen in Betrieb genommen werden muss. Ein Virtualisierungsserver ist meist nicht nur ein Server, der den Betrieb virtueller IT-Systeme ermöglicht. Vielmehr integriert er die virtuellen IT-Systeme in das Rechenzentrum und steuert dabei deren Anbindung an weitere Infrastrukturelemente wie z. B. Netze und Speichernetze. Aus Sicht der virtuellen IT-Systeme stellt der Virtualisierungsserver also einen Bestandteil der Rechenzentrumsinfrastruktur dar.

In einer klassischen IT-Infrastruktur werden die (physischen) IT-Systeme häufig in einem arbeitsteiligen Prozess verwaltet. Die einzelnen Strukturelemente der IT-Infrastruktur werden von Administratoren betrieben, die sich auf die von ihnen betreuten IT-Systeme spezialisiert und konzentriert haben. In einer virtualisierten IT-Infrastruktur hingegen sind einzelne Strukturelemente der vorher getrennten Infrastruktur in einem Virtualisierungsserver zusammengefasst. Hierdurch verlagert sich möglicherweise ein Teil der Betriebsverantwortung für diese Rechenzentrumsressourcen von den spezialisierten Administratoren auf die Administratoren der Virtualisierungsserver.

Es verändert sich durch die Einführung der Virtualisierung auch die Sichtweise auf einen Informationsverbund insgesamt. Werden Infrastrukturkomponenten sowie eine Vielzahl von (virtuellen) Servern und (virtuellen) Arbeitsstationen innerhalb eines Virtualisierungsservers abgebildet, können die Unterschiede zwischen einem physischen und einem logischen Informationsverbund nicht wahrgenommen werden. Damit ist die logische Struktur nicht mehr klar erkennbar.

Fehlende oder mangelhafte Planung der Rollen und Verantwortlichkeiten

Virtualisierungsserver beinhalten meist auch einen großen Teil der für den Betrieb eines virtuellen IT-Systems notwendigen Infrastrukturkomponenten in virtueller Form. Diese Infrastrukturkomponenten, wie beispielsweise Switches oder Network-Attached-Storage-Systeme, werden sonst durch dedizierte Komponenten bereitgehalten. Dies bedeutet, dass Netzverbindungen eines virtualisierten IT-Systems nicht wie sonst üblich durch einen Switch, sondern in der Regel durch den Virtualisierungsserver bereitgestellt, verwaltet und überwacht werden. Ähnliches gilt für Speicherplatz in Speichernetzen und andere Ressourcen.

Wird beim Einsatz der Virtualisierungsserver nicht geplant, auf welche Weise die Server technisch und organisatorisch in das Rechenzentrum zu integrieren sind, besteht die Gefahr, dass

- die Verantwortlichkeiten für unterschiedliche Bereiche wie z. B. Anwendungen, Betriebssysteme und Netzkomponenten nicht klar definiert sind,
- sich die Zuständigkeiten für unterschiedliche Bereiche überschneiden oder
- eine passende Rechtestruktur, um administrative Zugriffsmöglichkeiten für die unterschiedlichen Bereiche zu trennen, nicht vorhanden ist.

Für Infrastrukturelemente, wie z. B. Switches oder Speichernetze, sind im klassischen Rechenzentrumsbetrieb häufig verschiedene Personen mit voneinander getrennten Rollen verantwortlich. Durch eine nicht ausreichend konzeptionierte Virtualisierung können jedoch diese Rollenkonzepte zur Administration

unterlaufen werden. So haben die Administratoren der virtuellen Infrastruktur weitreichenden Zugriff auf die Gastsysteme, auf deren Kommunikationsverbindungen und die durch sie verarbeiteten und bereitgestellten Informationen. Werden hier unklare oder womöglich keine Regelungen zur Verteilung und Delegation der Aufgaben zwischen den Administratoren getroffen oder wichtige Aspekte in der Planung übersehen und nicht berücksichtigt, können verantwortlichen Personen notwendige Informationen fehlen. In der Folge können durch Fehler, wie z. B.

- unzureichende Bestimmung der Ressourcenanforderungen für die Virtualisierungsinfrastruktur,
- nicht ausreichende Analyse der Performanceanforderungen der zu virtualisierenden Systeme,
- ungenügende Planung und Beschaffung von Infrastrukturkomponenten für Netze und Speichernetze,
- unzureichende Abstimmung der Infrastrukturkomponenten auf die virtuelle Infrastruktur und
- fehlende Integration der Virtualisierungsserver sowie ihrer virtuellen Infrastrukturkomponenten und der virtuellen IT-Systeme in vorhandene Monitoringsysteme weitreichende, negative Folgen für den gesamten Informationsverbund entstehen.

Fehlende Einsatzplanung für Virtualisierungsserver

Wird für den Einsatz der Virtualisierungsserver nicht sichergestellt, dass die virtuellen IT-Systeme auf einheitlich konfigurierten Virtualisierungsservern betrieben werden und damit eine einheitliche Infrastruktur vorfinden, können beim Betrieb der virtuellen IT-Systeme Probleme auftreten. Als Beispiel sei hier die Virtualisierungsechnik *Live Migration* genannt. Sie erlaubt es, ein virtuelles IT-System von einem Virtualisierungsserver auf einen anderen zu verschieben:

- Wird ein virtuelles IT-System in der Virtualisierungsinfrastruktur verschoben, kann es möglicherweise auf eine Ressource zugreifen, auf die ein Zugriff aus Gründen der Vertraulichkeit und Integrität nicht möglich sein sollte.
- Zum Anderen könnte bedingt durch eine fehlerhaft geplante Virtualisierungsinfrastruktur der Zugriff eines virtuellen IT-Systems auf eine benötigte Ressource wie z. B. Namensauflösung (DNS) nach einer *Live Migration* nicht mehr möglich sein. Dies kann unmittelbare Folgen für die Verfügbarkeit eines virtuellen IT-Systems haben.

Werden die Hardwareaustattung der Virtualisierungsserver nicht detailliert geplant und keine Vorgaben für die Beschaffung der notwendigen Hardwarekomponenten gemacht, könnten für das gewählte Virtualisierungsprodukt inkompatible Komponenten beschafft werden. Dies kann Nachteile für die Herstellerunterstützung für das gewählte Produkt haben. Weiterhin ist es möglich, dass z. B. bestimmte Prozessoreigenschaften, wie Intel VT und AMD-V fehlen, die für den Betrieb der Virtualisierungslösung zwingend notwendig sind.

Sind die Hardwarekomponenten, die für eine Farm von Virtualisierungsservern beschafft werden, nicht einheitlich ausgestattet, können die Verfügbarkeit und Integrität der virtuellen IT-Systeme gefährdet sein. Beispielsweise kann eine unterschiedliche Prozessorausstattung der Virtualisierungsserver zu Stabilitätsproblemen der virtuellen IT-Systeme führen. Stehen bestimmte Prozessoreigenschaften auf einem Virtualisierungsserver nicht zur Verfügung, wenn ein virtuelles IT-System mittels *Live Migration* dorthin verschoben wird, kann das virtuelle IT-System abstürzen.

Fehlerhafte Netzintegration

Im Rechenzentrumsbetrieb haben sich bestimmte Verfahren zur Integration von Servern und ähnlichen Systemen in die Netzinfrastruktur herausgebildet. Diese Verfahren, wie beispielsweise MAC-Filter, dienen dazu, die Verfügbarkeit sowie Integrität und Vertraulichkeit der Netzverbindungen zu schützen. Werden diese Verfahrensweisen nicht beachtet und geeignet angepasst, ist es möglich, dass Maßnahmen, die für physische Systeme geeignet sind, für den Betrieb virtueller Systeme negative Folgen haben. Werden MAC-Filter auf den Switchports der Virtualisierungsserver ungeeignet eingerichtet, können einige Virtualisierungsfunktionen wie die *Live Migration*, also das Verschieben laufender virtueller IT-Systeme zwischen Virtualisierungsservern, nicht funktionieren. In einem solchen Fall verliert die verschobene virtuelle Maschine ihre Netzverbindung, da ihre (virtuelle) MAC-Adresse auf dem Switch-Port des neuen Virtualisierungsservers abgewiesen wird.

Fehlerhafte Integration in Speichernetze

Die Besonderheiten der Virtualisierungsserver beim Zugriff auf Speichernetze müssen schon bei der Planung geeignet berücksichtigt werden. Virtualisierungsserver benötigen Zugriff auf alle *iSCSI*- und *Fibre Channel*-Ressourcen eines Speichernetzes, die für den Betrieb der virtuellen IT-Systeme notwendig sind. Virtuelle IT-Systeme greifen in der Regel nicht mit eigenen *iSCSI*- oder *Fibre Channel*-Schnittstellen auf solche Ressourcen zu, sondern nutzen dazu die entsprechenden Schnittstellen der Virtualisierungsserver. Daher benötigen die Virtualisierungsserver auch den Zugriff auf Ressourcen, die eigentlich nur durch die virtuellen IT-Systeme genutzt werden sollen, da die Virtualisierungsserver diese Ressourcen den virtuellen Systemen sonst nicht zur Verfügung stellen können. Werden also im Vorfeld der Inbetriebnahme unklare Regelungen getroffen oder bleiben funktionale sowie zeitliche Anforderungen bei der Planung unbeantwortet, sind Störungen der Verfügbarkeit, Vertraulichkeit und Integrität im weiteren Lebenszyklus der Virtualisierungsumgebung möglich.

Wenn Virtualisierungsserver im Rechenzentrum eingesetzt werden sollen, besteht die Gefahr, dass durch eine nicht an die Virtualisierung angepasste Segmentierung des Speichernetzes (SAN) Gefährdungen entstehen. Es kann beispielsweise dazu kommen, dass virtuelle IT-Systeme den Zugriff auf von ihnen benötigte Ressourcen verlieren, wenn sie zwischen Virtualisierungsservern verschoben werden. Die Verfügbarkeit der von ihnen bereitgestellten Dienste ist damit gefährdet. Andererseits kann eine ungeeignete Planung der Speichernetzintegration dazu führen, dass zu weitreichende Zugriffsmöglichkeiten auf die Speichernetze eingeräumt werden. Dies kann die Vertraulichkeit von in diesen Speichernetzen abgelegten Informationen gefährden.

Fehlende Einsatzplanung für virtuelle IT-Systeme

Planungsfehler können auch in anderen Bereichen entstehen, in denen bestehende Verfahrensweisen nicht überprüft werden, wenn Virtualisierung eingesetzt werden soll. Werden in den Bereichen Serverbeschaffung und -bereitstellung sowie Betriebssysteminstallation die im Rechenzentrum üblichen Verfahrensweisen nicht angepasst, kann es zu einem oder mehreren der folgenden Probleme kommen:

- Die fehlende Eignung einzelner Betriebssysteme, Dienste oder Anwendungen für die gewählte Virtualisierungsumgebung ist nie ganz auszuschließen. Weiterhin können Anpassungen der Virtualisierungsserver an die auf ihnen betriebenen virtuelle IT-Systeme bzw. deren Betriebssysteme und Anwendungen notwendig sein. Dies kann bei einer unzurei-

chenden Überprüfung durch qualifiziertes Fachpersonal sowie einer unangemessenen Synchronisation der Projektbeteiligten untereinander möglicherweise unentdeckt bleiben. In der Folge können beim weiteren Betrieb der Virtualisierungsserver bzw. der virtuellen IT-Systeme Performanceprobleme oder Verarbeitungsfehler auf Grund von Inkompatibilitäten der eingesetzten Applikationen mit der eingesetzten Virtualisierungslösung auftreten. Hierdurch ist sind besonders die Integrität und Verfügbarkeit von Informationen gefährdet, die auf den virtuellen IT-Systemen verarbeitet werden.

- Wird nicht geprüft, ob für die Applikationen, die auf virtuellen IT-Systemen betrieben werden sollen, bestimmte Hardwarekomponenten (wie z. B. Softwareschutzmodule (*Dongles*) oder ISDN-Karten), benötigt werden, die mit der gewählten Virtualisierungslösung genutzt werden können, kann es zu erheblichen Verzögerungen bei der Installation dieser IT-Systeme kommen. Möglicherweise kann ein solches System gar nicht virtualisiert werden, oder es muss erst eine mit der Virtualisierungslösung kompatible Komponente beschafft werden.
- Werden virtuelle IT-Systeme (virtuelle Server, Arbeitsstationen und Switches) nicht vollständig inventarisiert, fehlt der Überblick über die im Rechenzentrum überhaupt betriebenen IT-Systeme. Dies kann dazu führen, dass

  - beispielsweise zu wenige Betriebssystem- oder Anwendungslizenzen vorhanden sind, und die Institution somit unterlizenziert ist,
  - IT-Systeme betrieben werden, für die keine Betriebsdokumentation besteht oder die nicht durch die Sicherheitskonzepte der Organisation erfasst werden,
  - IT-Systeme betrieben werden, deren Einsatzzweck unbekannt ist (siehe hierzu auch G 5.66 *Unberechtigter Anschluss von IT-Systemen an ein Netz*),
  - IT-Systeme ohne die notwendige Planungs- und Betriebsvorbereitungen in Betrieb genommen werden,
  - IT-Systeme nicht nach den allgemeinen Regeln der Institution ausgesondert und aus den Inventarlisten gestrichen werden.

G 2.149 Nicht ausreichende Speicherkapazität für virtuelle IT-Systeme

Virtualisierungsserver benötigen für den Betrieb der virtuellen IT-Systeme Speicherplatz, der entweder lokal im Virtualisierungsserver selbst oder in einem Speichernetz bereitgestellt wird. Werden die hierfür benötigten Speicherkapazitäten nicht ausreichend groß geplant, bestehen weitreichende Risiken für die Verfügbarkeit der virtuellen IT-Systeme und die Integrität der in ihnen verarbeiteten Informationen. Dies gilt insbesondere dann, wenn spezielle Virtualisierungsfunktionen, wie Snapshots oder die Überbuchung von Speicherplatz, genutzt werden. Engpässe können nicht nur den Speicherplatz auf Festplatten oder in Speichernetzen betreffen, sondern auch den Arbeitsspeicher (RAM).

Virtualisierungsfunktionen wie Snapshots belegen zusätzlichen Speicherplatz

Das Einfrieren und Speichern von Betriebszuständen virtueller IT-Systeme (*Snapshots*), erfordert ausreichenden Speicherplatz. So werden der Inhalt der virtuellen Massenspeicher und unter Umständen auch die Zustände von Hauptspeicher und Prozessor auf die Festplatte geschrieben, wenn ein Snapshot erzeugt wird. Zusätzlich wird bei einigen Virtualisierungslösungen während der Laufzeit des Gastsystems eine Differenzdatei erzeugt. Diese Differenzdatei bildet zusammen mit dem Urzustand der Daten, der vor der Erstellung des Snapshots auf dem virtuellen Datenträger vorlag, den aktuellen Inhalt der virtuellen Festplatte. Auch Standby-Funktionen, die es ermöglichen, virtuelle Maschinen im laufenden Betrieb anzuhalten, verwenden eine ähnliche Technik und belegen somit Speicherressourcen bis der Betrieb fortgesetzt wird.

Überbuchung von Speicherplatz

Eine weitere Besonderheit virtueller Umgebungen ist, dass Speicherplatz überbucht werden kann. Das heißt, es wird kein fester Speicherplatz reserviert, wenn einem virtuellen IT-System eine bestimmte Speicherkapazität zugeordnet wird. Stattdessen wird der Speicherplatz dem virtuellen IT-System in den physisch vorhandenen Ressourcen erst dann zugeteilt, wenn er durch das virtuelle IT-System tatsächlich genutzt wird. Für das virtuelle System sind dann beispielsweise einhundert Gigabyte sichtbar, tatsächlich verbraucht dieses jedoch nur den aktuell genutzten Speicherplatz.

Der überbuchte Speicherplatz kann zum Beispiel durch einen anwachsenden Dateicontainer realisiert werden, der auf einer physisch im Virtualisierungsserver installierten Festplatte oder in einem Speichernetz abgelegt wird. Dieser Container wird immer größer, je stärker er genutzt wird. Werden innerhalb des virtuellen IT-Systems, das diesen Container nutzt, Daten gelöscht, wird der Container in der Regel jedoch nicht automatisch wieder kleiner.

Unabhängig davon, ob der Datenträger, auf dem der Container des virtuellen IT-Systems abgelegt wurde, lokal oder im Netz vorliegt, ist dessen Größe durch den physisch zur Verfügung stehenden Speicherplatz begrenzt. Ohne eine umsichtige Planung der erforderlichen maximalen Kapazitäten führt dies leicht zu Problemen. Ist der Speicher zu stark überbucht worden, steht möglicherweise vorzeitig kein freier Platz mehr zur Verfügung. Der Speicherbedarf des virtuellen IT-Systems kann dann im physischen Medium nicht gedeckt

werden und es kommt für die hiervon betroffene virtuelle Maschine zu einer Fehlersituation. Denn obwohl aus Sicht des virtualisierten IT-Systems freier Speicher nutzbar scheint, kann durch den Virtualisierungsserver kein weiterer Speicher für das Gastsystem bereitgestellt werden. Viele Virtualisierungsprodukte behelfen sich in einer solchen Situation damit, auf die von der Überbuchung betroffenen virtuellen Festplatten nur noch lesenden Zugriff zu gestatten, um die bis dahin vorhandenen Daten zu schützen. Hierdurch kann es dazu kommen, dass Daten auf diesen virtuellen Festplatten inkonsistent werden. Möglicherweise fällt das virtuelle IT-System sogar komplett aus, wenn z. B. das Betriebssystem des virtuellen IT-Systems die auftretenden Fehler nicht ausgleichen kann. Andere Virtualisierungslösungen legen automatisch einen Snapshot der betroffenen Systeme an und schalten diese Systeme danach aus, wenn der physische Speicher nicht mehr ausreicht.

Durch dieses Vorgehen ist die Verfügbarkeit der Dienste dieser virtuellen IT-Systeme gestört. Überdies wird der Betrieb aller durch den Virtualisierungsserver ausgeführten Gastsysteme in gleicher Weise behindert, wenn alle disponierbaren physischen Ressourcen des Virtualisierungsservers erschöpft sind.

Beispiel:

Ein international aktives Handelsunternehmen nutzt ein ERP-System *(Enterprise Resource Planning)*, um verschiedene Prozesse, unter anderem im Einkauf, zu automatisieren und zu unterstützen. Um den im Außendienst tätigen Handelsagenten des Unternehmens den Zugriff auf das ERP-System zu ermöglichen, stellt das Unternehmen eine Terminalserverfarm bereit, die von den Handelsagenten verwendet wird, um ihre Einkäufe zu verbuchen und an der Unternehmenskommunikation (Intranet und E-Mail) teilzunehmen. Die Plattform muss ständig zur Verfügung stehen, da die Handelsagenten im Warentermingeschäft tätig sind und es daher auf den genauen Zeitpunkt der Einkäufe ankommt, um einen guten Preis zu erzielen.

Aus Kostengründen entscheidet sich die Unternehmensleitung, die Terminalserverfarm und die ERP-Systeme künftig als virtuelle IT-Systeme zu betreiben. Bei der Analyse der bestehenden physischen Systeme stellt das Planungsteam fest, dass die Festplatten der bestehenden Systeme nur zu einem kleinen Teil ausgelastet sind. Bei einigen Datenbanksystemen tritt allerdings gelegentlich ein erhöhter Platzbedarf auf, wenn die monatliche Auswertung der Einkaufskennzahlen durchgeführt wird. Dieser Speicherplatz wird allerdings sofort wieder freigegeben, wenn die Auswertung beendet ist.

Des Weiteren wird geplant, bei einem Versionswechsel im ERP-System die Snapshot-Funktion der Virtualisierungsserver einzusetzen. Da es bei den Aktualisierungen gelegentlich zu Fehlern kommt, soll diese Funktion genutzt werden, um die Änderungen schnell wieder rückgängig machen zu können. Eine zeitraubende Wiederherstellung des Zustands vor der Aktualisierung kann sich im Warentermingeschäft schnell negativ auf den Geschäftserfolg auswirken. Aus diesem Grunde sind die Snapshot-Funktionen der Virtualisierungsserver ein wichtiger Faktor für die Einführung der Virtualisierungstechnik in diesem Unternehmen.

Da der Festplattenplatz der physischen Systeme nur gering ausgelastet ist, wird davon ausgegangen, dass dieser als Reserve für die Snapshots ausreichend groß ist. Daher wird beschlossen, in dem für die virtuellen IT-Systeme aufgebauten Speichernetz nur soviel Speicher vorzusehen, wie aktuell insgesamt in den physischen Systemen vorhanden ist. Dies wurde als ausreichend angesehen, da bei einer Aktualisierung der physischen Systeme auch nicht

mehr Speicher verbraucht werden könnte, als tatsächlich physisch vorhanden ist.

Kurz vor dem Monatsende wird eine Aktualisierung der ERP-Software durchgeführt. Hierbei müssen die ERP-Systeme selbst sowie die Terminalserver aktualisiert werden, da die neuen und dringend benötigten Funktionen nur dann genutzt werden können, wenn auch die Client-Software auf den Terminalservern ausgetauscht wird. Um möglichen Fehlfunktionen vorzubeugen, ist vor der Aktualisierung ein Snapshot aller Systeme, der ERP-Systeme und der Terminalserver, erzeugt worden. Der Snapshot wurde nach der Erzeugung der monatlichen Kennzahlen erzeugt, um bei einem Fehlschlag der Aktualisierung die Kennzahlen auf der Basis der alten Software schnell zur Verfügung zu haben.

Ab diesem Zeitpunkt werden alle Veränderungen an den Festplattencontainern der virtuellen IT-Systeme in eine Differenzdatei geschrieben und der Speicherverbrauch im Speichernetz steigt sprunghaft an. Es ist nicht bedacht worden, dass durch den Snapshot die bei der Aktualisierung der Software ersetzten Dateien nicht wie vorher physisch überschrieben werden, sondern im Snapshot weiterhin vorhanden sind. Der Speicherbedarf für die Aktualisierung der virtuellen IT-Systeme hat sich dadurch verdoppelt.

Als nun die monatliche Auswertung durchgeführt wird, geht der Speicherplatz im Speichernetz gänzlich zur Neige und es können keine weiteren Daten mehr geschrieben werden. Auch hier ist wiederum nicht beachtet worden, dass der Platz für die Auswertung in der Differenzdatei neu belegt werden muss. Der für die Auswertung zuständige Administrator des virtuellen IT-Systems hat die Speicherknappheit innerhalb der virtuellen Festplatte bemerkt und deshalb die alte Auswertung vor Erzeugung der neuen gelöscht. Allerdings hat dieses Vorgehen keine Auswirkung auf den physisch belegten Speicherplatz, da der für die Auswertung der Alt-Daten verwendete physische Speicherplatz jetzt Bestandteil des Snapshots ist.

Die Virtualisierungssoftware schützt die virtuellen IT-Systeme automatisch vor Datenverlust und -inkonsistenz, indem die virtuellen IT-Systeme angehalten werden. Dadurch fallen alle Terminalserver und alle ERP-Systeme vollständig und gleichzeitig aus. Die Handelsagenten sind von der Unternehmenskommunikation abgeschnitten und können über den Ausfall nicht informiert werden. Hierdurch verzögern sich die auf dem Warenterminmarkt getätigten Geschäfte und das Unternehmen muss wesentlich höhere Preise für die eingekauften Waren bezahlen.

Bevor die ausgefallenen Systeme wieder in Gang gebracht werden konnten, musste freier Speicherplatz für die virtuellen IT-Systeme geschaffen werden. Die Administratoren standen vor der Wahl, die virtuellen IT-Systeme wieder auf den Snapshot zurückzusetzen oder eine Speichererweiterung im Speichernetz vorzunehmen. Da die Terminalserverfarm und das ERP-System schnell wieder verfügbar sein mussten, wurde entschieden, die Systeme auf den Snapshot zurückzusetzen. Die Personalkosten für die Aktualisierung der Systeme mussten daher abgeschrieben werden.

Nachdem der für eine Aktualisierung der ERP-Software unter Verwendung von Snapshots tatsächlich benötigte Speicherplatz korrekt ermittelt worden ist, wurde eine Speichererweiterung des Speichernetzes vorgenommen. Die dringend benötigten Funktionserweiterungen der aktualisierten Software konnten erst genutzt werden, nachdem diese Erweiterung erfolgt war.

G 2.150 Fehlerhafte Integration von Gastwerkzeugen in virtuellen IT-Systemen

Mittels Gastwerkzeugen, wie z. B. den *Citrix XenTools* oder den *VMware Tools*, können die virtuellen IT-Systeme in der Virtualisierungsinfrastruktur durch den Administrator vom Virtualisierungsserver aus gesteuert und verwaltet werden. Des Weiteren integrieren diese Programme Treiber und Dienste zur Kommunikation der virtualisierten Betriebssysteme mit dem Host.

Über die Gastwerkzeuge werden verschiedene Funktionen verwirklicht, wie z.B.:

- Synchronisation der Systemzeit einer virtuellen Maschine mit dem Host,
- Anforderung von Hauptspeicher im virtuellen IT-System und Freigabe dieses Speichers für andere Gäste auf dem Virtualisierungsserver (Ballooning),
- Herunterfahren des Betriebssystems des virtuellen IT-Systems ohne Anmeldung,
- Optimierung virtueller Festplatten (Thin Provisioning).

Die Gastwerkzeuge verfügen im Kontext der virtuellen Maschine über weitreichende Berechtigungen auf Systemdateien und -dienste um die beschriebenen Funktionen zu ermöglichen. Diese Funktionen können einem etablierten Berechtigungskonzept sowie weiteren Anforderungen an die virtuelle Umgebung widersprechen, wenn die vorhandenen Konzepte und Anforderungen bei der Planung der Installation der Gastwerkzeuge nicht beachtet und umgesetzt werden. Dadurch können eventuell Funktionen genutzt werden, die mit den Richtlinien der Organisation nicht vereinbar sind.

Herunterfahren eines virtuellen IT-Systems ohne erforderliche Berechtigung

Wurde beispielsweise in einer Organisation festgelegt, dass virtuelle und physische Server grundsätzlich nur nach der Anmeldung eines zuständigen Administrators und unter Angabe einer Begründung heruntergefahren werden dürfen, können die Gastwerkzeuge dazu genutzt werden, diese Vorgaben zu umgehen. Mittels der Gastwerkzeuge ist es dem Administrator eines Virtualisierungsservers möglich, ein beliebiges, anderes virtuelles IT-System herunterzufahren. Dazu muss er selbst nicht notwendigerweise ein berechtigter Administrator des betreffenden virtuellen IT-Systems sein. Die Administratoren der Virtualisierungsserver können damit die für die virtuellen IT-Systeme bestehenden Richtlinien und Regelungen zur Nutzung von Systemen unterlaufen und somit die Verfügbarkeit, Integrität und Vertraulichkeit der virtuellen IT-Systeme gefährden.

Es gibt weiterhin Virtualisierungsprodukte (wie z.B. *VMware Workstation, VMware Server*), die umfangreiche Funktionen besitzen, um in eine Entwicklungsumgebung integriert zu werden. Hier gibt es für die Gastwerkzeuge in virtuellen IT-Systemen über die oben angegebenen Möglichkeiten hinaus zusätzliche Funktionen. So können Skripte für Testzwecke in einem virtuellen IT-System hinterlegt und durch Gastwerkzeuge von außen gesteuert werden. Dazu ist keine Interaktion mit und auch keine Authentisierung an dem virtuellen IT-System selbst notwendig. Die Aktionen werden nur durch die Virtualisierungssoftware bzw. den Hypervisor und die Gastwerkzeuge initiiert. Werden nun virtuelle IT-Systeme aus Entwicklungsumgebungen in die virtuelle Infrastruktur für den Produktivbetrieb übernommen, können Sicherheitslücken in der Pro-

duktivumgebung entstehen, da die speziellen für die Entwicklungsumgebung vorgesehenen Werkzeuge und Schnittstellen in der Produktivumgebung weiterhin wirksam sind.

Beispiel:

Eine Behörde plant die Aktualisierung einer komplexen Client-/Serveranwendung. Mit der Aktualisierung wird ein externes Beratungsunternehmen beauftragt. Die Entwicklung und der Test der Aktualisierungsschritte erfolgt in einer virtuellen Umgebung, die ein vollständiges Abbild der Produktivumgebung darstellt. Die Testsysteme sind Kopien der Produktivsysteme, die in einem abgeschotteten Netz bereitgestellt wurden.

Einer der externen Berater ist für die Aktualisierung der Clientanwendung zuständig. Die Installation der Anwendung ist auf dem Client recht komplex. Zudem müssen bei jeder Neuinstallation bestimmte festgelegte Konfigurationsschritte auf dem Server durchgeführt werden, damit die neue Clientversion funktionieren kann. Sind die Daten auf dem Server migriert, können Clients mit einer alten Softwareversion nicht mehr auf den Server zugreifen.

Um die immer gleichen Konfigurationsschritte nicht immer wieder manuell durchführen zu müssen, hat der externe Berater Skripte erstellt. Diese sollen zum einen den Client bei jedem Neustart neu konfigurieren und zum anderen über die Gastwerkzeuge Skripte auf dem Server installieren und ausführen.

Der zuständige Referatsleiter möchte sich über den Projektfortschritt informieren und bittet einen seiner Mitarbeiter darum, ihm den Client vorzuführen. Da noch keine Installationspakete für die Clientsoftware in der Produktivumgebung existieren, entscheidet sich der Mitarbeiter, das virtuelle Arbeitsplatzsystem des externen Beraters zu kopieren. Er transferiert es in das Produktivnetz und startet es, um es seinem Vorgesetzten zu demonstrieren.

Im Hintergrund werden jetzt die im Client integrierten Skripte des externen Beraters aktiviert und der Produktivserver der Behörde wird damit auf die neue Version aktualisiert. Die Mitarbeiter können nicht mehr auf den Server zugreifen und es kommt zu einem mehrstündigen Produktionsausfall, da eine Datenwiederherstellung durchgeführt werden muss.

G 2.151 Fehlende Herstellerunterstützung von Applikationen für den Einsatz auf virtuellen IT-Systemen

Die Virtualisierungstechnik nimmt erst seit wenigen Jahren außerhalb der Mainframe-Welt (*IBM Z-Series, Siemens BS2000, SUN Enterprise 25000*) stärkeren Einfluss auf das Design von Rechenzentren und erst seit ca. 2005 werden vermehrt auch produktive IT-Systeme virtualisiert. Vorher wurden virtuelle IT-Systeme hauptsächlich in Entwicklungs- und Testumgebungen eingesetzt. Es existiert eine große Anzahl unterschiedlicher Virtualisierungsprodukte, die zudem auf unterschiedlichen technischen Ansätzen (Server- und Betriebssystemvirtualisierung) beruhen. Daher ist bisher noch keine Standardisierung eines virtuellen IT-Systems erfolgt, wie dies beispielsweise für IT-Systeme möglich ist, die auf x86- oder x64-Hardware beruhen.

Anwendungen werden durch ihren Hersteller in der Regel für eine bestimmte Kombination aus Betriebssystem und Hardwareplattform freigegeben. d. h., sie unterstützen den Benutzer der Anwendung beispielsweise bei der Fehlersuche, wenn die Anwendung auf der freigegebenen Hardwareplattform mit dem entsprechenden Betriebssystem betrieben wird. Da jedoch noch keine Standardisierung der Hardwareplattform "virtuelles IT-System" erfolgt ist, können keine allgemeinen Aussagen der Anwendungshersteller dazu gemacht werden, inwieweit die Installation ihrer Anwendung auf einem beliebigen virtuellen IT-System unterstützt wird.

Virtuelle IT-Systeme können auf der Basis von völlig unterschiedlichen Virtualisierungstechniken (Server- oder Betriebssystemvirtualisierung) betrieben werden und daher stark unterschiedliche Eigenschaften haben. In virtuellen IT-Systemen, die auf Betriebssystemvirtualisierung (*SUN Solaris Zones, Parallels Virtuozzo*) basieren, also multiple Instanzen eines einzigen Betriebssystems darstellen, können beispielsweise unterschiedliche, betriebssystemnahe Softwarebibliotheken oder unterschiedliche Betriebssystemkerne nicht oder nur sehr eingeschränkt verwendet werden. Eine solche Einschränkung existiert bei virtuellen Systemen, die auf einer vollständigen Servervirtualisierung (z. B. *Citrix XenServer, Microsoft HyperV, QEMU*, *Sun VirtualBox*, *VMware ESX*) beruhen, in der Regel nicht, sodass eine allgemeingültige Aussage für alle denkbaren virtuellen IT-Systeme gleich welcher Virtualisierungstechnik nicht möglich ist.

Aus den vorgenannten Gründen geben Hersteller den Betrieb ihrer Anwendungen auf virtuellen IT-Systemen nicht generell frei, sondern erteilen diese Freigaben gegebenenfalls nur für bestimmte Kombinationen aus Betriebssystem und konkreten Virtualisierungsprodukten. Wird nicht geprüft, ob eine solche Freigabe existiert, besteht die Gefahr, dass Begleitung und Hilfe ("Support") bei aufgetretenen Schwierigkeiten abgelehnt oder eingeschränkt werden.

Beispiel:

Ein großes Unternehmen betreibt ein umfangreiches ERP-System, das aus einer Vielzahl von Servern besteht. Das ERP-System besteht aus mehreren Datenbanksystemen und circa 30 Anwendungs- und 80 Webservern. Mit dem Hersteller des ERP-Systems hat das Unternehmen einen Pflege- und Supportvertrag geschlossen, in dem der Hersteller seine Unterstützung bei auftre-

tenden Problemen zusichert. An den Supportvertrag ist die Bedingung gebunden, dass die ERP-Systeme mit dem Betriebssystem Windows Server 2003 auf physischer Hardware betrieben werden müssen. Für virtuelle Systeme behält sich der Hersteller eine Einzelfallprüfung vor und erteilt keine generelle Freigabe.

Das Unternehmen möchte die Serversysteme, auf denen das ERP-System betrieben wird, durch neue Systeme ersetzen, da die bestehenden Systeme mittlerweile recht alt geworden sind und sich Hardwarestörungen häufen. Die zuständigen Administratoren berichten, dass die einzelnen Server, vor allem die Anwendungs- und Webserver, nicht sehr stark ausgelastet sind und Lastspitzen nicht auf allen Systemen gleichzeitig auftreten, sondern sich auf die Systeme über den Tag verteilen. Aus diesen Gründen wird entschieden, die Anwendungs- und Webserver zu virtualisieren und in einer virtuellen Infrastruktur aus mehreren Virtualisierungsservern zu betreiben. Das Unternehmen wählt für die Anwendungsserver eine Servervirtualisierungslösung und für die Webserver ein Produkt, das auf Betriebssystemvirtualisierung basiert. Gerade die Betriebssystemvirtualisierung wird für die Bereitstellung einer großen Menge von Webservern als besonders geeignet angesehen, da hier sehr große Konsolidierungseffekte erzielt werden können, also sehr viele virtuelle Instanzen auf einem Virtualisierungsserver betrieben werden können. Die Administratoren erwarten mit der Virtualisierung der Server keine Probleme, die mit der Virtualisierungssoftware zusammen hängen könnten, und gehen davon aus, dass keine virtualisierungsbedingten Störungen auftreten werden.

Nachdem die ERP-Systeme ohne Rückfrage bei dem Hersteller der ERP-Software virtualisiert worden sind, läuft die ERP-Anwendung eine Zeit lang störungsfrei. Nach einigen Monaten bemerkt allerdings ein Mitarbeiter, dass Fehler im Lagerhaltungsmodul der ERP-Software auftreten. Es wird festgestellt, dass die über einen Webserver von den Lagerarbeitern eingegebenen Zu- und Abgänge im Lager falsch verarbeitet werden. Das ERP-System löst nun automatisch Bestellungen aus, obwohl noch genügend Ware im Lager vorhanden ist. Bei anderen Waren, die für die Produktion dringend benötigt werden, weist das ERP-System aber zu hohe Lagerbestände aus, was dazu führt, das keine Nachbestellungen ausgelöst werden und die Produktion stillsteht. Hierdurch entsteht dem Unternehmen durch den Produktionsausfall ein Schaden in großer Höhe.

Die Administratoren des ERP-Systems befassen sich mit dem Problem und vermuten im Zusammenspiel von Webserver und Anwendungsserver ein Übertragungsproblem, das zu der fehlerhaften Verarbeitung führt. Sie können allerdings keine Lösung dafür finden und wenden sich an den Hersteller. Der Hersteller lässt sich die Konfiguration der ERP-Server und automatisch erzeugte Reports zusenden, die er prüft, um den Fehler eingrenzen und beheben zu können.

Nachdem der Hersteller des ERP-Systems festgestellt hat, dass die Server auf virtuellen Plattformen betrieben werden, teilt er dem Unternehmen mit, dass das ERP-System auf einer nicht freigegebenen und damit unterstützten Plattform läuft. Der Hersteller hat ein Timing-Problem als Ursache ermittelt und lehnt die weitere Bearbeitung ab, da er vermutet, dass das Problem mit der Virtualisierung der Systeme zusammenhängt. Er fordert das Unternehmen auf, das Einsatzszenario auf nicht virtualisierter Hardware nachzustellen, um die Virtualisierung als Problemursache auszuschließen.

Das Unternehmen ist nun gezwungen, leihweise eine große Anzahl an physischen Servern für den Nachbau des Einsatzszenarios zu beschaffen. Dieser

Nachbau ist sehr komplex und zeitaufwendig. Die Fehlerbehebung wird dadurch zudem erheblich verzögert.

Es stellt sich heraus, dass der Fehler auch auf den physischen Servern auftritt und es damit weitgehend ausgeschlossen ist, dass die Virtualisierung der Server ursächlich für den Fehler war. Daraufhin setzt der ERP-Hersteller seine Bemühungen fort und das Problem wird nach eingehender Analyse auch vollständig gelöst.

Das Unternehmen, das das ERP-System nutzt, fordert nun Schadensersatz vom Hersteller der Software für die Kosten, die durch die Reproduktion des Fehlers auf physischen Servern entstanden ist, sowie die verlorene Arbeitszeit und den Produktionsausfall in der Zeit, die während des Aufbaus der Parallelumgebung aufgetreten ist. Das Unternehmen steht auf dem Standpunkt, dass die Problemlösung durch den Softwarehersteller unnötig verzögert worden ist, da die Virtualisierung sich nicht als problemverursachend herausgestellt hat. Der Hersteller wiederum verweist dagegen auf den Wortlaut des Pflege- und Supportvertrages und lehnt eine Haftung ab. Weiterhin betont er, dass er das Timing-Problem, das zu der Vermutung führte, das aufgetretene Problem hänge mit der Virtualisierung zusammen, nur aus Kulanz ermittelt hat, er hätte die Problembearbeitung auch vollständig ablehnen können. Es kommt zu einem Gerichtsverfahren, das der Hersteller der ERP-Software gewinnt.

G 3.16 Fehlerhafte Administration von Zugangs- und Zugriffsrechten

Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen dürfen nur in dem Umfang eingeräumt werden, wie sie für die Wahrnehmung der Aufgaben erforderlich sind. Werden diese Rechte fehlerhaft administriert, so kommt es zu Betriebsstörungen, falls erforderliche Rechte nicht zugewiesen wurden, bzw. zu Sicherheitslücken, falls über die notwendigen Rechte hinaus weitere vergeben werden.

Beispiel:

Durch eine fehlerhafte Administration der Zugriffsrechte hat ein Sachbearbeiter die Möglichkeit, auf die Protokolldaten zuzugreifen. Durch gezieltes Löschen einzelner Einträge ist es ihm daher möglich, seine Manipulationsversuche am Rechner zu verschleiern, da sie in der Protokolldatei nicht mehr erscheinen.

G 3.28 Ungeeignete Konfiguration der aktiven Netzkomponenten

Durch eine ungeeignete Konfiguration der Netzkomponenten kann es zu einem Verlust der Verfügbarkeit des Netzes oder Teilen davon, zu einem Verlust der Vertraulichkeit von Informationen oder zu einem Verlust der Datenintegrität kommen. Dabei können insbesondere die folgenden Fehlkonfigurationen unterschieden werden:

- Aktive Netzkomponenten, die zur Bildung von VLANs (Virtual LANs) eingesetzt werden, segmentieren das Netz logisch. Im Fall einer Fehlkonfiguration kann ggf. die Kommunikation innerhalb eines VLANs, zwischen einzelnen oder zwischen allen VLANs zum Erliegen kommen. In Abhängigkeit der VLAN-Strategie des betreffenden Herstellers betrifft dies zum einen die Zuordnung von miteinander kommunizierenden Systemen zu den gleichen VLANs, zum anderen auch das VLAN-Routing, insofern ein solches durch die aktiven Netzkomponenten unterstützt wird.
  Beispiel: Bei VLANs, die nur über Router miteinander kommunizieren können, werden die zentralen Infrastrukturserver, die beispielsweise Datei- und Druckdienste bereitstellen, nicht gleichzeitig auch den VLANs der Arbeitsplatzsysteme zugeordnet, Router sind ebenfalls nicht vorhanden. In diesem Fall können einige Arbeitsplatzsysteme die Dienste der zentralen Infrastrukturserver nicht nutzen, da diese in einem nicht erreichbaren Teilnetz sind.
- Ein Netz kann durch den Einsatz von Routern mittels Teilnetzbildung strukturiert werden. Für eine Kommunikation zwischen den Teilnetzen ist eine entsprechende Konfiguration der Router erforderlich, die hierzu die Leitwege zwischen den verschiedenen Teilnetzen in Routing-Tabellen vorhalten müssen. Routing-Tabellen können statisch oder dynamisch verwaltet werden. In beiden Fällen ist eine Kommunikation zwischen unterschiedlichen Teilnetzen nicht möglich, wenn die Routing-Tabellen keinen Leitweg zwischen den betreffenden Teilnetzen enthalten. Zu einer Fehlkonfiguration kann es dementsprechend durch eine fehlerhafte Definition statischer Routing-Tabellen oder durch eine fehlerhafte Konfiguration der Routing-Protokolle (wie z. B. RIP oder OSPF) kommen, die zum automatischen Abgleich dynamischer Routing-Tabellen verwendet werden.
  Beispiel: Eine Router-zu-Router-Verbindung ist durch einen statischen Eintrag der entsprechenden IP-Adressen konfiguriert. Bei einer Änderung der IP-Adresse einer der Router oder durch das Zwischenschalten eines weiteren Routers ist diese Kommunikationsstrecke nicht mehr verfügbar.
- Aktive Netzkomponenten, die in der Lage sind, Protokolle oder Netzadressen zu filtern, können mit dieser Technik eine Kommunikation bestimmter Protokolle unterbinden oder eine Kommunikation zwischen Systemen mit bestimmten Netzadressen verhindern. Eine Fehlkonfiguration der betreffenden Filter kann entsprechend zu einer unerwünschten Unterbindung der Kommunikation in Abhängigkeit des fehlkonfigurierten Filters und der Art der Fehlkonfiguration führen.
  Ebenso können fehlkonfigurierte Filter dazu führen, dass Verbindungen aufgebaut werden, die Eindringlingen die Möglichkeit bieten, Angriffe gegen IT-Systeme im geschützten Netz durchzuführen. Je nach Art des Angriffs kann daraus ein Verlust der Verfügbarkeit einzelner Netzkomponenten oder auch des ganzen Netzes resultieren. Weiterhin können z. B. durch die mögliche Manipulation der Verbindungswege Datenpakete umgeleitet werden oder Datenpakete verändert oder mitgelesen werden.

Beispiele:

- Ein Multiport-Repeater ist so konfiguriert, dass nur Systeme mit bestimmten MAC-Adressen an bestimmte Ports angeschlossen werden können. Nach einem Austausch der Netzkarte in einem der Endgeräte und der damit verbundenen Änderung der MAC-Adresse, wird dieses System keine Verbindung mehr zum Netz bekommen (Verlust der Verfügbarkeit).
- Durch eine ungeeignete Konfiguration von aktiven Netzkomponenten (insbesondere von VLANs oder Filterregeln) können Broadcast-Domänen unnötig groß werden oder es können unnötige Kommunikationsverbindungen entstehen. Dadurch kann es Unbefugten möglich sein, vertrauliche Daten zu lesen.

G 3.36 Fehlinterpretation von Ereignissen

Beim Einsatz eines Managementsystems ist es eine Aufgabe des jeweils verantwortlichen Systemadministrators, die Meldungen des Managementsystems zu analysieren und zu interpretieren, um dann geeignete Maßnahmen einzuleiten. In der Regel basieren die Meldungen des Managementsystems auf Überwachungsmechanismen, die Systemprotokolle unterschiedlichster Art automatisch nach gewissen Regeln durchsuchen. Es ist dabei nicht einfach, aus der Fülle der anfallenden Protokolldaten automatisiert Anomalien, die auf Systemfehler hindeuten, zu erkennen und entsprechende Meldungen an den Systemadministrator zu erzeugen. Darüber hinaus kann ein Fehler hier sogar unentdeckt bleiben. Die eingehenden Meldungen müssen daher immer vom Systemadministrator gesichtet und interpretiert werden, da die Meldungen (im Fehlerfall) auf Fehlersymptome und deren (automatischer) Interpretation beruhen. Ein Systemadministrator muss hier auch Fehlalarme und Falschmeldungen erkennen können. Werden Systemmeldungen vom Administrator falsch interpretiert, so führen vermeintlich korrigierende Gegenmaßnahmen u. U. zu einer Verschlimmerung der Situation.

G 3.79 Fehlerhafte Zuordnung von Ressourcen des SAN

Betriebssysteme reagieren unterschiedlich auf sichtbare Speicherressourcen. Wenn keine eindeutige und starke Zuordnung von Servern und Speicherressourcen vorgenommen wird, können unautorisierte Zugriffe auf Speicherressourcen, z. B. durch andere Server, das Schutzkonzept auf Ebene des Betriebssystems oder der Anwendung unterlaufen.

An dieser Stelle ist nicht nur der vorsätzliche Angriff zu betrachten, bei dem ein Angreifer versucht, Lücken der Konfiguration für seine Absichten auszunutzen. Beachtlich ist auch die Eigenart mancher Betriebssysteme, alle erreichbaren Festplatten an sich zu binden und in die eigene Hardwarekonfiguration einzubinden.

Gerade Windows Server neigen dazu, alle sichtbaren Speicherressourcen zu beanspruchen. Bei einem Speichernetz kann es so vorkommen, dass Speicherbereiche, die anderen Systemen zugeordnet sind, diesen entzogen werden oder Daten darauf verfälscht oder zerstört werden.

G 3.99 Fehlerhafte Netzanbindungen eines Virtualisierungsservers

Netzverbindungen für virtuelle IT-Systeme

Ein Virtualisierungsserver sorgt für die Netzzugänge der auf ihm betriebenen virtuellen IT-Systeme. Hierzu stellt er in der Regel den virtuellen IT-Systemen eine emulierte Netzkarte zur Verfügung. Diese wiederum ermöglicht es den virtuellen IT-Systemen, auf Netze oder Speichernetze zu zugreifen. Diese (Speicher-) Netze können entweder physische oder virtuelle Netze sein.

Damit virtuelle IT-Systeme physische Netze nutzen können, muss der Virtualisierungsserver eine Verbindung der virtuellen Netzkomponenten der virtuellen IT-Systeme zu den physischen Netzen ermöglichen. Dies wird dadurch realisiert, dass der Virtualisierungsserver seine physischen Interfaces den virtuellen IT-Systemen zur Verfügung stellt. Die Verfahrensweise ist bei den verschiedenen Virtualisierungsprodukten unterschiedlich. Es gibt jedoch zwei wesentliche Prinzipien, wie der Übergang von virtuellen zu physischen Netzkomponenten realisiert wird:

- durch direkte Zuordnung von virtuellen zu physischen Netzen. Die Netzkarte eines virtuellen IT-Systems wird direkt einer physikalischen Schnittstelle des Virtualisierungsservers zugeordnet.
- durch indirekte Zuordnung. Die (virtuellen) Netzkarten der virtuellen IT-Systeme werden mit einem virtuellen Switch verbunden. Dieser wird vom Virtualisierungsserver in Software nachgebildet. Der virtuelle Switch wiederum kann mittels einer physischen Netzkarte mit dem physischen Netz verbunden sein. Da ein virtueller Switch nicht zwingend einen physischen Netzübergang besitzen muss, kann auf diese Weise ein Netz realisiert werden, in dem die daran angeschlossenen virtuellen IT-Systeme keine Verbindung nach außen besitzen. Eine solche Konfiguration kann zum Beispiel für Testsysteme genutzt werden, die keine Außenverbindungen benötigen.

Innerhalb der Verwaltungssoftware des Virtualisierungsservers werden die Netzschnittstellen der virtuellen IT-Systeme den physikalischen Schnittstellen des Virtualisierungsservers zugeordnet. Wird diese Zuordnung fehlerhaft vorgenommen, kann eine virtuelle Maschine mit einem falschen Netz verbunden werden. Wird beispielsweise ein Intranet-Webserver mit vertraulichen Daten, der nur im internen Netz betrieben werden soll, auf diese Weise versehentlich am Sicherheitsgateway (Firewall) vorbei mit dem Internet verbunden, sind die vertraulichen Daten möglicherweise im Internet sichtbar.

Ein Virtualisierungsserver besitzt häufig eine im Vergleich zu sonstigen Servern große Anzahl an Netzkarten. Diese große Anzahl wird benötigt, um eine möglichst gute Integration des Virtualisierungsservers in das Netz des Rechenzentrums zu erreichen. Es wird dadurch möglich, auf einem Virtualisierungsserver virtuelle IT-Systeme zu betreiben, die in unterschiedlichen Netzsegmenten benötigt werden. Des Weiteren werden weitere Schnittstellen für verschiedene Funktionen der Virtualisierungsserver benötigt, beispielsweise für den Zugriff auf Speichernetze oder die *Live Migration*, die es erlaubt, ein laufendes virtuelles IT-System von einem Virtualisierungsserver auf einen anderen zu verschieben.

Auf Grund der für einen Server untypischen Anzahl an Netzkarten und Kabelverbindungen zu Switchen und ähnlichen IT-Systemen besteht verstärkt die Gefahr, durch eine fehlerhafte Verkabelung unbeabsichtigt Fehler in der Netzinfrastruktur zu erzeugen. Solche Fehler können neben den in G 3.4 *Unzuläs-*

sige Kabelverbindungen und G 3.29 *Fehlende oder ungeeignete Segmentierung* schon angeführten beispielsweise sein:

- Mittels zweier physischer Netzkarten des Virtualisierungsservers und einem virtuellen Switch wird fälschlicherweise eine Kopplung von zwei Netzsegmenten geschaltet (*Brücke*). Diese Netze sollten aber getrennt sein. Verbindungen zwischen diesen Netzen sollten nur durch ein Sicherheitsgateway ermöglicht werden. Durch die Falschverkabelung können nun direkte Verbindungen zwischen Systemen aufgebaut werden. Die eigentlich gewünschte Segmentierung des Netzes wird unbeabsichtigt aufgehoben.
- Zwei physische Netzkarten eines Virtualisierungsservers sind einem virtuellen Switch zugeordnet. Sie werden versehentlich mit zwei unterschiedlichen physischen Netzsegmenten verbunden. Der virtuelle Switch ist so konfiguriert, dass er auf der einen Netzschnittstelle empfangene Pakete nicht an die andere Schnittstelle weiterleitet und somit keine Brücke (s. o.) bildet. Auf Grund der zwei Netzschnittstellen, die mit unterschiedlichen Netzsegmenten verbunden sind, ist der virtuelle Switch nicht eindeutig einem physischen Segment zugeordnet. Durch diesen Fehler kommt es durch den Lastverteilungsmechanismus des virtuellen Switches dazu, das Netzpakete eines an diesen Switch angeschlossenen virtuellen IT-Systems mal in das eine, mal in das andere Netzsegment weitergeleitet werden. Hierdurch ist das virtuelle IT-System nur sporadisch im Netz erreichbar und die Verfügbarkeit des Systems gefährdet.
- Einige Virtualisierungsprodukte können eine Falschverkabelung (wie in den vorherigen zwei Fällen beschrieben) erkennen und schalten in einem solchen Fall eine oder mehrere physische Netzkarten ab. Mit welchem physischen Netzsegment der virtuelle Switch dann tatsächlich verbunden ist, kann möglicherweise nicht mehr vorhergesagt werden. Hierdurch kann es zu Verbindungsabbrüchen zu den mit dem betroffenen virtuellen Switch verbundenen IT-Systemen kommen.
- Mit zwei oder mehreren Virtualisierungsservern wird eine virtuelle Infrastruktur aufgebaut. Hierzu sollen diese Server mit mehreren physischen Netzsegmenten verbunden werden, die jeweils virtuellen Switches zugeordnet werden. Diese Switche werden korrespondierend mit dem jeweiligen physischen Segment benannt (Switch A - Segment A, Switch B - Segment B usw.). Durch einen Verkabelungsfehler wird nun auf einem der beiden Virtualisierungsserver das physische Segment A mit dem virtuellen Switch B verbunden. Wird jetzt die Funktion *Live Migration* in dieser virtuellen Infrastruktur genutzt, kommt es durch den Migrationsprozess dazu, dass sich ein virtuelles IT-System am Switch B nach einer Migration in einem anderen physischen Netzsegment befindet als vor der Migration. Der Grund dafür liegt darin, dass der Switch B auf dem einen Virtualisierungsserver mit dem Segment B, auf dem anderen jedoch mit dem Segment A verbunden ist. Die Verfügbarkeit des Systems ist dadurch gefährdet. Es besteht auch die Gefahr, dass auf die von diesem System bereitgehaltenen Daten in Netzen zugegriffen werden kann, in denen dieser Zugriff eigentlich nicht zulässig ist.
- Virtualisierungsserver benötigen zum Betrieb der virtuellen IT-Systeme meist Verbindungen zu Speichernetzen, in denen die Daten (Konfigurationsdateien, Dateicontainer virtueller Festplatten) liegen. Werden die Verbindungen zu diesen Speichernetzen fehlerhaft verkabelt, können Störungen auftreten, wenn die Virtualisierungsserver auf das Speichernetz zu greifen. Dies gefährdet die Verfügbarkeit der virtuellen IT-Systeme, die auf diesen Virtualisierungsservern betrieben werden. Hiervon kann möglicherweise eine große Anzahl virtueller IT-Systeme betroffen sein.
- Auch Fehler in der Verkabelung von Netzkarten, die die Virtualisierungsserver zur Kommunikation untereinander in einer virtuellen Infrastruktur

nutzen, haben weitreichende Folgen für deren Funktion. So basieren die Funktionen *Live Migration* und *Fault Tolerance* auf der Synchronisierung einer Kopie eines virtuellen IT-Systems auf zwei unterschiedlichen Virtualisierungsservern. Mit *Fault Tolerance* wird ein Verfahren bezeichnet, bei dem ein virtuelles IT-System auf zwei Virtualisierungsservern gleichzeitig betrieben wird, wobei nur eine Kopie aktiv, die andere passiv ist. Fällt einer der Virtualisierungsserver aus, übernimmt die auf dem weiterlaufenden Server beheimatete Kopie des virtuellen IT-Systems transparent alle Funktionen des ausgefallenen. Werden nun die Netzverbindungen, die die Virtualisierungsserver zur Synchronisation virtueller IT-Systeme für die *Live Migration* oder *Fault Tolerance* verwenden, fehlerhaft verkabelt, ist es möglich, dass diese Virtualisierungsfunktionen nicht einwandfrei funktionieren. Die Verfügbarkeit der virtuellen IT-Systeme ist aufgrund dessen gefährdet.

Netzverbindungen für Virtualisierungsserver

Die Netzverbindungen der Virtualisierungsserver werden häufig redundant ausgelegt, da von den physischen Schnittstellen eine Vielzahl von Funktionen der virtuellen Infrastruktur abhängt. Um die Verfügbarkeit von Netzschnittstellen zu steigern, werden meist mehrere Netzwerkkarten so konfiguriert, dass sie wechselweise oder sogar gleichzeitig die Funktion der jeweils anderen ausführen können. Hierzu existieren verschiedene Verfahren:

- Load Balancing: Die MAC-Adressen der virtuellen IT-Systeme werden auf der Basis eines Algorithmus auf die physischen Schnittstellen verteilt, um eine möglichst gleichmäßige Auslastung der einzelnen physischen Schnittstellen zu erreichen. Fällt eine der Schnittstellen aus, übernimmt eine der verbliebenen die Aufgabe der ausgefallenen. Hierbei wird die Netzverbindung der virtuellen IT-Systeme allerhöchstens unmerklich unterbrochen. Dieses Verfahren arbeitet mit allen gängigen physischen Switches zusammen und erfordert in der Regel keine spezielle Konfiguration dieser Switche. Load Balancing ist zwar nicht virtualisierungsspezifisch, dem Verfahren kommt jedoch beim Einsatz virtueller IT-Systeme eine besondere Bedeutung zu.
- *IEEE 802.3ad (Link Aggregation Control Protocol - LACP)* oder *Etherchannel* (Cisco) sind Protokolle, bei denen mehrere physische Schnittstellen zu einem logischen Kanal zusammengeschaltet werden. Diese Verfahren erfordern in der Regel eine angepasste Konfiguration auf dem verbundenen, physischen Switch.

Es existieren des Weiteren eine Reihe von herstellerspezifischen Bezeichnungen für verschiedene Protokolle und Verfahren zur Verfügbarkeitssteigerung von Netzwerkkarten wie *Bonding* im Linux-Umfeld, *Teaming, Port Aggregation, Link Aggregation* und *Trunking*. Hierbei erfordern einige Protokolle, dass entsprechend angepasste Konfigurationen auf den physischen Switchen vorgenommen werden müssen. Teilweise sind die Verfahren nur eingeschränkt kompatibel. Werden diese Verfahren unzulässig gemischt oder kommt es zu Missverständnissen zwischen den Administratoren der Virtualisierungsserver und denen der physischen Netzinfrastruktursysteme, können Inkompatibilitäten durch Fehlfunktionen auftreten. Die sich dabei ergebenden Verbindungsabbrüche treten häufig nur sporadisch auf und ihre Ursachen sind dementsprechend schwer zu ermitteln.

G 3.100 Unsachgemäße Verwendung von Snapshots virtueller IT-Systeme

Durch Snapshots kann der Zustand einer virtuellen Maschine zu einem beliebigen Zeitpunkt eingefroren werden. Es ist hierbei nicht von Belang, ob das System in dem Moment der Erzeugung des Snapshots läuft oder nicht. Auf diesem Weg ist es möglich, ohne aufwendigen Prozess zu dem im Snapshot konservierten Zustand des virtuellen IT-Systems zu gelangen. Der Snapshot kann auch auf einen anderen Virtualisierungsserver übertragen werden oder als Datensicherung dienen.

Wird die virtuelle Maschine nach der Erzeugung eines Snapshots weiter betrieben und der konservierte Zustand später geladen, gehen alle seitdem am Gastsystem erfolgten Änderungen verloren. Dies kann bei einer unbedachten Vorgehensweise zu Datenverlusten führen und ist bei Produktivsystemen meist unerwünscht. Auch Änderungen am Betriebssystem, Diensten und Anwendungen des virtuellen IT-Systems können so zurückgesetzt werden. Unzureichende Dateiberechtigungen, Sicherheitslücken und Schwachstellen oder auch gelöschte Benutzerkonten werden auf diese Weise erneut aktiv.

Bei virtuellen Servern, die über offene Dateien oder Datenbanksitzungen verfügen, können inkonsistente Daten entstehen. Dies ist beispielsweise der Fall, wenn Informationen durch einen Client auf den virtualisierten Server geschrieben werden, während der Snapshot erstellt wird. Der zu speichernde Dateiinhalt ist dann nicht vollständig im Snapshot enthalten. Wird der eingefrorene Zustand der virtuellen Maschine nun erneut eingesetzt, befinden sich dort mit hoher Wahrscheinlichkeit defekte Dateien oder in ihrer Integrität gestörte Datenbanken.

Verteilte Systeme wie Datenbank-Cluster oder auch Active Directory Domaincontroller nutzen in der Regel einen Replikationsmechanismus um sicher zustellen, dass ihre Daten synchronisiert werden. Hierbei können erhebliche Probleme auftreten, wenn diese auf einen Snapshot zurückgesetzt werden. Es kann in einem solchen Fall zu Inkonsistenzen in den Datenbanken kommen, die durch den Replikationsmechanismus nicht aufgelöst werden können.

Ist nicht genügend Speicherplatz für umfangreiche oder mehrere Snapshots vorhanden, kann es passieren, dass es zu Speicherplatzengpässen kommt und keine weiteren Informationen abgespeichert werden können.

Beispiel:

Ein großes Fotolabor entwickelt Filme für seine Kunden. Dazu sendet der Kunde seinen Film in einer Versandtasche ein und gibt auf dieser Tasche die Rücksendeadresse an. Alle Versandtaschen sind mit einer eindeutigen Nummer versehen. Im Labor wird den Filmen zusätzlich eine interne Bearbeitungsnummer zugeordnet. Diese interne Bearbeitungsnummer dient dazu, die Filme zu anonymisieren. Für das automatische Versandverfahren wird die Bearbeitungsnummer mit der maschinenlesbaren Versandtaschennummer in einer Datenbank abgelegt. Sind die Bilder fertig entwickelt, werden sie mittels der Bearbeitungsnummern automatisch wieder den Versandtaschen zugeordnet. Die Versandtasche wird dann dem Kunden per Post zugeschickt.

Die Geschäftsleitung des Fotolabors hat sich nun entschieden, neben anderen IT-Systemen auch das Datenbanksystem, das für die Zuordbarkeit von Bearbeitungs- und Versandtaschennummer sorgt, zu virtualisieren.

Während die Produktion im Labor läuft, stellt der zuständige Administrator fest, dass es auf dem virtuellen Datenbankserver zu einem Problem gekommen ist. Um dieses schnell zu beheben, setzt er den Server auf einen Snapshot zurück. Er weiß, dass der Server zum dem Zeitpunkt, bei dem der Snapshot erstellt wurde, einwandfrei funktionierte. Nun stimmt aber die Zuordnung von Bearbeitungs- und Versandtaschennummern nicht mehr, da auch die Tabelle mit der Zuordnung der Bearbeitungsnummern zu den Versandtaschennummern auf den Snapshot zurückgesetzt worden ist. Der Fehler bleibt beim Versand unbemerkt. In der Folge werden einigen Kunden die falschen Filme zugestellt. Sehr viele Filme können auch gar nicht mehr den Kunden zugeordnet werden und es kommt zu einem Ansehensverlust des Fotolabors, der zu starken Umsatzeinbußen führt.

G 3.101 Fehlerhafter Einsatz der Gastwerkzeuge in virtuellen IT-Systemen

Bei vielen Virtualisierungsprodukten können in den virtuellen IT-Systemen sogenannte Gastwerkzeuge installiert werden. Mit diesen Gastwerkzeugen können zum Einen die für Betriebssystemvirtualisierung notwendigen Gerätetreiber für virtuelle oder emulierte Geräte wie Netzwerkkarten, Festplatten oder Grafikkarten bereitgestellt werden. Zum Anderen stellen sie für virtuelle Maschinen eine Vielzahl anderer Funktionen bereit. Solche Funktionen sind zum Beispiel:

- Herunterfahren des Betriebssystems eines virtuellen IT-Systems ohne Interaktion im dem virtuellen IT-System direkt über den Virtualisierungsserver,
- Austausch des Inhalts der Zwischenablage zwischen der Konsolen-Emulation der virtuellen Maschine und dem Arbeitsplatzsystem des Benutzers,
- Nahtlose Integration des Mauszeigers des Arbeitsplatzsystems des Nutzers einer virtuellen Maschine mit ihrer Konsolenemulation,
- Vereinfachtes Laden und Entladen von Datenträgern in die virtuellen IT-Systeme. Dies können physische Disketten-, CD- oder DVD-Laufwerke, aber auch Abbilddateien von solchen Datenträgern sein (ISO-Images).

Diese Funktionen steigern die Bedienbarkeit der virtuellen IT-Systeme durch einen Benutzer und ermöglichen weiterhin eine automatisierte Verwaltung des Betriebszustands (Ein-/Ausschalten, Hoch- und Herunterfahren) virtueller IT-Systeme durch den Virtualisierungsserver.

Herunterfahren des Systems ohne Anmeldung / Interaktion

Wird die Funktion zum Herunterfahren eines IT-Systems durch einen Administrator des Virtualisierungsservers genutzt, werden gegebenenfalls restriktivere Konfigurationseinstellungen innerhalb des virtuellen IT-Systems selbst umgangen oder Richtlinien verletzt, die einen Neustart oder ein Herunterfahren ohne eine korrekte Autorisierung verbieten.

Zugriff auf CD- / DVD-Laufwerke oder Diskettenlaufwerke

Des Weiteren erlauben die Gastwerkzeuge bei entsprechender Konfiguration den direkten Zugriff auf Laufwerke des Virtualisierungsservers. So kann beispielsweise der Zugriff auf das im Virtualisierungsserver angeschlossene, physische CD-Laufwerk von einem virtuellen IT-System aus möglich sein. Auf eine CD-ROM mit vertraulichen Daten, die in das Laufwerk des Virtualisierungsservers eingelegt wurde, um die darauf enthaltenen Daten auf ein bestimmtes virtuelles IT-System zu übertragen, kann daher auch von anderen virtuellen Instanzen aus zugegriffen werden. Die Vertraulichkeit der Daten ist gefährdet, da möglicherweise die Daten von unberechtigten Personen gelesen wurden.

Bei einigen Virtualisierungsprodukten kann auch die CD- oder DVD-Laufwerksschublade des Virtualisierungsservers über die Gastwerkzeuge von einem virtuellen IT-Systeme aus geöffnet werden, wenn sie entsprechend konfiguriert sind. Das Laufwerk könnte beschädigt werden, wenn es beispielsweise gegen die Tür des Serverschrankes stößt oder von einer Zierblende am Servergehäuse gestoppt wird.

Beispiele:

- In einem mittelständischen Unternehmen werden mehrere Virtualisierungsserver eingesetzt. Auf diesen Servern werden mehrere virtuelle IT-Systeme betrieben. Einige davon gehören zu einem ERP-System, auf dem sämtliche kaufmännischen Anwendungen des Unternehmens betrieben werden. Dieses ERP-System wird nicht durch die gleichen Administratoren verwaltet wie die Virtualisierungsserver. Da für die Server, die zum ERP-System gehören, ein hoher Schutzbedarf festgestellt worden ist, dürfen diese Systeme nur heruntergefahren werden, wenn ein Wartungszeitraum mit den Nutzern des ERP-Systems vereinbart worden ist. Weiterhin dürfen die Server nur von dazu besonders berechtigten Administratoren heruntergefahren werden, was durch den jeweiligen Administrator des Weiteren protokolliert und dokumentiert werden muss. Um diese Richtlinie technisch umzusetzen, wurde im Betriebssystem der virtuellen IT-System die Berechtigung, die einzelnen ERP-Systeme zu stoppen, nur an die ERP-Administratoren vergeben. Weiterhin wurde das Betriebssystem so konfiguriert, dass es den Administrator zwingt, vor dem Herunterfahren den Grund dafür anzugeben.
  Bei einem der Virtualisierungsserver fällt nun ein Lüfter aus. Dies ist zwar für die Funktion des Servers nicht direkt kritisch, der defekte Lüfter sollte jedoch unverzüglich ausgetauscht werden. Der Administrator des Virtualisierungsservers vereinbart dazu mit einem Servicetechniker des Serverherstellers einen Termin für die Reparatur. Der Techniker des Herstellers erscheint am nächsten Tag im Laufe des Vormittags. Er hat das benötigte Ersatzteil dabei und möchte sofort mit der Reparatur beginnen, da er noch weitere Termine hat. Für den Austausch des Lüfters muss der Virtualisierungsserver ausgeschaltet werden. Der Administrator des Virtualisierungsservers fährt den Virtualisierungsserver nun über die Verwaltungskonsole herunter. Dabei werden alle virtuellen IT-Systeme ebenfalls über die Gastwerkzeuge automatisch heruntergefahren. Die Gastwerkzeuge fahren die Systeme ohne die erforderliche Protokollierung herunter und überprüfen auch nicht, ob der Administrator überhaupt die Berechtigung dazu hatte. Nach der Reparatur schaltet der Administrator den Virtualisierungsserver wieder ein und fährt alle virtuellen IT-Systeme wieder hoch.
  Während der Reparatur stehen wichtige Teile des ERP-Systems nicht zur Verfügung und es kommt zu einem großen Arbeitszeitverlust, da einige Mitarbeiter ihre Arbeit nicht erledigen können. Die Administratoren des ERP-Systems werden von der Geschäftsleitung des Unternehmens gerügt, da sie die Richtlinien missachtet haben sollen und nicht dafür gesorgt haben, dass die ERP-Systeme ausschließlich von berechtigten Administratoren heruntergefahren werden können, sowie Protokollierungsvorschriften ignoriert wurden.
- Der Administrator eines virtuellen IT-Systems hat Langeweile und erforscht dabei die Funktionen der auf dem virtuellen IT-System installierten Gastwerkzeuge. Er findet dabei die Funktion zum Verbinden und Trennen von physischen CD- oder DVD-Laufwerken des Virtualisierungsservers. Da er nicht weiß, dass das Öffnen der Laufwerksschublade im virtuellen IT-System tatsächlich zum Öffnen der physischen Laufwerkschublade des Virtualisierungsservers führt, spielt er mit der entsprechenden Funktion herum.
  Ein Techniker, der sich zu dieser Zeit im Serverraum befindet und Arbeiten an einem mit dem Virtualisierungsserver benachbarten IT-System durchführt, bemerkt das offene Laufwerk nicht und bleibt mit seinem Ärmel an der Schublade hängen. Dabei wird das Laufwerk beschädigt und muss ausgetauscht werden.

G 3.102 Fehlerhafte Zeitsynchronisation bei virtuellen IT-Systemen

Gängige Betriebssysteme verfügen über eine eigene interne Uhr. Die Uhrzeit wird dabei vom Betriebssystem in der Regel durch die Zählung von Prozessorzyklen und den gelegentlichen Abgleich mit einer verlässlichen Zeitquelle, wie einem Zeitserver oder einer internen Hardware-Uhr, ermittelt. Der Zeitpunkt und die Häufigkeit der Synchronisation mit der verlässlichen Zeitquelle hängt dabei vom verwendeten Betriebssystem ab.

Gastbetriebssysteme in virtuellen Umgebungen haben jedoch keine Kontrolle und Kenntnis über die tatsächlich verbrauchte Rechenzeit auf dem physischen IT-System. Die Berechnung der aktuellen Uhrzeit über die abgearbeiteten Rechenschritte als Taktgeber ist daher unzuverlässig. Je nachdem, mit welchem Algorithmus die Uhrzeit aus dem Vergleich von Prozessorzyklen und verlässlicher Zeitquelle ermittelt wird, kann die Uhr eines virtuellen IT-Systems der tatsächlichen Zeit nachlaufen oder vorauseilen. In Extremfällen kann es sogar dazu führen, dass die Uhr des Betriebssystems rückwärts läuft. Dies kann zu unerwünschten Effekten führen, die sich unter ungünstigen Umständen erheblich auf die Sicherheit der virtuellen Infrastruktur auswirken.

Beispielsweise sind Zeitstempel etwa im Dateisystem einer virtuellen Maschine mit einer falsch laufenden Uhr unzuverlässig. In der Folge können Inkonsistenzen in der Datensicherung entstehen, wenn diese über die Zeitstempel des Dateisystems ermittelt, welche Dateien zu sichern sind.

Auch die Fehlersuche bei Problemen wird nachhaltig behindert, da die zeitliche Abfolge der Ereignisse, die zu dem Problem geführt haben, nicht zuverlässig ermittelbar ist. Überdies sind beweiskräftige Aussagen bei Sicherheitsvorfällen mit inkorrekten Zeitstempeln in Ereignisprotokollen schlimmstenfalls unmöglich, da die Korrelation von Ereignissen über die Zeitstempel nicht möglich ist.

Werden in virtuellen IT-Systemen Verfahren zur Authentisierung genutzt, die auf korrekten Zeitstempeln für die Übermittlung von Authentisierungsschlüsseln basieren (z. B. Kerberos), können Anmeldungen fehlschlagen.

Verschiedene verteilte Datenbanksysteme und Verzeichnisdienste wie Active Directory nutzen Zeitstempel zur Konsistenzprüfung bei Replikationsvorgängen. Sind diese Zeitstempel unzuverlässig, können Inkonsistenzen in diesen Systemen auftreten.

Beispiel:

Ein Unternehmen hat sich für den Fernzugang für Telearbeiter für eine auf Token basierende Authentisierungsmethode entschieden. Auf den Token werden in bestimmten zeitlichen Abständen regelmäßig neue Passphrasen erzeugt, die zusammen mit dem Benutzernamen und dem Passwort eingegeben werden müssen. Die Token, die von den Benutzern mitgeführt werden, sind mit einer internen Uhr ausgestattet, die mit der Uhrzeit des Authentisierungsservers synchronisiert ist.

Nachdem der Authentisierungsserver virtualisiert wurde, können sich die Benutzer nach kurzer Zeit nicht mehr anmelden, da die angezeigten Einmalpasswörter nicht mehr mit denen auf dem Authentisierungsserver übereinstimmen. Die Ganggenauigkeit der Uhr in der virtuellen Umgebung reicht dazu nicht aus.

G 4.74 Ausfall von IT-Komponenten in einer virtualisierten Umgebung

Innerhalb einer klassischen IT-Infrastruktur werden Serverbetriebssysteme und deren Dienste, aber auch die Betriebssysteme der Arbeitsplatzrechner auf physikalischen IT-Systemen ausgeführt. Die zum Betrieb der Serversysteme notwendigen Infrastruktur-Komponenten (Netzkomponenten, Speichernetze und ähnliches) werden ebenfalls verteilt auf verschiedenen physikalischen IT-Systemen bereitgestellt.

In einer virtualisierten Umgebung hingegen werden die Serversysteme sowie Teile der notwendigen Infrastrukturkomponenten als eigene Server-Instanzen zu einem großen Teil durch die Virtualisierungsserver selbst bereitgestellt. Wenn also ein virtueller Server beispielsweise auf das Netz zugreift, so greift er nicht auf ein physikalisches IT-System wie einen Switch zu, sondern auf eine durch den Virtualisierungsserver zur Verfügung gestellte Komponente, die nur als Software, aber nicht als eigene Hardware betrieben wird.

Fällt ein physikalisches IT-System aus, kann oftmals noch mit den restlichen Systemen weiter gearbeitet werden. Zwar sind die Dienste, die durch den ausgefallenen Server bereitgestellt werden, nicht länger verfügbar, dies betrifft jedoch nicht zwingend alle anderen installierten Server. Ist beispielsweise ein Datenbankserver ausgefallen, kann dennoch der Zugriff auf den Dateiserver erfolgen. Nicht alle Geschäftsprozesse, die durch den Informationsverbund unterstützt werden, sind also betroffen.

Im Gegensatz dazu werden in einer virtualisierten IT-Infrastruktur in der Regel zahlreiche und unterschiedliche Instanzen virtualisierter IT-Systeme (Gäste) technisch auf wenigen physikalischen Maschinen zusammengeführt (konsolidiert). Hierdurch erhöhen sich die Auswirkungen auf die Verfügbarkeit bei Störungen eines Virtualisierungsservers erheblich. Bei Beschädigungen von physikalischen Komponenten des Virtualisierungsservers oder einer Fehlfunktion in dessen Betriebssystem werden alle darauf ablaufenden virtuellen IT-Systeme in Mitleidenschaft gezogen.

Beim Ausfall eines IT-Systems können die Daten beschädigt werden, die von diesem System verarbeitet werden. Es entsteht gegebenenfalls ein höherer Aufwand, um das System wieder in Betrieb zu nehmen, da die Daten möglicherweise aus der Datensicherung wieder hergestellt werden müssen. Es können auch Daten unwiederbringlich verloren gegangen sein. Fallen nun mehrere virtuelle IT-Systeme aufgrund eines Fehlers eines Virtualisierungsservers gleichzeitig aus, steigt die Wahrscheinlichkeit, dass mindestens eines der ausgefallenen Systeme von einer solchen Beschädigung betroffen ist. Daher kann es in einem solchen Fall zu einer längeren Betriebsunterbrechung kommen, als es beim Ausfall nur eines IT-Systems der Fall gewesen wäre.

Im Rechenzentrumsbetrieb hängen viele Dienste voneinander ab. Zum Beispiel benötigt ein Mailsystem einen Verzeichnisdienst, um Empfängeradressen den Postfächern zuzuordnen. Ein System zur Auftragsverwaltung benötigt das Mailsystem, um eingehende und ausgehende Aufträge zu verarbeiten. Es erstellt außerdem automatisch Aufträge im Warenwirtschaftssystem, um die Abarbeitung der Kundenaufträge zu unterstützen. Zudem greift das Warenwirtschaftssystem auf die Datenbank der Lagerverwaltung zu, um Lagerbestände zu überwachen.

Der Ausfall von einzelnen Komponenten des Informationsverbundes kann dazu führen, dass ebenso Dienste, die im Rechenzentrum bereitgestellt werden,

teilweise ausfallen. Werden nun mehrere IT-Systeme als virtuelle IT-Systeme auf einem Virtualisierungsserver betrieben, fallen mit dem Virtualisierungsserver zusammen gleich mehrere Komponenten eines Informationsverbundes aus. Hierdurch kann es zu einer stärkeren Beeinträchtigung des IT-Betriebs kommen, als es im klassischen, nicht virtualisierten Rechenzentrumsbetrieb der Fall wäre.

Beispiel:

Ein mittelständisches Unternehmen hat sich für die Verwendung einer Virtualisierungslösung entschieden. Es wird geplant, einige sehr leistungsfähige Server zu beschaffen und die Anzahl physikalischer Systeme stark zu reduzieren.

Auf den Virtualisierungsservern wurden IT-Systeme und deren Dienste nach Aspekten wie Prozessorlast und Speicherverbrauch verteilt. Dabei wurde überlegt, wie die virtuellen IT-Systeme auf die Virtualisierungsserver optimal verteilt werden können.

Das Unternehmen nutzt ein Mailsystem, das auf einem Verzeichnisdienst beruht. Dazu wird ein Buchhaltungssystem betrieben, das in einen Anwendungsserver und einen Datenbankserver aufgeteilt ist. Die weiterhin noch genutzten Warenwirtschafts- und Lagerhaltungssysteme verwenden ebenfalls die Buchhaltungsdatenbank für den Austausch von Daten.

Da der Datenbankserver des Buchhaltungssystems und der Mailserver zu den IT-Systemen mit den größten Performanceanforderungen gehören, wurde entschieden, sie auf getrennten Virtualisierungsservern zu betreiben. Dadurch soll erreicht werden, dass diese sich während des Betriebs nicht gegenseitig beeinträchtigen. Die weitere Analyse der Performanceanforderungen der Systeme ergab dabei, dass ein optimaler Konsolidierungsseffekt erreicht werden kann, wenn die virtuellen IT-Systeme wie folgt verteilt werden:

Erster Virtualisierungsserver: Datenbank, Verzeichnisdienst

Zweiter Virtualisierungsserver: Mailsystem, Buchhaltungssystem

Dritter Virtualisierungsserver: Warenwirtschafts-, Lagerhaltungssystem

Durch einen beschädigten Elektrolytkondensator auf der Hauptplatine des ersten Virtualisierungsservers kommt es zum Ausfall dieses Servers. Auf diesem Server befanden sich getrennt in virtuellen Maschinen die Datenbank für das Buchhaltungssystem und der Verzeichnisdienst der Firma.

Der Wegfall dieses einen physikalischen Servers hat insgesamt weitreichende Konsequenzen für den IT-Betrieb. Zwar liegen die Applikationsserver der Buchhaltung sowie der Lager- und Warenwirtschaft auf anderen Virtualisierungsservern, sind jedoch auf einen Datenaustausch mit der Datenbank angewiesen, um ordnungsgemäß zu funktionieren. In dem Unternehmen fielen zentrale Prozesse vollständig aus, sodass es zu einem Stopp der Auslieferung der Kundenaufträge kam und durch den Ausfall des Warenwirtschafts- und Lagerhaltungssystems ein mehrstündiger Produktionsausfall hingenommen werden musste.

Weiterhin konnten die Kunden des Unternehmens nicht sofort wie vertraglich vereinbart per E-Mail über den Produktionsausfall unterrichtet werden, da das Mailsystem ebenfalls ausgefallen war. Dadurch verletzte das Unternehmen wesentliche Pflichten aus seinen Lieferverträgen und musste neben den durch

den Produktionsausfall verursachten Kosten auch noch Vertragsstrafen übernehmen.

G 4.75 Störung der Netzinfrastruktur von Virtualisierungsumgebungen

Mehrere Virtualisierungsserver können zu einer so genannten virtuellen Infrastruktur zusammengefasst werden. In einer solchen virtuellen Infrastruktur können die virtuellen IT-Systeme beliebig auf die einzelnen Virtualisierungsserver verteilt werden. Weiterhin ist es möglich, die virtuellen Maschinen zwischen den Virtualisierungsservern zu verschieben. Dies kann bei einigen Produkten auch geschehen, wenn das virtuelle IT-Systeme gerade ausgeführt wird (Beispiele: Microsoft Hyper-V Live Migration, VMware VMotion, XEN LiveMigration). Ein solcher Prozess, im Folgenden Live Migration genannt, ist in der Regel transparent für das virtuelle IT-System, d. h. es bemerkt diesen Migrationsprozess nicht. Auf dieser Migrationstechnik bauen weitere Funktionen einer virtuellen Infrastruktur auf. Dies sind Funktionen wie z. B. die dynamische Zuteilung von Prozessor- und Hauptspeicherressourcen. Hierbei wird das virtuelle IT-System immer auf den Virtualisierungsserver migriert, der die benötigten Ressourcen optimal zur Verfügung stellen kann. Ein virtuelles IT-System erhält auf diese Weise immer die bestmögliche Ressourcenzuteilung.

Es gibt des Weiteren Virtualisierungsprodukte, bei denen der Ausfall eines Virtualisierungsservers kompensiert wird, indem die davon mit betroffenen virtuellen IT-Systeme auf einem anderen Virtualisierungsserver automatisch neu gestartet werden.

Um die beschriebenen technischen Möglichkeiten zu realisieren, wird zwischen den beteiligten Virtualisierungsservern ein Kommunikationsnetz zur Koordinierung dieser Funktionen (automatischer Neustart, Live Migration) benötigt. Kommt es zu Störungen in diesem Netz, sind die hierüber koordinierten Funktionen ebenfalls gestört.

Eine Störung in der Kommunikation zwischen Virtualisierungsservern kann eine Live Migration abbrechen lassen. Hierdurch können möglicherweise Mechanismen zur dynamischen Lastverteilung fehlschlagen, wenn eine virtuelle Maschine aufgrund eines Ressourcenengpasses auf einen anderen Zielserver verschoben werden soll. In der Folge führt der nicht behebbare Ressourcenengpass auf dem Quellserver zu einer Einschränkung der Verfügbarkeit des nicht verschiebbaren IT-Systems.

Um die Verfügbarkeit virtueller IT-Systeme zu steigern, können mehrere Virtualisierungsserver zu einem Cluster miteinander verbunden werden. Die Systeme, die an einem solcher Serververbund teilnehmen, benötigen eine reibungslose Kommunikation untereinander. Mittels dieser Kommunikation überwachen sich die Systeme gegenseitig und prüfen z. B., ob die auf ihren Partnern laufenden virtuellen IT-Systeme weiterhin verfügbar sind (Heartbeat). Fällt einer der Partner des Verbundes aus, werden die ebenfalls ausgefallenen IT-Systeme, sofern möglich, auf einem anderen Virtualisierungsserver neu gestartet.

Fällt das Kommunikationsnetz des Clusters, beispielsweise aufgrund eines Hardwarefehlers auf einem Switch, aus, ist die Funktion zur Ausfallkompensation des Clusters gestört. Möglicherweise sind die virtuellen IT-Systeme auf den Virtualisierungsservern, die Mitglieder des Clusters sind, ebenfalls in ihrer Verfügbarkeit gefährdet.

Das Kommunikationsnetz zwischen den am Hochverfügbarkeitsverbund beteiligten Systemen erfüllt im Übrigen neben den vorgenannten weitere wichtige Funktionen: Fällt die Kommunikation zwischen mehreren Systemen eines Verbundes gleichzeitig aus, muss jedes System entscheiden können, ob es selbst oder die anderen Systeme von dem Ausfall betroffen sind (Isolationsproblem). Würden zwei oder mehrere an einem Hochverfügbarkeitsverbund beteiligte Virtualisierungsserver isoliert voneinander ein virtuelles IT-System mehrfach starten, können die Daten, die dieses virtuelle System repräsentieren, beschädigt werden. Dadurch kann das virtuelle IT-System unbenutzbar werden. Es kann auch zu Störungen kommen, wenn ein und dasselbe IT-System mehrfach im Netz vorhanden ist (z. B. durch doppelte IP- oder MAC-Adressen).

Anbindung von Speichernetzen

Virtuelle IT-Systeme werden in der Regel durch eine Reihe von Dateien physisch repräsentiert. Diese Dateien enthalten neben der Konfiguration des virtuellen IT-Systems beispielsweise auch die Container für virtuelle Festplatten. Werden Snapshots, also Abbilder eines virtuellen IT-Systems in einem beliebigen, auch laufenden Betriebszustand, erzeugt, speichert der Virtualisierungsserver die hierbei entstehenden Daten ebenfalls in Dateien. Diese Dateien können entweder auf dem Virtualisierungsserver selbst oder in dem dazugehörigen zentralen Speichernetz gespeichert sein.

Virtuelle Serverumgebungen aus mehreren Virtualisierungsservern sind oftmals mit zentralen Speichernetzen verbunden, damit auf die Dateien, die die virtuellen IT-Systeme repräsentieren, von mehreren Stellen aus zugegriffen werden kann. Bricht die Verbindung zu diesen Speicherressourcen ab, wirkt sich dies auf die virtuellen IT-Systeme so aus, als würde einem physischen Server im laufenden Betrieb eine Festplatte entfernt. Da auf Speicherressourcen in einem Speichernetz häufig mehr als ein virtuelles IT-System gespeichert ist, ist bei einem Ausfall die Betriebssicherheit vieler virtueller IT-Systeme gefährdet. In den von dem Ausfall betroffenen virtuellen IT-Systemen und Virtualisierungsservern können bei einem Ausfall Dateisysteminkonsistenzen auftreten, die unter Umständen umfangreiche Wiederherstellungsmaßnahmen erfordern.

G 4.76 Ausfall von Verwaltungsservern für Virtualisierungssysteme

Mittels mehrerer Virtualisierungsserver kann eine virtuelle Infrastruktur aufgebaut werden. Dabei werden die Virtualisierungsserver in einer Weise miteinander verbunden, dass die auf ihnen laufenden virtuellen IT-Systeme immer auf dem Virtualisierungsserver ausgeführt werden, der die für dieses IT-System optimale Performance bereitstellen kann. Kann ein Virtualisierungsserver einem laufenden virtuellen IT-System mehr Ressourcen zur Verfügung stellen (dynamische Ressourcenzuteilung, z. B. *Citrix XenServer Workload Balancing* oder *VMware Dynamic Resource Scheduling*), ist es sogar möglich dieses IT-System mittels einer Migration (*Live Migration*) auf das IT-System mit den freien Ressourcen zu verschieben.

Zusätzlich kann die Verfügbarkeit der virtuellen IT-Systeme durch Hochverfügbarkeitsmechanismen wie den automatischen Neustart von ausgefallenen virtuellen Maschinen gesteigert werden. Diese Funktionen erfordern bei den meisten Virtualisierungsprodukten einen zentralen Verwaltungsserver, der den Betrieb der einzelnen virtuellen Maschinen und der Virtualisierungsserver koordiniert. Virtualisierungsprodukte, die einen solchen zentralen Verwaltungsserver verwenden können, sind beispielsweise *Citrix XenServer, Microsoft Hyper-V* oder *VMware ESX*. Der Verwaltungsserver (*Citrix XenCenter*, *Microsoft System Center Virtual Machine Manager*, *SUN Management Center* oder *Vmware vCenter*) besitzt in der Regel ebenfalls eine Monitoring-Komponente, mittels derer die Funktion der virtuellen IT-Systeme und der Virtualisierungsserver überwacht werden kann.

Da über den Verwaltungsserver sämtliche Funktionen einer virtuellen Infrastruktur gesteuert und administriert werden, führt ein Ausfall dieses Verwaltungssystems dazu, dass keine Konfigurationsänderungen an der virtuellen Infrastruktur durchgeführt werden können. Die Administratoren können in dieser Zeit weder auf auftretende Probleme wie Ressourcenengpässe oder den Ausfall einzelner Virtualisierungsserver reagieren noch einen neuen Virtualisierungsserver in die Infrastruktur integrieren bzw. neue virtuelle IT-Systeme anlegen.

Auch Funktionen wie *Live Migration* und damit die dynamische Zuteilung von Ressourcen für einzelne Gastsysteme stehen nicht mehr zur Verfügung, da die Instanz, die solche Funktionen koordiniert, nicht mehr betriebsbereit ist. In der Folge kann die virtuelle Infrastruktur nicht mehr automatisch auf Ressourcenengpässe reagieren und sowohl die Performance als auch die Verfügbarkeit einzelner virtueller IT-Systeme werden nachteilig beeinflusst. Dies tritt insbesondere dann auf, wenn die Ressourcen der Virtualisierungsserver überbucht wurden.

Zusätzlich dient der Verwaltungsserver der Überwachung der Virtualisierungsserver und der auf diesen betriebenen virtuellen IT-Systeme. Liefert der Verwaltungsserver oder dessen Monitoring-Komponente falsche oder gar keine Daten, kann die Funktion der virtuellen Infrastruktur durch die Administratoren nicht mehr hinreichend überwacht werden. Es besteht damit die Gefahr, dass Ressourcenengpässe in der virtuellen Infrastruktur unbemerkt bleiben und nicht rechtzeitig für eine Erweiterung der virtuellen Infrastruktur gesorgt wird. Der Ausfall von einzelnen virtuellen IT-Systemen kann möglicherweise ebenfalls nicht rechtzeitig festgestellt werden, wenn die Überwachung der virtuellen Infrastruktur ausgefallen ist.

Weiterhin kann sogar der Ausfall von Virtualisierungsservern unbemerkt bleiben, wenn die auf ihm laufenden virtuellen IT-Systeme zwar auf einen anderen Virtualisierungsserver migriert worden sind und damit keine Dienste im Rechenzentrum ausfallen, der Ausfall aber wegen eines Fehlers in der Verwaltungs- und Überwachungssoftware nicht signalisiert wird. Durch die damit verbundene Herabsetzung der Redundanz kann die Gesamtverfügbarkeit der virtuellen Infrastruktur massiv verringert werden.

Beispiel:

- Eine Organisation betreibt mehrere Virtualisierungsserver, die in zwei Farmen zusammengefasst sind. In diesen Farmen werden jeweils mehrere virtuelle IT-Systeme betrieben. Die Virtualisierungsserver sind auf zwei Farmen verteilt worden, da auf Grund unterschiedlicher Schutzbedarfsanforderungen bestimmte virtuelle IT-Systeme nicht mit anderen zusammen betrieben werden dürfen.
  Bei der Planung der beiden Farmen ist die Anzahl der jeweils notwendigen Virtualisierungsserver auf Grund einer Prognose des zukünftigen Performancebedarfs ermittelt worden. Nach einiger Zeit stellt sich jedoch heraus, dass die Prognose unzutreffend war. Es wird festgestellt, dass in der ersten der beiden Farmen ein weiterer Virtualisierungsserver benötigt wird, um die Performanceanforderungen der virtuellen IT-Systeme abzudecken.
  Die Administratoren der Virtualisierungsserver stellen nach einer Auswertung der Performancedaten der zweiten Farm fest, dass deren Auslastung weit hinter der Performanceprognose zurückliegt. Daher wird entschieden, keinen neuen Virtualisierungsserver zu beschaffen, sondern stattdessen einen aus der zweiten Farm in die erste zu verlagern.
  Nun werden die virtuellen IT-Systeme auf dem Virtualisierungsserver, der in die erste Farm verlagert werden soll, auf andere migriert und der Server wird in die erste Farm aufgenommen. In der Folge sind die Ressourcen in der zweiten Farm massiv überbucht und es kommt zu starken Performanceeinbrüchen. Dies war nach den Ergebnissen der Performanceanalyse nicht zu erwarten.
  Die Ursache für die massiven Performanceverluste der virtuellen IT-Systeme in der zweiten Farm lag darin, dass das Verwaltungssystem für diese Farm die Performancedaten der einzelnen Virtualisierungsserver falsch verarbeitet hat und deutlich zu niedrige Werte für den Ressourcenverbrauch angezeigt hat.

G 4.77 Ressourcenengpässe durch fehlerhafte Funktion der Gastwerkzeuge in virtuellen Umgebungen

Bei vielen Virtualisierungsprodukten können so genannte Gastwerkzeuge in den virtuellen IT-Systemen installiert werden. Diese dienen einerseits dazu, spezielle, optimierte Gerätetreiber für die virtuellen Hardwarekomponenten einer virtuellen Maschine bereitzustellen. Andererseits kann der Virtualisierungsserver bei bestimmten Produkten über diese Gastwerkzeuge den Ressourcenverbrauch eines virtuellen IT-Systems steuern. Dies ist insbesondere dann notwendig, wenn das verwendete Virtualisierungsprodukt die Überbuchung von Ressourcen wie Arbeitsspeicher oder Festplattenplatz ermöglicht. Konkurrieren beispielsweise zwei virtuelle IT-Systeme um Arbeitsspeicher, kann das Hostbetriebssystem oder der Hypervisor die Gastwerkzeuge anweisen, virtuelles RAM und damit dessen physische Entsprechung in einem der virtuellen IT-Systeme zu reservieren. Die physische Repräsentation dieses Speichers wird nun durch das virtuelle IT-System nicht genutzt und steht über die Gastwerkzeuge unter der Kontrolle des Hypervisors. Der Hypervisor kann nun diesen physischen Speicher dem anderen virtuellen IT-System als virtuelles RAM zur Verfügung stellen. Andersherum kann ein virtuelles IT-System über die Gastwerkzeuge auch Hauptspeicher anfordern. Eine solche Technik wird zum Beispiel bei dem Produkt *ESX* des Herstellers *VMware* genutzt. Hier wird die Speicherreservierung über einen so genannten *Ballooning-Treiber* realisiert. Dieser ist in den Gastwerkzeugen (*VMware Tools*) enthalten.

Weiterhin kann bei einigen Virtualisierungsprodukten über die Gerätetreiber der Gastwerkzeuge der Zugriff auf Ressourcen eingeschränkt werden. So ist es zum Beispiel möglich, die Bandbreite, mit der ein virtuelles IT-System auf das Netz oder das Speichernetz zugreift, zu begrenzen.

Programmierfehler in den Gastwerkzeugen können daher auf Grund ihrer vielfältigen Funktionen weitreichende Folgen für den Betrieb der davon betroffenen virtuellen IT-Systeme haben, da meist eine Vielzahl von IT-Systemen gleichzeitig davon betroffen ist.

Gerätetreiber

Der häufigste Anwendungszweck der Gastwerkzeuge ist es, optimierte Gerätetreiber für die vom Virtualisierungsserver bereitgestellte emulierte Hardware (Grafikkarte, Netzkarte, Massenspeicher) der virtuellen IT-Systeme bereitzustellen. Die emulierte Hardware kann vom virtuellen IT-System zwar meist auch mit den im Lieferumfang der gängigsten Betriebssysteme enthaltenen Treibern genutzt werden, jedoch ist eine optimale Nutzung erst mit speziell angepassten Treibern möglich. Da diese in der Regel in allen virtuellen IT-Systemen genutzt werden, sind von einem Fehler in diesen Treibern auch alle virtuellen Maschinen betroffen.

Überbuchung von Speicherressourcen

Werden der Hauptspeicher des Virtualisierungsservers überbucht und Speicheranforderungen innerhalb eines virtuellen IT-Systems durch die Gastwerkzeuge fehlerhaft verarbeitet, kann es passieren, dass Prozessen zu wenig Speicher zur Verfügung steht.

Fehler im Bandbreitenmanagement

Sind die Funktionen zum Bandbreitenmanagement in den Gastwerkzeugen fehlerhaft programmiert, können die hierfür definierten Richtlinien wirkungslos sein. Genauso kann es aber dazu kommen, dass einem virtuellen IT-System viel zu wenig oder gar keine Bandbreite zur Verfügung gestellt wird.

Wenn beispielsweise ein virtuelles System ständig sehr viel Netzverkehr verursacht und dadurch die physikalisch vorhandenen Ressourcen stark ausnutzt, können die Verbindungen anderer virtueller IT-Systeme in Mitleidenschaft gezogen werden, so dass in der Folge Verbindungen dieser IT-Systeme abbrechen und damit deren Verfügbarkeit gefährdet ist.

Über die Gastwerkzeuge könnte nun der Administrator des Virtualisierungsservers entweder die nutzbare Bandbreite des ersten virtuellen IT-Systems beschränken oder den anderen Systemen eine gewisse Mindestbandbreite garantieren. Sind die Richtlinien zur Bandbreitensteuerung beispielsweise nach einer Aktualisierung der Gastwerkzeuge auf Grund eines Programmierfehlers wirkungslos, werden die Ziele, die mit diesen Richtlinien verfolgt wurden, nicht erreicht. Die Verfügbarkeit der Systeme ist also weiterhin eingeschränkt.

Führt der Fehler in den Gastwerkzeugen trotz korrekter Richtlinien im genannten Szenario dazu, dass zu wenig Bandbreite für das erste IT-System zur Verfügung steht, kann dieses System in der Verfügbarkeit eingeschränkt sein, da es nicht mit der erforderlichen Bandbreite auf das Netz zugreifen kann. Gleiches gilt für die anderen IT-Systeme, deren Kommunikation geschützt werden sollte.

Beispiel:

Ein mittelständisches Unternehmen betreibt eine Reihe von Virtualisierungsservern, um auf diesen Virtualisierungsservern seine sonstige Server-Infrastruktur effizient bereitstellen zu können. Alle im Unternehmen genutzten Dienste hängen direkt oder indirekt von den virtuellen IT-Systemen in der virtuellen Infrastruktur ab. Dort laufen Systeme wie der Verzeichnisdienst, der zentrale Mailserver sowie das ERP-System. Weiterhin werden Datei- und Druckserver als virtuelle IT-Systeme betrieben.

Die Systeme laufen einige Zeit störungsfrei. Nachdem eine Aktualisierung der Virtualisierungssoftware auf den Virtualisierungsservern durchgeführt wurde, zeigte die zentrale Verwaltungssoftware der Virtualisierungsserver an, dass die Gastwerkzeuge der virtuellen IT-Systeme nicht mehr aktuell seien. Der zuständige Administrator entscheidet sich, die Gastwerkzeuge in den virtuellen IT-Systemen zu aktualisieren. Er hat mit dieser Aktualisierung in der Vergangenheit keine schlechten Erfahrungen gemacht. Da er selbst nicht auf allen virtuellen IT-Systemen Administratorrechte besitzt, benutzt für die Aktualisierung eine Funktion der Virtualisierungsserver, die es ermöglicht, die Werkzeuge auf allen Virtualisierungsservern ohne Interaktion mit den einzelnen virtuellen IT-Systemen zu erneuern. Er beginnt an einem Arbeitstag zwei Stunden vor allgemeinem Arbeitsbeginn mit dem Update. Er beobachtet, wie die Gastwerkzeuge in den virtuellen IT-Systemen neu installiert werden und stellt zunächst keine offensichtlichen Fehler fest, da auf der Konsole der virtuellen Systeme keine Fehlermeldungen protokolliert werden.

Nachdem aber eine gewisse Anzahl virtueller IT-Systeme aktualisiert wurde, bemerkt er, dass diese nicht mehr mit dem Netz verbunden sind. Er untersucht das Problem und stellt fest, dass die Netzkarten-Treiber der virtuellen IT-Systeme als Bestandteil der Gastwerkzeuge ebenfalls aktualisiert worden

sind. Hierbei ist dem Hersteller ein Fehler unterlaufen, der dazu führt, dass die Betriebssysteme der virtuellen IT-Systeme die virtuelle Netzkarte als neue Hardware erkennen. Hierdurch ist die Netzkarte unkonfiguriert. Erst nachdem die anderen Administratoren im Unternehmen eingetroffen sind, können die Netzkarten neu konfiguriert werden. Bis dahin können viele Mitarbeiter in der Verwaltung des Unternehmens zunächst nicht auf ihre Daten zugreifen. Dadurch geht viel Arbeitszeit verloren.

G 4.78 Ausfall von virtuellen Maschinen durch nicht beendete Datensicherungsprozesse

Klassische Datensicherungsmethoden basieren auf Agenten, die auf den zu sichernden IT-Systemen installiert werden. Diese Agenten übermitteln die zu sichernden Daten vom IT-System aus an den Datensicherungsserver. Dieser wiederum leitet die Daten an die Datensicherungsgeräte weiter.

Durch die Einführung von Speichernetzen können IT-Systeme und der von ihnen genutzte Massenspeicher entkoppelt werden. Dies bedeutet, dass die Datensicherung nicht mehr vom zu sichernden IT-System selbst, sondern vom Speichernetz an den Datensicherungsserver übermittelt werden kann. Bei einigen Speichernetz-Produkten sind die Datensicherungsgeräte selbst Bestandteile des Speichernetzes und werden nur noch durch den Datensicherungsserver gesteuert. Hierdurch wird das gesicherte IT-System und der Datensicherungsserver vom Transport der Daten der Datensicherung entlastet.

Dieses Konzept wird von einigen Virtualisierungsprodukten nachgebildet und erweitert. So können die Virtualisierungsserver den Massenspeicher virtueller IT-Systeme (virtuelle Festplatten) einem Datensicherungssystem zur Verfügung stellen, damit dieses Datensicherungssystem die auf dem Massenspeicher abgelegten Daten sichern kann. Es ist notwendig, dass diese virtuelle Festplatte sich in einem konsistenten Zustand befindet, damit keine inkonsistenten Daten in die Sicherung gelangen. Um dies zu erreichen, wird der Inhalt der virtuellen Festplatte eingefroren (Snapshot). Dieser Vorgang ist für das gesicherte virtuelle IT-System vollkommen transparent. Da das zu sichernde virtuelle IT-System weiterläuft und weiterhin Änderungen an dieser Festplatte erfolgen, werden diese Änderungen in eine Differenzdatei geschrieben. Hierbei wächst der insgesamt von diesem IT-System benötigte Speicherplatz an. Wie groß diese Differenzdatei wird, hängt davon ab, wie viele Änderungen im Dateisystem des virtuellen IT-Systems während der Dauer der Sicherung geschehen. Ist die Datensicherung beendet, werden die Änderungen, die in der Zwischenzeit erfolgt sind, auf den eingefrorenen Zustand angewendet und die Differenzdatei wird gelöscht.

Wird eine Datensicherung in der Virtualisierungsumgebung etwa aufgrund langer Laufzeit des Datensicherungsprozesses oder durch Kommunikationsprobleme im Netz nicht vollständig ausgeführt, kann die Differenzdatei, die angelegt wurde, als der Snapshot erzeugt wurde, sehr groß werden. Möglicherweise bleibt sie dauerhaft bestehen, wenn der Datensicherungsprozess unvorhergesehen abbricht. Dies kann dazu führen, dass der Speicherplatz, in dem die virtuellen Festplatten der zu sichernden virtuellen Maschinen liegen, vollkommen ausgeschöpft wird, insbesondere dann, wenn mehrere virtuelle IT-Systeme gleichzeitig auf diese Weise gesichert werden.

Ist der Speicherplatz, der für die oben erwähnte Differenzdatei genutzt wird, erschöpft, verweigert der Virtualisierungsserver dem virtuellen IT-System weitere Schreibzugriffe auf die virtuelle Festplatte, und das virtuelle IT-System gerät in eine Fehlersituation. Dies kann zu einem Absturz des virtuellen IT-Systems führen, wenn das Betriebssystem diese Fehlersituation nicht ausgleichen kann.

Beispiel:

Der Betreiber eines Rechenzentrums hat eine Vielzahl seiner Serversysteme virtualisiert. Auf diesen Servern werden täglich große Mengen an Daten verarbeitet. Diese Daten müssen täglich gesichert werden.

Die Sicherung der Daten beansprucht die virtuellen IT-Systemen auf Grund der hohen Datenmenge stark und kann nicht mehr ausschließlich während der Nachtstunden erfolgen. Es kommt daher zu Performanceeinbußen während der normalen Arbeitszeit. Daraufhin wurde entschieden, die Datensicherung nicht mehr auf klassische, agentenbasierte Weise auszuführen, sondern Snapshots zu verwenden. Diese werden jeweils abends zu einer bestimmten Zeit angelegt, die Daten werden gesichert und sobald der Sicherungsvorgang abgeschlossen ist, die Snapshots wieder gelöscht.

Diese Lösung läuft einige Zeit störungsfrei, jedoch wächst das Datensicherungsvolumen bald so stark an, dass ein neuer Datensicherungsprozess ausgelöst wird, bevor der vorherige abgeschlossen ist. Kurz darauf kommt es zu einem Ausfall aller virtuellen IT-Systeme auf dem Virtualisierungsserver, da der zur Verfügung stehende Speicherplatz erschöpft ist.

G 5.29 Unberechtigtes Kopieren der Datenträger

Werden Datenträger ausgetauscht oder transportiert, so bedeutet dies unter Umständen, dass die zu übermittelnden Informationen aus einer gesicherten Umgebung heraus über einen unsicheren Transportweg in eine unter Umständen unsichere Umgebung beim Empfänger übertragen werden. Unbefugte können sich in solchen Fällen diese Informationen dort durch Kopieren einfacher beschaffen, als es in der ursprünglichen Umgebung der Fall war.

Wegen der großen Konzentration schützenswerter Informationen auf Datenträgern elektronischer Archive (z. B. personenbezogene oder firmenvertrauliche Daten) stellen diese ein besonderes Angriffsziel für Diebstahl oder Kopie durch Unbefugte dar.

Beispiel:

- Vertrauliche Entwicklungsergebnisse sollen vom Entwicklungslabor in X-Stadt zur Produktion nach Y-Stadt transportiert werden. Werden die entsprechenden Datenträger unkontrolliert über den Postweg versandt, kann nicht ausgeschlossen werden, dass diese unberechtigterweise kopiert und gegebenenfalls an die Konkurrenz verkauft werden, ohne dass die Bloßstellung der Informationen bemerkt wird.

G 5.133 Unautorisierte Benutzung web-basierter Administrationswerkzeuge

Die Administration mit Webbrowser-basierten Werkzeugen hat stark an Bedeutung gewonnen. Einer der entscheidenden Vorteile für das technisch verantwortliche Personal ist die Unabhängigkeit von

- der Betriebssystem-Plattform des zu betreuenden IT-Systems
- dem Standort des zu betreuenden IT-Systems.

Allen Werkzeugen gemein ist, dass sie kritische Anmeldedaten verwenden. Sie sind auf gängige für das Internet standardisierte Authentisierungsmethoden angewiesen, um technischem Personal autorisierten Zugriff auf die kritischen lokalen Systeme zu gewähren. Viele Administrationswerkzeuge besitzen zusätzlich eigene Authentisierungsmechanismen oder bedienen sich lokaler, teils nicht standardisierter Authentisierungs- und Sicherheitsmechanismen. Es besteht die Gefahr der Kompromittierung durch nicht autorisierte Benutzer.

Eine hohe Gefährdung entsteht, wenn die Sicherheitsrichtlinie für die Authentisierung im Netz bzw. deren Umsetzung im betrachteten Informationsverbund durch ungeeignete Authentisierungsverfahren für Web-basierte Administrationswerkzeuge unterlaufen wird. Die häufigsten Ursachen dafür sind:

- die Wahl einer falschen oder veralteten Authentisierungsmethode, weil das jeweilige Werkzeug keine stärkere Authentisierung unterstützt oder weil andere beteiligte IT-Systeme (z. B. Sicherheitsgateways) das favorisierte Protokoll nicht unterstützen
- die ungeeignete Umsetzung bzw. Übernahme der Web-basierten Authentisierung in das lokale Authentisierungssystem.

Eine Gefährdung kann z. B. entstehen, wenn zum Zwecke der Nutzung Webbasierter Administrationshilfen die Windowskomponente Internetinformationsdienst aktiviert wird, ohne diese entsprechend den Empfehlungen zu konfigurieren. Eine Gefahr könnte dann darin bestehen, dass in der Standardkonfiguration nur schwächere Authentisierungsverfahren aktiviert sind. Es ist darauf hinzuweisen, dass eine mangelhafte Konfiguration ein großes Risiko für alle auf dem Markt befindlichen Lösungen zur Web-basierten Administration darstellt.

G 5.147 Unautorisiertes Mitlesen oder Stören des Virtualisierungsnetzes

Für den Betrieb einer virtuellen Infrastruktur sind vielfältige Netzverbindungen notwendig. Diese Verbindungen werden genutzt, um auf Speichernetze zugreifen zu können. Weiterhin werden Verbindungen zwischen den einzelnen Virtualisierungsservern benötigt, um die Steuerung und Überwachung der Virtualisierungsserver und der virtuellen IT-Systeme zu ermöglichen. Für Hochverfügbarkeitsfunktionen oder die so genannte *Live Migration* (Verschieben von virtuellen IT-Systemen zwischen Virtualisierungsservern im laufenden Betrieb) werden ebenfalls Netzverbindungen benötigt. Diese Netzverbindungen werden im Folgenden als "Virtualisierungsnetz" bezeichnet.

Innerhalb einer virtuellen Infrastruktur können zwischen Virtualisierungsservern einzelne virtuelle IT-Systeme übertragen werden (*Live Migration*). Dies geschieht z. B. zur Lastverteilung, zu Wartungszwecken oder zur Ausfallkompensation. Dabei müssen der Prozessorzustand und der Hauptspeicherinhalt sowie die Konfigurationsdaten des virtuellen IT-Systems von dem einen Virtualisierungsserver auf den anderen übertragen werden. Diese Übertragung erfolgt durch das so genannte Virtualisierungsnetz. Die von den Herstellern der Virtualisierungslösungen verwendeten Übertragungsprotokolle sehen häufig keine Verschlüsselungsmechanismen für diesen Datenstrom vor. Hierdurch ist es möglich, dass Personen, die unautorisiert Zugang zum Virtualisierungsnetz erlangen, vertrauliche Inhalte der transferierten Gastsysteme wie z. B. den Hauptspeicherinhalt mitlesen. Beispielsweise können im Hauptspeicher enthaltene vertrauliche Daten, die sonst nur verschlüsselt durch das Netz übertragen werden, mit gelesen und eventuell sogar verändert werden. Nutzen die Virtualisierungsservern ein zentrales Speichernetz, betrifft die mögliche Kompromittierung auch die Inhalte des angeschlossenen Speichernetzes (siehe hierzu auch G 5.129 *Manipulation von Daten über das Speichersystem* sowie G 5.7 *Abhören von Leitungen* und G 5.8 *Manipulation von Leitungen*).

Ein manipulierter Virtualisierungsserver kann das Virtualisierungsnetz darüber hinaus stören, in dem der Angreifer auf die im Netz übertragenen Informationen zugreift und Netzpakete unterdrückt oder verändert. Es kann beispielsweise sein, dass Veränderungen an Hauptspeicherinhalten eines virtuellen IT-Systems bei deren Übertragung während einer *Live Migration* durch den Virtualisierungsserver nicht geprüft werden. So könnten dann Hauptspeicherinhalte eines Gastsystems durch einen Angreifer verändert werden.

Wird die Kommunikation im Virtualisierungsnetz gestört, können Migrationen im laufenden Betrieb fehlschlagen. Hierdurch kann es zu Ressourcenengpässen in der virtuellen Infrastruktur kommen, wenn diese Migrationen ausgelöst wurden, um diese Engpässe zu verhindern.

Beispiel:

Ein mittelständisches Unternehmen setzt einen Datenbankserver zur Verarbeitung der Personaldaten seiner Mitarbeiter ein. Um diese Personaldaten zu schützen, werden die Datenbankinhalte nur verschlüsselt auf die Festplatten des Datenbankservers geschrieben. Die Client-Anwendung, mit der die Benutzer der Personalabteilung arbeiten, kommuniziert ebenfalls verschlüsselt mit dem Datenbankserver. Das Datenbanksystem selbst hält allerdings während der Verarbeitung die Daten teilweise unverschlüsselt in seinem Hauptspeicher.

Dieses Datenbanksystem ist im Zuge des Virtualisierungsprojektes im Unternehmen virtualisiert worden. Der Administrator der Virtualisierungsserver möchte nun an Gehaltsdaten der Personaldatenbank gelangen, um bei Gehaltsverhandlungen seine Position zu verbessern, da er das Gefühl hat, im Vergleich zu seinen Kollegen unterbezahlt zu sein. Er hat das Datenbanksystem aufgebaut und weiß daher, wie dieses System arbeitet. Er besitzt jedoch keine Möglichkeit, über Funktionen des Servers oder der Datenbanksoftware unbemerkt an die Daten des Systems heranzukommen. Daher installiert er im Virtualisierungsnetz ein Netzüberwachungswerkzeug, mit dem er den Netzverkehr in diesem Netz mitlesen kann.

Er weist nun die Virtualisierungsserver an, den Datenbankserver im laufenden Betrieb (*Live Migration*) zwischen zwei Servern zu verschieben. Er liest die Übertragung des Hauptspeichers im Netz mit und zeichnet sie auf. Nach mehreren mitgeschnittenen Migrationen kann er eine vollständige Kopie der Gehaltstabelle aus den aufgezeichneten Inhalten des Hauptspeichers des Datenbankservers rekonstruieren.

Dieser Angriff auf die Vertraulichkeit der Daten der Personalverwaltung bleibt unbemerkt, da die Live Migration völlig transparent für das Datenbanksystem und die Client-Anwendung verläuft.

G 5.148 Missbrauch von Virtualisierungsfunktionen

Die meisten Virtualisierungsprodukte enthalten Werkzeuge, um virtuelle Maschinen oder bestimmte Zustände der virtuellen Maschinen einfrieren zu können. Diese Funktionen basieren in der Regel darauf, dass die Festplattencontainer der virtuellen IT-Systeme kopiert oder die Zustände des Arbeitsspeichers und des Prozessors des virtuellen IT-Systems auf einen Massenspeicher des Virtualisierungsserver abgespeichert werden.

Jeder Virtualisierungsserver hat Zugriff auf alle Speicherressourcen der von ihm verwalteten virtuellen Maschinen. Es besteht daher die Gefahr, dass vom Virtualisierungsserver auf solche Ressourcen unautorisiert zugegriffen wird, um Daten unerlaubt zu kopieren oder zu verändern. Daher kann ein Angreifer leicht eine Kopie einer virtuellen Maschine herstellen, um diese unerlaubt aus dem Rechenzentrum zu entfernen und beispielsweise auf einem eigenen Virtualisierungsserver zu betreiben. Die erstellte Kopie kann er dazu nutzen, um die virtuelle Maschine zu untersuchen.

Des Weiteren kann ein unveränderter Klon einer virtuellen Maschine zu einem IP-Adressen- oder sonstigen Ressourcenkonflikt im Rechenzentrumsbetrieb führen, wenn ein solcher Klon vor dem Start nicht angepasst wird.

Bei einigen Virtualisierungsprodukten können Snapshots einer virtuellen Maschine auch im laufenden Betrieb erzeugt werden. In diesem Fall wird der Prozessorzustand und der Inhalt des Hauptspeichers auf eine Festplatte des Virtualisierungsservers geschrieben. Des Weiteren wird der Festplattencontainer der virtuellen Maschine ebenfalls eingefroren und Änderungen werden in eine Differenzdatei geschrieben. Diese Daten können kopiert werden, um mittels eines anderen Virtualisierungsservers einen laufenden Klon der virtuellen Maschine zu erzeugen. Die gespeicherten Inhalte des Prozessorzustands und des Hauptspeichers der virtuellen Maschine können zudem von einem Angreifer verwendet werden, um Speicherbereiche der virtuellen Maschine zu analysieren. Hier können beispielsweise Schlüssel von Verschlüsselungswerkzeugen, die unverschlüsselt im Hauptspeicher der virtuellen Maschine gespeichert sind, extrahiert werden.

Weiterhin ist es möglich, durch die Verwendung von Snapshots virtuelle Maschinen auf einen alten Stand zurück zu setzen. Hierdurch können Maßnahmen unterlaufen werden, die beispielsweise unternommen wurden, um Sicherheitslücken zu schließen.

Durch das Zurücksetzen einer virtuellen Maschine auf einen Snapshot können auch Angriffe verschleiert werden, die ansonsten in den Protokolldateien der virtuellen Maschinen aufgezeichnet würden. Mit dem Zustand der virtuellen Maschine wird ebenfalls ihre Protokolldatei zurückgesetzt.

Werden ältere Snapshots aktiviert, können auch Daten wiederhergestellt werden, die gelöscht sein sollten. Wird das virtuelle IT-System auf den Snapshot zurückgesetzt, sind die vermeintlich gelöschten Daten wieder vorhanden. Auch die Verwendung von Werkzeugen, die den Inhalt einer Datei mehrfach überschreiben, um eine Wiederherstellung unmöglich zu machen, ist wirkungslos, wenn ein Snapshot erzeugt wurde, bevor das Werkzeug innerhalb des virtuellen IT-Systems verwendet wird. Ist für eine virtuelle Maschine ein Snapshot erzeugt worden, wirken sich die Überschreibvorgänge nur auf die Differenzdatei aus, die die Änderungen enthält, die seit Erzeugung des Snapshots erfolgt sind. Wird der Snapshot gelöscht und die Änderungen in der Diffe-

renzdatei werden auf den Festplattencontainer angewandt, werden die scheinbar mehrfachen Überschreibvorgänge nur einmal in den Festplattencontainer geschrieben.

Beispiel:

Im Rechenzentrum eines Unternehmens, das in der Grundlagenforschung tätig ist, werden in einem virtuellen IT-System Daten mit einer hohen Schutzbedarfskategorie bezüglich Vertraulichkeit verarbeitet. Daher wird in der virtuellen Maschine ein Festplattenverschlüsselungsprogramm installiert. Dieses erfordert die Angabe eines Kennworts während des Startvorgangs. Das Kennwort ist nur wenigen, besonders vertrauenswürdigen Mitarbeitern des Unternehmens bekannt.

Das Festplattenverschlüsselungsprogramm arbeitet für das Betriebssystem der virtuellen Maschine transparent. Das heißt, es muss während des Betriebs der virtuellen Maschine kein weiteres Kennwort eingegeben werden.

Während des Betriebs der virtuellen Maschine sind die Daten durch die Einschränkung von Berechtigungen geschützt. Zudem werden Benutzerkonten automatisch gesperrt, wenn mehrfach versucht wird, mittels dieser Konten unberechtigt Zugang zu den Daten zu erlangen.

Durch den Einsatz des Festplattenverschlüsselungsprogramms sind die Daten der virtuellen Maschine im Speichernetz geschützt. Der Rechenzentrumsbetreiber geht daher davon aus, dass das Kopieren des Festplattencontainers der virtuellen Maschine keine für einen Angreifer verwertbaren Daten ergibt. Zudem glaubt er durch die Berechtigungsvergabe und die automatische Kontensperre ein ausreichendes Sicherheitsniveau erreicht zu haben.

Ein Mitarbeiter dieses Rechenzentrums befindet sich in finanziellen Schwierigkeiten. Ein Mitbewerber des Rechenzentrumsbetreibers bietet nun diesem Mitarbeiter eine hohe Summe an Geld, wenn dieser ihm Zugriff auf die Daten, die in der virtuellen Maschine verarbeitet werden, verschafft.

Der Mitarbeiter erzeugt infolgedessen auf dem Virtualisierungsserver einen Snapshot der virtuellen Maschine im laufenden Betrieb. In dem Snapshot sind die Arbeitsspeicherinhalte sowie der Prozessorzustand des virtuellen IT-Systems enthalten. Er kopiert die Konfigurationsdatei, den Festplattencontainer, den Inhalt des Arbeitsspeichers und den CPU-Zustand der virtuellen Maschine auf einen transportablen Massenspeicher und verlässt mit diesem die Institution.

Die Kopie der virtuellen Maschine kann jetzt auf dem Virtualisierungsserver des Mitbewerbers ausgeführt werden. Da der Virtualisierungsserver die Laufzeitumgebung der virtuellen Maschine aus den gespeicherten Daten wiederherstellt, erfolgt keine Passwortabfrage durch das Festplattenverschlüsselungsprogramm. Das Betriebssystem in der virtuellen Maschine "bemerkt" nichts von dieser Betriebsunterbrechung.

Der Angreifer versucht durch Brute Force-Attacken die Kennwörter der berechtigten Benutzer zu ermitteln. Um den Vorgang zu beschleunigen, erzeugt er mehrere Kopien der virtuellen Maschine. Wird ein Konto aufgrund der Fehlversuche gesperrt, setzt er die virtuelle Maschine wieder auf den Zustand vor der Kontensperre zurück und fährt mit der Brute Force-Attacke fort.

G 5.149 Missbräuchliche Nutzung von Gastwerkzeugen in virtuellen IT-Systemen

Bei vielen Virtualisierungsprodukten werden in den virtuellen IT-Systemen sogenannte Gastwerkzeuge installiert. Mit diesen Gastwerkzeugen können zum Einen die für Betriebssystemvirtualisierung notwendigen Gerätetreiber für virtuelle oder emulierte Geräte wie Netzwerkkarten, Festplatten oder Grafikkarten bereitgestellt werden. Zum Anderen werden mit diesen Werkzeugen innerhalb der virtuellen IT-Systeme Programme zur Kommunikation mit dem Hypervisor oder dem Hostbetriebssystem, zur Steigerung der Leistung des virtuellen IT-Systems und zur Vereinfachung der Bereitstellung neuer virtueller IT-Systeme installiert. Mit Hilfe der Gastwerkzeuge können des Weiteren die virtuellen IT-Systeme überwacht werden. Der Hypervisor oder das Hostbetriebssystem überwacht hierüber beispielsweise die Verfügbarkeit und die Leistung des Gastes.

Die Gastwerkzeuge werden wegen ihrer systemnahen Funktion häufig mit sehr hohen Berechtigungen ausgeführt. Häufig laufen sie im Kontext und damit mit den Rechten des Betriebssystemkerns der virtuellen Maschine.

Funktionen wie die Überbuchung von Hauptspeicher oder Massenspeicherplatz für virtuelle IT-Systeme werden zwischen dem Hypervisor und dem virtuellen IT-System durch die Gastwerkzeuge koordiniert. Diese Funktionen stellen einen wesentlichen Mehrwert der Virtualisierungstechnik im Rechenzentrumsbetrieb dar.

Bei einigen für die Software-Entwicklung spezialisierten Virtualisierungsprodukten ist weiterhin eine Möglichkeit für den komfortablen Aufbau komplexer Testszenarien vorgesehen. Dies wird häufig ebenfalls über die Gastwerkzeuge realisiert oder unterstützt. Hierzu haben die Gastwerkzeuge Schnittstellen, um Skriptdateien auf virtuelle IT-Systeme zu übertragen. Diese Skripte können dann ebenfalls über die Gastwerkzeuge im virtuellen IT-System ausgeführt werden. Es können alle in dem virtuellen IT-System verfügbaren Skriptsprachen genutzt werden. Der Start der Skripte kann entweder beim Systemstart, der Anmeldung eines Benutzers oder auch zu jeder anderen beliebigen Zeit angestoßen werden. Die Schnittstellen benötigen in der Regel keine Netzverbindung zwischen den Gastsystemen, sondern werden über den Hypervisor oder das Hostbetriebssystem bereitgestellt.

Diese Schnittstellen für Skripte können durch einen Angreifer ausgenutzt werden, um eine unerwünschte und nicht mit klassischen Mitteln kontrollierbare Kommunikation über mehrere virtuelle IT-Systeme hinweg aufzubauen. Hierbei überträgt der Angreifer die Daten über die Schnittstelle zum Transport von Skriptdateien.

Weiterhin ist es einem Angreifer bei den beschriebenen für die Software-Entwicklung konzipierten Virtualisierungsprodukten möglich, mittels der Gastwerkzeuge von einem virtuellen IT-System aus eigene Skriptdateien auf ein anderes virtuelles IT-System zu übertragen. Diese können mit den Rechten, mit denen die Gastwerkzeuge laufen, ausgeführt werden. Auf Grund der weit reichenden Berechtigung der Gastwerkzeuge ist dies besonders kritisch, da damit beliebige Aktionen in dem betroffenen Gastsystem ausführbar sind. Es können beispielsweise Schadprogramme gestartet, Benutzer angelegt, Grup-

penmitgliedschaften verändert oder die Konfiguration des Betriebssystems des virtuellen IT-Systems manipuliert werden.

Denial of Service durch Überbuchung von Ressourcen

Einige Virtualisierungsprodukte ermöglichen die Überbuchung verschiedener Ressourcen wie Festplattenplatz oder RAM. Konkurrieren beispielsweise zwei virtuelle IT-Systeme um Arbeitsspeicher, kann das Hostbetriebssystem oder der Hypervisor die Gastwerkzeuge anweisen, virtuelles RAM in dem einen virtuellen IT-System zu reservieren. Die physikalische Repräsentation dieses Speichers wird nun durch das virtuelle IT-System nicht genutzt. Der Hypervisor kann diesen physikalischen Speicher dem anderen virtuellen IT-System als virtuelles RAM zur Verfügung stellen. Andersherum kann ein virtuelles IT-System über die Gastwerkzeuge auch Hauptspeicher anfordern.

Hat ein Angreifer ein virtuelles IT-System unter seiner Kontrolle, könnte er über ein Schadprogramm so viel Hauptspeichern anfordern, dass dieser für andere virtuelle IT-Systeme knapp wird. Hierdurch wird die Leistungsfähigkeit der anderen virtuellen IT-Systeme bis hin zu einer Denial of Service-Attacke beeinflusst. Der gleiche Effekt tritt auf, wenn ein Angreifer von außen auf einen Dienst eines virtuellen IT-Systems in der Weise zugreift, dass dieser sehr viel Speicher belegt.

Wird eine Funktion zur Überbuchung von Festplattenplatz genutzt, existiert meist ebenfalls eine Möglichkeit, diesen Speicher wieder frei zu geben. Dies geschieht dadurch, dass unbenutzter Speicherplatz zusammengefasst und als frei markiert wird.

Löst ein Angreifer einen solchen Prozess in einem virtuellen IT-System aus, werden die Speichersysteme stark belastet. Auch hierdurch kann die Leistungsfähigkeit anderer IT-Systeme verringert werden.

Beispiele:

- Ein Systemhaus bearbeitet Softwareentwicklungsaufträge für verschiedene Kunden. Hierzu wird durch das Systemhaus eine auf Entwicklungsaufgaben spezialisierte Virtualisierungsumgebung betrieben, da für die Entwicklung von Client-Server-Anwendungen umfangreiche Testszenarien aufgebaut werden müssen. Die Testsysteme für diese Szenarien werden über mehrere Vorlagen für verschiedene virtuelle Server und Clients bereitgestellt, die bei Bedarf kopiert und an das jeweilige Testszenario angepasst werden.
  Aufgrund der schlechten Auftragslage des Systemhauses müssen einige Entwickler entlassen werden. Einer der entlassenen Entwickler will sich für seine Entlassung rächen und entwickelt ein Skript, dass ein virtuelles Testsystem immer wieder auf den Ursprungszustand der Vorlage zurücksetzt, sobald sich ein Benutzer zum zweiten Mal an dem virtuellen System anmeldet. Dabei sieht es so aus, als hätte der Benutzer, der sich angemeldet hat, den Rücksetzvorgang ausgelöst. Tatsächlich wird dieses Skript jedes mal durch die Virtualisierungssoftware in das Testsystem eingebracht, sobald es zum zweiten Mal gestartet wird. Zusätzlich überträgt sich das Skript selbständig über eine Virtualisierungsfunktion auf jedes in der virtuellen Infrastruktur laufende virtuelle Testsystem.
  Die Verantwortlichen des Systemhauses vermuten einen Wurmbefall ihrer Systeme und beauftragen ein IT-Beratungsunternehmen mit der Durchführung einer Netzanalyse, um die Ursache des Problems zu ermitteln. Das Beratungsunternehmen kann aber keine Auffälligkeiten im Netz des Systemhauses feststellen. Nur durch einen Zufall bemerkt einer der Ent-

wickler den von seinem ehemaligen Kollegen durchgeführten Angriff auf die Testumgebung.
Durch die Fehlersuche und die Störung des Testbetriebs wurden erhebliche personelle Ressourcen gebunden und Termine nicht eingehalten. Dadurch entstand dem schon finanziell geschwächten Systemhaus weiterer Schaden.

- Ein Dienstleister betreibt eine Webserverfarm für mehrere Kunden. Um Hardwarekosten zu sparen, hat er die Webserver virtualisiert. Dabei stellt er den Kunden für deren virtuelle Systeme in Summe sehr viel mehr Hauptspeicher zur Verfügung als in der virtuellen Infrastruktur tatsächlich vorhanden ist. Da die Webserver der Kunden in der Regel nur schwach ausgelastet sind, kommt es zu keinen spürbaren Performanceeinschränkungen in den virtuellen Systemen.
  Einer der Webserver der Kunden wird nun Opfer eines Denial of Service-Angriffs. Dabei verbraucht dieses virtuelle IT-System sehr viel Hauptspeicher. Dieser Speicher steht allerdings in dem physischen Virtualisierungsserver, auf dem der virtuelle Webserver läuft, nicht als frei zur Verfügung, sondern wird von anderen virtuellen Webservern genutzt. Um dem angegriffenen System diesen Speicher zur Verfügung stellen zu können, muss dieser von anderen virtuellen IT-Systemen freigegeben werden. Der Hypervisor des Virtualisierungsservers verknappt somit den Hauptspeicher für alle anderen unter seiner Kontrolle laufenden, virtuellen Webserver. In der Folge steigen die Antwortzeiten der virtuellen Webserver stark an. Teilweise kommt es hier zu Verbindungsabbrüchen, so dass auch die virtuellen Webserver, die nicht direkt Ziel des DoS-Angriffs waren, nicht mehr verfügbar sind.

G 5.150 Kompromittierung des Hypervisor virtueller IT-Systeme

Der Hypervisor ist die zentrale Komponente eines Virtualisierungsservers, er steuert alle auf diesem Virtualisierungsserver ausgeführten virtuellen Maschinen. Er teilt ihnen Prozessor- und Hauptspeicherressourcen zu und verteilt die zur Verfügung stehende Rechenzeit auf die virtuellen Maschinen. Des Weiteren verwaltet er den Zugriff der virtuellen IT-Systemen auf das Netz und die Speicher-Ressourcen. Ein erfolgreicher Angriff auf diese Komponente bedeutet den Verlust der Kontrolle über alle virtuellen IT-Systeme, die im Kontext dieses Hypervisors ausgeführt werden. Ein Angriff auf den Hypervisor kann im Wesentlichen folgendermaßen ausgeführt werden:

- Manipulation der CPU-Register, die bei Prozessoren mit integrierter Virtualisierungsunterstützung die Virtualisierungsfunktionen steuern. Mittels solcher Angriffe kann beispielsweise festgestellt werden, ob sich der Angreifer in einer virtuellen Umgebung befindet. Bei einigen Virtualisierungsprodukten kann über bestimmte Prozessorbefehle der Hypervisor selbst virtualisiert werden und so unter die Kontrolle eines Schadprogramms gebracht werden. Dies ist sogar aus einem virtuellen IT-System heraus möglich.
- Ausnutzung eines Fehlers in der Implementierung der Ressourcen, die den virtuellen IT-Systemen durch den Hypervisor zur Verfügung gestellt werden. Dies kann beispielsweise emulierte Netzwerkkarten, Massenspeichergeräte oder Grafikkarten betreffen. Bei einigen Virtualisierungsprodukten werden auch Kernkomponenten wie Prozessor und Hauptspeicher emuliert. Die Geräteemulationen werden durch die virtuellen IT-Systeme verwendet, um die entsprechenden Funktionen des Hypervisors bzw. des Hostbetriebssystems zu nutzen.
- Als zentrale Komponente übernimmt der Hypervisor eine Reihe von sicherheitskritischen Funktionen einer Virtualisierungslösung. Gelingt es einem Angreifer, den Hypervisor zu kompromittieren, ist dadurch der sichere Betrieb der jeweiligen virtuellen IT-Systeme und der jeweiligen Virtualisierungsserver in hohem Maße gefährdet. Angreifer können versuchen, auf diesem Wege virtuelle IT-Systeme zu manipulieren oder zu stören. Unter Umständen können dadurch auch vertrauliche Informationen an Unbefugte gelangen. Schwachstellen im eingesetzten Hypervisor-Produkt können deshalb erhebliche Risiken für die Informationsverarbeitung mit sich bringen.
- Einige Virtualisierungssysteme beinhalten zudem Funktionen zur Kommunikation zwischen dem Hypervisor und den virtuellen IT-Systemen. Diese werden in der Regel durch Gastwerkzeuge realisiert, die im virtuellen IT-System installiert werden. Um die Kommunikation zwischen den Gastwerkzeugen und dem Hypervisor zu ermöglichen, besitzt jedes virtuelle IT-System einen Kommunikationskanal für die Gastwerkzeuge zum Hypervisor. Hierzu existiert zum Beispiel in virtuellen IT-Systemen auf der Basis der Produkte des Herstellers VMware ein spezieller DMA-Kanal, der einen solchen Kanal öffnet, wenn die bestimmte Prozessorregister mit bestimmten Werten geladen werden. Dieser Weg kann nicht ausschließlich durch die Gastwerkzeuge sondern auch durch Schadprogramme genutzt werden. Kann ein Angreifer diesen Kommunikationskanal besetzen, hat er die Möglichkeit, Sicherheitslücken oder Designschwächen des Hypervisors auszunutzen, um die Kontrolle über den Hypervisor zu erhalten oder eigenen Code im Kontext des Hypervisors auszuführen. Hierüber kann der Angreifer andere virtuelle IT-Systeme unter seine Kontrolle bekommen. Da der Hypervisor alle Funktionen eines virtuellen IT-Systems über-

wacht und steuert, können über den Hypervisor Prozessorfunktionen oder Hauptspeicherinhalte des virtuellen IT-Systems direkt manipuliert werden, um Schadprogramme in das virtuelle IT-System einzubringen. Dies erfordert nicht notwendigerweise eine ausnutzbare Sicherheitslücke in dem über den Hypervisor angegriffenen virtuellen IT-System.

Beispiel:

Ein Rechenzentrumsdienstleister betreibt IT-Systeme für mehrere Kunden, die in einem Konkurrenzverhältnis zu einander stehen. Um die Kosten für den Systembetrieb für seine Kunden zu senken und weiterhin konkurrenzfähig zu sein, führt er eine Virtualisierungslösung in seinen Rechenzentrumsbetrieb ein. Er informiert seine Kunden darüber, dass ihre Systeme nun als virtuelle IT-Systeme betrieben werden. Da das Netz des Rechenzentrumsdienstleisters so aufgebaut ist, dass zwischen den IT-Systemen unterschiedlicher Kunden keine Kommunikationsbeziehungen über das Netz aufgebaut werden können, garantiert der Dienstleister weiterhin, dass die Vertraulichkeit der Daten der Kunden gewährleistet ist. Er überprüft dies durch regelmäßige Audits und räumt seinen Kunden ebenfalls Auditmöglichkeiten ein.

Ein Datenbankadministrator einer der Kunden hat die Möglichkeit, sich auf den IT-Systemen, die vom Rechenzentrumsdienstleister betrieben werden, interaktiv anzumelden. Er besitzt auf dem Datenbanksystem Administratorrechte. In der Hoffnung, Informationen über einen Mitbewerber seines Arbeitgebers zu gewinnen, startet er nun ein Schadprogramm, dass es ihm durch einen Fehler in der Grafikkartenemulation der Hypervisors ermöglicht, eigenen Code im Kontext des Hypervisors auszuführen. Dieser Code ermöglicht ihm die Überwachung aller Hypervisor-Funktionen. Dadurch kann er ein Datenbanksystem eines anderen Kunden des Rechenzentrumsdienstleisters als eines identifizieren, dass einem direkten Mitbewerber gehört. Über die Massenspeicherschnittstelle des Hypervisors gelingt es ihm, aus der Datenbank dieser virtuellen Maschine Daten auszulesen und Inhalte zu verändern. Hierdurch wird die Produktion des Konkurrenten empfindlich gestört und es entsteht dem Unternehmen des Administrators ein Wettbewerbsvorteil.

M 2.82 Entwicklung eines Testplans für Standardsoftware

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung
Verantwortlich für Umsetzung: Leiter Fachabteilung, Leiter IT

Die im nachfolgenden beschriebene Vorgehensweise beim Testen orientiert sich an den Standardwerken DIN ISO/IEC 12119 "Software-Erzeugnisse, Qualitätsanforderungen und Prüfbestimmungen", Vorgehensmodell für die Planung und Durchführung von IT-Vorhaben (V-Modell) und dem Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM), die als weiterführende Literatur empfohlen werden.

Vor der Entscheidung für ein geeignetes Standardsoftwareprodukt müssen die nach der Vorauswahl (siehe M 2.81 *Vorauswahl eines geeigneten Standardsoftwareproduktes*) in die engere Wahl gezogenen Produkte als Testlizenz beschafft und ausreichend getestet werden. War es aufgrund zeitlicher Beschränkungen, institutionsinterner Beschaffungsempfehlungen (Einhaltung von Hausstandards) oder anderen Gründen nicht möglich, dass Produkt vor der Beschaffung zu testen, müssen auf jeden Fall Tests vor der endgültigen Inbetriebnahme durchgeführt werden. Die Ergebnisse dieser Tests liefern dann die Grundlage für die Installationsvorschriften und anderer Freigabe-Bedingungen.

Obwohl bereits bei der Vorauswahl eine Überprüfung der notwendigen Anforderungen an das Produkt aufgrund der Herstelleraussagen stattgefunden hat, kann man nicht davon ausgehen, dass diese Anforderungen auch im gewünschten Maße erfüllt werden. Vielmehr muss nun durch systematisches Testen die Eignung und Zuverlässigkeit des Produktes auf Grundlage des Anforderungskataloges überprüft werden, um das geeignetste Produkt auszuwählen.

Dabei bietet es sich an, das Testen in vier Bereiche einzuteilen:

- Eingangsprüfungen (Prüfung auf Computer-Viren, Lauffähigkeit in der gewünschten IT-Einsatzumgebung, ...),
- funktionale Tests (Überprüfung der funktionalen Anforderungen),
- Tests weiterer funktionaler Eigenschaften (Überprüfung von Kompatibilität, Performance, Interoperabilität, Konformität mit Regelungen oder Gesetzen, Benutzerfreundlichkeit, Wartbarkeit, Dokumentation), und
- sicherheitsspezifische Tests (Überprüfung der Sicherheitsanforderungen).

Das prinzipielle Vorgehen beim Testen von Standardsoftware zeigt die folgende Abbildung.

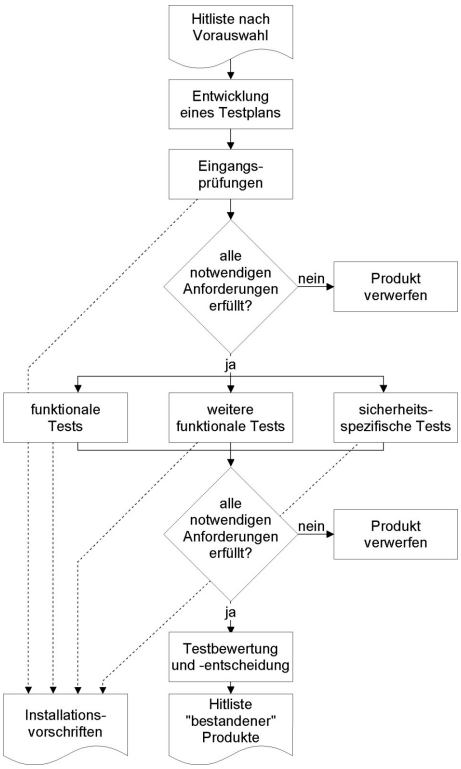


Abbildung 1: Prinzipielles Vorgehen beim Testen von Standardsoftware

Anhand der bei der Vorauswahl erstellten Hitliste sind diejenigen Produkte auszuwählen, die getestet werden sollen. Anschließend wird ein **Testplan** entwickelt.

Dieser umfasst folgende Inhalte:

- Festlegung der Testinhalte anhand des Anforderungskataloges,
- Überprüfung von Referenzen,
- Festlegung des Gesamtprüfaufwandes,
- Zeitplanung einschließlich Prüfaufwand je Testinhalt,
- Festlegung der Testverantwortlichen,
- Testumgebung,
- Inhalt der Testdokumentation,
- Festlegung von Entscheidungskriterien.

Die einzelnen genannten Punkte werden nachfolgend erläutert.

Festlegung der Testinhalte anhand des Anforderungskataloges

Aus dem Anforderungskatalog werden diejenigen Anforderungen ausgewählt, die überprüft werden sollen. Dies sollten insbesondere diejenigen Eigenschaften sein, die eine große Bedeutung oder einen hohen Vertrauensanspruch besitzen.

Überprüfung von Referenzen

Bei der Vorauswahl (siehe M 2.81 *Vorauswahl eines geeigneten Standardsoftwareproduktes*) wurden bereits erste Referenzen über die zu testenden Produkte eingeholt. Diese können ersatzweise herangezogen werden, wenn man der jeweiligen externen Testgruppe ausreichendes Vertrauen entgegenbringt.

Wurde für das Produkt ein Zertifikat nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC) oder den Common Criteria (CC) vergeben, ist anhand des Zertifizierungsreportes zu prüfen, inwieweit die dort dokumentierten Testergebnisse berücksichtigt werden können.

Gegebenenfalls können dann eigene Test unterbleiben oder in geringerem Umfang stattfinden. Die frei werdenden Kapazitäten können auf andere Testinhalte verteilt werden.

Festlegung des Gesamtprüfaufwandes

Um den Aufwand für die Tests nicht ausufern zu lassen, sollte vorab der Gesamtprüfaufwand festgelegt werden, z. B. in Personentagen oder durch Fristsetzung.

Zeitplanung einschließlich Prüfaufwand je Testinhalt

Beim Testen mehrerer Produkte empfiehlt es sich, diese vergleichend zu testen. Das heißt, alle Produkte werden von einer Testgruppe bzgl. einer Anforderung des Anforderungskataloges getestet. Der Prüfaufwand ist damit für jede Anforderung des Anforderungskataloges festzulegen und wird damit automatisch gleichmäßig auf alle zu testenden Produkte verteilt. Der Prüfaufwand ergibt sich dabei aus Prüftiefe und Komplexität der Eigenschaft. Die Prüftiefe der jeweiligen Eigenschaften sollte sich zum einen an ihrem Vertrauensanspruch, das heißt an dem Vertrauen orientieren, das der Korrektheit dieser Eigenschaft entgegengebracht werden muss.

Zum anderen muss aber auch die Fehleranfälligkeit und Nutzungshäufigkeit der jeweiligen Eigenschaft berücksichtigt werden. Ausführlichere Informationen sind der Norm ISO 12119 zu entnehmen.

Hinweise:
- Für sicherheitsspezifische Anforderungen kann die Prüftiefe entsprechend der geforderten Mechanismenstärke zusätzlich relativiert werden.
- Der Prüfaufwand für die Eingangsprüfungen sollte gemessen an den anderen Tests gering sein.

Abschließend ist der Gesamtprüfaufwand entsprechend dem relativen Prüfaufwand der jeweiligen Eigenschaft auf die einzelnen Testabschnitte zu verteilen.

Festlegung der Testverantwortlichen

Für jeden Testinhalt ist nun festzulegen, welche Aufgaben durchzuführen sind und wer dafür verantwortlich ist. Insbesondere ist zu beachten, dass bei einigen Testinhalten der Personal- bzw. Betriebsrat, der Datenschutzbeauftragte und der IT-Sicherheitsbeauftragte zu beteiligen ist.

Testumgebung

Testen ist immer destruktiv, da vorsätzlich nach Fehlern gesucht wird. Aus diesem Grund muss das Testen immer in einer isolierten Testumgebung erfolgen.

Die Testumgebung sollte nach Möglichkeit ein genaues funktionales Abbild der Produktionsumgebung sein. In der Regel ist es jedoch nicht wirtschaftlich, die Produktionsumgebung in vollem Umfang nachzubilden.

Damit für die ausgewählten Produkte gleiche Randbedingungen gegeben sind, sollte eine Referenztestumgebung definiert werden. Für einzelne Tests kann diese weiter angepasst oder eingeschränkt werden.

Die für die einzelnen Prüfungen benötigten Ressourcen (Betriebsmittel, IT-Infrastruktur) sind zu spezifizieren. Es sollte im Detail beschrieben werden, wann und in welchem Umfang sie verfügbar sein müssen.

Wichtig ist, dass alle Betriebssysteme in allen im Produktionsbetrieb eingesetzten Versionen (Releases) in der Testumgebung zur Verfügung stehen. Die Intention ist dabei die Ermittlung von systembedingten Schwachstellen von Komponenten der Produktionsumgebung im Zusammenspiel mit dem zu installierenden Standardsoftwareprodukt. In Ausnahmefällen, wenn sich Aspekte verallgemeinern lassen, kann auf einzelne Komponenten verzichtet werden.

Folgende weitere Aspekte sind unbedingt zu beachten und helfen, eine sichere und geeignete Testumgebung aufzubauen:

- Die Freiheit von Schadprogrammen der Testumgebung ist durch ein aktuelles Viren-Suchprogramm sicherzustellen.
- Die Testumgebung muss frei sein von Seiteneffekten auf den Echtbetrieb. Um Wechselwirkungen von vornherein zu vermeiden, empfiehlt es sich, dedizierte IT-Systeme zu installieren.
- Die Zugriffsrechte müssen in der Testumgebung derart konfiguriert werden, wie sie dem Produktionsbetrieb entsprechen.
- Der Zutritt und Zugang zur Testumgebung muss geregelt sein.
- Es muss sichergestellt werden, dass das Produkt genau in der Testumgebung ermittelten Konfiguration in den Produktionsbetrieb übernommen wird. Daher ist in der Testumgebung ein geeignetes Verfahren zum Integritätsschutz einzusetzen (digitale Signaturen, Checksummen).
- Die Kosten für den Aufbau der Testumgebung müssen angemessen sein.

Nach Beendigung aller geplanten Tests ist zu entscheiden, ob die Testumgebung abgebaut werden soll. Ggf. sind weitere Tests auch nach der Beschaffung eines Produktes notwendig, so dass es eventuell wirtschaftlich ist, die Testumgebung vorzuhalten. Vor dem Abbau der Testumgebung sind die Testdaten zu löschen, falls sie nicht mehr benötigt werden (z. B. für eine spätere Installation). Druckerzeugnisse sind ordnungsgemäß zu entsorgen, Programme sind zu deinstallieren. Die Testlizenzen der nicht ausgewählten Produkte sind zurückzugeben.

Inhalt der Testdokumentation

Im Testplan ist vorzugeben, wie ausführlich die Testdokumentation zu erstellen ist. Hierbei sind die Aspekte der Nachvollziehbarkeit, Reproduzierbarkeit und Vollständigkeit zu berücksichtigen.

Die Testdokumentation muss Testpläne, -ziele, -verfahren und -ergebnisse enthalten und die Übereinstimmung zwischen den Tests und den spezifizierten Anforderungen beschreiben. Sämtliche Testaktivitäten sowie die getroffene Testbewertung (inklusive Entscheidungsargumentation) sind schriftlich festzuhalten. Dazu gehören im einzelnen

- Produktbezeichnung und Beschreibung,
- Testbeginn, -ende und -aufwand,
- Testverantwortliche,
- Konfiguration der Testumgebung,
- Beschreibung der Testfälle,
- Entscheidungskriterien, Testergebnisse und Argumentationsketten, und

- nicht erfüllte Anforderungen des Anforderungskataloges.

Der Testgruppe sollte eine Möglichkeit zur übersichtlichen Dokumentation und Protokollierung der Testaktivitäten und -ergebnisse zur Verfügung gestellt werden (z. B. Protokollierungstool, Formblätter o. Ä.).

Wird beim Testen ein automatisiertes Werkzeug verwendet, muss die Testdokumentation ausreichende Informationen über dieses Werkzeug und die Art seines Einsatzes enthalten, damit die Entscheidung nachvollzogen werden kann.

Festlegung von Entscheidungskriterien

Bei der Bewertung der jeweiligen Testinhalte kann beispielsweise folgende dreistufige Skala verwendet werden:

Note		**Entscheidungskriterien**
0	-	Anforderungen sind nicht erfüllt.
	oder	
	-	Es wurden nicht tolerierbare Fehler festgestellt, die sich nicht beheben lassen.
1	-	Anforderungen sind erfüllt, aber es bestehen Vorbehalte (z. B. Funktion ist nur eingeschränkt geeignet).
	oder	
	-	Es sind geringfügige Fehler festgestellt worden. Diese spielen nur eine untergeordnete Rolle, da sie tolerierbare Auswirkungen auf den Produktionsbetrieb haben oder da sie nur mit vernachlässigbarer Wahrscheinlichkeit vorkommen können.
2	-	Anforderungen sind in vollem Umfang erfüllt.
	oder	
	-	Fehler, die ggf. aufgetaucht sind, sind entweder zu beheben oder haben für den Betrieb keinerlei Bedeutung.

Tabelle: Bewertungsskala

Sind Fehler aufgetaucht, die nicht reproduziert werden können, hat der Prüfer zu entscheiden, welcher Kategorie (Note) der Fehler zuzuordnen ist.

Sind Fehler aufgetreten, die während des Tests behoben werden können, ist nach deren Behebung erneut im erforderlichen Umfang zu testen.

Beispiel:

Das Beispiel des Kompressionsprogramms aus M 2.81 *Vorauswahl eines geeigneten Standardsoftwareproduktes* wird hier fortgesetzt, um eine Möglichkeit zu beschreiben, den Prüfaufwand für jede Anforderung des Anforderungskataloges festzulegen. Hier wird der Prüfaufwand aus Prüftiefe und Komplexität abgeleitet. Der Vertrauensanspruch kennzeichnet den Bedarf an Vertrauen in die Eigenschaft.

Die Nutzungshäufigkeit, Fehleranfälligkeit und Komplexität einer Eigenschaft werden wie folgt bewertet:

- 1 bedeutet "niedrig",
- 2 bedeutet "mittel",
- 3 bedeutet "hoch".

Ein besonderer Fall ist gegeben, wenn eine unveränderbare Eigenschaft des Produktes betrachtet werden soll, die unabhängig von der Fehleranfälligkeit oder Nutzungshäufigkeit ist. Für diesen Fall wird der Wert 0 vergeben. Für das Beispiel des Kompressionsprogramms ergibt sich folgende Abbildung:

	Vertrauensanspruch	Fehleranfälligkeit	Nutzungshäufigkeit	Prüftiefe	Komplexität	Prüfaufwand	in %
korrekte Kompression und Dekompression	5	2	3	10	2	20	23
Erkennen von Bitfehlern in einer komprimierten Datei	2	2	1	5	2	10	11
Löschen von Dateien nur nach erfolgreicher Kompression	3	2	1	6	1	6	7
DOS-PC, 80486, 8 MB	5	0	0	5	1	5	6
Windows-tauglich	1	0	0	1	1	1	1
Durchsatz bei 50 MHz über 1 MB/s	3	1	2	6	1	6	7
Kompressionsrate über 40% für Textdateien des Programms XYZ	3	2	2	7	1	7	8
Online-Hilfefunktion	1	1	2	4	1	4	5
Maximal Kosten 50,00 EUR pro Lizenz	5	0	0	5	1	5	5
Passwortschutz für komprimierte Dateien (Mechanismenstärke hoch)	5	1	2	8	3	24	27

Abbildung 2: Beispiel für Kompressionsprogramm

In diesem Beispiel wurde der Prüfaufwand folgendermaßen definiert:

*Prüfaufwand = Komplexität * Prüftiefe*

dabei ist

Prüftiefe = Vertrauensanspruch + Fehleranfälligkeit + Nutzungshäufigkeit

(Die Prozentzahlen für den Prüfaufwand in der letzten Spalte der Tabelle ergeben sich aus den für den Prüfaufwand errechneten Werten bei Division durch die Summe dieser Werte.)

Ein Beispiel für eine andere Methode, den Prüfaufwand zu berechnen und die Prüfergebnisse zu bewerten, findet sich in der Norm ISO 12119. Hier wird folgende Gewichtung der einzelnen Anforderungen vorgenommen: *Bewertung jedes Prüfinhaltes =(Komplexität+Fehleranfälligkeit) * (Benutzungshäufigkeit + Wichtigkeit)*.

Letztendlich muss der Testverantwortliche eine dem Produkt und der Institution adäquate Bewertungsmethode individuell festlegen.

Nach Erstellung des Testplans wird für jeden im Testplan spezifizierten Testinhalt ein Tester oder eine Testgruppe mit der Durchführung des ihr zugeteilten Tests beauftragt. Der Testplan ist der Testgruppe zu übergeben und die für die Einzeltests vorgegebenen Zeiten sind mitzuteilen.

Prüffragen:

- Ist ein Testplan für das Testen von Standardsoftware auf Basis des Anforderungskataloges erstellt?
- Ist die Testumgebung logisch oder physisch von der Produktivumgebung getrennt?
- Existiert eine nachvollziehbare, reproduzierbare und vollständige Testdokumentation?
- Enthält die Testdokumentation Testpläne, -ziele, -verfahren und -ergebnisse und zeigt die Übereinstimmung zwischen den Tests und den spezifizierten Anforderungen?

M 2.83 Testen von Standardsoftware

Verantwortlich für Initiierung: Leiter Fachabteilung, Leiter IT
Verantwortlich für Umsetzung: Tester

Das Testen von Standardsoftware lässt sich in die Abschnitte Vorbereitung, Durchführung und Auswertung unterteilen. In diesen Abschnitten sind folgende Aufgaben wahrzunehmen:

Testvorbereitung
- Festlegung der Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge)
- Generierung von Testdaten und Testfällen
- Aufbau der benötigten Testumgebung

Testdurchführung
- Eingangsprüfungen
- Funktionale Tests
- Tests weiterer funktionaler Eigenschaften
- Sicherheitsspezifische Tests
- Pilotanwendung

Testauswertung

Die einzelnen Aufgaben werden nachfolgend beschrieben.

Testvorbereitung

Festlegung der Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge)

Methoden zur Durchführung von Tests sind z. B. statistische Analyse, Simulation, Korrektheitsbeweis, symbolische Programmausführung, Review, Inspektion, Versagensanalyse. Hierbei muss beachtet werden, dass einige dieser Testmethoden nur bei Vorliegen des Quellcodes durchführbar sind. In der Vorbereitungsphase muss die geeignete Testmethode ausgewählt und festgelegt werden.

Es muss geklärt werden, welche Verfahren und Werkzeuge zum Testen von Programmen und zum Prüfen von Dokumenten eingesetzt werden. Typische Verfahren zum Testen von Programmen sind z. B. Black-Box-Tests, White-Box-Tests oder Penetrationstests. Dokumente können z. B. durch informelle Prüfungen, Reviews oder anhand von Checklisten kontrolliert werden.

Ein Black-Box-Test ist ein Funktionalitätstest ohne Kenntnis der internen Programmabläufe, bei dem z. B. das Programm mit allen Datenarten für alle Testfälle mit Fehlerbehandlung und Plausibilitätskontrollen durchlaufen wird.

Bei einem White-Box-Test handelt es sich um einen Funktionalitätstests unter Offenlegung der internen Programmabläufe, z. B. durch Quellcode-Überprüfung oder Tracing. White-Box-Tests gehen in der Regel über den IT-Grundschutz hinaus und können für Standardsoftware in der Regel nicht durchgeführt werden, da der Quellcode vom Hersteller nicht offengelegt wird.

Bei Funktionalitätstests soll der Nachweis erbracht werden soll, dass der Testinhalt der Spezifikation entspricht. Durch Penetrationstests soll festgestellt werden, ob bekannte oder vermutete Schwachstellen im praktischen Betrieb ausgenutzt werden können, beispielsweise durch Manipulationsversuche an

den Sicherheitsmechanismen oder durch Umgehung von Sicherheitsmechanismen durch Manipulationen auf Betriebssystemebene.

Weiterhin ist die Art und Weise der Ergebnissicherung und -auswertung festzuschreiben, insbesondere im Hinblick auf die Wiederholbarkeit von Prüfungen. Es muss geklärt werden, welche Daten während und nach der Prüfung festzuhalten sind.

Generierung von Testdaten und Testfällen

Die Vorbereitung von Tests umfasst auch die Generierung von Testdaten. Methode und Vorgehensweise sind zuvor festzulegen und zu beschrieben.

Für jeden einzelnen Testinhalt muss eine dem Testaufwand angemessene Anzahl von Testfällen generiert werden. Jede der folgenden Kategorien ist dabei zu berücksichtigen:

Standardfälle sind Fälle, mit denen die korrekte Verarbeitung der definierten Funktionalitäten überprüft werden soll. Die eingehenden Daten nennt man **Normalwerte** oder **Grenzwerte**. Normalwerte sind Daten innerhalb, Grenzwerte sind Eckdaten des jeweils gültigen Eingabebereichs.

Fehlerfälle sind Fälle, in denen versucht wird, mögliche Fehlermeldungen des Programms zu provozieren. Diejenigen Eingabewerte, auf die das Programm mit vorgegebenen Fehlermeldungen reagieren soll, nennt man **Falschwerte**.

Ausnahmefälle sind Fälle, bei denen das Programm ausnahmsweise anders reagieren muss als bei Standardfällen. Es muss daher überprüft werden, ob das Programm diese Fälle als solche erkennt und korrekt bearbeitet.

Beispiele:
- Wenn die Eingabeparameter zwischen 1 und 365 liegen dürfen, sind Testläufe mit Falschwerten (z. B. 0 oder 1000), den Grenzwerten 1 und 365, sowie mit Normalwerten zwischen 1 und 365 durchführen.
- Ein Programm zur Terminplanung soll Feiertage berücksichtigen. Ein Sonderfall ist dann gegeben, wenn ein bestimmter Tag Feiertag in allen Bundesländern ist, außer in einem. Für dieses Bundesland und für diesen Tag muss das Programm dann differenziert reagieren.

Ist die Generierung von Testdaten zu aufwendig oder schwierig, können auch anonymisierte Echtdaten für den Test eingesetzt werden. Aus Gründen des

Vertraulichkeitsschutzes müssen Echtdaten unbedingt zuverlässig anonymisiert werden. Zu beachten bleibt, dass die anonymisierten Echtdaten u. U. nicht alle Grenzwerte und Ausnahmefälle abdecken, so dass diese gesondert erzeugt werden müssen.

Über die Testdaten hinaus sollten auch alle Arten möglicher Benutzerfehler betrachtet werden. Problematisch sind insbesondere alle Benutzerreaktionen, die im Programmablauf nicht vorgesehen und dementsprechend nicht korrekt abgewiesen werden.

Aufbau der benötigten Testumgebung

Die im Testplan beschriebene Testumgebung muss aufgebaut und die zu testenden Produkte dort installiert werden. Die eingesetzten Komponenten sind zu identifizieren und deren Konfiguration ist zu beschreiben. Treten bei der Installation des Produktes Abweichungen von der beschriebenen Konfiguration auf, so ist dies zu dokumentieren.

Testdurchführung

Die Durchführung der Tests muss anhand des Testplans erfolgen. Jede Aktion sowie die Testergebnisse müssen ausreichend dokumentiert und bewertet werden. Insbesondere wenn Fehler auftreten, sind diese derart zu dokumentieren, dass sie reproduziert werden können. Die für den späteren Produktionsbetrieb geeigneten Betriebsparameter müssen ermittelt und für die spätere Erstellung einer Installationsanweisung festgehalten werden.

Werden zusätzliche Funktionen beim Produkt erkannt, die nicht im Anforderungskatalog aufgeführt, aber trotzdem von Nutzen sein können, so ist hierfür mindestens ein Kurztest durchzuführen. Zeigt sich, dass diese Funktion von besonderer Bedeutung für den späteren Betrieb sind, sind diese ausführlich zu testen. Für den zusätzlich anfallenden Prüfaufwand ist ggf. eine Fristverlängerungen bei den Verantwortlichen zu beantragen. Die Testergebnisse sind in die Gesamtbewertung mit einzubeziehen.

Zeigt sich bei Bearbeitung einzelner Testinhalte, dass eine oder mehrere Anforderungen des Anforderungskataloges nicht konkret genug waren, sind diese gegebenenfalls zu konkretisieren.

Beispiel: Im Anforderungskatalog wird zum Vertraulichkeitsschutz der zu bearbeitenden Daten Verschlüsselung gefordert. Während des Testens hat sich gezeigt, dass eine Offline-Verschlüsselung für den Einsatzzweck ungeeignet. Daher ist der Anforderungskatalog hinsichtlich einer Online-Verschlüsselung zu ergänzen. (Eine Offline-Verschlüsselung muss vom Anwender angestoßen und die zu verschlüsselnden Elemente jeweils spezifiziert werden; eine Online-Verschlüsselung erfolgt transparent für den Anwender mit voreingestellten Parametern.)

Eingangsprüfungen

Vor allen anderen Tests sind zunächst die folgenden grundlegenden Aspekte zu testen, da ein Misserfolg bei diesen Eingangsprüfungen zu direkten Aktionen oder dem Testabbruch führt:

- Die Computer-Virenfreiheit des Produktes ist durch ein aktuelles Virensuchprogramm zu überprüfen.
- In einem Installationstest muss festgestellt werden, ob das Produkt für den späteren Einsatzzweck einfach, vollständig und nachvollziehbar zu installieren ist. Ebenfalls muss überprüft werden, wie das Produkt vollständig deinstalliert wird.
- Die Lauffähigkeit des Produktes ist in der geplanten Einsatzumgebung zu überprüfen; dies beinhaltet insbesondere eine Überprüfung der Bildschirmaufbereitung, der Druckerausgabe, der Mausunterstützung, der Netzfähigkeit, etc.
- Die Vollständigkeit des Produktes (Programme und Handbücher) ist zu überprüfen, z. B. durch einen Vergleich mit dem Bestandsverzeichnis, der Produktbeschreibung oder ähnlichem.
- Es sollten Kurztests von Funktionen des Programms durchgeführt werden, die nicht explizit in den Anforderungen erwähnt wurden, im Hinblick auf Funktion, Plausibilität, Fehlerfreiheit, etc.

Funktionale Tests

Die funktionalen Anforderungen, die im Anforderungskatalog an das Produkt gestellt wurden, sind auf folgende Aspekte zu untersuchen:

- *Existenz der Funktion* durch Aufruf im Programm und Auswertung der Programmdokumentationen.

- Fehlerfreiheit bzw. Korrektheit der Funktion
  Um die Fehlerfreiheit bzw. Korrektheit der Funktion sicherzustellen, sind je nach Prüftiefe bei der Untersuchung unterschiedliche Testverfahren wie Black-Box-Tests, White-Box-Tests oder simulierter Produktionsbetrieb anzuwenden.
  Die in der Vorbereitungsphase erstellten Testdaten und Testfälle werden im Funktionalitätstest eingesetzt. Bei den Funktionalitätstests ist es notwendig, die Testergebnisse mit den vorgegebenen Anforderungen zu vergleichen. Außerdem ist zu überprüfen, wie das Programm bei fehlerhaften Eingabeparametern oder fehlerhafter Bedienung reagiert. Die Funktion ist auch mit den Grenzwerten der Intervalle von Eingabeparametern sowie mit Ausnahmefällen zu testen. Diese müssen entsprechend erkannt und korrekt behandelt werden.
- Eignung der Funktion
  Die Eignung einer Funktion zeichnet sich dadurch aus, dass die Funktion

  - tatsächlich die Aufgabe im geforderten Umfang und effizient erfüllt und
  - sich leicht in die üblichen Arbeitsabläufe integrieren lässt.

  Ist die Eignung der Funktion nicht offensichtlich, bietet es sich an, dies in einem simulierten Produktionsbetrieb, aber immer noch in der Testumgebung zu testen.
- Widerspruchsfreiheit
  Die Widerspruchsfreiheit der einzelnen Funktionen ist zu überprüfen und zwar jeweils zwischen Anforderungskatalog, Dokumentation und Programm. Eventuelle Widersprüche sind zu dokumentieren. Abweichungen zwischen Dokumentation und Programm sind so festzuhalten, dass sie bei einem späteren Einsatz des Produktes in den Ergänzungen zur Dokumentation aufgenommen werden können.

Tests weiterer funktionaler Eigenschaften

Die im Anforderungskatalog neben den funktionalen und den sicherheitsspezifischen Anforderungen spezifizierten weiteren funktionalen Eigenschaften sind ebenfalls zu überprüfen:

- Performance
  Das Laufzeitverhalten sollte für alle geplanten Konfigurationen des Produktes ermittelt werden. Um die Performance ausreichend zu testen, sind in der Regel Tests, in denen der Produktionsbetrieb simuliert wird oder auch Pilotanwendung bei ausgewählten Anwendern sinnvoll. Es muss festgestellt werden, ob die gestellten Performanceanforderungen erfüllt sind.
- Zuverlässigkeit
  Das Verhalten bei zufälligen oder mutwillig herbeigeführten Systemabstürzen ("Crash-Test") ist zu analysieren und es ist festzustellen, welche Schäden dabei entstehen. Es ist festzuhalten, ob nach Systemabstürzen ein ordnungsgemäßer und korrekter Wiederanlauf des Produktes möglich ist. Es ist ebenfalls zu überprüfen, ob ein direkter Zugriff auf Datenbestände unabhängig von der regulären Programmfunktion erfolgen kann. In vielen Fällen kann ein solcher Zugriff zu Datenverlusten führen und sollte dann vom Produkt verhindert werden. Ebenfalls sollte festgehalten werden, ob das Programm Möglichkeiten unterstützt, "kritische Aktionen" (z. B. Löschen, Formatieren) rückgängig zu machen.
- Benutzerfreundlichkeit

Ob das Produkt benutzerfreundlich ist, ist in besonderem Maße vom subjektiven Empfinden der Testperson abhängig. Jedoch können bei der Beurteilung folgende Aspekte Anhaltspunkte liefern:

- Technik der Menüoberflächen (Pull-Down-Menüs, Scrolling, Drag & Drop, etc.),
- Design der Menüoberflächen (z. B. Einheitlichkeit, Verständlichkeit, Menüführung),
- Tastaturbelegung,
- Fehlermeldungen,
- problemloses Ansprechen von Schnittstellen (Batchbetrieb, Kommunikation, etc.),
- Lesbarkeit der Benutzerdokumentation,
- Hilfefunktionen.

Die Analyse der Benutzerfreundlichkeit muss mögliche Betriebsarten des Produktes beschreiben, einschließlich des Betriebes nach Bedien- oder Betriebsfehlern, und ihre Konsequenzen und Folgerungen für die Aufrechterhaltung eines sicheren Betriebes.

- Wartbarkeit
  Der personelle und finanzielle Aufwand für die Wartung und Pflege des Produktes sollte während des Testens ermittelt werden. Dieser kann z. B. anhand von Referenzen wie anderen Referenzinstallationen oder Tests in Fachzeitschriften oder anhand des während des Testens ermittelten Installationsaufwandes geschätzt werden. Hierfür muss dokumentiert werden, wie viele manuelle Eingriffe während der Installation notwendig waren, um die angestrebte Konfiguration zu erreichen. Sind bereits Erfahrungen mit Vorgängerversionen des getesteten Produktes gesammelt worden, sollte hinterfragt werden, wie aufwendig deren Wartung war.
  Es sollte nachgefragt werden, inwieweit Support durch den Hersteller oder Vertreiber angeboten wird und zu welchen Konditionen. Wird vom Hersteller oder Vertreiber eine Hotline angeboten, sollte auch deren Erreichbarkeit und Güte betrachtet werden.
- Dokumentation
  Die vorliegende Dokumentation muss daraufhin überprüft werden, ob sie vollständig, korrekt und widerspruchsfrei ist. Darüber hinaus sollte sie verständlich, eindeutig, fehlerfrei und übersichtlich sein.
  Es muss weiterhin kontrolliert werden, ob sie für eine sichere Verwendung und Konfiguration ausreicht. Alle sicherheitsspezifischen Funktionen müssen beschrieben sein.

Darüber hinaus sind als weitere Punkte des Anforderungskatalogs zu testen:

- Kompatibilitätsanforderungen
- Interoperabilität
- Konformität zu Standards
- Einhaltung von internen Regelungen und gesetzlichen Vorschriften
- Softwarequalität

Sicherheitsspezifische Tests

Wurden sicherheitsspezifische Anforderungen an das Produkt gestellt, so sind zusätzlich zu den vorgenannten Untersuchungen auch folgende Aspekte zu untersuchen:

- Wirksamkeit und Korrektheit der Sicherheitsfunktionen,
- Stärke der Sicherheitsmechanismen und
- Unumgänglichkeit und Zwangsläufigkeit der Sicherheitsmechanismen.

Als Grundlage für eine Sicherheitsuntersuchung könnte beispielsweise das Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEM) herangezogen werden, in dem viele der nachfolgend aufgezeigten Vorgehensweise beschrieben sind. Die weiteren Ausführungen dienen zur Orientierung und zur Einführung in die Thematik.

Zu Beginn muss durch funktionale Tests zunächst nachgewiesen werden, dass das Produkt die erforderlichen Sicherheitsfunktionen bereitstellt.

Anschließend ist zu überprüfen, ob alle erforderlichen Sicherheitsmechanismen im Anforderungskatalog genannt wurden, ggf. ist dieser zu ergänzen. Um die Mindeststärke der Mechanismen zu bestätigen oder zu verwerfen sind **Penetrationstests** durchzuführen. Penetrationstests sind nach allen anderen Tests durchzuführen, da sich aus diesen Tests Hinweise auf potentielle Schwachstellen ergeben können.

Durch Penetrationstests kann das Testobjekt oder die Testumgebung beschädigt oder beeinträchtigt werden. Damit solche Schäden keine Auswirkungen haben, sollten vor der Durchführung von Penetrationstests Datensicherungen gemacht werden.

Penetrationstests können durch Verwendung von Sicherheitskonfigurations- und Protokollierungstools unterstützt werden. Diese Tools untersuchen eine Systemkonfiguration und suchen nach gemeinsamen Schwachstellen wie etwa allgemein lesbaren Dateien und fehlenden Passwörtern.

Mit Penetrationstests soll das Produkt auf Konstruktionsschwachstellen untersucht werden, indem dieselben Methoden angewandt werden, die auch ein potentieller Angreifer zur Ausnutzung von Schwachstellen benutzen würde, wie z. B.

- Ändern der vordefinierten Befehlsabfolge,
- Ausführen einer zusätzlichen Funktion,
- Direktes oder indirektes Lesen, Schreiben oder Modifizieren interner Daten,
- Ausführen von Daten, deren Ausführung nicht vorgesehen ist,
- Verwenden einer Funktion in einem unerwarteten Kontext oder für einen unerwarteten Zweck,
- Aktivieren der Fehlerüberbrückung,
- Nutzen der Verzögerung zwischen dem Zeitpunkt der Überprüfung und dem Zeitpunkt der Verwendung,
- Unterbrechen der Abfolge durch Interrupts, oder
- Erzeugen einer unerwarteten Eingabe für eine Funktion.

Die Mechanismenstärken werden anhand der Begriffe Fachkenntnisse, Gelegenheiten und Betriebsmittel definiert, in der ITSEM werden diese näher erläutert. Beispielsweise können zur Bestimmung der Mechanismenstärke folgende Regeln angewandt werden:

- Kann der Mechanismus innerhalb von Minuten von einem Laien allein überwunden werden, dann kann er **nicht einmal als niedrig** eingestuft werden.
- Kann ein erfolgreicher Angriff von jedem bis auf einen Laien innerhalb von Minuten durchgeführt werden, dann ist der Mechanismus als **niedrig** einzustufen.
- Wenn für einen erfolgreichen Angriff ein Experte benötigt wird, der mit der vorhandenen Ausstattung Tage braucht, dann ist der Mechanismus als **mittel** einzustufen.

- Kann der Mechanismus nur von einem Experten mit Sonderausstattung überwunden werden, der dafür Monate braucht und eine geheime Absprache mit einem Systemverwalter treffen muss, dann ist er als **hoch** einzustufen.

Es muss sichergestellt werden, dass die durchgeführten Tests alle sicherheitsspezifischen Funktionen umfassen. Wichtig ist zu beachten, dass durch Testen immer nur Fehler oder Abweichungen von den Spezifikationen festgestellt werden können, niemals jedoch die Abwesenheit von Fehlern.

An einigen **Beispielen** sollen typische Untersuchungsaspekte aufgezeigt werden:

Passwortschutz:
- Gibt es vom Hersteller voreingestellte Passwörter? Typische Beispiele für solche Passwörter sind der Produktname, der Herstellername, "SUPERVISOR", "ADMINISTRATOR", "USER", "GUEST".
- Welche Datei ändert sich, wenn ein Passwort geändert wurde? Kann diese Datei durch eine alte Version aus einer Datensicherung ersetzt werden, um alte Passwörter zu aktivieren? Werden die Passwörter verschlüsselt gespeichert oder sind sie im Klartext auslesbar? Ist es möglich, in dieser Datei Änderungen vorzunehmen, um neue Passwörter zu aktivieren?
- Wird der Zugang tatsächlich nach mehreren fehlerhaften Passworteingaben gesperrt?
- Werden in Zeitschriften oder Mailboxen Programme angeboten, die die Passwörter des untersuchten Produkts ermitteln können? Für einige Standardapplikationen sind solche Programme erhältlich.
- Wenn Dateien mit Passwörtern geschützt werden, kann durch einen Vergleich einer Datei vor und nach der Passwortänderung die Stelle ermittelt werden, an der das Passwort gespeichert wird. Ist es möglich, an dieser Stelle Änderungen oder alte Werte einzugeben, um bekannte Passwörter zu aktivieren? Werden die Passwörter verschlüsselt gespeichert? Wie ist die Stelle belegt, wenn der Passwortschutz deaktiviert ist?
- Kann die Passwort-Prüfroutine unterbrochen werden? Gibt es Tastenkombinationen, mit denen die Passworteingabe umgangen werden kann?

Zugriffsrechte:
- In welchen Dateien werden Zugriffsrechte gespeichert und wie werden sie geschützt?
- Können Zugriffsrechte von Unberechtigten geändert werden?
- Können Dateien mit alten Zugriffsrechten zurückgespielt werden und welche Rechte benötigt man dazu?
- Können die Rechte des Administrators so eingeschränkt werden, dass er keinen Zugriff auf die Nutz- oder Protokolldaten erhält?

Datensicherung:
- Können erstellte Datensicherungen problemlos rekonstruiert werden?
- Können Datensicherungen durch ein Passwort geschützt werden? Wenn ja, können die oben dargestellten Untersuchungsansätze für Passwörter eingesetzt werden.

Verschlüsselung:
- Bietet das Produkt an, Dateien oder Datensicherungen zu verschlüsseln?
- Werden mehrere verschiedene Verschlüsselungsalgorithmen angeboten? Hierbei ist im allgemeinen folgende Faustregel zu beachten: "Je schneller ein in Software realisierter Verschlüsselungsalgorithmus ist, um so unsicherer ist er."

- Wo werden die zur Ver- oder Entschlüsselung genutzten Schlüssel gespeichert?
  Bei einer lokalen Speicherung ist zu untersuchen, ob diese Schlüssel passwortgeschützt oder mit einem weiteren Schlüssel überschlüsselt geschützt werden. Bei einem **Passwortschutz** sind die obigen Punkte zu berücksichtigen. Bei einer Überschlüsselung ist zu betrachten, wie der zugehörige Schlüssel geschützt wird.
  Dazu können folgende Punkte betrachtet werden: Welche Datei ändert sich, wenn ein Schlüssel geändert wurde? Durch den Vergleich dieser Datei vor und nach der Schlüsseländerung kann die Stelle ermittelt werden, an der dieser Schlüssel gespeichert wird. Ist es möglich, an dieser Stelle Änderungen vorzunehmen, um neue Schlüssel zu aktivieren, die dann vom Anwender genutzt werden, ohne dass dieser die Kompromittierung bemerkt?
- Gibt es vom Hersteller voreingestellte Schlüssel, die vor der erstmaligen Benutzung des Programms geändert werden müssen?
- Was passiert, wenn bei der Entschlüsselung ein falscher Schlüssel eingegeben wird?
- Wird nach der Verschlüsselung einer Datei die unverschlüsselte Variante gelöscht? Wenn ja, wird sie zuverlässig überschrieben? Wird vor der Löschung überprüft, ob die Verschlüsselung erfolgreich war?

Protokollierung:
- Wird der Zugriff auf Protokolldaten für Unbefugte verwehrt?
- Werden die zu protokollierenden Aktivitäten lückenlos aufgezeichnet?
- Hat der Administrator die Möglichkeit aufgrund seiner privilegierten Rechte, sich unberechtigt und unbemerkt Zugriff auf Protokolldaten zu verschaffen oder kann er die Protokollierung unbemerkt deaktivieren?
- Wie reagiert das Programm, wenn der Protokollierungsspeicher überläuft?

Darüber hinaus muss festgestellt werden, ob durch das neue Produkt Sicherheitseigenschaften an anderer Stelle unterlaufen werden. **Beispiel:** das zu testende Produkt bietet eine Schnittstelle zur Betriebssystemumgebung, das IT-System war aber vorher so konfiguriert, dass keine solchen Schnittstellen existierten.

Pilotanwendung:

Nach Abschluss aller anderen Tests kann noch eine Pilotanwendung, also ein Einsatz unter Echtbedingungen, für notwendig gehalten werden.

Erfolgt der Test in der Produktionsumgebung mit Echtdaten, muss vorab durch eine ausreichende Anzahl von Tests die korrekte und fehlerfreie Funktionsweise des Programms bestätigt worden sein, um die Verfügbarkeit und Integrität der Produktionsumgebung nicht zu gefährden. Dabei kann das Produkt beispielsweise bei ausgewählten Benutzern installiert werden, die es dann für einen gewissen Zeitraum im echten Produktionsbetrieb einsetzen.

Testauswertung:

Anhand der festgelegten Entscheidungskriterien sind die Testergebnisse zu bewerten, alle Ergebnisse zusammenzuführen und mit der Testdokumentation der Beschaffungsstelle bzw. Testverantwortlichen vorzulegen.

Anhand der Testergebnisse sollte ein abschließendes Urteil für ein zu beschaffendes Produkt gefällt werden. Hat kein Produkt den Test bestanden, muss überlegt werden, ob eine neue Marktsichtung vorgenommen werden soll, ob

die gestellten Anforderungen zu hoch waren und geändert werden müssen oder ob von einer Beschaffung zu diesem Zeitpunkt abgesehen werden muss.

Beispiel:

Am Beispiel eines Kompressionsprogramms wird nun eine Möglichkeit beschrieben, Testergebnisse auszuwerten. Getestet wurden vier Produkte, die nach der dreistufigen Skala aus M 2.82 *Entwicklung eines Testplans für Standardsoftware* bewertet wurden.

Eigenschaft	**Notwendig/ wünschenswert**	**Bedeutung**	**Produkt 1**	**Produkt 2**	**Produkt 3**	**Produkt 4**
korrekte Kompression und Dekompression	N	10	2	2	j	0
Erkennen von Bitfehlern in einer komprimierten Datei	N	10	2	2	n	2
Löschung von Dateien nur nach erfolgreicher Kompression	N	10	2	2	j	2
DOS-PC, 80486, 8 MB	N	10	2	2	j	2
Windows-tauglich	W	2	0	2	j	2
Durchsatz bei 50 MHz über 1 MB/s	W	4	2	2	j	2
Kompressionsrate über 40%	W	4	2	1	n	0
Online-Hilfefunktion	W	3	0	0	n	2
Passwortschutz für	W	2	2	1	n	2

Eigenschaft	Notwendig/ wünschenswert	Bedeutung	Produkt 1	Produkt 2	Produkt 3	Produkt 4
komprimierte Dateien						
Bewertung			100	98	K.O.	K.O.
Preisermittlung (maximale Kosten 50.- EUR pro Lizenz)			49,- EUR	25,- EUR		39,- EUR

Tabelle: Testplan für Standardsoftware

Produkt 3 war bereits in der Vorauswahl gescheitert und wurde daher nicht getestet.

Produkt 4 scheiterte in dem Testabschnitt "korrekte Kompression und Dekompression", weil die Erfüllung der Eigenschaft mit 0 bewertet wurde, es sich dabei aber um eine notwendige Eigenschaft handelt.

Bei der Berechnung der Bewertungspunktzahlen für die Produkte 1 und 2 wurden die Noten als Multiplikatoren für die jeweilige Bedeutungskennzahl benutzt und schließlich die Summe gebildet:

Produkt 1: 10*2+10*2+10*2+10*2+2*0+4*2+4*2+2*2 = 120
Produkt 2: 10*2+10*2+10*2+10*2+2*2+4*2+4*1+2*1 = 118

Nach der Testauswertung ist somit Produkt 1 auf dem ersten Platz, wird aber knapp gefolgt von Produkt 2. Die Entscheidung für ein Produkt hat jetzt die Beschaffungsstelle anhand der Testergebnisse und des daraus resultierenden Preis-/Leistungsverhältnisses zu treffen.

Prüffragen:

- Werden in der Testvorbereitung die Testmethoden für die Einzeltests mit Testarten, -verfahren und -werkzeugen festgelegt?
- Sind im Testumfang Standard-, Fehler- und Ausnahmefälle berücksichtigt?
- Bei Einsatz von Echtdaten zu Testzwecken: Werden die Echtdaten für Tests anonymisiert?
- Ist die Installation und Konfiguration der Testumgebung dokumentiert?
- Erfolgt die Durchführung der Tests anhand von Testplänen?
- Werden funktionale Tests durchgeführt, die auch fehlerhafte Eingabeparameter überprüfen?
- Werden sicherheitsspezifische Tests durchgeführt, die auch Penetrationstests umfassen?
- Existiert eine Dokumentation der Tests, die alle Testergebnisse anhand der Entscheidungskriterien bewertet?

M 2.314 Verwendung von hochverfügbaren Architekturen für Server

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, IT-Sicherheitsbeauftragter

Die Verfügbarkeit von Geschäftsprozessen, Anwendungen und Diensten hängt oft von der Funktion eines zentralen Servers ab. Je mehr Anwendungen aber auf einem Server laufen, desto ausfallsicherer muss dieser sein. Ein Server enthält in der Regel verschiedene potentielle Fehlerquellen ("Single Points of Failure"), also Komponenten, deren Ausfall den Ausfall des Gesamtsystems auslösen kann: IEC, Festplatten, Stromversorgung, Lüfter, Backplane, etc. Die Wiederherstellung des Gesamtsystems kann in diesem Fall erhebliche Zeit in Anspruch nehmen. Neben der Vorhaltung von Ersatzteilen können zusätzlich folgende Möglichkeiten zur Steigerung der Verfügbarkeit eingesetzt werden:

- Cold-Standby
- Hot-Standby (manuelles Umschwenken)
- Cluster (automatisches Umschwenken)
  - Load balanced Cluster
  - Failover Cluster

Jede einzelne dieser Techniken bietet ein unterschiedliches Niveau an Verfügbarkeit und ist in der Regel mit unterschiedlichen Kosten verbunden.

Cold-Standby

Beim Cold-Standby wird neben dem eigentlichen Produktivsystem ein zweites baugleiches Ersatzsystem bereitgehalten, das aber nicht aktiv ist. Wenn das erste System ausfällt, kann das Ersatzsystem manuell hochgefahren und ins Netz integriert werden.

Nach der Vorhaltung von einzelnen Ersatzteilen ist dies die einfachste Redundanz-Lösung, die mit den entsprechenden Vorteilen und Nachteilen verbunden ist:

Vorteile einer Cold-Standby Lösung	**Nachteile einer Cold-StandbyLösung**
- Cold-Standby Lösungen bringen keine Komplexitätserhöhung für das Gesamtsystem mit sich. - Die Kosten für ein Cold-Standby System belaufen sich lediglich auf die Kosten der zusätzlichen Hardware und sind so mit am geringsten unter den vorgestellten Möglichkeiten. - Neuaufsetzen oder Änderungen im System sind ohne Verfügbarkeitseinbußen möglich. Der Produktivbetrieb wird dafür während der Änderungen auf das Cold-Standby System umgelegt.	- Zum bestehenden System muss ein zweites System vorgehalten werden. - Das Ersatzsystem muss ständig auf dem aktuellen Konfigurations- und Patch-Stand gehalten werden. - Da das Ersatzsystem manuell aktiviert werden muss, müssen Administratoren das System kontinuierlich überwachen und im Notfall einschreiten. - Wenn die Applikationsdaten nicht auf einem externen Speichersystem liegen, so dass der Zugriff direkt aus dem Ersatzsystem möglich ist, dann müssen diese

Vorteile einer Cold-Standby Lösung	Nachteile einer Cold-StandbyLösung
	auf das Cold-Standby System migriert werden.

Tabelle: Vor-und Nachteile einer Cold-Standby Lösung

Der Einsatz eignet sich gut für Server mit Anwendungen, bei denen kurze bzw. begrenzte Ausfallzeiten, bis der Eingriff des Administrators möglich ist, unkritisch sind. Beispiele dafür sind:

- Server in kleineren Netzen (Intranet)
- Wenig frequentierte Server im Internet

Hot-Standby (manuelles Umschwenken)

Bei einem Hot-Standby steht ebenfalls ein Ersatzsystem bereit, das aber neben dem Produktivsystem parallel in Betrieb gehalten wird. Die Funktion des Produktivsystems wird überwacht, bei Ausfall wird das Ersatzsystem aktiv. Der Wechsel kann automatisch erfolgen oder auch manuell. Für den automatischen Wechsel sind zusätzliche Funktionalitäten im Gesamtsystem erforderlich z. B. die automatische Erkennung von Ausfällen. Dieser Fall wird im nächsten Abschnitt unter "Cluster" behandelt.

Um die Ausfallzeiten möglichst gering zu halten, muss der Zustand des Ersatzsystems kontinuierlich überprüft werden.

Vorteile einer Hot-Standby Lösung	Nachteile einer Hot-Standby Lösung
- Die Ausfallzeiten sind im Vergleich zu Cold-Standby geringer. - Wie beim Cold-Standby ist diese Lösung auch relativ kostengünstig, verglichen mit höherwertigen Hochverfügbarkeitslösungen, die im Folgenden beschrieben werden. - Das Ersatzsystem ist in Betrieb und kann auch zu Datenreplikation benutzt werden. - Neuaufsetzen oder Änderungen im System sind ohne Verfügbarkeitseinbuße möglich. Der Produktivbetrieb wird dafür während der Änderungen auf das Hot-Standby System umgelegt.	- Es wird auch hier immer nur die Hälfte der vorhandenen Hardware genutzt. - Das Ersatzsystem muss ständig auf dem aktuellen Stand gehalten werden. - Im Falle der manuellen Aktivierung des Hot-Standby Systems ist eine kontinuierliche Überwachung von einem Systemverantwortlichen erforderlich.

Tabelle: Vor- und Nachteile einer Hot-Standby Lösung

Der Einsatz von Hot-Standby Systemen eignet sich für Anwendungen, bei denen kurze Ausfallzeiten unkritisch sind. Die Problematik der Systemüberwachung und der Aktivschaltung des Hot-Standby Servers muss dabei mitbedacht werden. Mögliche Einsatzbereiche sind z. B. für:

- Webserver mit oft variierendem Content
- Server in kleineren Netzen (Application-Server, Mailserver)
- Datenbank-Server und Fileserver (z. B. sekundärer Server repliziert primären Server ständig und wird im Fehlerfall als primärer Server geschaltet).

Cluster (automatisches Umschwenken)

Ein Cluster besteht aus einer Gruppe von zwei oder mehreren Rechnern, die zur Steigerung der Verfügbarkeit oder auch der Leistung einer Anwendung oder eines Dienstes parallel betrieben werden. Die Anwendung oder der Dienst kann dabei auf einem der Rechner aktiv durchgeführt werden oder auf mehreren verteilt (Performance-Steigerung).

Cluster werden je nach Funktionsart in

- Load balanced Cluster
- Failover Cluster und

unterschieden.

Load balanced Cluster

Beim Load balanced Cluster werden Instanzen einer Anwendung oder eines Dienstes in Abhängigkeit von der Auslastung unter den Servern verteilt. Wenn dies für eine Anwendung oder einen Dienst möglich ist, dann kann damit nicht nur eine Lastverteilung (Load balancing) und somit eine Performancesteigerung erreicht werden, sondern auch die Probleme bei Ausfällen werden verringert.

Eine der Voraussetzungen für den Einsatz von Load balancing ist, dass die jeweiligen Anwendungen oder Dienste keinen schreibenden Datenzugriff benötigen dürfen.

Eine Redundanz kann in diesem Fall geschaffen werden, indem Systeme mit ähnlicher Leistung mit Hilfe eines Load-Balancing Prozesses "nebeneinander" gestellt werden und dafür gesorgt wird, dass beim Ausfall eines Servers die anderen Server diesen Ausfall auffangen.

Vorteile eines Load balanced Clusters	**Nachteile eines Load balanced Clusters**
- Es können damit sowohl Verfügbarkeitssteigerung als auch Leistungssteigerung erreicht werden. - Alle verfügbare Ressourcen werden dauerhaft genutzt. - Die Lösung ist hochgradig skalierbar. - Die Komplexität des Gesamtsystems ist geringer als bei einem Failover Cluster.	- Der Einsatz ist nicht für alle Arten von Anwendungen möglich. Insbesondere Anwendungen, die keine reinen Lesezugriffe verwenden und zugleich den Zugriff aller Server auf die gleichen Speicherressourcen verlangen, sind für Load Balancing nicht geeignet.

Tabelle: Vor- und Nachteile eines Load balanced Clusters

Wenn neben der Verfügbarkeit die Performance hohen Stellenwert hat und die Applikation einen verteilten Einsatz erlaubt, bietet ein Load balanced Cluster eine optimale Lösung. Das kann z. B. der Fall sein für:

Web-Server, für Front-end Applikationen mit ausschließlichen Lesezugriffen (z. B. Web-Server-Farmen) Failover Cluster

Als Failover Cluster wird hier ein Cluster bezeichnet, wenn bei Ausfall eines der Cluster-Systeme automatisch der aktive Betrieb der Anwendung oder des Dienstes von einem anderen Teil des Clusters übernommen wird (Takeover). Die automatische Übernahme von Diensten beim Ausfall einer Systemkom-

ponente durch eine funktional äquivalente Komponente wird Failover genannt. Für die Failover-Funktionalität ist eine dedizierte "heartbeat" (Herzschlag) Verbindung üblich, die die Kommunikation zwischen den Cluster-Servern gewährleistet. Die Cluster-Server müssen neben der Verbindung mit dem Client-Netz auch mit dem Administrationsnetz dediziert verbunden sein, um einen direkten Zugriff im Notfall zu gewähren.

Ein automatisches Failover setzt voraus, dass alle Software- und Hardware-Komponenten geeignet überwacht werden. Daher ist es wichtig sicherzustellen, dass der Failover Mechanismus auf keinen falschen Annahmen basiert.

Folgende Punkte müssen beim Einsatz eines Failover-Clusters berücksichtigt werden:

- **Zugriff auf gemeinsamen Speicher:**
  Neben den servereigenen Festplatten, die das Betriebssystem und die für den Betrieb notwendigen Daten enthalten, ist es in einem Cluster ratsam, die Anwendungsdaten auf gemeinsamen Speicher zu verwalten.
  Der Zugriff auf diese Festplatten wird dem Teil des Clusters gewährt, der gerade aktiv ist. Es ist auch möglich, statt gemeinsamen Festplatten replizierte Festplatten zu verwenden. Dies ist dann sinnvoll, wenn das Failover von einem entfernten Standort aus stattfindet. Bei einem lokalen Failover sollte überlegt werden, ob die durch die Replikation erzeugte Komplexität und entstandene Abhängigkeiten nicht eine zusätzliche Bedrohung für die Verfügbarkeit darstellen.
- **Portabilität der Anwendung:**
  Die Installation und Inbetriebnahme einer Anwendung auf zwei oder mehreren Servern parallel erfordert in den meisten Fällen den Einsatz zusätzlicher Lizenzen. Darüber hinaus muss überprüft werden, ob die Applikation eine Failover-Funktionalität erlaubt.
- **NSPoF (No Single Points of Failure):**
  Wenn die Failover-Funktionalität des Clusters durch den Ausfall einer einzigen Komponente gestört werden kann, widerspricht dies dem eigentlichen Zweck der Cluster-Architektur. Um Single Points of Failure zu vermeiden, muss das Gesamtsystem analysiert werden und der Ausfall einzelner Komponenten (Netzteile, Systemspeicher, Hauptspeicher, Netzwerkkarten, Switche, Hubs etc.) in Betracht gezogen werden.
- **Betriebssystem und Konfiguration der Cluster-Server:**
  Die Cluster-Server sollten mit gleichen Betriebssystemversionen, Patches, Libraries und Applikationsversionen ausgestattet sein. Eine möglichst identische Hardware- und Software-Konfiguration kann ein möglichst identisches Verhalten im Falle eines Failovers gewährleisten. Darüber hinaus reduziert sich im Falle von identischen Systemen die Komplexität des Gesamtsystems (Einsatz der gleichen Failover Software, Netz-Schnittstellen, Kompatibilität der gemeinsamen Speichersystems, Administration, Service).
- **Dedizierte und redundante Verbindung zwischen den Servern:**
  Die Kommunikation zwischen den Cluster-Servern muss unabhängig von der Netzlast, möglichst verzögerungsfrei erfolgen, damit das Failover schnellstmöglichst stattfinden kann. Die Redundanz ist aufgrund der hohen Verfügbarkeitsanforderungen ebenfalls erforderlich.
- **Einsatz von ausgereiften Software-Produkten für das Failover Management:**
  Die Entscheidung, ob ein Failover stattfinden muss oder nicht, ist eine sehr komplexe. Neue oder selbstentwickelte Tools können Fehler enthalten und dadurch letztendlich die Verfügbarkeit des Gesamtsystems reduzieren.

- **Ausführliches Testen aller möglichen Failover-Aspekte:**
  Ein ausführliches Testen ist unter anderem auch dazu notwendig, um festzustellen, dass keine unerwarteten Fehlerquellen (Single Points of Failure) vorhanden sind. Insbesondere muss das Monitoring der Server und das Failover-Management auf alle möglichen Fehler getestet werden.

Vorteile eines Failover Clusters	Nachteile eines Failover Clusters
- Durch das automatische Takeover kann die Verfügbarkeit erheblich gesteigert werden. - Es sind keine manuellen Eingriff nötig.	- Diese Lösung ist hoch komplex. - Failover Cluster sind nicht gut skalierbar. - Es wird immer nur ein Teil der Ressourcen genutzt. - Es entstehen hohe Kosten aufgrund zusätzlicher Hardware und Software

Tabelle: Vor- und Nachteile eines Failover Clusters

Wie aus der Gegenüberstellung der Vorteile und Nachteile hervorgeht, ist der Einsatz eines Failover Clusters nur dann sinnvoll, wenn eine oder mehrere Applikationen sehr hohe Verfügbarkeitsanforderungen haben. Neben dem hohen Kostenaufwand sind sehr gute Kenntnisse des verantwortlichen Personals sowohl über die eingesetzten Betriebssysteme und Applikationen als auch über die Failover-Funktionalität erforderlich. Der Einsatz von Failover Lösungen für Server macht zudem nur dann Sinn, wenn auch alle Abhängigkeiten wie beispielsweise Netzanbindung oder Verfügbarkeit der Clients auch mit den entsprechenden Redundanzen ausgelegt sind.

Bereiche, für die typischerweise bei hohen Verfügbarkeitsanforderungen Failover Cluster eingesetzt werden, sind z. B.:

- Datenbank Anwendungen
- File Storage
- Anwendungen mit dynamischem Inhalt
- Mail Server

Wenn Geschäftsprozesse, Anwendungen oder Dienste hohe Anforderungen an die Verfügbarkeit haben, sollte auf jeden Fall überlegt werden, wodurch diese Anforderungen abgedeckt werden können. Die IT-Veranstwortlichen und das Sicherheitsmanagement sollten für die entsprechenden Server ein Konzept erarbeiten und angemessene Architekturen auswählen.

Prüffragen:

- Berücksichtigt die gewählte Server-Architektur die Verfügbarkeitsanforderungen?

M 2.392 Modellierung von Virtualisierungsservern und virtuellen IT-Systemen

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Leiter IT

Um eine angemessene Gesamtsicherheit für den IT-Betrieb zu erreichen, müssen alle Virtualisierungsserver und alle virtuellen IT-Systeme systematisch im Sicherheitskonzept berücksichtigt werden. In Bezug auf die IT-Grundschutz-Vorgehensweise bedeutet dies insbesondere, dass alle virtuellen IT-Systeme in die Strukturanalyse und in die Modellierung einbezogen werden müssen.

Als Modellierung wird in der IT-Grundschutz-Vorgehensweise die Zuordnung von Bausteinen zu den vorhandenen Zielobjekten (IT-Systeme, Anwendungen, Räume, etc.) bezeichnet. Grundsätzlich erfolgt die Modellierung virtueller IT-Systeme nach den gleichen Regeln wie bei eigenständigen physischen IT-Systemen. Das heißt, es sind die Hinweise in Kapitel 2.2 der IT-Grundschutz-Kataloge zu beachten. Die Zuordnung der IT-Grundschutz-Bausteine richtet sich in erster Linie nach der Funktion des IT-Systems (Server, Client, etc.), nach dem verwendeten Betriebssystem (Unix, Windows, etc.) und nach den darauf betriebenen Applikationen (Datenbank, Webserver, etc..).

Um die Pflege des Sicherheitskonzepts zu erleichtern und die Komplexität zu reduzieren, sollte besonders sorgfältig geprüft werden, inwieweit die virtuellen IT-Systeme zu Gruppen zusammengefasst werden können. Prinzipiell können auch solche virtuellen IT-Systeme, die sich auf unterschiedlichen physischen Computern befinden, in einer Gruppe zusammengefasst werden. Dies muss jedoch im Einzelfall geprüft werden. Hinweise zur Gruppenbildung finden sich in der IT-Grundschutz-Vorgehensweise.

Falls unterhalb der Virtualisierungsschicht ein vollwertiges und eigenständiges Basis-Betriebssystem zum Einsatz kommt, muss dieses Betriebssystem unabhängig von den virtuellen IT-Systemen in die Modellierung einbezogen werden. Auch hier ist zu prüfen, ob eine Gruppierung vorgenommen werden kann.

Beispiel-Szenario

Als Beispiel wird ein physischer Server S1 betrachtet, auf dem mit Hilfe einer Virtualisierungssoftware die drei virtuellen Server VM1, VM2 und VM3 betrieben werden. Als Basis-Betriebssystem kommt auf dem physischen Server S1 eine Unix-Version zum Einsatz. Die Virtualisierungsschicht ist in diesem Beispiel eine Software-Komponente, die unter Unix läuft, also eine hostbasierte Servervirtualisierung (Typ 2). Die beiden virtuellen Server VM1 und VM2 werden mit Windows 2003 betrieben, auf VM3 ist hingegen Unix installiert. Applikationen können sowohl auf den drei virtuellen Servern als auch (unter Umgehung der Virtualisierungsschicht) direkt auf dem Basis-Betriebssystem des physischen Servers S1 ablaufen.

Die folgende Abbildung zeigt ein Schema dieser Beispiel-Konfiguration:

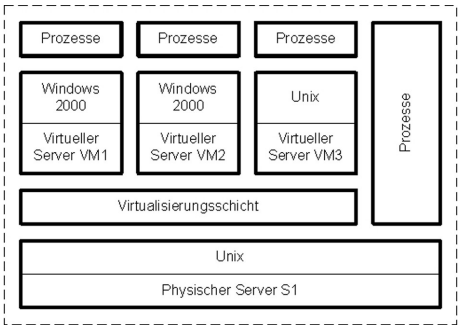


Abbildung: Schema der Beispiel-Konfiguration mit drei virtuellen Servern

Hinweis: Nicht bei allen Lösungen zur Virtualisierung kommt ein vollwertiges Basis-Betriebssystem unterhalb der Virtualisierungsschicht zum Einsatz.

Falls die Voraussetzungen für eine Gruppierung von VM1 und VM2 erfüllt sind, könnte die Modellierung für das oben dargestellte Beispiel-Szenario wie folgt aussehen (Auszug):

Baustein	**Zielobjekt**
B 3.101 Allgemeiner Server	S1
B 3.101 Allgemeiner Server	VM3
B 3.101 Allgemeiner Server	Gruppe aus VM1 und VM2
B 3.102 Server unter Unix	S1
B 3.102 Server unter Unix	VM3
B 3.108 Windows Server 2003	Gruppe aus VM1 und VM2

Tabelle: Zuordnung Bausteine zu Zielobjekten

Prüffragen:

- Existiert eine Planung für den Einsatz von virtuellen IT-Systemen, in der die Ziele des Einsatzes sowie die Auswirkungen auf die IT-Risiken betrachtet werden?
- Steht der Einsatz von virtuellen IT-Systemen im Einklang mit den Sicherheitszielen der Organisation?
- Sind die Anforderungen an die virtuellen IT-Systeme hinsichtlich deren Isolation voneinander sowie Verfügbarkeit und Durchsatz definiert?
- Wird vor der Überführung von virtuellen IT-Systemen geprüft, ob ausreichende Antwortzeiten bzw. Verarbeitungsgeschwindigkeiten erzielt werden?
- Ist festgelegt, welche Anwendungen sich auf virtuelle IT-Systeme stützen?
- Sind die Auswirkungen auf administrative und betriebliche Prozesse auf den virtuellen IT-Systemen untersucht?
- Sind die Auswirkungen auf Anwender und Benutzer auf den virtuellen IT-Systemen untersucht?
- Werden alle virtuellen Systeme im IT-Sicherheitskonzept berücksichtigt?
- Wurden alle virtuellen Systeme in die IT-Strukturanalyse, die Schutzbedarfsfeststellung und die Modellierung mit einbezogen?
- Sind die Administratoren für Planung, Einrichtung und Betrieb von virtuellen IT-Systemen ausgebildet?
- Werden die Leistungsdaten der virtuellen IT-Systeme überwacht?

M 2.444 Einsatzplanung für virtuelle IT-Systeme

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator

Für virtuelle IT-Systeme sind bei der Planung neben den schon in M 2.315 *Planung des Servereinsatzes* angegebenen Voraussetzungen für einen sicheren Serverbetrieb weitere Punkte zu beachten. Im Folgenden werden zusätzliche Vorgaben hinsichtlich der Planung virtueller IT-Systeme beschrieben.

Herstellerunterstützung für virtuelle IT-Systeme

Es ist zu prüfen, dass alle Anwendungen, die auf virtuellen IT-Systemen betrieben werden sollen, durch ihre Hersteller auf der gewählten Virtualisierungsplattform unterstützt werden. Die Hersteller geben Ihre Software in der Regel für eine bestimmte Kombination aus Betriebssystem und Hardwareplattform frei. Sie sichern nur dann Support für eventuell auftretende Probleme zu, wenn die Software gemäß diesen Vorgaben genutzt wird. Da die Hardwareplattform "virtuelles IT-System" bisher nicht standardisiert ist, sagen nicht alle Softwarehersteller eine pauschale Unterstützung virtueller IT-Systeme zu. Die Hersteller bieten meistens nur für eine bestimmte Kombination von Betriebssystem und Virtualisierungsprodukt Support an, z. B. bei der Fehleranalyse und -behebung.

Lebenszyklus virtueller IT-Systeme

Weiterhin ändern sich etablierte Verfahrensweisen für die Inbetriebnahme, Inventarisierung, den Betrieb und die Außerbetriebnahme von (virtuellen) IT-Systemen beim Betrieb in einer virtuellen Infrastruktur. Es ist daher detailliert zu planen und festzulegen, wie diese Prozesse angepasst werden. Folgende Punkte sind sicherzustellen:

- Es muss geprüft werden, ob die eingesetzten Betriebssysteme und Anwendungen für den Betrieb in virtualisierten IT-Systemen geeignet sind.
- Es ist zu gewährleisten, dass das Virtualisierungsprodukt für den Einsatzzweck der IT-Systeme geeignet ist.
- Es dürfen keine Virtualisierungsfunktionen wie z. B. Snapshots verwendet werden, die zu Problemen mit dem Applikationen führen können (Siehe auch M 4.347 *Deaktivierung von Snapshots virtueller IT-Systeme*).
- Für die Applikationen sollten keine Hardwarekomponenten wie z. B. Softwareschutzmodule (*Dongles*) oder ISDN-Karten benötigt werden, die den virtuellen IT-Systemen innerhalb der virtuellen Infrastruktur nicht zur Verfügung gestellt werden können.
- Alle virtuellen IT-Systeme müssen von der Inventarisierung des Informationsverbundes vollständig erfasst werden, damit beispielsweise eine Unterlizenzierung vermieden wird oder Systeme betrieben werden, deren Einsatzzweck unbekannt ist.
- Die für die Inbetriebnahme von physischen IT-Systemen üblichen Verfahrensweisen sowie Planungs- und Betriebsvorbereitungen sind auf angemessene Weise und ihrem Sinn nach auf die virtuellen IT-Systeme zu übertragen. Werden beispielsweise physische IT-Systeme mit einem Aufkleber versehen, auf dem Name und IP-Adresse dokumentiert werden, so ist dies bei virtuellen IT-Systemen nicht möglich. Diese Vorgaben können aber bei der Benennung dieser virtuellen IT-Systeme in der Verwaltungssoftware umgesetzt werden.

- Mit den Server- und Anwendungsbetreibern sind zusammen realistische und angemessene Performance- und Ressourcenanforderungen für die virtuellen IT-Systeme festzulegen, bevor die Systeme in Betrieb genommen werden. Werden die Performanceanforderungen bestimmt, ist zu prüfen, ob Leistungseinschränkungen bei gelegentlich auftretenden Lastspitzen hingenommen werden können: So sind beispielsweise Skripte zur automatisierten Verarbeitung von Datenbankinhalten häufig nicht zeitkritisch und müssen daher nicht mit maximaler Performance ausgeführt werden.
- Es ist zu regeln, wie Routinetätigkeiten während des Betriebs virtueller IT-Systeme auszuführen sind. Dabei muss sichergestellt werden, dass Tätigkeiten, wie das Starten und Stoppen virtueller IT-Systeme, das Anlegen und Löschen von sowie das Zurücksetzen auf Snapshots mit den Serverbetreibern und Applikationsbesitzern abgestimmt werden.
- Die Performance virtueller IT-Systeme ist zu überwachen. Es muss sichergestellt sein, dass ihre Performanceanforderungen ausreichend erfüllt werden.
- Es ist ein Prozess zu etablieren, mit dem Engpässe beim Verbrauch an Prozessorleistung, Hauptspeicher und Festplattenspeicher rechtzeitig erkannt werden und bei dem auf solche Engpässe angemessen reagiert wird.

Test- und Entwicklungsumgebungen

In Test- und Entwicklungsumgebungen, bei denen lediglich eine funktionale Analyse virtueller IT-Systeme durchgeführt werden soll, kann von den oben angegebenen Vorgaben abgewichen werden. Allerdings ist ein Prozess innerhalb der Organisation zu etablieren, der gewährleistet, dass die Konfiguration und die Ressourcenzuteilungen der virtuellen IT-Systeme überprüft und unter Umständen angepasst werden, bevor sie produktiv in Betrieb genommen werden. Beispielsweise sollten virtuelle IT-Systeme nicht einfach aus der Test- und Entwicklungsumgebung heraus kopiert oder geklont, sondern neu installiert werden. Wird das IT-System nicht neu installiert, muss für die zu kopierenden beziehungsweise zu klonenden virtuellen IT-Systeme sorgfältig geprüft werden, ob sie sich für den Produktivbetrieb eignen. Es ist insbesondere zu prüfen, ob bestimmte in Test- und Entwicklungsumgebungen verwendete Virtualisierungsfunktionen (wie z. B. Skripte in Gastwerkzeugen) noch aktiv sind. Die Tests sollten dabei in einer Umgebung durchgeführt werden, die die gleiche Virtualisierungslösung wie das Zielsystem verwendet. Dies soll gewährleisten, dass das Verhalten der virtuellen IT-Systeme in der Testumgebung nicht von der Produktivumgebung abweicht.

Prüffragen:

- Werden virtuelle IT-Systeme aus Test- und Entwicklungsumgebungen vor der Inbetriebnahme im Produktivnetz daraufhin geprüft, dass sie für den Produktiveinsatz geeignet sind?
- Ist eine Vorgehensweise für die Inbetriebnahme von Virtualisierungsservern und virtuellen IT-Systemen festgelegt worden?
- Ist für virtuelle IT-Systeme festgelegt worden, welche Virtualisierungsfunktionen (wie beispielsweise Snapshots) verwendet werden dürfen?
- Ist sichergestellt, dass die Performance der virtuellen IT-Systeme laufend überwacht wird?
- Sind alle virtuellen IT-Systeme des Informationsverbundes in der Inventarisierung erfasst?
- Ist eine Vorgehensweise für die Außerbetriebnahme von Virtualisierungsservern und virtuellen IT-Systemen festgelegt worden?

M 2.445 Auswahl geeigneter Hardware für Virtualisierungsumgebungen

Verantwortlich für Initiierung: Leiter IT
Verantwortlich für Umsetzung: Leiter Beschaffung

Die gängigen Betriebssystem- und Servervirtualisierungslösungen haben individuelle Anforderungen an die zugrunde liegende Hardwarearchitektur bzw. die Ausstattung des Virtualisierungsservers mit Hardwarekomponenten wie Netzschnittstellen oder Massenspeicherkarten. Diese Anforderungen müssen bei der Beschaffung von Serversystemen bedacht werden, wenn diese als Virtualisierungsserver eingesetzt werden sollen. Für die unterschiedlichen Arten der Virtualisierung (Betriebssystem-, hypervisorbasierte und hostbasierte Servervirtualisierung) bestehen einige grundsätzliche Unterschiede in den Hardwareanforderungen. Diese sind im Folgenden dargestellt.

Anforderungen von Betriebssystemvirtualisierung und hostbasierter Servervirtualisierung

Systeme zur Betriebssystemvirtualisierung und so genannte hostbasierte Servervirtualisierungslösungen können meist auf eine umfangreiche Treiberunterstützung des Basisbetriebssystems, auf dem sie installiert werden, zurückgreifen. Ein Beispiel für eine Betriebssystemvirtualisierung ist *Sun Solaris Zones*, die in das Betriebssystem *Solaris* integriert ist. Hostbasierte Servervirtualisierungen sind beispielsweise *Microsoft Virtual PC, Sun VirtualBox,* oder *VMware Server*, die wie ein herkömmlicher Dienst auf einem kompatiblen Betriebssystem installiert werden können. In der Regel kann jede Hardwarekomponente (Netzschnittstellen, SCSI-Controller und ähnliches) verwendet werden, die vom gewählten Betriebssystem unterstützt wird. Üblicherweise ist in solchen Fällen eine Vielzahl an Komponenten nutzbar.

Anforderungen von Hypervisorprodukten

Erheblich strengere Anforderungen an die Auswahl der in Kombination mit der Virtualisierungslösung einzusetzenden Hardwarekomponenten werden jedoch durch die Hypervisorprodukte gestellt. Hier sind z. B. *Microsoft Hyper-V, VMware ESX* oder *XEN* zu nennen. Diese stellen ein auf für die Virtualisierung reduziertes Betriebssystem dar und haben meist eine eingeschränkte Hardwareunterstützung beziehungsweise Treiberausstattung oder besondere Hardwareanforderungen an den verwendeten Prozessor. Z. B. kann die Virtualisierungslösung *XEN* nur dann ohne Einschränkungen genutzt werden, wenn der Prozessor Virtualisierungsfunktionen enthält (*Intel VT, AMD-V*). Gleiches gilt für *Microsoft Hyper-V.*

Unabhängig von der Wahl der zu nutzenden Virtualisierungslösung sind Kompatibilitäten bei der Planung der Virtualisierungsumgebung vorab zu prüfen. Untersucht werden muss bei Betriebssystemvirtualisierungslösungen und hostbasierten Servervirtualisierungslösungen die Lauffähigkeit der Virtualisierungssoftware unter dem entsprechenden Betriebssystem mit der gewählten Hardware.

Auswahl der Hardware

Als Hardwareplattform für die Virtualisierungslösung sind geeignete physische Server auszuwählen. Die Hersteller der Virtualisierungslösungen veröffentlichen in regelmäßigen Abständen aktualisierte Kompatibilitätslisten, die bestimmte Hardwarekonfigurationen als tauglich für ihr Produkt zertifizieren, al-

so eine Gewähr für die Eignung der Hardware geben. Solche Listen sollten bei der Wahl der Hardware berücksichtigt werden, vor allem, wenn diese im Produktivbetrieb eingesetzt werden sollen.

Zudem werden die in Wartungsverträgen für die Virtualisierungssoftware vereinbarten Unterstützungsleistungen und Garantien häufig nicht oder nur eingeschränkt gewährt, wenn die verwendete Hardware vom Hersteller nicht zertifiziert ist. Bei bereits produktiv eingesetzten und problemlos funktionierenden Umgebungen ist zu prüfen, inwieweit der Hersteller Support für sein Virtualisierungsprodukt auch mit der vorhandenen Hardware gewährt, auch wenn diese nicht zertifiziert ist.

Prüffragen:

- Wurde die Kompatibilität der Virtualisierungslösung zur verwendeten Hardware überprüft?
- Ist sichergestellt, dass der Hersteller der eingesetzten Virtualisierungslösung Support für die betriebene physische Hardware gewährt?

M 2.446 Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator

Bei Virtualisierungsinfrastrukturen kommen zusätzlich zu den üblichen Rollen und Administrationstätigkeiten (siehe M 2.38 *Aufteilung der Administrationstätigkeiten*) weitere administrative Aufgaben im Rechenzentrumsbetrieb hinzu.

Die Besonderheit der Rolle von Administratoren in einer virtuellen Infrastruktur besteht darin, dass diese potenziell eine sehr weitgehende Machtbefugnis über die virtuellen IT-Systeme, die in der virtuellen Infrastruktur betrieben werden, haben können. Dies schließt mit ein, dass sie

- die Kontrolle über die emulierte Hardwareausstattung haben,
- die virtuellen IT-Systeme mit Netzen verbinden können,
- den virtuellen IT-Systemen Speicherressourcen aus dem Speichernetz zuweisen können und
- meist Zugriff auf die Konsolen der virtuellen IT-Systeme

haben.

Eine Aufteilung der Administratorrolle ermöglicht die gegenseitige Kontrolle der unterschiedlichen Administratorengruppen in einem arbeitsteiligen Rechenzentrumsbetrieb.

So können bei einigen Virtualisierungsprodukten, wie z. B. *Citrix XENCenter, Microsoft System Center Virtual Machine Manager* oder *VMware vSphere*, Administratorrollen definiert werden, die bestimmten Benutzergruppen eine Auswahl von Rechten in der virtuellen Infrastruktur zuweisen. Hier können beispielsweise bestimmte Benutzergruppen daran gehindert werden, virtuelle IT-Systeme aus der virtuellen Infrastruktur zu exportieren. Des Weiteren können Berechtigungen zum Ein- und Ausschalten von virtuellen IT-Systemen oder zur Erzeugung von Snapshots erteilt oder entzogen werden.

Es ist zu prüfen, ob für die virtuell zu betreibenden IT-Systeme eine Aufteilung der Administratorrollen notwendig ist. Dies kann beispielsweise der Fall sein, wenn eine bestimmte Administratorengruppe keine Berechtigung für die Zuweisung von Netzen für ein virtuelles IT-System mit erhöhtem Schutzbedarf bezüglich Vertraulichkeit erhalten soll.

Wird die Aufteilung der Administratorrollen benötigt, so ist die Definition entsprechender Administratorrollen für die Virtualisierungsinfrastruktur zu nutzen. Einige Virtualisierungsprodukte bieten eine solche Möglichkeit nicht. In diesem Fall ist zu prüfen, ob eine Aufteilung der Administratorrollen ausschließlich organisatorisch, das heißt z. B. mittels einer Richtlinie ausreicht.

Prüffragen:

- Wurde geprüft, ob eine Aufteilung der Administratorrollen für die virtuelle Infrastruktur notwendig ist?
- Wurde die Aufteilung der Administratorrollen, wenn sie notwendig ist, organisatorisch oder, falls möglich, mit technischen Mitteln des Virtualisierungsproduktes umgesetzt?

M 2.447 Sicherer Einsatz virtueller IT-Systeme

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Leiter IT

Bei der Inbetriebnahme virtueller IT-Systeme müssen einige Besonderheiten beachtet werden, die über die für physische IT-Systeme notwendigen Maßnahmen hinaus gehen (beispielsweise M 2.318 *Sichere Installation eines IT-Systems*). Dies resultiert aus der Dynamik und Flexibilität der virtuellen IT-Systeme sowie der Möglichkeit, dass mehrere virtuelle IT-Systeme, die unterschiedliche Daten verarbeiten, auf einem Virtualisierungsserver nebeneinander betrieben werden.

Virtuelle IT-Systeme sind zunächst genauso wie physische Computer gemäß ihrem Typ und Einsatzzweck (Anwendungsserver oder Client, aber auch beispielsweise Switch) in Betrieb zu nehmen. Daher sind die für physische Systeme einschlägigen und etablierten Maßnahmen bei der Installation und im späteren Betrieb ebenfalls für virtuelle IT-Systeme umzusetzen. Darüber hinaus muss berücksichtigt werden, dass für Applikationen, falls sie von eigenständigen physischen IT-Systemen auf virtuelle IT-Systeme verlagert werden, zusätzliche Gefährdungen entstehen können. Beispielsweise kann es unter Umständen zu Engpässen bei der Verarbeitungsgeschwindigkeit oder bei der Speicherkapazität kommen. Daher kann es erforderlich sein, eine bestehende Installationsdokumentation für ein in Betrieb zu nehmendes, virtuelles IT-System anzupassen.

Die Inbetriebnahme virtueller IT-Systeme muss deshalb sorgfältig vorbereitet werden (siehe auch M 2.444 *Einsatzplanung für virtuelle IT-Systeme*). Es sollten insbesondere folgende Punkte vor der unmittelbaren Inbetriebnahme beachtet werden:

- Es muss sichergestellt werden, dass nur die hierfür zuständigen Administratoren die Virtualisierungssoftware bezüglich der virtuellen IT-Systeme konfigurieren sowie virtuelle IT-Systeme einrichten oder löschen können.
- Die Zugriffsrechte auf die virtuellen IT-Systeme müssen gemäß den Anforderungen eingerichtet werden. Als Grundregel gilt auch hier, dass nur die tatsächlich erforderlichen Zugriffsmöglichkeiten erlaubt werden sollten. Dies gilt nicht nur für die Verwaltungssoftware des Virtualisierungsservers, sondern insbesondere auch für die Daten, mit denen das virtuelle IT-System auf dem Virtualisierungsserver repräsentiert wird.
- Es muss gewährleistet sein, dass die für die virtuellen IT-Systeme notwendigen Netzverbindungen in der virtuellen Infrastruktur zur Verfügung stehen.
- Die Auswirkungen der Virtualisierung (beispielsweise bei der Systemüberwachung oder der Nutzung virtueller Hardware-Ressourcen), die sich für die Administratoren des virtuellen IT-Systems selbst und der darauf betriebenen Applikationen ergeben, sind zu ermitteln und zu beachten.
- Abhängig vom Einsatzzweck müssen die einzelnen virtuellen IT-Systeme auf einem physischen Computer mehr oder weniger stark isoliert und gekapselt sein (siehe auch M 3.72 *Grundbegriffe der Virtualisierungstechnik* und M 3.70 *Einführung in die Virtualisierung*). Dies gilt insbesondere dann, wenn virtuelle IT-Systeme unterschiedlichen Schutzbedarfs auf einem Virtualisierungsserver betrieben werden sollen.

- Der Einsatz mehrerer virtueller IT-Systeme auf einem physischen Computer kann erhebliche Auswirkungen auf die Verfügbarkeit, den Durchsatz und die Antwortzeiten der betriebenen Anwendungen haben.
  Es ist zu prüfen, ob die Anforderungen an die Verfügbarkeit und den Durchsatz der Applikationen mit der eingesetzten Virtualisierungslösung erfüllt werden können. Dies kann dadurch geschehen, dass vor der Überführung in den Wirkbetrieb getestet wird, ob das virtuelle IT-System akzeptable Antwortzeiten und Verarbeitungsgeschwindigkeiten erreicht.
- Weiterhin sollten die Leistungseigenschaften virtueller Server überwacht werden, damit bei Engpässen zeitnah Anpassungen der Konfiguration vorgenommen werden können. Die Überwachung kann auf der Ebene der virtuellen IT-Systeme oder auf der Ebene des jeweiligen Virtualisierungsservers erfolgen. Hierbei ist zu beachten, dass Leistungswerte, die durch die virtuellen IT-Systeme selbst ermittelt werden, nicht immer der Realität entsprechen. Bei einigen Virtualisierungsprodukten wird einem virtuellen IT-System beispielsweise ein gewisser Anteil an der Gesamt-Prozessorzeit zugeteilt. Meldet das virtuelle System nun eine Auslastung seines (virtuellen) Prozessors, entspricht dies nicht in jedem Fall der tatsächlichen Auslastung des physischen Prozessors, sondern nur einer Auslastung der zugeteilten Prozessorzeit.

Prüffragen:

- Werden die Zugriffsrechte der Administratoren auf die virtuellen IT-Systeme auf das notwendige Maß beschränkt und nur die tatsächlich erforderlichen Zugriffsmöglichkeiten erlaubt?
- Stehen die für die virtuellen IT-Systeme notwendigen Netzverbindungen zur Verfügung?
- Sind die Administratoren der Virtualisierungsumgebung, der virtuellen IT-Systeme und der darauf betriebenen Anwendungen mit den Auswirkungen der Virtualisierung vertraut?
- Sind die Anforderungen an die Isolation und Kapselung der virtuellen IT-Systeme sowie der darauf betriebenen Anwendungen hinreichend erfüllt?
- Sind die Anforderungen an die Verfügbarkeit und den Durchsatz der virtuellen IT-Systeme ermittelt worden?
- Wird die Performance der virtuellen IT-Systeme im laufenden Betrieb überwacht?

M 2.448 Überwachung der Funktion und Konfiguration virtueller Infrastrukturen

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator

Die Konfigurationsdateien von Virtualisierungsservern enthalten die für den Betrieb einer virtuellen Maschine notwendigen Informationen der virtuellen Infrastruktur. Hierzu gehören die Ressourcenzuteilung für jedes virtuelle IT-System und die Definition der Netze für die virtuellen IT-Systeme.

Überwachung der Konfiguration virtueller IT-Systeme

Die Konfiguration der virtuellen IT-Systeme für Server- und Betriebssystemvirtualisierung in einer virtuellen Infrastruktur bestimmt die Eigenschaften des virtuellen IT-Systems. Es wird festgelegt,

- welche Prozessorressourcen,
- wie viel Hauptspeicher und
- wie viel Festplattenplatz

einem virtuellen IT-System vom Virtualisierungsserver zur Verfügung gestellt werden.

Darüber hinaus werden bei einer Servervirtualisierung, bei der die Hardware vollständig virtualisiert wird, zusätzlich in der Konfiguration noch Eigenschaften der Hardwareemulation festgelegt. Hierzu gehören z. B.:

- Art eines Massenspeichergeräts und der Netzwerkkarten,
- Zugriff auf Laufwerke (Floppy, CD/DVD etc.) und andere, dem virtuellen IT-System zur Verfügung zu stellende Hardware sowie
- Verbindung der virtuellen IT-Systeme mit physischen Netzen.

Werden Konfigurationen der virtuellen IT-Systeme verändert, können diese unter Umständen nicht auf dringend benötigte Ressourcen zugreifen. Es ist auch möglich, dass ein virtuelles IT-System unbeabsichtigt Zugriff auf Ressourcen erhält, auf die es nicht zugreifen dürfen sollte. Ein Beispiel hierfür wäre die entstehende Zugriffsmöglichkeit auf sämtliche Lohndaten eines Unternehmens für die Mitarbeiter der Entwicklungsabteilung.

Somit sind die Konfigurationsdateien der virtuellen IT-Systeme besonders hinsichtlich ihrer Integrität oft besonders schutzbedürftig. Es sollte festgelegt werden, wie eine Prüfung dieser Konfigurationsdateien auf unautorisierte Änderungen erfolgen soll. In Abhängigkeit vom Schutzbedarf der auf dem Virtualisierungsserver laufenden virtuellen IT-Systeme sind

- automatisierte Prüfungen (z. B. mittels Prüfsummenverfahren) oder
- regelmäßige Prüfungen durch die Administratoren der Virtualisierungsserver

zu erwägen.

Überwachung der Funktion der virtuellen Infrastruktur

Auf einem Virtualisierungsserver werden in der Regel virtuelle Netze definiert, mittels derer die virtuellen IT-Systeme mit den physischen Netzen verbunden werden. Diese Netzfunktionen der Virtualisierungsserver können durch eine fehlerhafte Konfiguration oder falsche Verkabelung unbeabsichtigt Kommunikationswege öffnen, die sonst nicht nutzbar sein sollen. Ein Beispiel hierfür

wäre die fälschliche Anbindung eines hoch schutzbedürftigen ERP-Systems an eine DMZ, die für die Einwahl von Kunden vorgesehen ist. Daher ist regelmäßig zu überprüfen, dass die Netzkonfiguration bezüglich der Verkabelung und der logischen Einrichtung der Virtualisierungsserver den Planungen entspricht. Dies betrifft die Netzinfrastruktur und die Einbindung der Virtualisierungsserver in Speichernetze.

Bei einigen Virtualisierungsprodukten werden Ressourcen, wie z. B. Netzverbindungen, nur anhand eines nahezu frei zu vergebenen Namens unterschieden. Diese Ressourcen werden nun den virtuellen IT-Systemen über diesen Namen zugewiesen. Diese Zuordnung bleibt häufig erhalten, wenn ein virtuelles IT-System von einem Virtualisierungsserver auf einen Anderen migriert wird. Sind physisch oder logisch unterschiedliche Netzverbindungen mit dem gleichen Namen versehen, wird ein virtuelles IT-System möglicherweise mit einem falschen Netz verbunden. Dies kann gegebenenfalls fatale Folgen haben, wenn wegen eines Fehlers in der Konfiguration beispielsweise *Internet* und *Intranet* verwechselt worden sind.

Aus diesem Grund ist eine eindeutige und aussagekräftige Benennung der Netze zu wählen und regelmäßig zu prüfen, ob solche Netzzuordnungen korrekt sind. Dies kann durch eine Funktionsprüfung wie z. B. einem Erreichbarkeitstest des virtuellen Systems im zugewiesenen Netz geschehen.

Prüffragen:

- Ist sichergestellt, dass die Konfigurationsdateien der virtuellen Infrastruktur regelmäßig auf unautorisierte Änderungen überprüft werden?
- Wird überwacht, ob Netzzuordnungen dem dokumentierten Zustand entsprechen?
- Wurden eindeutige und aussagekräftige Identifikatoren für die Netze gewählt?

M 2.449 Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator

Zahlreiche gängige Lösungen zur Virtualisierung von IT-Systemen bieten die Möglichkeit, sich entweder lokal am Virtualisierungsserver oder über ein Netz von einer entfernten Arbeitsstation aus mit Hilfe einer Clientsoftware an der Virtualisierungssoftware anzumelden (z. B. *Citrix XenCenter* oder *VMware Console*). Diese Clientsoftware dient dazu, die Virtualisierungssoftware auf dem Virtualisierungsserver einzurichten, sowie sie zu warten und zu überwachen. Bei Produkten zur Servervirtualisierung muss sie aber auch genutzt werden, um auf die Konsolen der virtuellen Maschinen zu zugreifen. Dies ist bei diesen Produkten in der Regel auf Grund der Architektur der virtuellen IT-Systeme auch nicht anders realisierbar, da ein virtuelles IT-System keine physische Konsole besitzt. Auf diese Weise kann z. B. der Betriebszustand einer virtuellen Maschine auch während des Bootprozesses überwacht werden.

Virtuelle IT-Systeme bestehen bei einer Servervirtualisierung ausschließlich aus virtuellen Hardwarekomponenten. Diese Geräte, wie Netzwerkkarten, Massenspeichergeräte und Grafikkarten, müssen durch die Virtualisierungssoftware nachgebildet (emuliert) werden. Bei der Emulation von Netzwerkkarten und Massenspeichergeräten können die Befehle der virtuellen IT-Systeme in der Regel einfach an die jeweiligen physischen Geräte übermittelt werden. Sie müssen daher nicht vollständig emuliert werden. Grafikkarten müssen jedoch in der Regel vollständig durch die Virtualisierungssoftware emuliert werden. Daher wird dem virtuellen IT-System aus Performancegründen die ständige Existenz der Grafikkarte nur vorgespiegelt. Erst beim Zugriff auf die Konsolenschnittstelle eines virtuellen IT-Systems wird die tatsächliche Emulation in Software gestartet. Dies bindet in der Regel erhebliche Prozessor- und Speicherressourcen auf dem Virtualisierungsserver.

Da Konsolenzugriffe auf die virtuellen IT-Systeme starken Einfluss auf die Leistungsfähigkeit der Verwaltungssoftware eines Virtualisierungsservers haben, sind sie auf ein Mindestmaß zu beschränken.

Virtuelle IT-Systeme sollten somit möglichst nicht über direkte Konsolenzugriffe, sondern bevorzugt über das Netz, z. B. via RDP oder X-Window mittels SSH-Tunneling, gesteuert werden.

Prüffragen:

- Sind die Konsolenzugriffe auf die virtuellen IT-Systeme auf ein Mindestmaß beschränkt, damit sie keinen Einfluss auf die Leistungsfähigkeit des Virtualisierungsservers haben?
- Werden die virtuellen IT-Systeme über das Netz, z. B. via RDP oder X-Window mittels SSH-Tunneling gesteuert?

M 2.477 Planung einer virtuellen Infrastruktur

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator

Aufgrund der hohen Komplexität ist eine detaillierte Planung beim Aufbau einer virtuellen Infrastruktur unerlässlich. Daher sollte schon bei einer konzeptionellen Betrachtung und im Vorfeld einer Projektierung eine genaue Analyse der notwendigen Rahmenbedingungen durchgeführt werden.

Festlegung der Virtualisierungstechnik

In einem ersten Planungsschritt ist daher unter Berücksichtigung der für eine Virtualisierung infrage kommenden IT-Systeme festzulegen, auf welcher Virtualisierungstechnik (Server- oder Betriebssystemvirtualisierung) die virtuelle Infrastruktur basieren soll. Hierbei sind im Wesentlichen folgende Kriterien heranzuziehen:

- Die Servervirtualisierung, bei der ein vollständiger Server mit all seinen Hardwarekomponenten virtuell dargestellt wird, eignet sich besonders gut für den Betrieb von sehr unterschiedlichen virtuellen IT-Systemen mit stark variierenden Aufgaben. Bei Systemen auf der Basis einer Servervirtualisierung ist es möglich, unterschiedliche Betriebssysteme (Windows, Linux, Solaris) in den virtuellen IT-Systemen gleichzeitig auf einem Virtualisierungsserver zu betreiben, da jedes virtuelle System seinen eigenen Betriebssystemkern nutzen kann. Mit Hilfe der Servervirtualisierung kann eine sehr starke Kapselung der virtuellen IT-Systeme erreicht werden. Dies bedeutet, dass das virtuelle IT-System beispielsweise keine Betriebssystemkomponenten oder Softwarebibliotheken des Virtualisierungsservers oder anderer virtueller IT-Systeme nutzt. Weiterhin sind bei der Servervirtualisierung die virtuellen Systeme stärker voneinander isoliert als bei der Betriebssystemvirtualisierung, d. h. eine wechselseitige funktionale Beeinflussung ist weitgehend ausgeschlossen.
- Mittels der Betriebssystemvirtualisierung können auf einfache Weise große Mengen gleichartiger Server auf einem Virtualisierungsserver betrieben werden. Mit der Betriebssystemvirtualisierung können daher hohe Verdichtungsgrade (Verhältnis von virtualisierten IT-Systemen zu Virtualisierungsservern) erreicht werden. Es ist allerdings mit der Betriebssystemvirtualisierung in der Regel nicht möglich, unterschiedliche Betriebssysteme auf einem Server als virtuelle Systeme zu betreiben, da die virtuellen IT-Systeme meist den Betriebssystemkern und die Softwarebibliotheken des Virtualisierungsservers nutzen. In Grenzen ist dies bei einigen Produkten innerhalb einer Betriebssystemfamilie möglich. Beispielsweise ermöglicht *Parallels Virtuozzo* die Nutzung unterschiedlicher Editionen des Betriebssystems *Microsoft Windows Server 2003*. Die virtuellen IT-Systeme sind untereinander nicht so stark isoliert wie bei der Servervirtualisierung. Beispielsweise werden Softwarebibliotheken gemeinsam genutzt und die virtuellen IT-Systeme nutzen den selben Betriebssystemkern. Die Kapselung der virtuellen IT-Systeme ist meist gar nicht vorhanden oder nur sehr schwach ausgeprägt, da sie Soft- und Hardwarekomponenten des Virtualisierungsservers mit nutzen.

Diese schwache Kapselung der virtuellen IT-Systeme bei der Betriebssystemvirtualisierung führt dazu, dass virtuelle IT-Systeme mit stark unterschiedlichen Anforderungen an den Schutzbedarf nicht ohne Weiteres gemeinsam auf einem Virtualisierungsserver betrieben werden können. Dies ist bei Virtua-

lisierungslösungen auf Basis einer Servervirtualisierung in der Regel anders, da die Kapselung der virtuellen Systeme stärker ausgeprägt ist. Ob allerdings virtuelle IT-Systeme mit unterschiedlichem Schutzbedarfs auf einem Virtualisierungsserver zusammen betrieben werden können, hängt neben dem verwendeten Produkt auch von den individuellen Gefährdungen und Anforderungen der Organisation bzw. der virtuellen IT-Systeme ab. Daher ist bei der Planung zu bewerten, inwieweit die in Frage kommende Virtualisierungstechnik dafür geeignet ist, virtuelle IT-Systeme unterschiedlichen Schutzbedarfs auf einem Virtualisierungsserver gemeinsam zu betreiben.

Auswahl eines Virtualisierungsproduktes

Ist die Virtualisierungstechnik ausgewählt, müssen konkrete Virtualisierungsprodukte geprüft werden, ob sie für den konkreten Anwendungsfall geeignet sind. Die hierbei zu berücksichtigenden Anforderungen leiten sich dabei aus den innerhalb der virtuellen Umgebung benötigten Prozessorarten sowie deren Funktionen und der Verfügbarkeit von erforderlichen Geräteemulationen oder Schnittstellen ab.

In einer möglichst frühen Planungsphase muss geprüft und entschieden werden, mit welcher Technik virtuelle IT-Systeme mit dem Netz des Rechenzentrums verbunden werden sollen: Entweder durch eine direkte Zuordnung von physischen Netzkarten des Servers zu den virtuellen IT-Systemen oder die Verbindung der virtuellen Systeme über einen so genannten virtuellen Switch. Auf dieser Basis kann festgelegt werden, wie Regelungen und Richtlinien umgesetzt werden können, die auf der Basis der Maßnahmen M 2.141 *Entwicklung eines Netzkonzeptes*, M 5.61 *Geeignete physikalische Segmentierung* sowie M 5.62 *Geeignete logische Segmentierung* entwickelt worden sind. Hierdurch ergeben sich schon frühzeitig Vorgaben für den Aufbau der Virtualisierungsserver und der dazugehörigen Infrastruktur.

Sind die Anforderungen an die Zielumgebung geklärt, können eine passende Virtualisierungslösung und hierzu kompatible physische IT-Systeme ausgewählt werden.

Rechenzentrumsübergreifende Planung

Auf Virtualisierungsservern können eine Vielzahl von virtuellen IT-Systemen betrieben werden. Auf diesen virtuellen IT-Systemen, in der Regel Serversysteme mit unterschiedlichen Betriebssystemen, können weiterhin eine große Anzahl von verschiedenen Applikationen ausgeführt werden. Diese Applikationen wiederum benötigen in der Regel grundlegende Dienste wie DNS, Verzeichnisdienste zur Authentisierung oder Datenbanken. Daher müssen die Virtualisierungsserver auf alle Ressourcen zugreifen können, die für den Betrieb der Virtualisierungsserver selbst sowie der virtuellen IT-Systeme nötig sind. Die folgenden Anforderungen müssen bei der Planung eines Virtualisierungsprojektes beachtet werden. Die Virtualisierungsserver benötigen

- physische Verbindungen in alle Netze, in denen virtuelle IT-Systeme betrieben werden sollen.
- Verbindungen in Speichernetze zum Zugriff auf Massenspeicherkomponenten.
- Zugriff auf Infrastruktursysteme wie DNS-, DHCP- und Verzeichnisdienstserver.

Daher sollten alle Administratorengruppen, die mit der Bereitstellung dieser Dienste beauftragt sind, bei der Einführung der Virtualisierung angemessen beteiligt werden, damit diese ihre Kenntnisse einbringen und ihrerseits Anforderungen an das Virtualisierungsprojekt formulieren können.

Planung der Rollen und Verantwortlichkeiten

Da die Virtualisierungsserver häufig den Zugriff der virtuellen IT-Systeme und der darauf betriebenen Applikationen auf grundlegende Dienste des Rechenzentrums, sowie Netze und Speichernetze bereitstellen, sind sie aus der Sicht der virtuellen IT-Systeme selbst Bestandteil der Rechenzentrumsinfrastruktur. Daher wird empfohlen, für den Zugriff auf Netze und Speichernetze existierende Regelungen und Richtlinien an die Erfordernisse der virtuellen Infrastruktur anzupassen. Werden zum Beispiel gemäß M 5.130 *Absicherung des SANs durch Segmentierung* Vorgaben zur Segmentierung des Speichernetzes und zur Zugriffsregelung auf Speicherressourcen gemacht, muss sichergestellt sein, dass diese auch innerhalb der virtuellen Infrastruktur umgesetzt werden können. Der Zugriff auf Speicherressourcen muss für die Virtualisierungsserver möglicherweise weiter gefasst werden, da diese auf die Speicherressourcen vieler virtueller IT-Systeme zugreifen können müssen, damit sie wiederum selbst den virtuellen IT-Systemen Ressourcen zur Verfügung stellen können. Trotzdem sind die Anforderungen der angegebenen Maßnahme im Rahmen des Bausteins B 3.303 *Speicherlösungen / Cloud Storage* umzusetzen. Die Umsetzung muss hier jedoch mit den Mitteln der verwendeten Virtualisierungslösung möglich sein. Dies zeigt, dass durch die Administratoren der Virtualisierungsserver möglicherweise Aufgaben wahrgenommen werden müssen, die vorher durch die Administratoren des Speichernetzes bzw. der Speicherkomponenten darin ausgeführt wurden.

Gleiches gilt für die Aufgaben der Netzadministration. Die Verbindung von virtuellen IT-Systemen zu den unterschiedlichen Netzen des Informationsverbunds wird auf einem Virtualisierungsserver durch dessen Administratoren festgelegt, da sie die virtuellen IT-Systeme den physischen Netzverbindungen des Virtualisierungsservers zuordnen. Dies ist traditionell eine Aufgabe der Netzadministratoren. Sollen auf einem Virtualisierungsserver virtuelle IT-Systeme in unterschiedlichen Netzen betrieben werden, muss die Verantwortung für die richtige Netzzuordnung und die Überwachung dieser Zuordnung durch die Administratoren der Virtualisierungsserver übernommen werden. Zusätzlich muss berücksichtigt werden, dass das mit der Segmentierung des Netzes verfolgte Ziel, die Sicherheit durch Aufteilung der IT-Systeme auf verschiedene Bereiche des Rechenzentrums zu steigern, durch eine fehlende Kapselung und Isolation der virtuellen IT-Systeme auf dem Virtualisierungsserver nicht unterlaufen werden kann.

Es muss daher bei der Planung einer virtuellen Infrastruktur entschieden werden, wie die Aufgaben der Netz- und Speichernetzadministratoren, falls bei der gewählten Virtualisierungslösung notwendig, von den Administratoren der Virtualisierungsserver wahrgenommen werden sollen. Weiterhin ist zu prüfen, ob die Aufgaben der Verwaltung von Netz- und Speichernetzverbindungen durch die Administratoren der Virtualisierungsserver an die Netz- und Speichernetzadministratoren delegiert werden können. Die Betriebsverantwortung für die Umsetzung von bestehenden Regelungen und Richtlinien muss eindeutig und klar festgelegt werden.

Anpassung der Infrastruktur an die Virtualisierung

In klassischen Informationsverbünden sind IT-Systeme wie Server meist mit nur einem, seltener mit mehreren Netzen verbunden. Ein Virtualisierungsserver muss jedoch mit mehreren Netzen verbunden sein, wenn auf diesem Server virtuelle IT-Systeme in unterschiedlichen Netzen betrieben werden sollen.

Daher wird empfohlen, die Umsetzung der folgenden Maßnahmen aus dem Baustein B 4.1 *Heterogene Netze* und B 3.302 *Router und Switches*

- M 2.141 *Entwicklung eines Netzkonzeptes*,
- M 2.142 *Entwicklung eines Netz-Realisierungsplans*,
- M 5.61 *Geeignete physikalische Segmentierung*,
- M 5.62 *Geeignete logische Segmentierung*,
- M 5.77 *Bildung von Teilnetzen*,
- M 4.81 *Audit und Protokollierung der Aktivitäten im Netz*und
- M 4.206 *Sicherung von Switch-Ports*

an die Besonderheiten und Erfordernisse der Virtualisierungsserver anzupassen. Es muss darauf geachtet werden, dass die Virtualisierungsserver in einer virtuellen Infrastruktur alle Verbindungsanforderungen der virtuellen IT-Systeme erfüllen können.

Werden beispielsweise MAC-Filter auf Switch-Ports (siehe auch M 4.206 *Sicherung von Switch-Ports*) eingesetzt, muss die Konfiguration dieser Filter an die Erfordernisse der virtuellen Infrastruktur angepasst werden. Wenn das nicht der Fall ist, können virtuelle IT-Systeme, die bei einigen Virtualisierungslösungen eine eigene MAC-Adresse besitzen, nicht von einem Virtualisierungsserver auf einen anderen verschoben werden. Da diese Funktion möglicherweise für die Verteilung von virtuellen IT-Systemen auf Virtualisierungsserver benötigt wird, um auf Performance-Engpässe zu reagieren, ist ohne geeignete Anpassungen der Filterregeln die Verfügbarkeit von virtuellen IT-Systemen gefährdet.

Auch bei der Umsetzung der folgenden Maßnahmen aus dem Baustein B 3.303 *Speichersysteme und Speichernetze* müssen gegebenenfalls Anforderungen, die sich aus der Nutzung von Virtualisierungstechniken ergeben, berücksichtigt werden:

- M 2.525 *Erstellung einer Sicherheitsrichtlinie für Speicherlösungen*
- M 5.130 *Absicherung des SANs durch Segmentierung*
- M 4.275 *Sicherer Betrieb einer Speicherlösung*

Einsatzplanung für Virtualisierungsserver

Bei der Einsatzplanung müssen neben der Umsetzung der Maßnahme M 2.315 *Planung des Servereinsatzes* einige Besonderheiten beachtet werden. Diese Besonderheiten ergeben sich daraus, dass auf einem Virtualisierungsserver in der Regel mehrere virtuelle IT-Systeme betrieben werden sollen. Es muss daher ermittelt werden, wie viel Prozessorleistung, Hauptspeicher und Festplattenplatz für den Betrieb der virtuellen IT-Systeme benötigt wird. Weiterhin muss festgelegt werden, welche Netzverbindungen für die Virtualisierungsserver und die virtuellen IT-Systeme benötigt werden (siehe auch M 5.135 *Sicherer Medientransport mit SRTP*).

Für die Auswahl geeigneter Virtualisierungsserver sind die Gesamtanforderungen bezüglich Performance und Ressourcenverbrauch für die geplanten virtuellen IT-Systeme zu ermitteln. Hierdurch erst kann die Anzahl und die benötigte Leistungsfähigkeit der Virtualisierungsserver festgelegt werden.

Bei einer Migration bereits produktiv betriebener physischer IT-Systeme in virtuelle Umgebungen sollte zudem der tatsächliche Ressourcenbedarf nicht einfach durch Addition der Ressourcen der zu virtualisierenden IT-Systeme ermittelt werden. Stattdessen empfiehlt es sich, die Performance der zu virtualisierenden Systeme zu messen und die Anforderungen an die Virtualisierungsserver auf Basis der erforderlichen Performancewerte der gemessenen physischen Server festzulegen.

Neben ausreichenden Ressourcen für die individuellen virtuellen Maschinen müssen darüber hinaus weitere Kapazitäten in der virtuellen Infrastruktur vorgehalten werden, die durch die Virtualisierungssoftware selbst benötigt werden. So entsteht ein zusätzlicher Bedarf an Massenspeicherkapazität etwa für die Speicherung von Snapshots, Ereignisprotokollen und Auslagerungsdateien des Virtualisierungsservers. Weiterhin benötigt der Hypervisor eines Virtualisierungsservers ebenfalls Prozessorkapazität und Hauptspeicherplatz.

In Test- und Entwicklungsumgebungen kann von den obigen Vorgaben abgewichen werden. Es ist bei der Planung solcher Umgebungen darauf zu achten, dass sich keine unerwünschten Wechselwirkungen mit Produktivsystemen ergeben. Daher sind Test- und Entwicklungsumgebungen hinreichend von Produktivumgebungen abzuschotten.

Verfügbarkeit der virtuellen Infrastruktur

Es wird empfohlen, in der Planungsphase schon zu berücksichtigen, dass für die Virtualisierungsserver möglicherweise höhere Anforderungen an die Verfügbarkeit bestehen, da auf Virtualisierungsservern eine große Zahl an IT-Systemen betrieben wird. Fällt ein Virtualisierungsserver aus, sind auch alle darauf laufenden virtuellen IT-Systeme nicht mehr lauffähig. Dadurch übertragen sich alle Verfügbarkeitsanforderungen der einzelnen virtualisierten IT-Systeme auf den Virtualisierungsserver (*Kumulationsprinzip*). Es ist ratsam, zu prüfen, ob für Virtualisierungsserver eine hochverfügbare oder fehlertolerante Architektur gewählt werden sollte, oder ob in einer aus mehreren Virtualisierungsservern aufgebauten virtuellen Infrastruktur Mechanismen existieren, die den Ausfall eines oder mehrerer Virtualisierungsserver kompensieren.

Prüffragen:

- Steht die Vorgehensweise zur Nutzung von Virtualisierungsservern und virtuellen IT-Systemen in Einklang mit den Regelungen und Richtlinien für den Betrieb von IT-Systemen, Applikationen, Netzen und Speichernetzen?
- Sind die Aufgaben der einzelnen Administratorengruppen (Anwendungs-, Server-, Netz- und Speichernetzadministratoren) klar voneinander abgegrenzt?
- Ist die Betriebsverantwortung für die einzelnen Komponenten einer virtuellen Infrastruktur (Virtualisierungsserver, virtuelle IT-Systeme, Speichernetz, Netz) klar geregelt und können die jeweiligen Verantwortlichen ihre Aufgabe auch technisch wahrnehmen?
- Enthält die virtuelle Infrastruktur ausreichend Redundanzen, um den Verfügbarkeitsanforderungen Rechnung zu tragen?

M 3.70 Einführung in die Virtualisierung

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator, Leiter IT

Mit der so genannten Virtualisierung von IT-Systemen steht eine Technik zur Verfügung, mit der ein oder mehrere virtuelle IT-Systeme auf einem physischen Computer betrieben werden können. Ein solcher physischer Computer wird als Virtualisierungsserver bezeichnet. Diese Technik wird bereits seit den 1970er Jahren bei den Mainframes (z. B. IBM zSeries) eingesetzt. Sie hat aber erst Ende der 1990er Jahre im Bereich der Midrange Server weitere Verbreitung gefunden. Beispiele für Software-Produkte zur Virtualisierung von IT-Systemen mit x86-Architektur sind Microsoft Virtual PC/Server, Parallels Virtuozzo, Sun VirtualBox, VMware Workstation/Server/ESX und Xen. Ein weiteres Beispiel ist SUN Solaris Zones, das für die SPARC- und INTEL-Plattformen von Solaris verfügbar ist. Für die Enterprise Serie der SUN Server ist des Weiteren eine hardwaregestützte Virtualisierung (hier Partitionierung genannt) über die Verwendung so genannter Domains möglich. Im Bereich der zSeries-Großrechner kann eine Virtualisierung beispielsweise über die Nutzung von Logical Partitions (LPARs, hardwaregestützte Virtualisierung) oder über das Produkt z/VM (softwaregestützt) erfolgen (siehe auch B 3.107 *S/390- und zSeries-Mainframe*).

Die Virtualisierungstechnik hat sich sehr schnell als strategisches Mittel zur besseren Auslastung und Konsolidierung von Serversystemen durchgesetzt, da sie es ermöglicht, viele Dienste auf einem physischen Serversystem zu konzentrieren, ohne dass die Aufteilung der Dienste auf einzelne IT-Systeme aufgegeben werden muss. Dadurch werden die Ressourcen der physischen Server besser ausgenutzt und es können vielfach Einsparungen im Serverbetrieb erreicht werden. Diese Einsparungen beziehen nicht nur auf die Anzahl der einzusetzenden physischen IT-Systeme sondern auch auf die Stromkosten, den Platz in Serverräumen und Rechenzentren sowie die Klimatisierung. Weiterhin ist es möglich, durch die Virtualisierung Prozesse zur Bereitstellung neuer Server zu beschleunigen, da beispielsweise nicht für jedes neue Serversystem eine Bestellung durchgeführt werden muss. Bei einigen Virtualisierungslösungen können virtuelle IT-Systeme kopiert werden, wodurch Installationsprozesse vereinfacht werden können, oder es können so genannte Snapshots von virtuellen IT-Systemen angelegt werden, die es ermöglichen, nach einer fehlerhaften Konfigurationsänderung schnell den ursprünglichen Zustand wiederherzustellen.

Mehrere Virtualisierungsserver können des Weiteren zu einer so genannten virtuellen Infrastruktur zusammengefasst werden. In einer solchen virtuellen Infrastruktur werden mehrere Virtualisierungsserver gemeinsam mit den darauf laufenden virtuellen IT-Systemen verwaltet. Damit sind weitere Funktionen möglich. Beispielsweise können virtuelle IT-Systeme von einem Virtualisierungsserver auf einen anderen verschoben werden. Dies kann teilweise auch dann durchgeführt werden, während das virtuelle IT-System in Betrieb ist (*Live Migration*). Weiterhin gibt es Möglichkeiten, die Verfügbarkeit der virtuellen IT-Systeme zu steigern. So können mittels der *Live Migration* virtuelle Systeme immer auf den Virtualisierungsserver verschoben werden, der gerade die beste Performance für den Betrieb des virtuellen Systems zur Verfügung stellen kann. Eine weitere Möglichkeit besteht darin, virtuelle IT-Systeme automatisch auf einem anderen Virtualisierungsserver neu zu starten, wenn der ursprüngliche Virtualisierungsserver beispielsweise wegen eines Hardwaredefekts ausgefallen ist.

Die reichhaltigen Möglichkeiten zu Manipulation der virtuellen IT-Systeme durch die Virtualisierungssoftware lassen Virtualisierungsserver besonders für den Aufbau von Test- und Entwicklungsumgebungen geeignet erscheinen. Es ist mittels der Virtualisierung möglich, für Test- und Entwicklung schnell IT-Systeme bereitzustellen und komplexe Umgebungen schnell und effizient aufzubauen. Weiterhin können produktive virtuelle IT-Systeme für eine Test- und Entwicklungsumgebung kopiert werden, damit Aktualisierungen und Anpassungen ohne Störungen des Produktivbetriebes getestet werden können.

Voraussetzungen für den Betrieb virtueller IT-Systeme auf einem Virtualisierungsserver

Um verschiedene virtuelle IT-Systeme auf einem Virtualisierungsserver sicher nebeneinander betreiben zu können, muss die Virtualisierungssoftware bestimmte Voraussetzungen erfüllen. Die Virtualisierungssoftware muss dafür sorgen, dass

- sich jedes virtuelle IT-System für die darin ablaufende Software nahezu wie ein eigenständiger physischer Computer darstellt (Kapselung),
- die einzelnen virtuellen IT-Systeme voneinander isoliert werden und nur über festgelegte Wege miteinander kommunizieren können (Isolation),
- die einzelnen virtuellen IT-Systeme in geordneter Weise auf die Ressourcen der Hardware zugreifen können.

Abhängig davon, wie die Virtualisierung der Ressourcen realisiert ist, werden diese Funktionen der Virtualisierungsschicht möglicherweise nur eingeschränkt erfüllt. So gibt es beispielsweise Lösungen, bei denen die Betriebssystem-Software leicht angepasst werden muss, bevor sie in einem virtuellen IT-System laufen kann. Ein anderes Beispiel für Einschränkungen bei der Virtualisierung sind Lösungen, bei denen alle virtuellen IT-Systeme auf einem Virtualisierungsserver verschiedene Instanzen des gleichen Betriebssystems verwenden müssen.

Die Virtualisierungsschicht muss nicht notwendigerweise eine reine Software-Komponente sein. Bei einigen Plattformen unterstützt auch die Hard- oder Firmware die Virtualisierung der Ressourcen. Die Virtualisierungsschicht stellt den virtuellen IT-Systemen in der Regel konfigurierbare Zugriffsmöglichkeiten auf lokale Laufwerke und Netzverbindungen zur Verfügung. Dies erlaubt es den virtuellen IT-Systemen, miteinander und mit fremden IT-Systemen zu kommunizieren.

In der Praxis werden zwei Arten von Virtualisierungssoftware unterschieden, die Servervirtualisierung und die Betriebssystemvirtualisierung.

Servervirtualisierung

Die Servervirtualisierung bildet die Basis für virtuelle IT-Systeme, die meist eine vom Virtualisierungsserver abstrahierte, virtualisierte und vollständige Hardwareumgebung besitzen. In dieser virtuellen Hardwareumgebung wird ein vollständiges Betriebssystem installiert, auf dem dann im Folgenden Anwendungen auf gewohnte Weise betrieben werden können.

In der Regel ist das Betriebssystem, das auf dem virtuellen IT-System installiert werden kann, völlig unabhängig von dem Betriebssystem, unter dem die Virtualisierungssoftware betrieben wird. Der Zugriff des virtuellen IT-Systems auf die Ressourcen (Prozessor, Arbeitsspeicher, Massenspeicher, Netz) des Virtualisierungsservers wird durch die Virtualisierungssoftware gesteuert. Dazu erhält jedes virtuelle IT-System virtuelle Geräte, die den Zugriff auf diese Ressourcen erlauben. Diese Geräte werden entweder vollständig emuliert,

oder es werden die physischen Geräte durch die Virtualisierungssoftware an das virtuelle IT-System weiter gereicht. Im jedem Fall sorgt die Virtualisierungssoftware dafür, dass die physischen Geräte auf geordnete Weise durch die virtuellen IT-Systeme genutzt werden können, so dass sich diese gegenseitig möglichst wenig beeinflussen können. Die Treiber, mit denen die virtuellen IT-Systeme auf die Hardwarekomponenten des Virtualisierungsservers zugreifen, müssen in der Regel nach der Betriebssysteminstallation innerhalb der virtuellen IT-Systeme nachinstalliert werden.

Bei der Servervirtualisierung wird zwischen so genannten hypervisorbasierten (Typ 1-) und hostbasierten (Typ 2-) Virtualisierungsprodukten unterschieden. Bei den hypervisorbasierten Virtualisierungsprodukten wird auf der physischen Hardware nur ein auf die Virtualisierung spezialisiertes Rumpf-Betriebssystem, der so genannte Hypervisor, installiert. Dieser erzeugt die für den Betrieb der virtuellen IT-Systeme notwendige virtuelle Hardware-Umgebung und steuert den Zugriff der virtuellen IT-Systeme auf die physischen Ressourcen. Bei den hostbasierten Virtualisierungsprodukten wird der Hypervisor als Dienst in einem voll ausgestatteten und nicht auf den Verwendungszweck optimierten Betriebssystem installiert.

Betriebssystemvirtualisierung

Die Betriebssystemvirtualisierung unterscheidet sich von der Servervirtualisierung sehr stark in der Art, wie die virtuellen IT-Systeme erzeugt werden. Die Servervirtualisierung stellt den virtuellen IT-Systemen eine vollständige Hardwareumgebung zur Verfügung. Die Betriebssystemvirtualisierung hingegen stellt eine Lösung dar, in der den virtuellen IT-Systemen isolierte Instanzen des Betriebssystems zur Verfügung gestellt werden, auf dem das Virtualisierungsprodukt installiert wurde. Daher sind beispielsweise für den Zugriff auf die Hardwarekomponenten des physischen Systems in der Regel keine speziellen Treiber notwendig, da die Hardwarekomponenten unverändert an das virtuelle IT-System "durchgereicht" werden. Die Virtualisierungssoftware steuert hier nur den Zugriff, so dass sich die virtuellen IT-Systeme nicht gegenseitig beeinflussen.

Durch diese Art der Virtualisierung ergeben sich einige Einschränkungen für die virtuellen IT-Systeme, die mittels einer Betriebssystemvirtualisierungslösung betrieben werden. Es ist in der Regel nicht möglich, unterschiedliche Betriebssysteme in den auf einem Virtualisierungsserver laufenden IT-Systemen zu nutzen, da das Betriebssystem vom Virtualisierungsserver übernommen werden muss. Bei einigen Produkten können allerdings unterschiedliche Kernelversionen des gleichen Betriebssystems auf einem Virtualisierungsserver genutzt werden.

Bei beiden Virtualisierungstechniken steht für die Administration des Virtualisierungsservers, des Hypervisors und der virtuellen IT-Systemen eine Verwaltungssoftware zur Verfügung. Dies kann eine webbasierte Verwaltungsoberfläche, eine spezielle Verwaltungssoftware oder auch eine kommandozeilen-basierte Benutzerschnittstelle sein. Bei einigen Typ 1-Servervirtualisierungsprodukten wird diese Verwaltungsschnittstelle als virtuelles IT-System unter der vollständigen Kontrolle des Hypervisors ausgeführt.

Vergleich von Server- und Betriebssystemvirtualisierung

Der große Vorteil der Betriebssystemvirtualisierung ist es, dass auf dem Virtualisierungsserver so gut wie keine Ressourcen für die Emulation einer virtuellen Hardware benötigt werden, so wie es bei der Servervirtualisierung der Fall ist. Dadurch können mit der Betriebssystemvirtualisierung deutlich mehr

virtuelle IT-Systeme auf einem physischen System betrieben werden als bei der Servervirtualisierung. Dies ermöglicht einen höheren Verdichtungsgrad, also ein höheres Verhältnis von virtuellen zu physischen IT-Systemen.

Wesentliche Nachteile der Betriebssystemvirtualisierung sind allerdings die geringere Flexibilität bei der Verwendung unterschiedlicher Betriebssysteme sowie die schwächere Kapselung der virtuellen IT-Systeme. Für den Einsatz unterschiedlicher Anwendungen innerhalb der virtuellen IT-Systeme können daher ebenfalls Einschränkungen bestehen. Dies hängt im Wesentlichen damit zusammen, dass die Verzahnung von virtuellen IT-Systemen und Virtualisierungsserver stärker ist als bei der Servervirtualisierung. Bei der Betriebssystemvirtualisierung werden häufig viele Teile des Betriebssystems des Virtualisierungsservers gemeinsam mit den virtuellen IT-Systemen genutzt. So werden meist die gleichen Software-Bibliotheken und Betriebssystemkomponenten genutzt, bei einigen Virtualisierungsprodukten werden z. B. Software-Bibliotheken nur einmal im Arbeitsspeicher des physischen Systems gehalten und von allen virtuellen IT-Systemen genutzt.

Die Kapselung der virtuellen IT-Systeme ist daher bei der Betriebssystemvirtualisierung im Vergleich mit der Servervirtualisierung geringer ausgeprägt. In der Folge kann auch die Isolation der virtuellen IT-Systeme untereinander und im Verhältnis zum Virtualisierungsserver weniger stark sein.

Bei der Servervirtualisierung ist der Ressourcenverbrauch pro virtuellem IT-System auf dem Virtualisierungsserver in der Regel höher als bei der Betriebssystemvirtualisierung. Der Aufwand zur Wartung und Pflege (Beispiel: Einspielen von Softwareaktualisierungen) der virtuellen IT-Systeme ist ebenfalls höher, da diese auf Grund der starken Kapselung häufig für jedes virtuelle IT-System einzeln erfolgen muss. Bei der Betriebssystemvirtualisierung können solche Softwareaktualisierungen teilweise durch Installation des Patches auf dem Virtualisierungsserver in allen virtuellen IT-Systemen mit installiert werden.

Weiterhin wird die größere Flexibilität der Servervirtualisierungslösungen mit einem höheren Komplexitätsgrad erkauft. Diese höhere Komplexität ergibt sich durch den etwas höheren Aufwand, mit dem Virtualisierungsserver für eine Servervirtualisierung in die Infrastruktur des Informationsverbundes integriert werden müssen. Die Verfahrensweisen für die Integration dieser Systeme in Netze und Speichernetze sind in der Regel komplexer. Des Weiteren müssen bestehende Prozesse zum Ausrollen neuer IT-Systeme möglicherweise angepasst werden.

Daher eignet sich die Betriebssystemvirtualisierung dann besonders gut, wenn eine große Menge gleichartiger virtueller IT-Systeme benötigt wird, beispielsweise viele gleich oder ähnlich konfigurierte Webserver. Die Servervirtualisierung kann ihre Vorteile dann ausspielen, wenn viele verschiedene virtuelle IT-Systeme betrieben werden müssen. Sollen heterogene Serverlandschaften virtualisiert werden, existiert häufig keine Alternative zur Servervirtualisierung.

Netzwerkintegration der Virtualisierungsserver und virtuellen IT-Systeme

Bei den verschiedenen Virtualisierungslösungen bestehen viele unterschiedliche Methoden, den virtuellen IT-Systemen Zugriff auf die Netze des Informationsverbundes zu ermöglichen. Im Wesentlichen können zwei Prinzipien unterschieden werden, wie diese Netzverbindungen realisiert werden.

- Den virtuellen IT-Systemen werden direkt physische Netzschnittstellen des Virtualisierungsservers zugeordnet. Hierbei sind die virtuellen IT-Sy-

steme direkt mit dem Netz verbunden, mit dem der Virtualisierungsserver selbst verbunden ist.
- Die physischen Netzschnittstellen werden indirekt mit den virtuellen IT-Systemen verbunden. Dabei wird ein virtueller Switch durch den Hypervisor erzeugt, mit dem die virtuellen Netzschnittstellen der virtuellen IT-Systeme verbunden sind. Dieser virtuelle Switch wiederum kann mittels einer physischen Netzschnittstelle des Virtualisierungsserver mit dem physischen Netz verbunden werden. Es ist mit dieser Technik auch möglich, virtuelle Switche und Netze zu definieren, die keine Verbindung in das physische Netz des Informationsverbundes haben.

Diese zwei unterschiedlichen Netzintegrationstechniken haben unterschiedliche Auswirkungen darauf, wie die Integration der virtuellen IT-Systeme und der Virtualisierungsserver in das Netz des Informationsverbundes vorgenommen werden muss. Besonders mit der zweiten Variante ist es möglich, flexibel auf unterschiedliche Schutzbedarfsanforderungen der virtuellen IT-Systeme zu reagieren.

Gastwerkzeuge

Viele Hersteller stellen für die virtuellen IT-Systeme so genannte Gastwerkzeuge zur Verfügung, mit denen die virtuellen IT-Systeme auf einfache Weise durch die Virtualisierungssoftware gesteuert werden können. Diese Werkzeuge ermöglichen es beispielsweise, virtuelle IT-Systeme über die Virtualisierungssoftware herunterzufahren, ohne dass mit dem virtuellen System direkt interagiert werden muss. Weitere Funktionen sind z. B. der Austausch der Zwischenablage zwischen virtuellem IT-System und dem Rechner des Benutzers des virtuellen IT-Systems oder der vereinfachte Zugriff auf Datenträger wie CD- oder DVD-ROMs, die in die entsprechenden Laufwerke des Virtualisierungsservers oder des Rechners des Benutzers des virtuellen IT-Systems eingelegt werden. Die Treiber für den Zugriff auf die virtualisierte Hardware und die Werkzeuge zur Steuerung der virtuellen IT-Systeme werden häufig als ein integriertes Installationspaket bereitgestellt.

M 3.71 Schulung der Administratoren virtueller Umgebungen

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter, Leiter IT

Virtuelle Infrastrukturen stellen ein wichtiges Infrastrukturelement in einem Rechenzentrum dar. Sie bieten ein deutliches Einsparpotenzial gegenüber herkömmlichen Serverstrukturen und finden eine hohe Verbreitung in Rechenzentren. Daher sollte sichergestellt werden, dass alle mit der Administration der Virtualisierungskomponenten betrauten Personen ausreichende Kenntnisse über die der virtuellen Infrastruktur zugrunde liegenden Produkte besitzen.

Virtualisierungsserver haben einen hohen Komplexitätsgrad. Neben virtuellen IT-Systemen enthalten sie auch einen Hypervisor sowie Netzkomponenten wie beispielsweise virtuelle Switches und eigene Dienste. Da Fehlkonfigurationen auf Virtualisierungsservern häufig gravierende Folgen für die darauf betriebenen virtuellen IT-Systeme haben, erhöhen sich die Anforderungen an die Administratoren der Virtualisierungsumgebung. Daher ist es wichtig, dass diese Administratoren ausreichend geschult sind, damit sie Probleme aus eigenem Handeln heraus vermeiden, technische Probleme rechtzeitig erkennen und beseitigen sowie die Funktionen und Sicherheitsmerkmale der Virtualisierungswerkzeuge optimal nutzen. Sie werden dadurch in die Lage versetzt, die Funktionen des jeweiligen Virtualisierungsproduktes zu beherrschen und die Folgen von Konfigurationsänderungen abzuschätzen.

Die Schulungen sollen ausreichende Kenntnisse für die Planung, den Aufbau und den Betrieb der für den Einsatz ausgewählten Virtualisierungsumgebung vermitteln.

Auch bei einer Aufteilung von Administratorenrollen (siehe M 2.446 *Aufteilung der Administrationstätigkeiten bei Virtualisierungsservern*) müssen alle Administratoren die Grundlagen der ausgewählten Virtualisierungstechnik beherrschen, da die bislang vorherrschende Trennung von Fachbereichen wie Server-, Netz- und Speicherbetrieb aufgelöst wird.

Bereits bei der Planung einer Virtualisierungsumgebung sollte ein ausreichendes Budget für Schulungsmaßnahmen einkalkuliert werden. Ebenfalls sollten Zeiträume für die Schulungen rechtzeitig eingeplant werden, um personelle Ressourcenengpässe zu vermeiden.

Schulungen zur Virtualisierung von IT-Systemen sollten mindestens folgende Elemente enthalten:

- Grundlagen und Konzepte des jeweiligen Virtualisierungssystems
- Erstellung und Umsetzung von internen Richtlinien und Regelungen zum Rechenzentrumsbetrieb
- Kenntnisse der Kommandos oder der Benutzeroberfläche der jeweiligen Komponenten.
- Planung einer Virtualisierungsumgebung in Bezug auf die Netzdimensionierung und -absicherung sowie die Dimensionierung der Hardware für CPU-, RAM-, Netz- und Speichernetzressourcen
- Vorbereiten des Betriebssystems des Virtualisierungsservers
- Installation und Konfiguration des Virtualisierungssystems
- Installation der Betriebssysteme in dem virtuellen IT-System
- Netzkonfiguration des virtuellen IT-Systems

- Betrieb
- Überwachung, Verwaltung
- Protokollierung
- Sicherung und Verwaltung von Konfigurationen
- Sicherung virtueller Maschinen
- Automatisierungsprozesse
- Analyse und Fehlerbehandlung

Es sollte darauf geachtet werden, dass die Schulung neben der Theorie ausreichende praktische Anteile enthält.

Prüffragen:

- Werden Schulungen für die Administratoren virtueller Umgebungen mit den empfohlenen Mindestinhalten durchgeführt?
- Sind die Administratoren der Virtualisierungsumgebung ausreichend geschult, sodass sie Probleme aus eigenem Handeln heraus vermeiden, technische Probleme rechtzeitig erkennen und die Funktionen und Sicherheitsmerkmale der Virtualisierungswerkzeuge optimal nutzen können?

M 3.72 Grundbegriffe der Virtualisierungstechnik

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter, Leiter IT

Der Begriff "Virtualität" und das dazugehörige Adjektiv "virtuell" werden in der Computertechnologie schon sehr lange in sehr unterschiedlichen Anwendungsfällen verwendet. In den meisten Szenarien wird ein Objekt mit der Eigenschaft "virtuell" versehen, wenn es zwar physisch nicht vorhanden, seiner Wirkung nach jedoch existent erscheint. Somit kann ein virtuelles Objekt durchaus reale Auswirkungen haben, also die Realität verändern oder mit der Realität interagieren. Daher sind die Begriffe "Virtualität" und "Realität" nicht als Gegensätze zu begreifen. Als "Virtualisierung" wird auch der Prozess verstanden, bei dem ein Objekt von einem realen in ein virtuelles transformiert wird oder von vornherein in virtueller Form bereitgestellt wird.

Speziell in der Informationstechnik wird die Virtualisierung von Objekten als technische Substitution dieser Objekte (Ersetzung durch etwas Gleichwertiges oder Gleichwirkendes) verwendet. Wird beispielsweise realer Arbeitsspeicher eines IT-Systems durch virtuellen Arbeitsspeicher substituiert (gleichwertig ersetzt), kann dieser wie der reale verwendet werden, obwohl er beispielsweise auf der Festplatte des Systems als Datei repräsentiert wird. Diese Datei ist tatsächlich kein realer Arbeitsspeicher, ist aber in ihrer Wirkung dem Arbeitsspeicher gleich. Diese Technik wird angewendet, um mehr Arbeitsspeicher verwenden zu können, als tatsächlich vorhanden ist. Durch die Nutzung virtuellen Arbeitsspeichers können allerdings Performancenachteile entstehen. Es existieren noch viele weitere Beispiele für virtualisierte Ressourcen wie VLANs, VPNs oder auch virtuelle Prozessoren (*Intel Hyperthreading*).

In der Vergangenheit ist, wie aus den Beispiel im vorigen Absatz deutlich wird, die Virtualisierung hauptsächlich verwendet worden, um knappe und teure Ressourcen durch solche zu substituieren, die im Übermaß vorhanden oder preiswerter zu beschaffen waren. Mittlerweile hat sich allerdings die Computertechnik und insbesondere die Performance der Rechner soweit entwickelt, dass das Konzept der Virtualisierung auch auf weitere Anwendungsfälle ausgedehnt wird. Der Computer kann mit Hilfe einer entsprechenden Virtualisierungssoftware als universelles Werkzeug eingesetzt werden, um sehr viele Objekte zu virtualisieren, insbesondere den Computer selbst.

Kapselung und Isolation

Isolation und Kapselung sind zwei wichtige Sicherheitsanforderungen an eine Virtualisierungslösung. Isolation bedeutet in diesem Zusammenhang, dass zwei virtuelle IT-Systeme, die auf dem gleichen Virtualisierungsserver ablaufen, nur über die hierzu vorgesehenen Mechanismen miteinander kommunizieren können. Isolation trägt unter anderem dazu bei, dass von einem virtuellen IT-System nicht unberechtigt auf die Daten eines anderen virtuellen IT-Systems zugegriffen werden kann.

Kapselung bedeutet im Kontext von Virtualisierung, dass jedes virtuelle IT-System nur mit den Ressourcen kommunizieren kann, die hierfür jeweils freigeschaltet sind. Ressourcen können dabei beispielsweise Hardware-Komponenten, Netzverbindungen oder Prozesse, die direkt auf dem Virtualisierungsserver laufen, sein. Die Kapselung trägt somit nicht nur zum Schutz virtueller IT-Systeme vor unberechtigten Zugriffen bei, sondern umgekehrt auch zum

Schutz der Ressourcen vor unberechtigten Zugriffen seitens der virtuellen IT-Systeme. Darüber hinaus dient die Kapselung auch der Portierbarkeit von virtuellen IT-Systemen.

Isolation und Kapselung sind eng verwandte Sicherheitsanforderungen, die auf technischer Ebene mit ähnlichen Mechanismen erreicht werden. In der Praxis wird zwischen den beiden Aspekten häufig nicht unterschieden.

Systemvirtualisierung

Durch das Überangebot an Leistung in modernen Rechneranlagen, die durch traditionelle Betriebssysteme und Anwendungen nicht mehr ausgelastet werden, entsteht der Wunsch, diese Leistungsreserven effizienter zu nutzen. Dies könnte beispielsweise durch die Kumulation von Anwendungen auf einem wenig ausgelasteten Rechnersystem geschehen. Aus guten Gründen (siehe auch M 4.97 *Ein Dienst pro Server*) ist eine solche Strategie zur Effizienzsteigerung abzulehnen: Solche Systeme würden nahezu unbeherrschbar, da Applikationen sich möglicherweise auf unvorhersehbare Weise gegenseitig beeinflussen, wenn sie auf einem Rechnersystem installiert sind. Werden sie getrennt betrieben, entstehen solche Beeinflussungen erst gar nicht. Veränderungen an den Betriebssystemen (z. B. Aktualisierungen oder Patches) müssen nicht mit einer Vielzahl von Anwendungen geprüft werden, sondern nur mit einer. Es ist weiterhin weitgehend ausgeschlossen, dass die Aktualisierung einer Anwendung Einfluss auf die Funktionsfähigkeit einer anderen Anwendung hat. Wird nun durch eine geeignete Technik dafür gesorgt, dass

- die auf einem einzelnen Rechnersystem naturgemäß gegebene gemeinsame **Kapselung** von Betriebssystem und Anwendung sowie
- die auf mehreren Rechnersystemen entstehende **Isolation** von Betriebssystem und Anwendungen auf diesen Rechnern voneinander

erhalten bleibt, wenn diese Rechnersysteme als virtuelle Instanzen auf einem Rechnersystem betrieben werden, verbleiben die Vorteile der Aufteilung auf einzelne Rechnersysteme. Die Ausnutzung der Rechnerressourcen wird hingegen verbessert. Durch die Virtualisierung von Rechnersystemen können daher die Leistungsreserven besser ausgenutzt werden, ohne die übersichtliche Aufteilung einzelner Anwendungen und Dienste auf einzelne Serversysteme aufzugeben.

Dieses Konzept der Aufteilung eines Rechnersystems in mehrere virtuelle Instanzen wurde zuerst in der Großrechnerwelt eingeführt. Hier wurde der Großrechner mittels einer so genannten Partitionierungstechnik in viele einzelne Rechner (logische Partitionen z. B. *IBM LPAR*s bei der *z-Series*) mit jeweils eigenem Betriebssystem und eigenen Anwendungen aufgeteilt. Diese Technik wurde später auch auf Server der mittleren Leistungsklasse und auf Serversysteme auf der Basis der x86- bzw. x64-Architektur übertragen, als diese leistungsfähig genug waren, um mehrere Rechnerinstanzen auf einer Hardwareplattform betreiben zu können.

Im Folgenden wird nun beschrieben, wie sich die Virtualisierungstechnik auf Serversystemen auf Basis der x86- bzw. x64-Architektur entwickelt hat und welche Basistechniken und Hardwarevoraussetzungen dafür geschaffen wurden. Weiterhin werden einige Anwendungen der Virtualisierungstechnik vorgestellt.

Vollständige Systememulation

Die Virtualisierungstechnik ist zuerst als reine Softwarelösung implementiert worden. Dies bedeutet, dass durch die Virtualisierungssoftware einem virtuel-

len System eine emulierte Hardwareumgebung präsentiert wurde. Die Rechnerkomponenten des virtuellen IT-Systems wie Prozessor, Arbeitsspeicher und Massenspeicher sowie Netzschnittstellen wurden aufwändig emuliert und vollständig in Software nachgebildet. Hierdurch ist die Performance eines solchen virtuellen Systems sehr begrenzt. Sie ermöglicht aber, vor allem auf Grund der Prozessoremulation, sehr flexible Möglichkeiten, da hier auch plattformübergreifende Virtualisierungen von IT-Systemen möglich sind. Es ist mittels solcher vollständiger Rechnervirtualisierungssoftware beispielsweise (hier: Microsoft Virtual PC für Mac 7) möglich, ein Betriebssystem wie Microsoft Windows XP, dass ausschließlich für die x86-Plattform entwickelt wurde und nur dort lauffähig ist, auf einem PowerPC-basierenden Rechner mit Mac OS X 10.4 auszuführen, indem der x86-Prozessor vollständig in Software nachgebildet wurde. Eine solche vollständige Rechnervirtualisierung ist allerdings hochgradig ineffizient, da die vollständige Emulation von Prozessor-Architektur und sonstiger Hardwarebestandteile sehr viele Ressourcen benötigt und das virtuelle IT-System damit nur einen Bruchteil der physisch verfügbaren Performance nutzen kann.

Servervirtualisierung

Wesentlich effizienter als die vollständige und plattformübergreifende Virtualisierung eines Rechnersystems ist daher eine plattformspezifische Virtualisierungstechnik. Hier muss keine vollständige Rechnerumgebung (Prozessor, Arbeitsspeicher, Festplattenspeicher usw.) in Software nachgebildet werden. Die Virtualisierungssoftware muss nur so gestaltet sein, dass innerhalb der gegebenen Hardwarearchitektur die Kapselung und Isolation (s. o.) der jeweiligen virtuellen Instanzen ähnlich der von physischen Systemen ist. Eine aufwändige vollständige Emulation von Hardwarekomponenten ist dann nicht mehr notwendig. Die Software, die die Steuerung der virtuellen Systeme und deren Hardwareumgebung simuliert, wird als *Hypervisor* bezeichnet.

Die Virtualisierungssoftware (bzw. der Hypervisor) hat im Wesentlichen nur die folgenden Aufgaben:

- Bereitstellung einer gekapselten und isolierten Laufzeitumgebung für die einzelnen virtuellen Instanzen und
- Steuerung der Zugriffe des virtuellen Systems auf Hardwarekomponenten des physischen Systems.

Diese hier beschriebene plattformspezifische Virtualisierungstechnik wird als Servervirtualisierung bezeichnet. Bei Lösungen auf der Basis einer Servervirtualisierung wird weiterhin noch zwischen hypervisorbasierten (Typ 1) und hostbasierten Lösungen (Typ 2) unterschieden.

Bei den hostbasierten Virtualisierungslösungen wird die Virtualisierungssoftware auf einem Standard-Betriebssystem wie Unix oder *Microsoft Windows Server* installiert, während bei Virtualisierungslösungen vom Typ 1 (Hypervisorbasiert) auf der physischen Hardware nur der Hypervisor installiert wird. Dieser Hypervisor stellt dann ein auf die Virtualisierung spezialisiertes Minimal-Betriebssystem dar. Eine Typ 1-Virtualisierungssoftware wird gelegentlich auch als *Bare Metal Virtualization* bezeichnet.

Produkte, die die Servervirtualisierungstechnik verwenden, sind beispielsweise

- Microsoft Hyper-V (Typ 1), Microsoft VirtualPC (Typ 2) oder Microsoft VirtualServer (Typ 2)
- QEMU (Typ 2, Anmerkung: QEMU kann auch zur vollständigen Systememulation verwendet werden)

- Sun VirtualBox (Typ 2)
- VMware Server (Typ 2) und VMware Workstation (Typ 2)
- VMware vSphere bzw. VMware ESX(i) (Typ 1),
- auf Xen basierende Produkte wie Citrix XenServer, Sun OpenVM (Typ 1)

Bei der Servervirtualisierung wird durch die Virtualisierungssoftware in der Regel ein virtueller Rechner erzeugt, der aus virtualisierten Hardwarekomponenten besteht. Diese Hardwarekomponenten werden dem Betriebssystem des virtuellen Systems präsentiert. Die Virtualisierungssoftware kann nun die Zugriffs- und Steuerungsbefehle, die vom Betriebssystem des virtuellen IT-Systems an dessen virtuelle Hardware gesandt werden, direkt in solche für die physische Hardware umsetzen. Diese Umsetzung ist deutlich effizienter als die oben beschriebene vollständige Emulation der Hardwarekomponenten.

Diese Technik wird als so genannte *Vollvirtualisierung* bezeichnet. Eine weitere Steigerung der Performance kann mittels der so genannten *Paravirtualisierung* erreicht werden. Hierbei wird unter der Kontrolle des Hypervisors ein speziell angepasstes Betriebssystem in dem virtuellen IT-System ausgeführt. Dieses ist so modifiziert, dass keine hardwarenahen Systembefehle mehr im Kernel des Betriebssystems des virtuellen IT-Systems enthalten sind. Diese Systembefehle werden häufig auch als "Ring 0-Befehle" oder "Dom0-Befehle" bezeichnet. Das virtuelle IT-System wird dann im "Ring 1" bzw. in der "DomU" ausgeführt. Unterstützt der Prozessor des Virtualisierungsservers die Paravirtualisierung (z. B. AMD-V und Intel VT), so kann auf ein angepasstes Betriebssystem verzichtet werden. Diese Möglichkeit nutzt beispielsweise XEN 3.0.

Betriebssystemvirtualisierung

Die Effizienz der Virtualisierungssoftware kann jedoch noch weiter gesteigert werden, in dem nicht nur die Hardwareplattform allen virtuellen Systemen gemein ist, sondern auch das Betriebssystem für alle virtuellen Instanzen festgelegt wird. Solche Virtualisierungstechniken werden Betriebssystemvirtualisierung genannt. Die Steuerung der Hardwarezugriffe der virtuellen IT-Systeme kann extrem vereinfacht werden, da hier keine virtuellen Hardwarekomponenten notwendig sind. Das virtuelle System hat das gleiche Betriebssystem wie das physische, auf dem es ausgeführt wird, und kann daher die gleichen Hardware-Treiber verwenden. Der Umsetzungsaufwand zwischen virtueller und physischer Hardware fällt somit vollständig weg. Die Kapselung der virtuellen IT-Systeme ist hier allerdings zumindest für das Betriebssystem nicht mehr sehr stark ausgeprägt, da alle virtuellen Instanzen das gleiche (nicht das selbe!) Betriebssystem nutzen. Die Virtualisierungssoftware stellt also nur noch die Isolation der einzelnen virtuellen Instanzen sicher.

Beispiele für solche Betriebssystemvirtualisierungslösungen sind:

- Sun Solaris Containers
- BSD jails
- Parallels Virtuozzo
- User Mode Linux

Der Vorteil der auf einer Betriebssystemvirtualisierung beruhenden Produkte liegt in der hohen Performance der virtuellen Instanzen und ihrem geringen relativen Ressourcenverbrauch auf dem Virtualisierungsserver im Vergleich zur Servervirtualisierung. Hierdurch ist ein sehr großer Verdichtungsgrad (Verhältnis der Anzahl von Virtualisierungsservern zu virtuellen Systemen) erreichbar. Mit einigen Betriebssystemvirtualisierungslösungen können bis zu 200 virtuelle IT-Systeme auf einem Virtualisierungsserver mittlerer Leistungsklasse betrieben werden. Auf einem gleich ausgestatteten Server, der eine Servervirtualisierungslösung nutzt, sind meist nur 10 bis 15 virtuelle Systeme möglich.

Der Nachteil der Betriebssystemvirtualisierungslösungen liegt allerdings in der schwachen Kapselung von Betriebssystem und Anwendungen auf dem Virtualisierungsserver. Diese schwache Kapselung führt dazu, dass virtuelle IT-Systeme mit stark unterschiedlichen Schutzbedarfsanforderungen nicht ohne Weiteres gemeinsam auf einem Virtualisierungsserver betrieben werden können. Dies ist bei Virtualisierungslösungen auf Basis einer Servervirtualisierung in der Regel anders, da die Kapselung der virtuellen Systeme stärker ausgeprägt ist. Ob allerdings virtuelle IT-Systeme unterschiedlicher Schutzbedarfsanforderungen auf einem Virtualisierungsserver zusammen betrieben werden können, hängt neben dem verwendeten Produkt auch von der Schutzbedarfsfestellung und den individuellen Gefährdungen der Organisation bzw. der virtuellen IT-Systeme ab.

Anwendungen der Virtualisierungstechnik

Mit Mitteln der Virtualisierungstechnik können einige Anwendungen entwickelt werden, die für physische Systeme in der Regel nur mit unverhältnismäßig hohem Aufwand realisiert werden könnten. Diese Anwendungen basieren in der Regel darauf, dass die Virtualisierungssoftware direkte Kontrolle über den Prozessor, den Arbeitsspeicher und die Massenspeicher des virtuellen IT-Systems hat. Sie kann direkt beeinflussen, wie diese Ressourcen durch das virtuelle System genutzt werden. Die Virtualisierungssoftware kann damit beispielsweise jederzeit den Zustand des Prozessors oder des Arbeitsspeicher des virtuellen IT-Systems auslesen. Diese Möglichkeiten können genutzt werden, um das virtuelle IT-System für unbestimmte Zeit einzufrieren. Weiterhin ist es möglich, in den Prozessor oder den Arbeitsspeicher zuvor gespeicherte Inhalte hinein zu laden. Der zuvor auf die Festplatte des Virtualisierungsservers gespeicherte Zustand von Prozessor und Arbeitsspeicher wird nach der Betriebsunterbrechung wieder geladen und die Ausführung der virtuellen Instanz wird genau an der Stelle fortgesetzt, an der das System eingefroren wurde. Dieses Verfahren ist nicht mit anderen Verfahren wie dem "Ruhezustand", der von *Microsoft Windows XP* oder *Windows Vista* bekannt ist, zu verwechseln. Im Gegensatz zum Ruhezustand geschieht diese Betriebsunterbrechung für das virtuelle IT-System völlig transparent. Die Möglichkeiten, ein virtuelles IT-System einzufrieren, werden genutzt, um so genannte Snapshots im laufenden Betrieb zu erzeugen.

Snapshots

Die meisten Virtualisierungslösungen ermöglichen das Konservieren des Zustands eines virtuellen IT-Systems zu einem beliebigen Zeitpunkt, ohne dass die Ausführung des virtuellen IT-Systems hierdurch beeinträchtigt wird. Beim Anlegen eines Snapshots wird die virtuelle Festplatte eingefroren und nachfolgende Schreibzugriffe werden in eine separate Datei umgeleitet. Der aktuelle Zustand ergibt sich bei Maschinen mit aktiven Snapshots aus der Überlagerung aller Snapshot-Dateien mit der Basis-Datei.

Snapshots können mit oder ohne Inhalt des Arbeitsspeichers des virtuellen IT-Systems angelegt werden. Snapshots ohne Arbeitsspeicherinhalt spiegeln meist den Zustand des virtuellen IT-Systems wieder, das nicht heruntergefahren, sondern im laufenden Betrieb ausgeschaltet wurde. Snapshots mit Arbeitsspeicherinhalt erlauben es, das IT-System exakt in den Zustand zu versetzen, wie er zum Zeitpunkt des Snapshots vorlag, d. h., es ist eine Rückkehr in ein laufendes Betriebssystem mit geöffneten Anwendungen möglich. So lange der Snapshot nicht gelöscht wird, befindet sich der Speicherinhalt vom Zeitpunkt des Snapshots meist in Form einer Datei im Verzeichnis des virtuellen IT-Systemes.

***Live Migration* von virtuellen IT-Systemen**

Techniken wie Live Migration für XEN, Citrix XenMotion und Microsoft HyperV Server 2008 R2 oder auch VMotion für VMware erlauben die Übertragung (Migration) von virtuellen IT-Systemen auf andere physische Virtualisierungsserver im laufenden Betrieb.

Aus Benutzersicht, aber auch aus Sicht des virtuellen IT-Systems, geschieht dies unterbrechungsfrei. Hierdurch wird es z. B. möglich, Hardware eines Virtualisierungsserver zu erweitern oder auszutauschen, die Auslastung der Virtualisierungsserver gezielt neu zu verteilen sowie einen bestimmten Dienst oder eine Anwendung auf einen anderen Virtualisierungsserver zu verlagern.

Sowohl vor, während, als auch nach dem Migrationsvorgang muss der Zugang des virtuellen IT-Systems zum eigenen Dateisystem gewährleistet sein. Hierfür kommen Speichernetze (SAN-Storage-Systeme) mittels Fibre Channel oder iSCSI und Netzdateisysteme wie NFS in Frage.

Diese Technik funktioniert im Wesentlichen so, dass zuerst ein Snapshot eines virtuellen IT-Systems vom Quell-Virtualisierungsserver auf den Ziel-Virtualisierungsserver übertragen wird. Der Zielserver lädt nun den Arbeitsspeicher des zu übertragenden virtuellen IT-Systems in seinen Speicher. Da das System auf dem Quellserver weiterläuft, hat sich der Speicher des virtuellen Systems in der Zwischenzeit verändert. Diese Änderungen werden nun fortlaufend übertragen und in Folge dessen wird das Zielsystem mit dem Quellsystem synchronisiert. Ist die Synchronizität hergestellt, wird das virtuelle IT-System auf dem Quellserver gestoppt, der Prozessorzustand auf den Zielserver übertragen und das virtuelle IT-System mit dem übertragenen Prozessorzustand auf dem Zielserver fortgesetzt. Dieser Vorgang erfolgt für das virtuelle IT-System vollständig transparent.

Die *Live Migration* kann genutzt werden, um Performanceengpässen vorzubeugen. Dieser Prozess kann automatisiert werden, so dass jedem virtuellen IT-System immer die maximal mögliche Performance zur Verfügung gestellt werden kann.

Überbuchung von Arbeitsspeicher

Bei einigen Virtualisierungslösungen kann den virtuellen IT-Systemen in Summe mehr Arbeitsspeicher zugewiesen werden, als auf dem Virtualisierungsserver insgesamt vorhanden ist. Einem einzelnen virtuellen IT-System kann allerdings nicht mehr Speicher zugewiesen werden, als dem Hypervisor zur Verfügung steht. Ein Virtualisierungsserver verfügt beispielsweise über insgesamt zwei Gigabyte Hauptspeicher. Auf ihm werden drei virtuelle Server betrieben, die jeweils ein Gigabyte, also zusammen drei Gigabyte Hauptspeicher besitzen sollen. Um diese Überbuchung zu ermöglichen, wird den virtuellen IT-Systemen der entsprechende Hauptspeicher nicht zur Gänze zugeteilt. Stattdessen wird dem einzelnen virtuellen IT-System nur dann eine Speicherseite physisch zugewiesen, wenn sie von diesem virtuellen System tatsächlich gebraucht wird. Einmal durch ein virtuelles IT-System angeforderter Speicher kann grundsätzlich nicht durch den Hypervisor wieder zurückgefordert werden. So wächst der physische Speicherbedarf eines virtuellen IT-Systems sukzessive bis zur Konfigurationsgrenze an. Da allerdings davon ausgegangen werden kann, dass das Betriebssystem des virtuellen IT-Systems den ihm zur Verfügung stehenden Speicher mit der Zeit komplett nutzen wird, muss eine Möglichkeit bestehen, wie mit einer Ressourcensättigung auf dem

Virtualisierungsserver umgegangen werden soll. Eine solche Möglichkeit wird in den folgenden Absätzen an einem Beispiel verdeutlicht.

Das Produkt *ESX Server* des Herstellers *VMware* beispielsweise ermöglicht die Überbuchung von Hauptspeicher auf drei verschiedene, miteinander kombinierte Vorgehensweisen:

- *Transparent Memory Sharing*
  Der Hypervisor überwacht alle Speicherseiten aller virtuellen IT-Systeme. Kann der Hypervisor zwei identische Speicherseiten identifizieren, werden diese nur einmal im physischen Arbeitsspeicher des Virtualisierungsservers vorgehalten. Ändert eines der virtuellen IT-Systeme eine dieser Seiten, wird sie für dieses System kopiert, und die anderen virtuellen IT-Systeme nutzen weiter die nicht modifizierte Seite. Diese Technik hat ein hohes Potenzial zur Speichereinsparung, da z. B. bei vielen virtuellen IT-Systemen die gleichen Betriebssystemkerne oder Softwarebibliotheken verwendet werden. Das Speicherabbild dieser Kerne oder Bibliotheken muss nur einmal physisch im Speicher des Virtualisierungsservers gehalten werden.
- *Ballooning*
  In Abhängigkeit vom Hauptspeicherverbrauch des Gesamtsystems kann die Zuordnung von virtuellem Arbeitsspeicher zu den einzelnen virtuellen Systemen dynamisch angepasst werden. Möglich wird dies durch einen Treiber in dem virtuellen System, der gezielt Speicher belegt (Ballooning) und so das Betriebssystem des virtuellen IT-Systems zwingt, Hauptspeicherinhalte auf seine virtuelle Festplatte auszulagern. Der durch den Ballooning-Treiber belegte Speicher wird vom ESX Server erkannt und kann an andere virtuelle IT-Systeme vergeben werden. Mittels dieses Verfahrens können Speicherengpässe kurzzeitig ausgeglichen werden. Da das Betriebssystem des virtuellen IT-Systems kontrolliert, welche Prozesse ausgelagert werden, ist der negative Performanceeinfluss meist kurzzeitig hinnehmbar.
- *Paging*
  Kann der benötigte Speicher für ein virtuelles IT-System weder über *Transparent Memory Sharing* des Virtualisierungsservers noch über *Ballooning* im virtuellen IT-System freigegeben werden, wird der Speicher anderer, gerade nicht aktiver virtueller IT-Systeme durch den Hypervisor auf die Festplatten des ESX-Servers ausgelagert. Wenn dies geschieht, wird die Performance der virtuellen IT-Systeme sehr stark herabgesetzt, da der Hypervisor hier keine Rücksicht auf laufende Prozesse des Betriebssystems der ausgelagerten virtuellen IT-Systeme nimmt.

Der Festplattenplatz des Virtualisierungsservers kann ebenfalls überbucht werden. Hierbei wird den virtuellen IT-Systemen mehr Festplattenplatz zur Verfügung gestellt, als tatsächlich vorhanden ist. Dabei wird der verfügbare Festplattenplatz so zugewiesen, dass die virtuelle Maschine ein Laufwerk mit beispielsweise einer Größe von zehn Gigabyte erkennt und ein Dateisystem von diesen Dimensionen anlegen kann. Auf der Festplatte des Virtualisierungsservers belegt das virtuelle IT-System jedoch nur den tatsächlich genutzten Platz in einer Containerdatei, die dynamisch mit der aktuell benötigten Speichergröße mitwächst. Sobald das virtuelle IT-System weiteren Platz nutzt, wird dieser auch auf der physischen Festplatte des Virtualisierungsservers belegt. Vom virtuellen IT-System freigegebener Speicher wird allerdings in der Regel nicht automatisch wieder physisch freigegeben. Es muss weiterhin beachtet werden, dass die virtuellen IT-Systeme in eine Fehlersituation geraten, wenn der physische Speicher nicht mehr ausreicht, um weitere Speicheranforderungen zu erfüllen: Die virtuellen IT-Systeme "wissen" nichts von der Überbuchung des Speichers und versuchen weiter auf ihre virtuellen Fest-

platten zu schreiben. Es kommt zu Schreibfehlern in den virtuellen IT-Systemen und in der Folge zu Inkonsistenzen im Dateisystem.

Fehlertoleranz für Hardware-Komponenten

Virtuelle IT-Systeme können bei einigen Virtualisierungsprodukten von Toleranzmechanismen bei Hardwarefehlern profitieren. Da die Virtualisierungssoftware die Zuordnung beispielsweise einer virtuellen Netzschnittstelle zu einer physischen steuert, kann die Kommunikation des virtuellen IT-Systems auf eine andere Netzschnittstelle umgeleitet werden, wenn die ursprüngliche Schnittstelle von einem Fehler betroffen ist. Stehen also in einem Virtualisierungsserver mehrere redundante Komponenten zur Verfügung, kann die Virtualisierungssoftware beim Ausfall einer Komponente für die Nutzung der noch funktionsfähigen Komponenten sorgen.

Fehlertoleranz bei virtuellen IT-Systemen

Die Virtualisierungsprodukte *Citrix XenServer (Marathon EverRun)* und *VMware vSphere (Fault Tolerance)* beispielsweise verfügen über Mechanismen, um für den Fall des Ausfalls eines Virtualisierungsservers fehlertolerante virtuelle IT-Systeme zu erzeugen. Um diese Fehlertoleranz eines virtuellen IT-Systems zu erreichen, wird auf einem anderen Virtualisierungsserver eine Kopie des virtuellen IT-Systems erzeugt. Diese Kopie wird fortlaufend mit dem Original synchronisiert und bleibt solange nicht mit dem Netz verbunden, wie das Original weiterhin funktioniert. Fällt der Virtualisierungsserver aus, auf dem das Original läuft, kann die Kopie mit dem Netz verbunden werden und sofort alle Funktionen des Originals übernehmen. Danach wird auf einem weiteren Virtualisierungsserver sofort wieder eine neue Kopie des virtuellen IT-Systems erzeugt.

M 4.97 Ein Dienst pro Server

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator

Viele Schwachstellen in IT-Systemen sind einzeln nicht für einen potentiellen Angreifer ausnutzbar. Häufig wird erst durch die Kombination von Schwachstellen ein erfolgreiches Eindringen in einen Rechner möglich. Abhängig von der Bedrohungslage und dem Schutzbedarf der Dienste kann es deshalb zweckmäßig sein, auf einem Rechner nur *einen* Dienst zu betreiben. Dies betrifft vor allem Server, die Dienste auch ins Internet oder in andere Fremdnetze anbieten.

Beispielsweise kann das Sicherheitsniveau dadurch gesteigert werden, dass sowohl der Webserver als auch der E-Mailserver jeweils auf eigenständigen, dedizierten Rechnern, die als Minimalsystem ausgelegt sind (siehe auch M 4.95 *Minimales Betriebssystem*), betrieben werden.

Außerdem sind einzelne Dienste auch unterschiedlich in ihrer Sicherheitseinstufung. So ist ein erfolgreiches Eindringen in einen Webserver unter Umständen sehr ärgerlich, insbesondere wenn der Angreifer die extern verfügbaren Webseiten abändert. Zugriff auf vertrauliche Informationen ist dem Angreifer hierdurch aber meist nicht möglich. Ist der Webserver aber gleichzeitig der E-Mailserver, so kann der Angreifer unter Umständen den gesamten E-Mail-Verkehr mitlesen, was möglicherweise viel schlimmere Auswirkungen hat.

Die Aufteilung kann sogar noch verstärkt werden, indem für einen einzelnen Dienst verschiedene Aufgaben auf unterschiedliche Rechner verteilt werden. So könnte es beispielsweise einen E-Mailserver A geben, der E-Mails aus dem Internet annimmt und in das interne Netz weiterleitet, und einen anderen E-Mailserver B, der E-Mails aus dem internen Netz an das Internet weiterleitet. Da die Kommunikationsaufnahme aus dem Internet nur mit dem E-Mailserver A möglich ist, kann ein Angreifer auch nur diesen direkt attackieren. Der E-Mailserver A darf selber keine E-Mails in das Internet verschicken, deshalb kann dieser Rechner auch nicht für E-Mail-Spamming missbraucht werden.

Eine Aufteilung verschiedener Dienste auf unterschiedliche Rechner hat unter anderem folgende Vorteile:

- Leichtere Konfiguration der einzelnen Rechner
- Einfachere und sicherere Konfiguration eines vorgeschalteten Paketfilters
- Erhöhte Widerstandsfähigkeit gegenüber Angriffen
- Erhöhte Ausfallsicherheit

Durch ein geeignetes zentrales Systemmanagement kann der zusätzliche Administrationsaufwand, der durch die höhere Anzahl der Rechner entsteht, begrenzt werden.

Virtualisierung

Im Falle von sicherheitskritischen Diensten sollten auch in virtuellen IT-Systemen jeweils nur ein Dienst betrieben werden, wie dies auch für physische Systeme gilt. Ein virtuelles IT-System selbst ist jedoch in diesem Sinne kein "Dienst" eines Virtualisierungsservers. Daher können auf einem Virtualisierungsserver mehrere virtuelle IT-Systeme betrieben werden. Je nachdem, auf welcher Virtualisierungstechnik (Server- oder Betriebssystemvirtualisierung) der Virtualisierungsserver beruht, kann allerdings die Varianz der durch die virtuellen IT-Systeme bereitgestellten Dienste eingeschränkt sein. Ob das ein-

gesetzte Virtualisierungsprodukt geeignet ist, unterschiedliche Dienste in virtuellen IT-Systemen auf einem Virtualisierungsserver bereitzustellen, muss für das konkrete Produkt geprüft werden. Als Kriterien sind hierfür die Stärke der Isolation und der Kapselung der virtuellen IT-Systeme auf dem Virtualisierungsserver heranzuziehen (siehe M 3.72 *Grundbegriffe der Virtualisierungstechnik*). Je stärker die virtuellen IT-Systeme auf dem Virtualisierungsserver isoliert sind, desto eher eignet sich das Virtualisierungsprodukt dazu, unterschiedliche Dienste in den verschiedenen virtuellen IT-Systemen zu betreiben. Die folgenden Grundsätze lassen sich für eine erste Beurteilung heranziehen:

- Auf Virtualisierungsservern mit einer Betriebssystemvirtualisierungslösung sollten in der Regel nur virtuelle IT-Systeme mit einer Funktion bereitgestellt werden. So sollten auf einem solchen Virtualisierungsserver beispielsweise ausschließlich Webserver oder ausschließlich Mailserver, aber keine Mischung aus diesen Gruppen betrieben werden. Bei einigen Produkten zur Betriebssystemvirtualisierung ist die Isolation der virtuellen IT-Systeme allerdings stark genug, so dass von dieser Vorgabe abgewichen werden kann.
- Auf Virtualisierungsservern mit einer Servervirtualisierungslösung ist es meist zulässig, virtuelle IT-Systeme mit unterschiedlichen Diensten zu betreiben. Es können also unter Umständen Webserver und Mailserver auf einem Virtualisierungsserver in jeweils getrennten virtuellen IT-Systemen gemeinsam bereitgestellt werden.

Auf einem Virtualisierungsserver selbst sollten allerdings neben der Virtualisierungssoftware und damit direkt verbundener Dienste (Verwaltungsdienst für die Virtualisierung etc.) keine weiteren Dienste betrieben werden.

Prüffragen:

- Wird darauf geachtet, nur einen Dienst pro Server anzubieten?

M 4.346 Sichere Konfiguration virtueller IT-Systeme

Verantwortlich für Initiierung: Leiter IT
Verantwortlich für Umsetzung: Administrator

Virtuelle IT-Systeme (gelegentlich auch als virtuelle Maschinen bezeichnet) sind in erster Linie IT-Systeme. Sie sind daher wie in M 2.392 *Modellierung von Virtualisierungsservern und virtuellen IT-Systemen* beschrieben genauso zu behandeln und zu modellieren wie physische IT-Systeme.

Allerdings gelten für virtuelle IT-Systeme einige Besonderheiten, die beachtet werden müssen.

Virtuellen IT-Systemen muss oft der Zugang zu Geräten, die an den Virtualisierungsserver angeschlossen sind, wie beispielsweise CD- oder DVD-Laufwerke, USB-Dongles, Bandlaufwerke (SCSII) und andere Peripheriegeräte, ermöglicht werden. Dabei können Geräte, die der Virtualisierungsserver den virtuellen IT-Systemen zur Verfügung stellt, häufig über Gastwerkzeuge aus der virtuellen Maschine heraus gesteuert werden. So kann beispielsweise die Netzwerkkarte deaktiviert oder es können Datenträger über das physische in das virtuelle CD-/DVD-Laufwerk oder Diskettenlaufwerk geladen werden.

Bei einigen Virtualisierungssystemen besteht des Weiteren die Möglichkeit, Hauptspeicher oder Festplattenplatz zu überbuchen. Es wird von einer "Überbuchung" von Ressourcen gesprochen, wenn den virtuellen IT-Systemen in Summe mehr Ressourcen zugewiesen werden können, als tatsächlich physisch vorhanden sind. Um Ressourcenengpässen vorzubeugen, können durch die Gastwerkzeuge in virtuellen IT-Systemen Funktionen bereitgestellt werden, um diese Überbuchungsfunktionen zu steuern. Die Gastwerkzeuge des Herstellers VMware (VMware Tools) besitzen beispielsweise eine Funktion, um Hauptspeicher zu belegen, der anderen virtuellen IT-Systemen zur Verfügung gestellt werden kann (Balooning). Diese Werkzeuge können auch eine virtuelle Festplatte für eine Verkleinerung des Dateicontainers, in dem sie enthalten ist, vorbereiten. Hierzu werden alle belegten Blöcke einer virtuellen Festplatte an den Anfang des Containers verschoben und die frei gewordenen Blöcke mit Nullen überschrieben, damit sie von der Virtualisierungsschicht als frei erkannt werden können.

Daher sind bei der Inbetriebnahme von virtuellen IT-Systemen neben den aus dem physischen Serverbetrieb schon bekannten Maßnahmen noch die folgenden Aspekte zu beachten:

- Veränderungen der Binärdateien von Kernel, Anwendungen und Systembibliotheken wirken sich bei der Betriebssystemvirtualisierung im Gegensatz zur Servervirtualisierung auf alle virtuellen IT-Systeme, die auf dem Virtualisierungsserver betrieben werden, sowie auf den Virtualisierungsserver selbst aus. Diese Daten sind auf Veränderungen hin zu überwachen, vor allem, da beispielsweise durch eine Kompromittierung solcher Dateien ein sehr hohes Schadenspotenzial entsteht. Siehe hierzu auch M 4.93 *Regelmäßige Integritätsprüfung*.
- Die Gastwerkzeuge können es Benutzern der virtuellen IT-Systeme ermöglichen, auf Datenträger in Disketten- oder CD-/DVD-Laufwerken des Virtualisierungsservers zuzugreifen. Auch mechanische Vorgänge wie das Öffnen und Schließen der Laufwerksschublade eines physischen Laufwerkes können hierüber gesteuert werden. Es besteht daher die Möglichkeit, dass unberechtigt auf Datenträger in physischen Laufwerken zugegriffen

wird, oder der Datenträger einem virtuellen IT-System entzogen wird, indem das Laufwerk von einem anderen virtuellen System aus geöffnet wird. Die virtuellen IT-Systeme und der Virtualisierungsserver müssen so konfiguriert sein, dass dies weitgehend ausgeschlossen ist. Am einfachsten kann dies geschehen, wenn den virtuellen IT-Systemen diese Geräte nur dann exklusiv zugeordnet werden, wenn sie aktuell benötigt werden. Werden sie nicht gebraucht, sollte die Verbindung zu diesen Geräten getrennt werden. Besteht die Möglichkeit, CD- oder DVD-Datenträger als Imagedateien (ISO-Images) statt über physische Laufwerke bereitzustellen, sollte sie genutzt werden.

- Funktionen, die die Überbuchung von Hauptspeicher oder Festplattenplatz ermöglichen, sind bei den virtuellen IT-Systemen zu deaktivieren, bei denen hohe Performanceanforderungen bestehen oder deren Datenintegrität besonders wichtig ist. Ressourcenengpässe bei einer Überbuchung von Hauptspeicher auf einem Virtualisierungsserver führen in der Regel zu starken Performanceeinbußen der davon betroffenen virtuellen IT-Systeme. Wird Festplattenplatz überbucht und reicht der physisch vorhandene Platz nicht mehr aus, werden durch den Virtualisierungsserver in der Regel keine weiteren Schreibzugriffe auf den überbuchten Speicherplatz zugelassen. Hierdurch treten in den virtuellen IT-Systemen Festplattenfehler auf, die zu Inkonsistenzen der abgespeicherten Daten führen können.
- Die Vorbereitung von virtuellen Festplatten auf eine Verkleinerung ihres physischen Containers bedeutet eine starke Belastung der Massenspeicher der Virtualisierungsserver. Dies kann zu Einschränkungen der Performance aller virtuellen IT-Systeme führen, die auf dem Virtualisierungsserver ausgeführt werden. Greifen mehrere Virtualisierungsserver auf ein Speichernetz zu, können unter Umständen alle Virtualisierungsserver davon betroffen sein. Daher sollte diese Funktion deaktiviert werden, wenn sie nicht benötigt wird.
- Die Deaktivierung von Geräten wie Netzwerkkarten über Gastwerkzeuge bildet ein virtuelles Äquivalent zur Entfernung des Netzwerkkabels eines physischen IT-Systems. Da dies in virtualisierten Umgebungen auch oft ohne Zutritt zu diesem System möglich ist, sollte diese Funktion deaktiviert werden. Sie sollte nur dann zeitweise aktiviert werden, wenn sie zwingend benötigt wird.

Einige der oben beschriebenen Funktionen werden über Gastwerkzeuge, die in den virtuellen IT-Systemen installiert werden können, gesteuert oder ermöglicht. Es sind daher verbindliche Regelungen zur Konfiguration und zum Einsatz dieser Gastwerkzeuge in virtuellen IT-Systemen zu erstellen.

Prüffragen:

- Ist bei Umgebungen mit Betriebssystemvirtualisierungen die Integrität von Daten des Betriebssystemkerns, der Systembibliotheken und gemeinsam genutzten Anwendungen gewährleistet?
- Sind verbindliche Regelungen zum Einsatz von Gastwerkzeugen in virtuellen IT-Systemen getroffen und umgesetzt worden?
- Werden Geräte wie CD-Laufwerke nur dann mit einem virtuellen IT-Systemen exklusiv verbunden, wenn sie im betreffenden IT-System benötigt werden?
- Sind für virtuelle IT-Systeme bei denen hohe Performanceanforderungen bestehen oder ein hoher Schutzbedarf bezüglich Integrität festgestellt worden ist, Überbuchungsfunktionen für Hauptspeicher oder Festplattenplatz deaktiviert?

- Ist die Funktion, mit der Geräte wie Netzwerkkarten oder CD-/DVD-Laufwerke über die Gastwerkzeuge aktiviert oder deaktiviert werden können, standardmäßig ausgeschaltet?

M 4.347 Deaktivierung von Snapshots virtueller IT-Systeme

Verantwortlich für Initiierung: Behörden-/Unternehmensleitung, IT-Sicherheitsbeauftragter
Verantwortlich für Umsetzung: IT-Sicherheitsbeauftragter, Leiter IT

Die Möglichkeit, den Zustand virtueller IT-Systeme zu einem bestimmten Zeitpunkt im laufenden Betrieb einzufrieren und diesen Zustand beliebig lang zu konservieren, in dem er beispielsweise auf auf eine Festplatte abgespeichert wird, ist eine technische Besonderheit virtueller IT-Systeme. Kann ein solcher Zustand abgespeichert und das System danach weiter fortgesetzt werden, besteht auch die Möglichkeit, das System wieder auf den abgespeicherten Zustand zurückzusetzen. Ein solcher Zustand wird bei den meisten Virtualisierungsprodukten "Snapshot" genannt. Dieses Verfahren kann für vielfältige Administrationstätigkeiten eingesetzt werden. So kann zum Beispiel nach einem fehlgeschlagenen *Update* auf einfache Weise ein *Downgrade* auf die vorherige Version durchgeführt werden. Auch elementare Funktionen einer virtuellen Infrastruktur, wie die Migration von Gastsystemen zwischen Virtualisierungsservern über *LiveMigration*, *vMotion* oder *XenMotion*, basieren auf der Fähigkeit, Snapshots zu erzeugen. Dies betrifft in der Folge auch die daran gekoppelten Hochverfügbarkeitsmechanismen.

Daher sind beim Einsatz solcher Snapshots die folgenden Aspekte zu beachten:

Schutz der Vertraulichkeit und Integrität bei gefährdeten Gästen

In einer virtuellen Infrastruktur können bestimmte IT-Systeme einem hohen oder sehr hohen Schutzbedarf in Bezug auf die Vertraulichkeit oder Datenintegrität unterliegen. Daten eines Prozesses werden häufig in voneinander abgeschotteten Hauptspeicherbereichen verarbeitet, so dass andere Prozesse auf einem IT-System nicht darauf zugreifen und die Daten lesen oder verändern können. Hierdurch bleibt die Vertraulichkeit und Integrität dieser Daten während der Verarbeitung im Hauptspeicher eines (virtuellen) IT-Systems gewahrt. Wird nun ein beliebiger Zustand des virtuellen IT-Systems eingefroren, um das System zu einem späteren Zeitpunkt wieder in diesen Zustand zu versetzen, werden die Arbeitsspeicherdaten auf einen Massenspeicher des Virtualisierungsservers geschrieben. Der Zugriffsschutz, den das Betriebssystem des virtuellen IT-Systems für die Daten der einzelnen Prozesse gewährt, kann nun durch einen Angreifer umgangen werden, indem er die Datei analysiert, in der die Arbeitsspeicherdaten enthalten sind.

Das folgende Beispiel soll dies verdeutlichen: Ein virtuelles IT-System ist mit einer Festplattenverschlüsselung ausgestattet, um die Vertraulichkeit und Integrität der gespeicherten Daten zu gewährleisten. Da der Hauptspeicherinhalt der virtuellen Maschine beim Erzeugen des Snapshots ausgelesen und auf einer Festplatte des Virtualisierungsservers gespeichert wird, können dabei die kryptographischen Schlüssel der Festplattenverschlüsselungssoftware in unverschlüsselter Form auf die Festplatte geschrieben werden. Das gleiche passiert im Übrigen, wenn das System über die Virtualisierungssoftware nur angehalten und der Zustand für eine spätere Fortsetzung des Betriebs auf die Festplatte geschrieben wird. Aus der Datei mit dem abgespeicherten Hauptspeicherinhalt lässt sich dann möglicherweise der Schlüssel zur Entschlüsselung des Festplatteninhaltes herauslesen.

Dies zeigt, dass Maßnahmen zur Sicherung der Vertraulichkeit und Integrität von physischen IT-Systemen bei virtuellen IT-Systemen häufig nur noch eine eingeschränkte Wirksamkeit haben. Sie können möglicherweise mit Mitteln der Virtualisierungsserver umgangen werden. Um die Offline-Analyse eines Snapshots eines virtuellen IT-Systems mit hohem Schutzbedarf zu erschweren, sollte daher überlegt werden, für solche Systeme die Möglichkeit, Snapshots zu erzeugen oder das System einzufrieren, zu deaktivieren. In diesem Fall ist zu prüfen, ob die eventuell eingesetzten Snapshot-basierten Datensicherungsverfahren weiterhin funktionieren.

Beständigkeit von Datenveränderungen

Snapshots eines virtuellen IT-Systems enthalten den kompletten Zustand des IT-Systems inklusive aller abgelegten Daten zum Zeitpunkt seiner Erzeugung. Wenn ein virtuelles IT-System mittels eines Snapshots auf einen früheren Stand zurückgesetzt wird, können hierdurch Veränderungen an Daten zurückgenommen werden. Beispiele hierfür sind der Datenbestand eines Dateiservers oder Struktur und Inhalt eines Verzeichnisdienstes wie Active Directory.

Für ein virtuelles IT-System, das auf keinen Fall auf einen früheren Stand zurückgesetzt werden darf, muss ebenfalls die Option, Snapshots zu erzeugen, deaktiviert werden.

Falls auf die Funktionalität von Snapshots nicht verzichtet werden kann, sollte der Umfang des Snapshots eingegrenzt werden, in dem beispielsweise nur bestimmte Laufwerke vom Snapshot erfasst werden, oder die Arbeitsschritte jeweils bevor und nachdem ein Snapshot erzeugt oder zurückgespielt wurde, spezifiziert werden. Wird beispielsweise ein Active Directory Domaincontroller auf einen Snapshot zurückgesetzt, sind Maßnahmen zur Wiederherstellung seiner Active Directory-Datenbank durchzuführen, da diese sonst inkonsistente Daten enthält.

Der Umfang der eingegrenzten Snapshots und die notwendigen Arbeitsschritte sind zu dokumentieren.

Prüffragen:

- Ist gewährleistet, dass für alle virtuellen IT-Systeme mit nicht deaktivierter Snapshot-Funktionalität die Umfänge der Snapshots sowie die darüber hinaus für den Umgang mit Snapshots notwendigen Arbeitsschritte evaluiert und dokumentiert sind?
- Ist die Möglichkeit, Snapshots zu erzeugen oder das System einzufrieren, für virtuelle IT-Systeme deaktiviert worden, bei denen Gefährdungen der Integrität oder Vertraulichkeit besonderes schwerwiegende Konsequenzen haben?

M 4.348 Zeitsynchronisation in virtuellen IT-Systemen

Verantwortlich für Initiierung: Leiter IT
Verantwortlich für Umsetzung: Administrator

Viele Anwendungen benötigen eine korrekte Systemzeit, um einwandfrei zu funktionieren. Dies beginnt schon bei Dateiservern damit, dass die auf ihm gespeicherten Dateien mit einem Zeitstempel versehen werden. Andere Systeme verwenden die Systemzeit auf unterschiedliche Weise. Bestimmte Authentisierungssysteme wie Kerberos oder auch tokenbasierte Systeme benötigen eine korrekte Systemzeit, um störungsfrei zu arbeiten. Monitoringsysteme wie beispielsweise *mrtg* nutzen die Systemzeit üblicherweise als Index für ihre in einer Datenbank abgelegten Aufzeichnungen.

Aus diesen Gründen muss darauf geachtet werden, dass auch die Systemzeit eines virtuellen IT-Systems stets korrekt voranschreitet. Bei Virtualisierungsprodukten, die auf einer vollständigen Servervirtualisierung beruhen, ist dies häufig nicht ohne Weiteres gewährleistet.

Die Berechnung der Systemzeit durch Taktzählung

Moderne Betriebssysteme ermitteln die Systemzeit nicht, indem die Systemuhr ständig ausgelesen wird, sondern indem Prozessorzyklen gezählt und diese Zyklen mit einer externen Zeitquelle verglichen werden. Diese externe Zeitquelle kann ein Zeitserver oder auch eine Hardware-Uhr sein. Der Grund für diese auf den ersten Blick umständliche Zeitermittlungsmethode ist, dass für moderne Prozessoren eine Zeitquelle benötigt wird, die eine höhere Auflösung als die meisten Uhren besitzt. Diese Auflösung muss im Bereich des Taktes eines modernen Prozessors liegen. Durch ständigen Vergleich der Prozessorzyklen mit der verlässlichen Zeitquelle wird ein Umrechungsfaktor gebildet, der es erlaubt, die Prozessorzyklen in die Zeit umzuwandeln. In bestimmten Zeitabständen wird dieser Umrechnungsfaktor durch Vergleich der vergangenen Zyklen mit der Zeitquelle korrigiert, um eine etwaige Ungenauigkeit in der Berechnung auszugleichen.

Die meisten Produkte für eine Servervirtualisierung ordnen den virtuellen IT-Systemen und damit den virtuellen Prozessoren abhängig von deren Last dynamisch Prozessorzyklen zu. Daher läuft der Zähler für die Prozessorzyklen aus Sicht der virtuellen Maschine mit unterschiedlichen Geschwindigkeiten. Der Algorithmus zur Zeitbestimmung und -korrektur ermittelt damit bei jedem Durchlauf andere Werte, was dazu führt, dass auch die Systemzeit in einem virtuellen IT-System scheinbar mit unterschiedlichen Geschwindigkeiten voranschreitet. Dadurch kann es in virtuellen IT-Systemen durchaus zu Abweichungen von mehreren Minuten kommen, sodass in Extremfällen die Zähler überkorrigiert werden und die Systemzeit des virtuellen IT-Systems zum Teil scheinbar rückwärts läuft.

Normalerweise läuft die Systemuhr in virtuellen IT-Systemen, die eine gleichmäßige Prozessorauslastung haben, mit ausreichender Genauigkeit. Hierbei ist es belanglos, ob die Auslastung hoch oder niedrig ist, entscheidend ist die Gleichmäßigkeit. Bei Systemen mit zeitweise hoher und zeitweise niedriger Auslastung kommt es zu den bereits beschriebenen Effekten. Hierbei verhalten sich die Betriebssysteme abhängig von ihrer Konfiguration sehr unterschiedlich.

Korrekturmethoden und deren Grenzen

Die meisten Virtualisierungsprodukte besitzen einen Mechanismus, um die Systemzeit in den virtuellen IT-Systemen zu korrigieren. Dies wird häufig über eine Funktion der Gastwerkzeuge realisiert. Die Produkte der Hersteller Citrix und VMware beispielsweise beinhalten eine Funktion zur Synchronisierung der Systemzeit der virtuellen IT-Systeme mit der Systemzeit des Virtualisierungsservers.

Diese Mechanismen sind allerdings nicht immer für die in einem virtuellen IT-System betriebenen Anwendungen ausreichend, da sie in der Regel nicht auf alle Timer eines Betriebssystems wirken, sondern nur auf die so genannte Time of Day Clock. Zudem erfolgt die Synchronisierung nicht ständig, sondern in bestimmten Abständen. Diese Abstände liegen meist im Bereich von einigen wenigen Bruchteilen von Sekunden, sind aber für eine genaue Zeitanpassung häufig zu groß.

Dieser Aspekt ist beim Betrieb von Anwendungen in virtuellen IT-Systemen zu beachten. Die Anwendungen müssen entweder mit einer ungleichmäßig laufenden Systemuhr auskommen können oder es müssen Konfigurationsänderungen am Virtualisierungsserver oder dem virtuellen IT-System vorgenommen werden, die die Genauigkeit der Systemuhr der virtuellen IT-Systeme steigern.

Solche Konfigurationsänderungen bestehen darin, die Abfrage einer externen Zeitquelle häufiger durchzuführen, als dies standardmäßig der Fall ist. Dies kann über die Gastwerkzeuge geschehen, wenn diese eine entsprechende Konfigurationsmöglichkeit besitzen. Es ist aber auch möglich, dass betreffende virtuelle IT-System so einzurichten, dass es beispielsweise öfter einen NTP-Server abfragt und dadurch seine Systemuhr korrigiert. Hierdurch werden die Intervalle kleiner, in denen die Uhr mit einer falschen Geschwindigkeit läuft und der Umrechnungsfaktor für die Prozessorzyklen wird schneller angepasst. In der Regel ist es nicht sinnvoll, diese beiden Möglichkeiten miteinander zu kombinieren, da ansonsten mit geringen Performanceverlusten gerechnet werden muss. Für Unix-Betriebssysteme müssen häufig auf die Virtualisierung abgestimmte Kernel verwendet werden. Hier sind in Abhängigkeit von den eingesetzten Unix-Derivaten z. B. im Bootloader entsprechende Parameter zu setzen. Unter Umständen muss ein solcher Kernel auch dediziert erzeugt (selbst kompiliert) werden.

Prinzipiell sollte ein Vorgehen etabliert werden, welches sicherstellt, dass Probleme mit der Synchronizität der Systemzeit erkannt und beseitigt werden können, bevor die virtuellen Systeme ausgerollt werden. Während des Pilotbetriebs eines neuen virtuellen IT-Systems ist die Systemzeit des Systems verstärkt zu überwachen. Dabei ist zu ermitteln, ob die interne Uhr des virtuellen IT-Systems von der tatsächlichen Zeit abweicht. In diesem Fall muss geprüft werden, ob sich dies nachteilig auf die im virtuellen IT-System betriebene Applikation auswirkt, gegebenenfalls sind Korrekturmaßnahmen durchzuführen. Der Erfolg der Korrekturmaßnahmen ist im weiteren Pilotbetrieb und auch nach der Überführung in den Produktivbetrieb zu prüfen.

Prüffragen:

- Sind die Einflüsse der Virtualisierung auf die Systemzeit bei der Virtualisierung eines bestimmten IT-Systems oder einer bestimmten Anwendung hinreichend bedacht worden?

- Wurden die Anwendungen der virtuellen IT-Systeme auf Probleme mit unregelmäßig laufender Systemzeit geprüft?
- Ist ein allgemeines Konzept entwickelt worden, wie eine ausreichende Synchronizität der Systemzeit in den virtuellen IT-Systemen gewährleistet wird?

M 4.349 Sicherer Betrieb von virtuellen Infrastrukturen

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator

Auf Virtualisierungsservern werden in der Regel mehrere virtuelle IT-Systeme betrieben. Da die einzelnen virtuellen IT-Systeme allesamt von dieser Infrastruktur abhängen, kann ein Fehler auf einem Infrastruktursystem wie einem Virtualisierungsserver Auswirkungen auf sämtliche auf diesem System betriebenen virtuellen IT-Systeme haben.

Im Folgenden werden einige Hinweise gegeben, die für den sicheren Betrieb der Virtualisierungsserver bzw. der virtuellen Infrastruktur beachtet werden sollten. Empfehlungen bezüglich des Virtualisierungsservers selbst, die nicht den Aspekt der Virtualisierung betreffen und zu den Grundsätzen des Serverbetriebs gehören, sind in den Maßnahmen des Bausteins B 3.101 *Allgemeiner Server* beschrieben.

Administrationszugänge

Virtualisierungsserver besitzen Funktionen, um die auf ihnen betriebenen virtuellen IT-Systeme zu steuern, warten und überwachen. Diese Verwaltungsfunktionen können in der Regel entweder lokal auf dem Virtualisierungsserver selbst oder über das Netz von der Arbeitsstation eines Administrators aus genutzt werden. Dazu werden entweder webbasierte Administrationsoberflächen auf dem Virtualisierungsserver oder eine spezielle Administrationssoftware wie z. B. *VMware vSphere Client* bereitgestellt.

Weiterhin besteht bei einigen Virtualisierungslösungen die Möglichkeit, mehrere Virtualisierungsserver sowie alle darauf betriebenen virtuellen IT-Systeme von einem zentralen System aus zu verwalten (z. B. *Citrix XenCenter, Microsoft System Center Virtual Machine Manager, SUN Management Center, VMware vCenter*).

Die entsprechenden Netzschnittstellen der Virtualisierungsserver bzw. des zentralen Verwaltungssystems ermöglichen einen vollständigen Zugriff auf die Virtualisierungsserver und die virtuellen IT-Systeme. Aus diesem Grund müssen die Administrationsschnittstellen abgesichert werden. Hierzu ist auch die Maßnahme M 5.154 *Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen* zu berücksichtigen.

Überwachung des Betriebszustands

Die Administratoren der virtuellen Infrastruktur sollten in regelmäßigen Abständen entsprechend der Sicherheitsrichtlinien (siehe M 2.477 *Planung einer virtuellen Infrastruktur*) Überwachungstätigkeiten ausführen. Hierzu gehört:

- das Anlegen, Löschen von Snapshots.
- die Überwachung des Betriebszustandes der Virtualisierungsserver und der virtuellen IT-Systeme.
- die Prüfung der Auslastung von Ressourcen.
- die Prüfung, ob ausreichend Prozessorressourcen zur Verfügung stehen, um die Performance-Anforderungen der virtuellen IT-Systeme zu befriedigen.
- die Prüfung, ob Hauptspeicherengpässe bestehen, die die Verfügbarkeit der virtuellen IT-Systeme gefährden.

- die Prüfung, ob ausreichend Massenspeicher (Festplattenplatz bzw. zugeordnete und Gesamtkapazität im Speichernetz) zur Verfügung steht.
- die Prüfung, ob es Engpässe bei der Netzbandbreite gibt.
- die Prüfung der Verbindungen zu den physikalischen Netzen.
- der Integritätscheck der Konfiguration der Virtualisierungsserver und der virtuellen IT-Systeme (siehe auch M 2.449 *Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme*, M 4.93 *Regelmäßige Integritätsprüfung* und M 5.8 *Regelmäßiger Sicherheitscheck des Netzes*)

Insbesondere dann, wenn die von einigen Virtualisierungsprodukten gebotene Möglichkeit zur Überbuchung von Hauptspeicher und Festplattenplatz genutzt wird, muss ein ständiger Prozess zur Überwachung dieser Ressourcen etabliert werden. Geschieht dies nicht, drohen im Fall von zu stark überbuchtem Hauptspeicher massive Performanceverluste. Wenn ein Engpass bezüglich des Festplattenplatzes entsteht, können alle davon betroffenen IT-Systeme gleichzeitig ausfallen. Wenn Snapshots verwendet werden, sollte die Auslastung des Massenspeichers ebenfalls sorgfältig beobachtet werden, da Snapshotdateien in der Regel dynamisch wachsen.

Die in regelmäßigen Abständen durchzuführenden Überwachungsaufgaben können in vielen Fällen automatisiert werden (z. B. E-Mail-Benachrichtigung etc.).

Tests von Konfigurationsänderungen

Von Konfigurationsänderungen auf den Virtualisierungsservern können viele IT-Systeme betroffen sein. Fehler hierbei können dazu führen, dass alle IT-Systeme auf diesen Virtualisierungsservern nicht mehr starten können oder die Verbindung zu von ihr benötigten Ressourcen verliert. Wird die Konfiguration auf Virtualisierungsservern geändert, so muss diese Änderung auf technische Korrektheit überprüft werden, bevor sie aktiviert wird. Dies kann z. B. in einer Testumgebung oder mittels Vier-Augen-Prinzip erfolgen.

Prüffragen:

- Besteht ein abgesicherter Zugang zu den administrativen Schnittstellen der virtuellen Infrastruktur?
- Werden regelmäßige Überwachungsaufgaben bezüglich der virtuellen Infrastruktur durchgeführt?
- Werden Konfigurationsänderungen an der Virtualisierungsinfrastruktur vor der Umsetzung geprüft?

M 5.153 Planung des Netzes für virtuelle Infrastrukturen

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator

Virtualisierungsserver müssen allen virtuellen IT-Systemen den Zugriff auf von diesen benötigte Infrastrukturkomponenten wie Netze und Speichernetze, sowie auf Infrastrukturdienste wie DNS oder DHCP ermöglichen. Hierbei sind die folgenden Aspekte bei der Planung der Netzanbindung der Virtualisierungsserver zu beachten:

- Netzanbindung der Virtualisierungsserver
  Virtualisierungsserver benötigen in der Regel Zugriff auf Infrastrukturdienste wie DNS sowie auf Speichernetze. Weiterhin werden sie häufig über das Netz administriert und bestimmte Virtualisierungsfunktionen wie die *Live Migration*, also das Verschieben eines virtuellen IT-Systems im laufenden Betrieb von einem Virtualisierungsserver auf den anderen, nutzen ebenfalls Netzverbindungen zwischen den Virtualisierungsservern. Daher werden auf den Virtualisierungsservern selbst Netzschnittstellen für diese Zwecke benötigt. Da über diese Schnittstellen auch die virtuellen IT-Systeme, die auf dem Virtualisierungsserver betrieben werden, verwaltet werden können, sind diese Schnittstellen besonders zu schützen und in einem Verwaltungsnetz zu betreiben. Der Zugriff auf dieses Verwaltungsnetz stellt das virtuelle Pendant des Zugangs zum Rechenzentrum oder Serverraum dar und sollte genau wie der Zutritt zu Serverräumen restriktiv gehandhabt werden (siehe auch Maßnahme M 1.58 *Technische und organisatorische Vorgaben für Serverräume*). Das Verwaltungsnetz sollte deshalb separat betrieben werden, um sicherzustellen, dass die Verwaltungsfunktionen der Virtualisierungsserver nur von den vorgesehenen Arbeitsstationen aus und nur für die berechtigten Administratoren erreichbar sind. Das Verwaltungsnetz sollte insbesondere von den Netzen der virtuellen IT-Systeme getrennt werden.
  Es muss des Weiteren geprüft werden, ob für die Virtualisierungsfunktion *Live Migration* ein dediziertes Netz geschaffen werden soll. Da bei einer *Live Migration* die Hauptspeicherinhalte eines virtuellen IT-Systems möglicherweise unverschlüsselt über das Netz übertragen werden, kann eine solche Trennung je nach Schutzbedarf der virtuellen IT-Systeme notwendig sein.
- Netzanbindung der virtuellen IT-Systeme
  Für virtuelle IT-Systeme (virtuelle Server, Clients und gegebenenfalls virtuelle Switche) sind die Maßnahmen des Bausteins B 3.101 *Allgemeiner Server* und B 3.302 *Router und Switches* genauso umzusetzen wie für physische. Bezüglich der Netzanbindung virtueller IT-Systeme sind bei der Planung einige Besonderheiten zu beachten. Virtuelle IT-Systeme nutzen die physischen Netzschnittstellen der Virtualisierungsserver, um auf Netze zuzugreifen. Hierbei existiert in der Regel keine direkte, eindeutige Zuordnung von Schnittstellen zu virtuellen IT-Systemen. Dies bedeutet, dass sich bei einigen Virtualisierungsprodukten mehrere virtuelle IT-Systeme dieselbe physische Schnittstelle teilen können. Da bei einer Störung dieser Schnittstelle gleich mehrere virtuelle IT-Systeme vom Netz getrennt werden, wird empfohlen, dass die Verfügbarkeit dieser mehrfach genutzten Netzschnittstellen gesteigert wird (*Kumulationsprinzip*). Dies kann z. B. durch redundante Netzschnittstellen und Techniken wie *IEEE 802.3ad* (*Link Aggregation Control Protocol - LACP*) oder anderer *Load Balancing*-Verfahren geschehen. Hierbei ist besonders zu beachten, dass die Ver-

wendung solcher Protokolle in der Regel eine angepasste Konfiguration auf dem physischen Switch erfordert, an den diese Schnittstellen angeschlossen sind. Falls möglich, sind die physischen Schnittstellen mit unterschiedlichen Switchen zu verbinden.

Trennung von Netzsegmenten

Virtualisierungsserver werden oft mit einer Vielzahl von Netzen verbunden. Einige Virtualisierungsprodukte verfügen über Funktionen, um mehrere *VLANs* über eine physische Schnittstelle (*Port Trunking* gemäß *IEEE 802.1q*) zu nutzen. Es ist zudem möglich, auch in der virtuellen Infrastruktur *VLANs* zur Netzsegmentierung zu verwenden. Genügen zur Segmentierung der Netze *VLANs*, die lediglich eine logische Trennung darstellen, kann dies auch innerhalb der virtuellen Infrastruktur geschehen. Die virtuellen Netzkarten der betreffenden virtuellen IT-Systeme sind dann so auf physische Netzschnittstellen zu verteilen, dass diese nur untereinander Netzpakete austauschen können.

Wurden vor der Virtualisierung Netze aufgrund unterschiedlichen Schutzbedarfs physikalisch getrennt, müssen diese Netze auch in virtuellen Umgebungen voneinander isoliert werden. Es ist dann zu prüfen, ob die Mechanismen zur Netztrennung, sowie der Kapselung und Isolation der virtuellen IT-Systeme in der eingesetzten Virtualisierungslösung ausreichen, um virtuelle IT-Systeme mit hohem Schutzbedarf gemeinsam mit solchen niedrigen Schutzbedarfs auf einem Virtualisierungsserver betreiben zu können. Diese Prüfung kann z. B. darin bestehen, dass der Hersteller der betreffenden Virtualisierungslösung die genannten Mechanismen für diesen Einsatzzweck (Trennung von Maschinen unterschiedlichen Schutzbedarfs) als geeignet bezeichnet und dies durch eine entsprechende Zertifizierung nachweist.

Bei erhöhtem Schutzbedarf kann der Betrieb der jeweiligen Netze auf einem einzelnen Virtualisierungsserver jedoch problematisch sein, beispielsweise wenn Administratoren der virtuellen Infrastruktur keinen Zugriff auf virtuelle IT-Systeme in bestimmten Netzen außerhalb ihres Verantwortungsbereichs haben sollen. In diesem Fall sind die virtuellen Maschinen, die Zugang zu den betreffenden Netzen haben müssen, auf isolierten dedizierten Virtualisierungsservern bereitzustellen. Gegebenenfalls sollte das betreffende IT-System statt in einer virtuellen Umgebungen auf einem physischen IT-System betrieben werden.

Hochverfügbare virtuelle Infrastrukturen

Der kumulierte Schutzbedarf der einzelnen virtuellen IT-Systeme kann zu einem hohen oder sehr hohen Schutzbedarf dieses Virtualisierungsservers führen. In einem solchen Fall wird daher empfohlen, mehrere Virtualisierungsserver beispielsweise zu einem Cluster zu verbinden. Hierbei werden die virtuellen IT-Systeme auf den verbleibenden Virtualisierungsservern neu gestartet, wenn einer der Virtualisierungsserver im Cluster ausgefallen ist.

Fällt die Kommunikation zwischen mehreren Systemen eines Clusterverbundes gleichzeitig aus, muss jedes System entscheiden können, ob es selbst oder die anderen Systeme von dem Ausfall betroffen sind (*Isolationsproblem*), damit die durch einen Serverausfall betroffenen virtuellen IT-Systeme nicht mehrfach neu gestartet werden. Dieses Isolationsproblem wird in der Regel dadurch gelöst, dass ein Clustersystem prüft, ob bestimmter Ressourcen wie z. B. das Standardgateway erreichbar sind. Kann es diese Ressourcen nicht erreichen, betrachtet es sich als isoliert und entfernt sich selbst aus dem Cluster, je nach Konfiguration werden die auf ihm betriebenen virtuellen IT-Systeme dabei gestoppt.

Daher wird empfohlen, bei der Planung eines solchen Virtualisierungsclusters zu ermittelt, welche Ressourcen zur Prüfung der Isolation herangezogen werden. Diese Ressourcen sind dann in der Rechenzentrumsinfrastruktur mit einer ausreichenden Verfügbarkeit bereitzustellen. Die Netzverbindungen zwischen den Virtualisierungsservern, die Bestandteil des Clusters sind, sind ebenfalls mit einer ausreichenden Verfügbarkeit auszulegen.

Prüffragen:

- Wurde für die Verwaltung der virtuellen Infrastruktur ein getrenntes Verwaltungsnetz realisiert?
- Ist geprüft worden, ob für Virtualisierungsfunktionen wie die Live Migration ein eigenes Netz realisiert werden muss?
- Wurde für die Anbindung der produktiven Gastsysteme ein getrenntes Netz realisiert?
- Ist die Verfügbarkeit der für virtuelle IT-Systeme genutzten Netzschnittstellen ausreichend geplant?
- Ist die Trennung der Netzsegmente durch das eingesetzte Virtualisierungsprodukt ausreichend sichergestellt, wenn virtuelle IT-Systeme unterschiedlichen Schutzbedarfs auf einem Virtualisierungsserver betrieben werden?
- Sind die Netzverbindungen eines Clusters aus Virtualisierungsservern mit einer ausreichenden Verfügbarkeit geplant worden?

M 5.154 Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator

Virtualisierungsserver benötigen eine Vielzahl von Kommunikationsbeziehungen. Dies sind einerseits Verbindungen zu Verwaltungsnetzen und bei Bedarf Verbindungen zu Speichernetzen, um entsprechende Ressourcen des Rechenzentrums nutzen zu können. Andererseits stellen sie für die virtuellen IT-Systeme die jeweiligen Netzverbindungen zur Verfügung.

Hierbei kommen bei den verschiedenen Virtualisierungsprodukten unterschiedliche Techniken zum Einsatz. Bei einigen Virtualisierungsprodukten werden den einzelnen virtuellen IT-Systemen jeweils eigene Netzwerkkarten zugeordnet, die direkt mit den zu nutzenden Netzen verbunden sind. Dies können virtuelle oder physische Netzwerkkarten sein.

Bei anderen Virtualisierungsprodukten werden vollständige Netzinfrastrukturen innerhalb des Virtualisierungsservers abgebildet. Hierfür werden virtuelle Switches erzeugt, die zum einen für die virtuellen IT-Systeme die notwendigen Netzverbindungen bereitstellen und zum anderen den Übergang des virtuellen Netzes in das physische Netz steuern. Dabei ist es auch möglich, rein virtuelle Netze zu erzeugen, die keinen Übergang in das physische Netz besitzen.

Einige der Virtualisierungslösungen unterstützen ebenfalls die Möglichkeit, neben einer physischen eine logische Segmentierung, wie mit einem VLAN (*Virtual Local Area Network*), zu etablieren.

Weiterhin ist die Art und Weise, wie die Kommunikation zwischen virtuellen IT-Systemen untereinander realisiert wird, höchst unterschiedlich. Teilweise wird die Kommunikation zwischen virtuellen IT-Systemen in unterschiedlichen Netzen auf dem gleichen Virtualisierungsserver durch das physische Netz geleitet (Beispiel: *Citrix XenServer*, *Sun VirtualBox* oder *VMware ESX*), teilweise wird diese Kommunikation immer innerhalb der Virtualisierungsschicht durch geleitet, so dass keine Routinginstanz außerhalb der Virtualisierungsschicht an der Kommunikation beteiligt ist (*Sun Solaris Containers*).

Für eine sichere Konfiguration der Netze der Virtualisierungsserver sind mehrere Aspekte zu betrachten:

- Die Verwaltungsschnittstellen der Virtualisierungsserver sollten in einem eigenen Netz angeschlossen werden. Dieses ist physisch oder logisch von dem Netz zu trennen, in dem die virtuellen IT-Systeme betrieben werden. Eine logische Netztrennung ausschließlich mittels *VLAN* ohne darüber hinaus gehende Maßnahmen reicht an dieser Stelle nicht aus, da die Virtualisierungsserver über die Verwaltungsschnittstellen schützenswerte Informationen austauschen.
- Eine Authentisierung muss für alle Benutzer der Verwaltungsschnittstellen erzwungen werden, anonyme Zugriffe dürfen nicht erlaubt werden. Die Übertragung der Authentisierungsdaten sollte außerdem verschlüsselt erfolgen. Des Weiteren sollten die Verwaltungsschnittstellen durch lokale Paketfilter auf dem Virtualisierungsserver selbst geschützt werden.
- In für den Speichernetzzugriff genutzten Netzen kann auf die Targets (=Festplatte) und Initiatoren (=Server) zugegriffen werden. Hierdurch kön-

nen den Virtualisierungsservern oder den virtuellen IT-Systemen gefälschte Initiatoren oder Targets präsentiert werden. Daher ist der Zugriff auf Ressourcen der Speichernetze über ein geeignetes Authentisierungsverfahren zu sichern. Die hierfür verwendeten Netze müssen ebenfalls von den Netzen der virtuellen IT-Systeme separiert werden. Siehe hierzu auch M 5.130 *Absicherung des SANs durch Segmentierung*.

- Werden in einer virtualisierten Infrastruktur Funktionen wie die Migration zur Laufzeit (*VMotion, XENmotion, Live Migration*) genutzt, erfolgt der Transport der Laufzeitumgebung der virtuellen IT-Systeme über das Netz von einem Virtualisierungsserver zum anderen. Hierbei werden alle in dem IT-System verarbeiteten Daten über das Netz übertragen. Diese Daten sind möglicherweise hoch schutzbedürftig. Aus diesem Grunde sollte das für diesen Zweck verwendete Netz ebenfalls separiert werden.
- Die Kommunikation der virtuellen IT-Systeme mit anderen virtuellen oder physischen IT-Systemen sollte detailliert geplant werden. Hierbei ist sicherzustellen, dass bestehende Sicherheitsrichtlinien beachtet werden. Im Netz existierende Sicherheitsgateways oder Monitoring-Systeme dürfen nicht mit den Mitteln der Virtualisierung umgangen werden können. Dies betrifft insbesondere Virtualisierungsprodukte, bei denen der Netzverkehr zwischen virtualisierten IT-Systemen nicht zwingend über physische Netze geführt wird (siehe oben, Beispiele: *SUN Solaris Containers* und *VMware ESX Server*).
- Müssen virtuelle IT-Systeme mit mehreren Netzen verbunden werden, muss geeignet sichergestellt werden, dass über diese keine unerwünschten Netzverbindungen aufgebaut werden können. Es sollten insbesondere keine Verbindungen zwischen Verwaltungsnetzen der Virtualisierungsserver und den Netzen der produktiven virtuellen IT-Systeme ermöglicht werden, um einer Kompromittierung der Virtualisierungsserver durch ein kompromittiertes virtuelles IT-System vorzubeugen.
- In virtuellen Infrastrukturen können auch virtuelle Sicherheitsgateways (virtuelle Firewalls) betrieben werden. Der Einsatz solcher Gateways direkt am Perimeter des eigenen Netzes und somit zur Trennung von Netzen stark unterschiedlichen Schutzbedarfs sollte jedoch genau geprüft werden. Zur Trennung interner Netze mit nicht stark unterschiedlichem Schutzbedarf hingegen sind virtuelle Sicherheitsgateways denkbar. Die Planung solcher Gateways ist sorgfältig durchzuführen. Es muss dabei bedacht werden, dass je nach gewähltem Virtualisierungsprodukt der Netzverkehr durch die Virtualisierungsschicht nicht so geroutet wird, wie dies möglicherweise erwartet wird. Zudem ist nicht gewährleistet, dass die Schutzfunktion des virtuellen Sicherheitsgateways für andere virtuelle oder physische IT-Systeme auch dann noch gegeben ist, wenn die Virtualisierungsserver selbst kompromittiert worden sind. Eine Umgehung dieser Sicherheitsgateways ist nach einer Kompromittierung der Virtualisierungsserver sehr leicht zu realisieren. Da Sicherheitsgateways häufig ebenfalls das Ziel von Angriffen darstellen, sollte davon abgesehen werden, die Virtualisierungsserver selbst ausschließlich durch virtuelle Sicherheitsgateways zu schützen. In solchen Fällen ist eine geeignete Aufteilung der beteiligten Netze über Sicherheitsgateways notwendig. Siehe auch B 3.301 *Sicherheitsgateway (Firewall)*.
- Virtuelle IT-Systeme sind bezüglich ihrer Netzintegration und ihres Schutzes durch Sicherheitsgateways genauso zu behandeln wie physische IT-Systeme, da die Virtualisierungsserver diesen in der Regel keinen zusätzlichen Schutz bieten.

Prüffragen:

- Sind Verwaltungs- und Administrationsnetz vom Netz der virtuellen IT-Systeme separiert und ist diese Trennung gemessen am Schutzbedarf der virtuellen IT-Systeme ausreichend?
- Ist ein anonymer Zugriff auf die Verwaltungsschnittstellen der Virtualisierungsserver ausgeschlossen?
- Existiert ein geeignetes Authentisierungsverfahren für den Zugriff auf Speichernetzressourcen und sind die Speichernetze von den Netzen der virtuellen IT-Systeme separiert?
- Sind die Netze für Live Migrationen von den Netzen der virtuellen IT-Systeme separiert?
- Werden bestehende Sicherheitsrichtlinien bei den Netzverbindungen zwischen virtuellen und physischen IT-Systemen beachtet?
- Ist sichergestellt, dass Sicherheitsgateways und Monitoring-Systeme nicht mit virtuellen Netzen umgangen werden können?
- Ist ausgeschlossen, dass über virtuelle IT-Systeme, die mit mehreren Netzen verbunden sind, unerwünschte Netzverbindungen aufgebaut werden können?
- Falls virtuelle Sicherheitsateways eingesetzt werden sollen: Steht die Nutzung virtueller Sicherheitsateways in Einklang mit den Sicherheitsanforderungen des Informationsverbunds?

M 6.138 Erstellung eines Notfallplans für den Ausfall von Virtualisierungskomponenten

Verantwortlich für Initiierung: IT-Sicherheitsbeauftragter, Leiter IT
Verantwortlich für Umsetzung: Administrator

Der Ausfall von Virtualisierungsservern hat in der Regel weitreichende Folgen für den Informationsverbund. Dies liegt daran, dass nicht nur die Virtualisierungskomponente selbst von dem Ausfall betroffen ist, sondern auch alle virtualisierten IT-Systeme, die auf der Komponente betrieben werden.

Daher kann der Ausfall einer Virtualisierungskomponente nicht isoliert betrachtet werden. Es muss im Rahmen der Planung des Einsatzes der Virtualisierung von IT-Systemen im Rechenzentrum bedacht werden, dass durch die angestrebten Konsolidierungseffekte im Bereich des Hardwareeinsatzes auch das Schadensausmaß eines Ausfalls steigt. Dieses Schadensausmaß ist umso höher, je stärker sich die Konsolidierungseffekte auswirken. Daher muss der Schutzbedarf der Gesamtheit der virtuellen IT-Systeme auf den Schutzbedarf der Virtualisierungskomponenten abgebildet werden. Hierbei müssen das *Maximumprinzip* und das *Kumulationsprinzip* beachtet werden.

Es reicht des Weiteren häufig nicht aus, nur den Ausfall von Virtualisierungsservern, auf denen virtualisierte IT-Systeme betrieben werden, zu betrachten. Weitere IT-Systeme, die für den Betrieb der Virtualisierungsserver notwendig sind, müssen einbezogen werden. Der Ausfall dieser Systeme kann die Verfügbarkeit der Virtualisierungssysteme einschränken. Daher muss für die folgenden Systeme, falls vorhanden, eine Vorgehensweise bei ihrem Ausfall festgelegt werden:

- Virtualisierungsserver
- Verwaltungsserver (insbesondere auch Connection-Broker)
- Lizenzierungsserver

Je nachdem, wie die Virtualisierungssysteme in den Informationsverbund integriert sind, müssen auch weitere Systeme wie Verzeichnisdienste und Dienste zur Namensauflösung mit betrachtet werden.

Da Infrastrukturdienste, wie Verzeichnisdienste oder Namensauflösungsdienste, auch auf virtualisierten IT-Systemen ausgeführt werden können, ist es möglich, dass sich durch den Ausfall einer oder mehrerer Virtualisierungskomponenten eine sehr komplexe Situation ergibt. So muss beispielsweise der Wiederanlauf eines stark virtualisierten Rechenzentrums wegen der sich hierbei häufig ergebenden Dienstabhängigkeiten detailliert geplant werden.

Folgende Aspekte müssen grundsätzlich berücksichtigt werden:

- Die Notfallplanung für Virtualisierungssysteme muss in den existierenden Notfallplan integriert werden (siehe Baustein B 1.3 *Notfallmanagement*).
- Durch einen Systemausfall eines Virtualisierungsservers kann es zu Datenverlusten in allen virtuellen IT-Systemen kommen, die auf dem ausgefallenen Virtualisierungsserver ausgeführt werden. Daher muss für alle virtuellen IT-Systeme geprüft werden, inwieweit die vorhandenen Datensicherungskonzepte (vergleiche dazu Baustein B 1.4 *Datensicherungskonzept*) an die gewählte Virtualisierungstechnik angepasst werden müssen. Es sollte für die virtuellen IT-Systeme geprüft werden, ob die neuen Techniken der Virtualisierung (Snapshots) zur Datensicherung genutzt

werden können und welche Vor- und Nachteile sich hieraus ergeben könnten. Wichtige Images müssen in die Datensicherung einbezogen werden.
- Fällt ein Virtualisierungsserver aus, so fallen alle darauf laufenden virtuellen IT-Systeme ebenfalls aus. Die Wahrscheinlichkeit, dass es bei mindestens einem betroffenen virtuellen IT-System zu einem ernsthaften Datenverlust kommt, steigt mit der Anzahl der betroffenen Systeme. Es ist also bei der Notfallplanung zu berücksichtigen, dass möglicherweise ein umfangreicherer Wiederherstellungsaufwand eingeplant werden muss.
- Werden mehrere Virtualisierungsserver in einer Farm eingesetzt (virtuelle Infrastruktur), ist darauf zu achten, dass eine sinnvolle Gruppierung der virtuellen IT-Systeme gewählt wird. So sollten beispielsweise zwei Systeme, die wechselseitig die Aufgaben des jeweils anderen ausführen können, nicht auf einem Virtualisierungsserver betrieben werden.
- Es muss sichergestellt werden, dass im Notfall für den Umgang mit virtuellen Infrastrukturen geschultes Personal zur Verfügung steht.
- Die Systemkonfiguration der Virtualisierungsserver (siehe M 2.318 *Sichere Installation eines IT-Systems*, M 2.315 *Planung des Servereinsatzes* und M 4.237 *Sichere Grundkonfiguration eines IT-Systems*) muss für die Administratoren jederzeit einsehbar sein. Sie muss so gestaltet sein, dass die Virtualisierungsserver im Notfall auch von Personal wiederhergestellt werden können, das mit der vorher vorhandenen Konfiguration nicht detailliert vertraut ist.
- Es muss ein Wiederanlaufplan erstellt werden, der den geregelten Neustart der Virtualisierungsserver und der mit ihm ausgefallenen virtuellen IT-Systeme gewährleistet.
- Es muss sichergestellt sein, dass die Wiederinbetriebnahme der Virtualisierungssysteme nicht von einem Dienst im Rechenzentrum abhängt, der ausschließlich von einem virtuellen IT-System bereitgestellt wird.

Im Rahmen der Notfallvorsorge sollten unterschiedliche Szenarien betrachtet werden, in dem die Virtualisierungssysteme ganz oder in Teilen kompromittiert worden sind. Für diese Szenarien ist präzise zu beschreiben, wie hierauf zu reagieren ist und welche Aktionen jeweils auszuführen sind. Die Vorgehensweise sollte regelmäßig geübt werden.

Eine rechtzeitige Notfallplanung mit vorgegebenen Handlungsanweisungen, die auch von Personen ausgeführt werden können, die nicht detailliert mit der Administration der Virtualisierungssysteme vertraut sind, kann die Folgen im Schadensfall verringern. Die entsprechenden Dokumente für Notfallsituationen müssen für berechtigte Personen zugreifbar sein. Da sie allerdings wichtige Informationen beinhalten, müssen sie geschützt aufbewahrt werden.

Im Einzelnen sollten mindestens die folgenden Notfallsituationen betrachtet werden:

Angriff

Wurden Angriffe auf die Virtualisierungssysteme entdeckt, kann nicht davon ausgegangen werden, dass diese auf die Virtualisierungssysteme selbst begrenzt waren. Es muss vielmehr geprüft werden, ob die auf den Virtualisierungssystemen betriebenen virtuellen IT-Systeme kompromittiert worden sind. Dabei muss in Betracht gezogen werden, dass auf den Virtualisierungsservern selbst, aber auch auf den virtuellen IT-Systemen, Schadprogramme (*Backdoors, Trojanische Pferde*) installiert worden sind. Des Weiteren ist es möglich, dass über die Netzkonfiguration der Virtualisierungsserver unerwünschte Kommunikationswege geöffnet worden sind. Zudem können virtuelle IT-Systeme kopiert worden sein.

Um zuverlässig solche Schadprogramme zu entfernen, wird eine komplette Wiederherstellung der Virtualisierungskomponenten empfohlen. Hierzu können die erstellten Datensicherungen herangezogen werden, aber auch die Dokumentation der Systemkonfiguration und die Installationsanweisungen. Besitzt die eingesetzte Virtualisierungsumgebung eine Benutzerverwaltung zur Steuerung von administrativen Zugriffen, sind die Benutzerkonten, insbesondere die der Superuser, auf korrekte Gruppenmitgliedschaften zu überprüfen. Sämtliche Passwörter sollten geändert werden, um die Erfolgschancen von Folgeangriffen zu senken.

Für die virtualisierten IT-Systeme, die auf den kompromittierten Virtualisierungsservern betrieben worden sind, sollten die in den entsprechenden Notfallplänen für diese Systeme aufgeführten Maßnahmen durchgeführt werden.

Diebstahl von (physischen) Virtualsierungsservern

Beim Diebstahl von Virtualisierungsservern sind alle Konten zur Verwaltung der Virtualisierungsserver mit neuen Passwörtern zu versehen. Es muss damit gerechnet werden, dass auch virtuelle IT-Systeme mit dem Virtualisierungsserver gestohlen worden sind, insbesondere dann, wenn diese auf lokalen Festplatten des Virtualisierungsservers abgelegt waren. Auch wenn dies nicht der Fall ist, muss davon ausgegangen werden, dass dem Dieb weite Teile der Systemkonfiguration der virtuellen IT-Systeme und der Virtualisierungsinfrastruktur im Rechenzentrum bekannt geworden sind. Daher muss geprüft werden, inwieweit Verbesserungen oder Veränderungen der Virtualisierungsinfrastruktur dazu dienen können, dass die Infrastruktur einem zukünftigen Angriff besser standhalten kann. Im Zweifelsfall sollte die komplette virtuelle Infrastruktur neu gestaltet werden.

Diebstahl von virtuellen IT-Systemen

Der Diebstahl eines virtuellen IT-Systems erfordert in der Regel keinen physischen Zugang zum Rechenzentrum. Ein Angreifer kann virtuelle IT-Systeme über Funktionen der Virtualisierungsserver z. B. kopieren. Hierzu benötigt er nur einen Netzzugang, um auf die Speicherressourcen zugreifen zu können, auf denen die virtuellen IT-Systeme abgelegt sind.

Vorbeugend sind Maßnahmen zu entwickeln, die diese Möglichkeiten erschweren (M 2.477 *Planung einer virtuellen Infrastruktur*, M 4.349 *Sicherer Betrieb von virtuellen Infrastrukturen*). Des Weiteren muss geprüft werden, inwieweit solche Angriffe erkannt werden können.

Die Notfallplanung für virtuelle IT-Systeme sollte daher Regelungen enthalten, welche die Verfahrensweise nach einem solchen Diebstahl beschreiben.

Fehlkonfigurationen

Fehlkonfigurationen von Virtualisierungsservern können zu weitreichenden negativen Folgen für den Rechenzentrumsbetrieb führen. Daher ist die Virtualisierungssoftware im Rahmen der Notfallvorsorge regelmäßig auf Fehlkonfigurationen zu überprüfen. Werden solche entdeckt, muss ihr Ausmaß bewertet werden. Hierbei ist insbesondere zu prüfen, ob virtuelle IT-Systeme durch die Fehlkonfiguration betroffen sind.

Die notwendigen Änderungen zur Behebung der Konfigurationsfehler können je nach Ausprägung direkt vorgenommen werden. Es muss allerdings beachtet werden, dass virtuelle IT-Systeme möglicherweise während solcher Änderungen beeinträchtigt werden können. Daher kann es notwendig werden, die

virtuellen IT-Systeme vor Konfigurationsänderungen an den Virtualisierungssystemen herunterzufahren.

Ausfälle durch höhere Gewalt

Durch Gefährdungen aufgrund von höherer Gewalt, z. B. Erdbeben, Überschwemmung, Feuer, Sturmschäden, Kabelbeschädigungen, kann die Verfügbarkeit der Virtualisierungsserver negativ beeinflusst werden. Hier sind angemessene Maßnahmen zur Erhöhung der Verfügbarkeit zu prüfen, wie beispielsweise redundante Kommunikationsverbindungen der IT-Systeme.

Prüffragen:

- Wurden die Auswirkungen der mit einer virtuellen Infrastruktur einhergehenden Konsolidierungseffekte auf die Verfügbarkeitsanforderungen der Virtualisierungsserver geprüft?
- Wurde eine Vorgehensweise bei einem Ausfall von Virtualisierungskomponenten festgelegt?
- Wurden die Notfallpläne an die virtuelle Infrastruktur angepasst?
- Wurden die Datensicherungskonzepte an die virtuelle Infrastruktur angepasst?
- Ist sichergestellt, dass im Notfall entsprechende Dokumente und geeignetes Personal zur Verfügung stehen?
- Wurden Regelungen erstellt, die die Verfahrensweise nach einem Diebstahl von virtuellen IT-Systemen beschreiben?
- Werden die Virtualisierungsserver regelmäßig auf Fehler geprüft?
- Wurde die Notwendigkeit für Maßnahmen geprüft, die die Verfügbarkeit in Fällen höherer Gewalt steigern?

			G 2.29	G 2.32	G 2.37	G 2.60	G 2.148	G 2.149	G 2.150	G 2.151	G 3.16	G 3.28	G 3.36	G 3.79	G 3.99	G 3.100	G 3.101	G 3.102	G 4.74	G 4.75	G 4.76	G 4.77	G 4.78	G 5.29	G 5.133	G 5.147	G 5.148	G 5.149	G 5.150
M 2.82	PK	B	X																										
M 2.83	UM	B	X																										
M 2.314	PK	Z																	X		X								
M 2.392	PK	A					X																						
M 2.444	PK	A					X	X	X	X						X	X		X					X			X	X	
M 2.445	BE	C					X																						
M 2.446	UM	B				X					X	X			X	X								X			X		
M 2.447	UM	A		X				X	X	X	X		X	X	X	X	X					X		X	X		X	X	
M 2.448	BT	B						X								X	X						X	X	X	X	X		X
M 2.449	BT	Z																										X	X
M 2.477	PK	A		X		X	X	X						X	X				X	X				X	X		X	X	
M 3.70	PK	W					X																						
M 3.71	PK	B											X			X	X												
M 3.72	UM	W					X																						
M 4.97	UM	Z												X												X			X
M 4.346	UM	A						X	X		X	X			X	X	X						X	X			X	X	
M 4.347	UM	Z						X								X											X		
M 4.348	BT	C																X											X
M 4.349	BT	A		X	X			X	X		X			X	X	X								X	X		X		X
M 5.153	PK	B			X	X	X					X		X	X					X					X	X			
M 5.154	UM	B		X	X							X		X	X					X					X	X			X
M 6.138	NV	C					X												X										