Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Server-Virtualisierung

1 Ausgangslage

Aktuelle Server-Hardware ist so leistungsfähig, dass klassische Server-Installationen, auf denen eine Applikation pro physischem Server läuft, die Hardware-Ressourcen oftmals nicht auslasten. Daher wird Virtualisierung eingesetzt, um die Hardware effizienter zu nutzen, d. h. um Energie und Platz in den Rechenzentren und damit Kosten zu sparen. Gleichzeitig kann die erforderliche Bereitstellungszeit von Systemen durch den Einsatz von Virtualisierung massiv reduziert und zusätzlich die Verfügbarkeit durch die Entkopplung von Systemen und Hardware gesteigert werden.

Insbesondere bei der Konsolidierung und Zusammenführung von Informationstechnik bei Hosting Providern gibt es aufgrund der rechnerischen Anzahl der benötigten Server keine handhabbare und wirtschaftliche Alternative zu virtuellen Servern.

Durch den Einsatz von Virtualisierung werden IT-Systeme, die bislang auf unterschiedlichen physischen Servern realisiert waren, auf einer Hardware-Plattform zusammengefasst. Eine Virtualisierungsumgebung stellt den IT-Systemen virtuelle Hardware zur Verfügung, auf der die IT-Systeme, auch Gast-Systeme genannt, ausgeführt werden. Weiterhin sorgt die Virtualisierungsumgebung für ausgeglichene Ressourcenzuteilung, für die Separierung der Gast-Betriebssysteme sowie für die Separierung der Gast-Systeme von der unterliegenden Virtualisierungsumgebung, auch Host-System genannt. Läuft auf der Hardware nur die Virtualisierungsumgebung, wird diese Bare-metal Hypervisor genannt (siehe Abbildung 1).

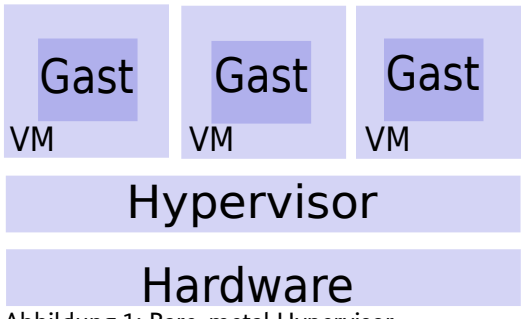

Abbildung 1: Bare-metal Hypervisor

Virtualisierung ist zudem eine der entscheidenden Grundlagen des Cloud Computings, da virtuelle Server automatisiert und deutlich schneller als physische Server aufgesetzt und bereitgestellt werden können.

2 Ziel der Empfehlung

Diese Empfehlung richtet sich an Verantwortliche für die Planung und den Betrieb von IT-Infrastrukturen sowie an Betreiber von IT-Rechenzentren. Sie beinhaltet produktunabhängige Empfehlungen zum sicheren Einsatz von Server-Virtualisierungsprodukten, die als Bare-metal-Hypervisoren eingesetzt werden.

Bei Bare-metal-Hypervisoren laufen neben dem Hypervisor keine anderen Anwendungen auf der physischen Hardware. Der Hypervisor ist ein speziell für Virtualisierung optimiertes Betriebssystem.

3 Abgrenzung

Dieses Dokument beinhaltet Empfehlungen zur Server-Virtualisierung, es geht nicht auf Cloud-Techniken und -Produkte ein. Ansatzweise werden Empfehlungen zur Netz- und Speicher-Virtualisierung sowie deren Konfiguration gegeben.

Durch das Zusammenfassen mehrerer Server auf einer Hardware muss diese unter Umständen physisch besser abgesichert werden, als ein einzelner Server. Werden z. B. Rechenzentren zusammengelegt, muss die physische Absicherung insgesamt anhand der Rechner mit dem höchsten Schutzbedarf erfolgen (siehe auch IT-GS 200-2, Abschnitt 8.2.4). Zu dieser physischen Absicherung der IT-Infrastruktur werden im Dokument keine weiteren Angaben gemacht. Ebenfalls nicht betrachtet werden Client-, Desktop- und Applikations-Virtualisierung. Es werden auch keine Compliance-Themen wie z. B. Lizenz-Management behandelt.

Der Einsatz von Virtualisierung von Sicherheitskomponenten, die dem Perimeterschutz dienen (insbesondere in einer DMZ), wird hier nicht betrachtet. Die hier definierten Kriterien sind in solchen Szenarien nicht anwendbar.

4 Server-Virtualisierung aus Sicherheitssicht

Virtualisierte Systeme bringen neue Anforderungen mit sich, die bei der Absicherung einer IT-Infrastruktur berücksichtigt werden müssen. Bei einem klassischen physischen Server lassen sich Sicherheitsmaßnahmen noch weitestgehend losgelöst von z. B. der Netzwerk-Sicherheit umsetzen. Durch Virtualisierung wird eine zusätzliche virtuelle Hardware-Schicht eingeführt, so dass mehrere Server auf einer physischen Hardware betrieben werden können. Meistens ist bereits dann eine separate Management-Software nötig, um sowohl die virtuelle Umgebung als auch die virtuellen Maschinen zu administrieren. Die Netzanbindung erfolgt häufig durch virtuelle Netzkomponenten, die ggf. Bestandteil des Hypervisors sind. Generell gilt, dass die bei klassischen IT-Systemen und Netzen vorhandene physische Trennung zu Gunsten einer logischen Trennung aufgehoben wird.

Physische Server, auf denen eine Virtualisierungsumgebung läuft, werden meistens nicht stand-alone betrieben, sondern sind von der IT-Infrastruktur, in die sie eingebettet sind, abhängig. Meistens werden sie mit anderen Servern zu Clustern zusammengeschlossen. Dadurch wird eine Steigerung der Verfügbarkeit der Gast-Systeme erreicht, da die virtuellen Maschinen zwischen den physischen Servern im laufenden Betrieb verschoben werden können (Live-Migration). Zudem wird die Administration vereinfacht, die in einer virtualisierten Infrastruktur üblicherweise aus einer separaten Management-Umgebung durchgeführt wird. Als Speicherort für die virtuellen Maschinen sowie deren virtuellen Festplatten und deren Konfiguration wird meistens ein zentraler Massenspeicher (SAN oder NAS) eingesetzt.

Dieser Aufbau der IT-Infrastruktur hat Konsequenzen für die Vernetzung der IT-Systeme: neben dem Managementnetz gibt es die Anbindung des Massenspeichers, das Produktivnetz der Gast-Systeme sowie das Netz, das Virtualisierungsumgebungen untereinander nutzen, über das z. B. Live Migration realisiert wird (siehe auch den Abschnitt „Vernetzung“).

Bezüglich Sicherheit bietet die Virtualisierung einer IT-Infrastruktur folgende Vorteile:

- Höhere Ausfallsicherheit durch die Clusterbildung der Hosts
- Verwendung von Templates zur Bereitstellung von aktuellen gepatchten und standardisierten IT-Systemen
- Zentrales Management, dadurch weniger Administrationsaufwand (die Server werden zentral angelegt, gestartet, gestoppt, modifiziert, vernetzt, überwacht und entsorgt)
- Die IT-Infrastruktur ist leichter skalierbar und erweiterbar
- Unabhängigkeit von konkret eingesetzter Hardware

Folgende Nachteile hat eine virtualisierte Infrastruktur aus Sicherheitssicht:

- Es wird eine zusätzliche Software-Schicht eingeführt, die Fehler enthalten kann und abgesichert werden muss.
- Eine virtuelle Trennung von Servern besitzt eine geringere Mechanismenstärke gegenüber einer physischen Trennung, d. h. das Sicherheitsniveau ist niedriger.
- Durch die Installation von Gastwerkzeugen im Gast-Betriebssystem werden zusätzliche virtuelle Treiber und Hardware eingeführt, die eine weitere Angriffsfläche bieten.
- Neben den virtualisierten Servern gibt es üblicherweise noch eine virtualisierte Netzwerk-Ebene, die zusätzliche Komplexität erzeugt.
- Das zentrale Management wird zum attraktiven Angriffspunkt.
- Die Fehlkonfiguration der Virtualisierungsumgebung hat weitreichendere Auswirkungen als die Fehlkonfiguration eines einzigen Servers
- Die Konsolidierung der IT zieht meist eine Reduzierung des Administrationspersonals nach sich. Dadurch vergrößert sich der Verantwortungsbereich für die einzelnen Personen.

5 Einordnung in die IT-Infrastruktur

Es wird davon ausgegangen, dass es in der Organisation ein Sicherheitskonzept und -prozesse gibt, in die die Absicherung von Virtualisierungsumgebungen eingebettet wird. Folgende Maßnahmen werden vorausgesetzt:

- Die Hardware für die Virtualisierungsumgebung muss hinsichtlich Leistung und Performance ausreichend dimensioniert sein. Hierbei sollten die Empfehlungen des Herstellers berücksichtigt werden. Aus Verfügbarkeitsgründen müssen redundante Systeme sowohl für die Server-Hardware als auch die Netzanbindung geplant werden. Speicherplatz und Management-Umgebung müssen ebenfalls ausreichend dimensioniert sein.
- Beim Einsatz von Blade-Systemen ist es systembedingt nicht möglich, eine physische Trennung des Netzverkehrs vorzunehmen, da es bei diesen Systemen nur eine Backplane gibt, die alle Blades mit dem Interconnect-Switch verbindet. Zudem gibt es häufig nur noch zwei Netzwerk-Schnittstellen in das Gehäuse, über die jeglicher Netzverkehr geleitet werden muss. Blade-Systeme sind daher (s. u.) für den Einsatz bei sehr hohem Schutzbedarf nicht geeignet.
- In der Organisation sind regelmäßige Updates gewährleistet z. B. durch ein Patch- und Änderungsmanagement. Für virtualisierte Umgebungen ist darauf zu achten, dass nicht nur die Gast-Betriebssysteme, sondern auch der Hypervisor, die Management-Umgebung und evtl. genutzte Gastwerkzeuge in das Patchmanagement integriert sind.

- Die bisherigen Abläufe für Backup und Restore müssen erweitert werden, um sowohl die virtuellen Maschinen als auch die Konfiguration des Hypervisors zu berücksichtigen. Zu beachten ist, dass auch die Management-Umgebung an das Backup angeschlossen wird, hier insbesondere die Konfigurationseinstellungen der virtuellen Maschinen (z. B. durch eine Sicherung der Datenbank der Management-Umgebung). Weiterhin muss geprüft werden, ob in der Organisation vorhandene Backup- und Restore-Konzepte und -Produkte für den Einsatz in einer virtualisierten Infrastruktur geeignet sind. Ggf. müssen neue Verfahren etabliert und neue Produkte eingeführt werden.
- Monitoring, Logging, Intrusion Detection und Verhinderung von Datenabfluss muss sowohl für die VMs als auch den Hypervisor gewährleistet sein.
- Das Netz- bzw. Zonenkonzept muss an die veränderte Umgebung angepasst werden. Durch den Einsatz von Server-Virtualisierung ändert sich der Netzverkehr von der streng hierarchischen Nord-Süd-Ausrichtung hin zur Ost-West-Richtung. Gemeint sind die Netzverbindungen zwischen den (virtuellen) Servern (Ost-West), die u. U. nicht mehr über externe Netzkomponenten (Nord-Süd) geleitet werden. Dementsprechend müssen auch die Sicherheitskomponenten angepasst werden (siehe auch Kapitel 8).
- Es muss ein Speicher-Konzept vorliegen. Durch den Einsatz der Server-Virtualisierung entstehen auch in diesem Bereich neue Strukturen, da aus Verfügbarkeitsgründen meist ein zentraler Speicher verwendet wird, in dem die virtuellen Maschinen liegen. Diese müssen ggf. voneinander isoliert werden und die korrekte und zuverlässige Netzanbindung muss gewährleistet sein. Je nach Virtualisierungsumgebung kann die virtuelle Maschine z. B. als Verzeichnis mit Plattenimage und Konfigurationsdatei realisiert sein oder aber nur als Image-Datei, deren Konfigurationsoptionen in der Management-Umgebung vorgehalten werden. Unabhängig von der Realisierung sieht das Gast-Betriebssystem einfach eine gewöhnliche Festplatte.

6 Konzeption der Virtualisierungsumgebung

Virtualisierung bedeutet eine Konsolidierung der Server, d. h. die Möglichkeit mehrere Server virtuell auf einem physischen Host zu betreiben. Die Server unterliegen unterschiedlichem Schutzbedarf aufgrund der verschiedenen Anwendungen und Dienste, die darauf laufen. Daher muss vor einer Virtualisierung festgelegt werden, welche Dienste oder Anwendungen zusammen in einer virtuellen Umgebung betrieben werden dürfen und welche durch geeignete Maßnahmen separiert werden müssen. Da sich Separierung durch alle Bereiche einer IT-Infrastruktur fortsetzen muss, werden im Folgenden neben dem Bereich „Compute“ auch die Bereiche „Network“, „Storage“ und „Management“ im Ansatz betrachtet (siehe Tabelle 2).

Bei der Entscheidung, welche Systeme auf einer gemeinsamen physischen Hardware virtualisiert werden dürfen, ist Folgendes zu beachten:

1. Zonenkonzept: Die Server sollten aus organisatorischer Sicht und aus Sicherheitssicht sinnvoll in Zonen gruppiert werden. Zonen sollten nicht zusammen mit der Sicherheitskomponente, die für die Separierung der Zonen sorgt, virtualisiert werden.
2. Was zusammen auf einer gemeinsamen physischen Hardware virtualisiert werden kann, ist abhängig von Schutzbedarf und Bedarfsträger.

Bedarfsträger können unterschiedliche Mandanten (Hosting-Szenarien), unterschiedliche Organisationseinheiten innerhalb eines Unternehmens oder einer Organisation oder unterschiedliche Verfahren sein. Im ersten Fall besteht die Herausforderung bei der Planung, ein gleiches Verständnis der Bedarfsträger über die unterschiedlichen Schutzbedarfskategorien zu erreichen.

Die folgende Matrix beinhaltet einen Vorschlag zur Gestaltung virtualisierter Infrastrukturen. Es wird von drei unterschiedlichen Schutzbedarfskategorien (normal, hoch, sehr hoch, siehe auch [IT-GS])) ausgegangen sowie von zwei Bedarfsträgern.

Der im Folgenden dargestellte Schutzbedarf zielt primär auf die Gewährleistung des Schutzziels Vertraulichkeit und erst in zweiter Linie auf die Verfügbarkeit und Integrität.

In Tabelle 1 werden für verschiedene Schutzbedarfsszenarien zwischen Bedarfsträger 1 und Bedarfsträger 2 sicherheitstechnisch mögliche Separierungen dargestellt. Tabelle 1 muss in Kombination mit Tabelle 2 gelesen werden, da erst in Tabelle 2 eine Ausdifferenzierung der Separierungsstufe erfolgt.

Die Tabellen können beliebig verfeinert und ergänzt werden und sind daher Anhaltspunkte und Vorschläge zur Realisierung einer IT-Infrastruktur. Ausnahmen sind möglich.

Nr.	Bedarfsträger-Kombination	Separierungsstufe gem. Tabelle 2
1	(1 normal, 1 normal)	Basis-Separierung
2	(1 normal, 1 hoch)	Durchgängige logische Separierung
3	(1 normal, 1 sehr hoch)	Einzelfallbetrachtung
4	(1 hoch, 1 hoch)	Durchgängige logische Separierung
5	(1 normal, 2 normal)	Durchgängige logische Separierung[1]
6	(1 normal, 2 hoch)	Durchgängige logische Separierung sowie in Teilen physische Separierung
7	(1 normal, 2 sehr hoch)	Physische Separierung
8	(1 hoch, 2 hoch)	Durchgängige logische Separierung sowie in Teilen physische Separierung
9	(1 sehr hoch, 2 sehr hoch)	Physische Separierung

Tabelle 1

Beispiele:

2. Zeile: Bedarfsträger 1 möchte die Anwendung „Intranet-Webserver“ (Schutzbedarf normal) und „Zeiterfassung“ (Schutzbedarf hoch) virtualisieren. Hierfür ist die Umsetzung der Separierungsstufe „Durchgängige logische Separierung“ gem. Tabelle 2 anzuwenden.

6. Zeile: Bedarfsträger 1 möchte die Anwendung „Intranet-Webserver“ (Schutzbedarf normal), Bedarfsträger 2 die „Zeiterfassung“ (Schutzbedarf hoch) virtualisieren. Hierfür ist die Umsetzung der Separierungsstufe „Durchgängige logische Separierung sowie in Teilen physische Separierung “ gem. Tabelle 2 anzuwenden.

Da die oben angeführte Separierung ganzheitlich in der gesamten IT-Infrastruktur umgesetzt werden sollte, werden im folgenden Vorschläge für die Bereiche Compute, Network, Storage und Management aufgeführt:

1 Sind die Bedarfsträger unterschiedliche juristische Personen, sollte der Netzverkehr physisch separiert werden. Wenn beide einverstanden sind, kann auch logisch separiert werden.

Separierungsstufe	Compute	Network	Storage	Management
Basis-Separierung	VMs zusammen auf einem Hypervisor, Gastwerkzeuge erlaubt	VMs dürfen über einen gemeinsamen (virtuellen) Switch angebunden werden, Netzseparierung über Access Control Lists.	LUN-Binding, LUN-Masking	Eine gemeinsame Management-Umgebung
Durchgängige logische Separierung	VMs zusammen auf einem Hypervisor, keine Gastwerkzeuge erlaubt	VMs dürfen über einen gemeinsamen virtuellen Switch angebunden werden, Separierung der Netze über VLANs (virtueller Switch ist VLAN-Trunk).	LUN-Binding, LUN-Masking, Hard-Zoning	Logische Separierung innerhalb des Managements anhand von Rollen (RBAC)
Durchgängige logische Separierung sowie in Teilen physische Separierung	VMs zusammen auf einem Hypervisor, keine Gastwerkzeuge erlaubt	VMs müssen an dedizierte virtuelle Switche angeschlossen werden, die jeweils über eigene physische Netzwerkkarten angebunden sind, physischer Switch ist VLAN-Trunk.	Segmentierung des SANs (VSAN im Sinne des IT-GS), Hard-Zoning, LUN-Binding, LUN-Masking	Separierung von Netz-, Server- und Speicher-Administration
Physische Separierung	Physisch getrennte Hypervisoren oder physische Server	Physische Trennung aller Netze. VMs müssen an dedizierte virtuelle Switche angeschlossen werden, die jeweils über eigene physische Netzwerkkarten angebunden sind, VLANs innerhalb der Umgebung eines Bedarfsträgers sind erlaubt wenn nötig.	Verschlüsselung von data-in-motion und data-at-rest ODER physisch getrenntes Netz sowie Speicherlösung	Getrennte Instanzen der Managementumgebung
Einzelfallbetrachtung	Ob eine Zusammenlegung möglich ist, kann nicht pauschal festgelegt werden. Dies muss für jede Spalte einzeln geprüft werden.			

Tabelle 2

Bei den Szenarien, die nur einen Bedarfsträger betrachten, z. B. (1 normal, 1 normal) oder (1 normal, 1 hoch), ist die Kommunikation zwischen verschiedenen Schutzzonen durch eine Firewall abzusichern.

6.1 Risikobetrachtung

Im Folgenden wird für die oben angeführten Maßnahmen deren Schutzwirkung beschrieben.

Schutzmaßnahme	Schutzwirkung	Restrisiko
Dedizierter virtueller Switch	Virtuelle Switche sind separate Objekte im Speicher der Virtualisierungsumgebung, dadurch wird eine Isolation erreicht.	Ausnutzbare Fehler in der Software.
Zonenkonzept (hier ist nicht Soft-Zoning gemeint)	Zonen lassen sich sowohl aus organisatorischer als auch sicherheitstechnischer Sicht klassifizieren. Es können Regeln für die Kommunikation zwischen Zonen festgelegt werden. Weiterhin können den Zonen bestimmte Sicherheitseigenschaften zugewiesen werden. Die klassische flache Netzinfrastruktur, die meist nur in Clients und Server aufgeteilt war, wird strukturiert.	Unklare Konzeption führt zu Sicherheitsrisiken.
Getrennte Instanzen der Management-Umgebung	Wird eine Management-Umgebung kompromittiert, ist nicht gleich die ganze virtuelle Infrastruktur kompromittiert.	Alle Management-Umgebungen werden kompromittiert, z. B. durch Ausnutzung der gleichen Schwachstelle.
Keine Gastwerkzeug/Gastwerkzeuge vermeiden	Gastwerkzeuge weichen durch ihre Para-virtualisierungsfunktion die Trennung sowohl von Virtualisierungsumgebung und VMs als auch die Trennung zwischen VMs auf.	Da ohne Gastwerkzeuge u.U. deutliche Performance-Einbußen entstehen (sowohl hinsichtlich Arbeitsspeicher, als auch Netzverkehr als auch Grafikleistung), ist nicht ausgeschlossen, dass sie in Teilen doch installiert werden.
Logische Separierung innerhalb des Managements anhand von Rollen (RBAC), kombiniert mit Gruppierungen der verwalteten Komponenten.	Im Management-Produkt werden Geräte (Server, Netzkomponenten, Netze) einer Zone durch entsprechende Mechanismen wie Clusterbildung zusammen gruppiert. Für die Gruppen können Berechtigungen vergeben werden, die wiederum an Rollen gebunden sind. Es ist zu verhindern, dass ein Administrator alles darf, bzw. dass Änderungen nicht nachvollzogen werden können.	Fehler durch falsche Zuordnungen.
LUN-Binding und LUN-Masking	LUN-Binding und LUN-Masking verhindern, dass jeder Rechner, der in einer Speicherzone mit einem Speichersystem stationiert ist, alle logischen oder physischen Platten dieses Systems sieht ([IT-GS SpL]).	Ausnutzbare Fehler in der Software.
Physisch getrennte Hypervisoren	Durch die physische Trennung wird eine sehr gute Isolierung erreicht. Trotzdem kann eine Virtualisierung der Server durchgeführt werden, um z. B. eine Verbesserung der Verfügbarkeit oder eine einfache Verwaltung zu erreichen.	Es können immer noch Angriffe über die Netzkomponenten erfolgen.
Physische NIC pro virtuellem Switch	Netzverkehr wird nicht zusammengeführt.	Ausnutzbare Fehler im virtuellen Switch.
RBAC in der Management-Umgebung	Der Zugriff auf das Management ist abhängig von Rollen, nicht von Personen. Dies hat den Vorteil, dass bei Abwesenheit oder Wechsel von Personal keine Zugriffsrechte angepasst werden müssen, sondern nur die Zuordnung von Personen zu Rollen geändert werden muss.	Falsche Zuordnung von Personen zu Rollen, Fehler im eingesetzten Produkt.

Schutzmaßnahme	Schutzwirkung	Restrisiko
Soft-Zoning	Durch Soft-Zoning sehen sich nur Geräte der gleichen Speicherzone. Auf diese Weise kann eine Gruppierung vorgenommen werden.	WWN-Spoofing und Datenübertragungen zu gültigen WWNs werden nicht verhindert.
Verschlüsselung der Daten (in-motion und at-rest)	Daten sind für Unbefugte nicht lesbar.	Ausnutzbare Fehler in der Software, zu schwache Kryptographie, unzureichendes Schlüsselmanagement.
VSAN	Ein VSAN erweitert das Konzept des Soft-Zonings und bietet sowohl einen besseren Zugriffsschutz auf die Daten und Applikationen als auch Schutz vor einer breiteren Wirkung von Störungen, die so auf einen Teil des Netzes begrenzt werden können ([IT-GS SpL]).	Ausnutzbare Fehler in der Software.

7 Absicherung von Virtualisierungsumgebungen

Verschiedene Maßnahmen tragen zur Absicherung von Virtualisierungsumgebungen bei. Diese sind im Folgenden aufgeführt, zugeordnet zu Hypervisor und VM sowie zu den Gast-Betriebssystemen.

7.1 Hypervisor und virtuelle Maschinen

Der Hypervisor übernimmt die Ressourcenverwaltung und -zuteilung für die virtuellen Maschinen. Aus Sicherheitssicht ist er zudem zuständig für die Isolierung der VMs untereinander. Es muss verhindert werden, dass ein nicht zulässiger Informationsfluss zwischen den virtuellen Maschinen besteht, sei es durch gemeinsam genutzte Ressourcen oder durch Mitlesen des Netzverkehrs.

Folgende Maßnahmen tragen zur Sicherheit einer Virtualisierungsumgebung bei.

Härtung und Minimierung des Systems

- Aktuelle, minimierte und standardisierte Installations-Images für die Virtualisierungsumgebung erzeugen.
- Konfigurationsvorgaben des Herstellers hinsichtlich Sicherheit umsetzen.
- Integrität der Installations-Images sicherstellen und prüfen.
- Schnittstellen auf ein Minimum reduzieren, um die Angriffsfläche zu reduzieren.

Cluster-Bildung

- Bei Cluster-Bildung Hardware-Anforderungen beachten (z. B. CPU-Typen). Auf korrekte Konfiguration der beteiligten Hosts achten. Braucht ein Gast-System spezielle Hardware, muss diese in allen physischen Servern vorliegen, auf die dessen VM durch Live-Migration verschoben werden kann.
- Verfügbarkeitsmechanismen der Virtualisierungsumgebung wie Failover und Lastverteilung aktivieren (setzt Clusterbildung von Hosts voraus).

Virtuelle Hardware der virtuellen Maschine

- Minimierung des Systems, in dem den VMs nur die benötigte (virtuelle) Hardware zugewiesen wird und nicht benötigte Schnittstellen und Interfaces wie USB oder Sound abgeschaltet werden.
- Ab hohem Schutzbedarf sollten Ressourcen-Zuweisungen statisch erfolgen sowie der Ressourcenverbrauch begrenzt werden. Dies gilt sowohl für den Netzverkehr, die Kapazität der virtuellen Festplatte sowie den Arbeitsspeicher. Dies gewährleistet, dass alle VMs die benötigten Ressourcen ausreichend zur Verfügung haben.

Kommunikation zwischen virtuellen Maschinen bzw. zwischen VM und Hypervisor

- Paravirtualisierte Treiber und Hardware sollten vermieden werden. Bei der Paravirtualisierung greift das Gast-Betriebssystem über Hypercalls direkt auf privilegierte Ressourcen zu. Dies weicht die Isolierung zwischen VM und Hypervisor auf.
- Alle Schnittstellen, die einen Austausch von Informationen zwischen Host und Gast ermöglichen, sollten ausgeschaltet werden.
- Alle Schnittstellen, die die Kommunikation von virtuellen Maschinen untereinander ermöglichen, sollten ausgeschaltet werden.

Lebenszyklus von virtuellen Maschinen

Für virtuelle Maschinen sollte ein Lebenszyklus entworfen werden, der Folgendes umfasst:

- Klare Regeln und Kriterien, wann eine VM angelegt und gestartet werden darf (Vermeidung von VM-Wildwuchs).
- VMs bzw. deren Gast-Betriebssysteme, müssen in das Patch- und Änderungsmanagement eingebunden sein, damit ein aktueller Patch-Stand gewährleistet ist. Auch für ausgeschaltete VMs müssen aktuelle Betriebssystem-Versionen gewährleistet sein.
- Festlegung, ob Kopien einer VM (z. B. in Form von Snapshots) gemacht werden dürfen. Protokollierung und Verzeichnis von allen Kopien, damit zu jedem Zeitpunkt klar ist, wo sich welche Kopien der VMs befinden.
- Lebensdauer einer VM festlegen, geregelte und nachvollziehbare Löschung nicht mehr benötigter VMs.

Konfiguration der Netzanbindung im Hypervisor

- Host-Firewall einrichten: Verbindungen nur aus und in die vorgesehenen Netze zulassen. Dies schützt allerdings nicht die Kommunikation von und zu den Gast-Systemen.
- Konfiguration des Hypervisors, sodass VMs nicht gegenseitig ihre Pakete sehen.
- Konfiguration der (virtuellen) Netzkomponenten, sodass VLAN-Hopping verhindert wird (vgl. Anhang des Dokuments [VLAN]).
- Durch hypervisor-interne Vernetzung dürfen externe Sicherheits-Komponenten wie Firewalls nicht umgangen werden.
- Getrennte physische Netze für Produktivbetrieb und Management (siehe auch Abschnitt „Vernetzung“).

Administration des Hypervisors

Im Folgenden wird auf einige hypervisor-spezifische Aspekte der Administration einer virtuellen Infrastruktur eingegangen. Weitere allgemeine Empfehlungen stehen im Abschnitt „Management“.

- Meistens gibt es viele Möglichkeiten, Konfigurationsänderungen auf dem Hypervisor durchzuführen, z. B. über die Management-Umgebung, lokal in einer Konsole auf dem physischen Rechner oder automatisiert über Skripte. Es sollte festgelegt werden, welche Schnittstellen genutzt werden dürfen, alle anderen sollten deaktiviert werden.
- Der Zugriff sollte durch die Festlegung von Rollen und Zuordnung von Rechten zu Rollen geregelt werden.
- Der Personenkreis, der Konfigurationsänderungen durchführen darf, sollte so klein wie möglich sein. Es sollten Rechte an Rollen gebunden werden und dann Personen den Rollen zugeordnet werden.
- Änderungen durch die Administratoren sollten geeignet protokolliert werden.

- Die Kommunikation mit dem Hypervisor sollte durch Verschlüsselung und Authentisierung gesichert sein.
- Grundlage für die Verschlüsselung und Authentisierung sollten Zertifikate sein, die einem Zertifikats-Management unterliegen.
- Die Konfigurationseinstellungen sollten gesichert werden und deren Wiederherstellung einfach möglich sein.

7.2 Absicherung der Gast-Betriebssysteme

Die Gewährleistung der IT-Sicherheit muss sich in den Gast-Betriebssystemen hin zu den Applikationen fortsetzen. Aus Sicht der Virtualisierungsumgebung kann dies durch folgende Maßnahmen unterstützt werden:

- Templates mit aktuellen gehärteten Gast-Betriebssystemen zum Aufsetzen von neuen Servern verwenden.
- Es müssen alle Absicherungen durchgeführt werden, die auch für physisch realisierte Server gelten, z. B. die Installation von Sicherheitskomponenten, wie lokale Firewalls oder Antiviren-Software.
- Gast-Werkzeuge und paravirtualisierte Treiber weichen die Trennung zwischen VM und Virtualisierungsumgebung auf. Daher sollten sie nur eingeschränkt verwendet werden.

8 Vernetzung

Wie bereits am Anfang des Dokuments erwähnt, hat der Einsatz von Server-Virtualisierung Konsequenzen für die Vernetzung der IT-Systeme. Der Netzverkehr ändert sich von streng hierarchischen Nord-Süd-Ausrichtung hin zu vermehrtem Ost-West-Verkehr. Durch Abbildung 2 wird dies verdeutlicht.

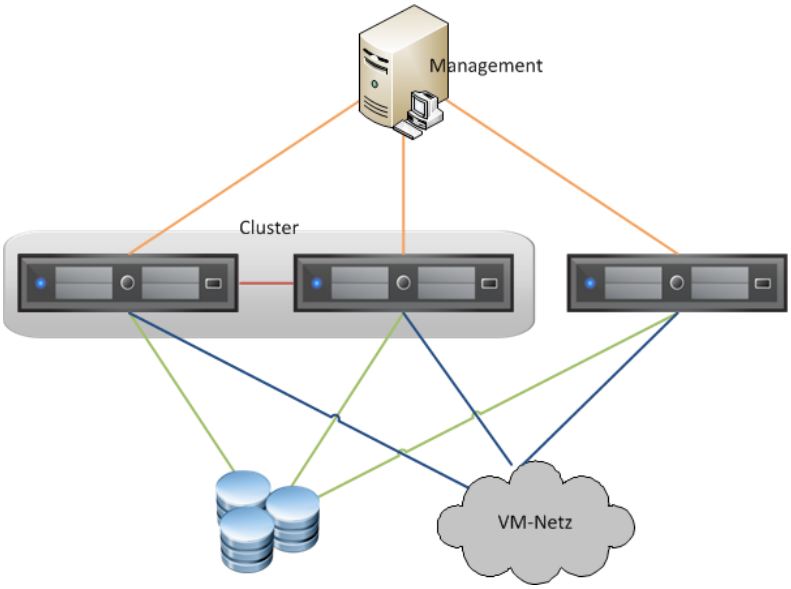

Abbildung 2: Schematischer abstrakter Aufbau einer virtualisierten IT-Infrastruktur

Neben dem Managementnetz (in orange in Abbildung 2) gibt es die Anbindung des Massenspeichers (in grün), das Produktivnetz der Gast-Systeme (in blau) sowie das Netz, das Virtualisierungsumgebungen untereinander nutzen (in rot), über das z. B. Live Migration realisiert wird. Letzteres verdeutlicht den Ost-West-Verkehr.

Es entstehen folgende Anforderungen an Netze in virtualisierten Infrastrukturen:

- Es ist eine physische Trennung des Management-Netzes von den anderen Infrastruktur-bildenden Komponenten erforderlich.
- Das für eine Live-Migration genutzte Netz muss logisch von den anderen Netzen getrennt sein.
- Sämtliche virtuelle Maschinen müssen über eine redundante Anbindung an den Nord-Süd-Verkehr verfügen.

9 Management

Die Management-Umgebung ist eine besonders schutzbedürftige Umgebung, die durch die inhärente Zentralisierung deutlich an Bedeutung gewonnen hat und damit auch als Angriffsziel attraktiver geworden ist. Daher müssen zum Schutz der Management-Umgebung, abhängig von der aufgrund des Schutzbedarfs erforderlichen Separierung, folgende Maßnahmen umgesetzt werden:

- Trennung der Administration des Hypervisors von der Administration der Gast-Betriebssysteme.
- Kein Zugriff der Rolle „Gast-Betriebssystem-Administrator“ auf die Virtualisierungs-Management-Umgebung und umgekehrt.
- Logische Trennung der verschiedenen Administrations-Netze im physischen Administrations-Netz.
- Rollenbasierte Zugriffskontrolle (Nicht Personen-gebunden) für Administratoren.
- Jump Host oder physischer Extra-Host für den Zugriff auf die Management-Umgebung mit Mehr-Faktor-Authentisierung.
- Härtung und Absicherung des IT-Systems, auf dem die Management-Umgebung läuft.
- Patch-Zyklen festlegen, auch für ausgeschaltete VMs.
- Festlegen, welche Management-Schnittstellen und Werkzeuge verwendet werden.
- Nicht benötigte Management-Zugriffe auf allen Ebenen deaktivieren: Hardware, Hypervisor, VMs, Gast-Betriebssysteme.
- Auswertung und Überwachung des Loggings, Monitorings, der Intrusion Detection sowie der Lösung zur Verhinderung von Datenabfluss.
- Regelmäßige Sicherung von Konfigurationseinstellungen, auf allen Ebenen: Hardware, Hypervisor, VMs, Gast-Betriebssysteme, Management-Umgebung.

10 Erklärungen

Im Folgenden wird zu den oben verwendeten Begriffen eine kurze Erläuterung gegeben. Die Begriffe sind alphabetisch sortiert.

Wort	Erklärung
Bedarfsträger	Bedarfsträger können unterschiedliche Mandanten (Hosting-Szenarien), unterschiedliche Organisationseinheiten innerhalb eines Unternehmens oder einer Organisation oder unterschiedliche Verfahren sein.
data-at-rest	Daten auf der Speichereinheit (siehe auch [IT-GS SpL], A 23)
data-in-motion	Daten auf dem Transportweg (siehe auch [IT-GS SpL], A 23)

Wort	Erklärung
Gastwerkzeuge	Gastwerkzeuge bestehen in der Regel aus Dienstprogrammen und Gerätetreibern. Sie umfassen aus Sicherheitssicht kritische Funktionen wie eine Zwischenablage zwischen VMs oder VM und Host sowie Funktionen zur Grafikbeschleunigung.
RBAC	Role-based Access Control
VLAN-Trunk	Die Stelle, ab der VLANs gebündelt weitergeleitet bzw. aufgeteilt werden.
Jump Host	Gehärteter Host mit Zugriffskontrolle, der als Proxy zum gesicherten Verbindungsaufbau in eine Schutzzone verwendet wird.
LUN	Logical Unit Number, Adressierung eines logischen Bereichs eines Massenspeichers
LUN-Binding	LUN-Binding ordnet die jeweiligen LUNs einer RAID-Gruppe oder einem Festplattenpool zu. (siehe [IT-GS SpL], A 14 / A 26)
LUN-Masking	Bei LUN-Masking werden Zugriffstabellen auf dem Plattensubsystem definiert, in denen die eindeutigen WWN-Adressen der zugriffsberechtigten Server registriert sind. Alle anderen (maskierten) Platten sind für den Server unsichtbar. (siehe auch [IT-GS SpL], A 14 / A 26)
Management-Umgebung	Software, die die Virtualisierungsumgebung sowie die VMs verwaltet
Mandant	Ein Mandant stellt datentechnisch und organisatorisch eine abgeschlossene Einheit eines IT-Systems dar und strukturiert somit die Nutzung des Systems. Jeder Mandant kann nur seine Daten sehen und ändern. Innerhalb eines Mandanten kann eine weitere Aufteilung des Systems mit Hilfe von Benutzern realisiert werden.
Nord-Süd-Verkehr	Klassischer hierarchischer Netzverkehr
Ost-West-Verkehr	Netzverkehr zwischen virtuellen Maschinen sowie zwischen Virtualisierungsumgebungen für Techniken wie Live Migration
Soft-Zoning	Beim Soft-Zoning werden durch die Gruppierung der eindeutigen Bezeichner der SAN-Geräte Zonen gebildet. (siehe auch [IT-GS SpL], A 14 / A26) Diese Zonen werden in Abgrenzung zu dem oben beschriebenen Zonenkonzept Speicherzone genannt.
Switch	Physischer Switch
Virtueller Switch	Switch aus Software, z. B. bei VMware als separate Objekte im Speicher des Hypervisors realisiert.
VM	Virtuelle Maschine
VSAN (virtuelles SAN)	Analog zur Segmentierung von LANs in virtuelle Teilnetze (VLANs) ist auch die Segmentierung eines SANs in VSANs möglich. (siehe auch [IT-GS SpL], A 14 / A 26)
WWN	World Wide Name, hier ist der Name eines SAN-Geräts gemeint (entspricht ungefähr einer MAC-Adresse im Ethernet).
Zone / Zonenkonzept	Das Zonenkonzept beschreibt die Zonen einer IT-Infrastruktur. Eine Zone ergibt sich aus dem Schutzbedarf und der Art der verarbeiteten Daten und entspricht meist bestimmten Netzsegmenten. Die einzelnen Zonen selbst sind durch Paketfilter voneinander getrennt. Dabei können mehrere Zonen gleicher Art erstellt werden, die trotzdem voneinander separiert werden müssen. Bestandteil des Zonenkonzepts ist eine Kommunikationsmatrix, die erlaubte zonenübergreifende Verbindungen beinhaltet.

11 Literaturverzeichnis

IT-GS 200-2: BSI, BSI-Standard 200-2, https://www.bsi.bund.de/dok/10027850

IT-GS: BSI, IT-Grundschutz, https://www.bsi.bund.de/grundschutz

IT-GS SpL: BSI, Baustein Speicherlösungen Cloud Storage SYS.1.8
https://www.bsi.bund.de/dok/10095764