Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.19

Virtualisierung

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

Inhalt

I. Zweck

Diese Regelung definiert die notwendigen Sicherheitsanforderungen an virtualisierte Server- und Desktop-Umgebungen, die wiederum virtualisierte Netzwerke und virtualisierten Speicher nutzen (siehe Abbildung 1), um eine sichere Trennung der virtualisierten Umgebungen herzustellen .Des Weiteren werden zum einen Anforderungen an virtualisierte Anwendungen (Remote-Anwendungen) als eine Variante virtualisierter Server definiert, als auch Anforderungen für Private Clouds.

Die auf Hardwarepartitionierung basierte Virtualisierung und die Hypervisor-Virtualisierung sind als gleichwertig anzusehen. Dies bedeutet, dass die Regelungen für Hypervisor-Virtualisierung ebenfalls für die Hardwarepartitionierte-Virtualisierung gelten.

Hinweis. Techniken zu Trennung, wie sie in LINUX üblich sind, wie Container, Anpassung des Routings und der Zonen werden nicht berücksichtigt, da das Ziel dieser Regelung eine sichere Emulation physikalischer Server, Desktops, Speicher und Netzwerkkomponenten, als auch lokal installierter Anwendungen ist.

Im Sinne dieser Regelung bezeichnet der Begriff Informationssicherheit die IT-Sicherheit als Bestandteil der ganzheitlichen Informationssicherheit.

1. Überblick

Abbildung 1 gibt einen Überblick über eine virtualisierte Umgebung für Server und Desktops.

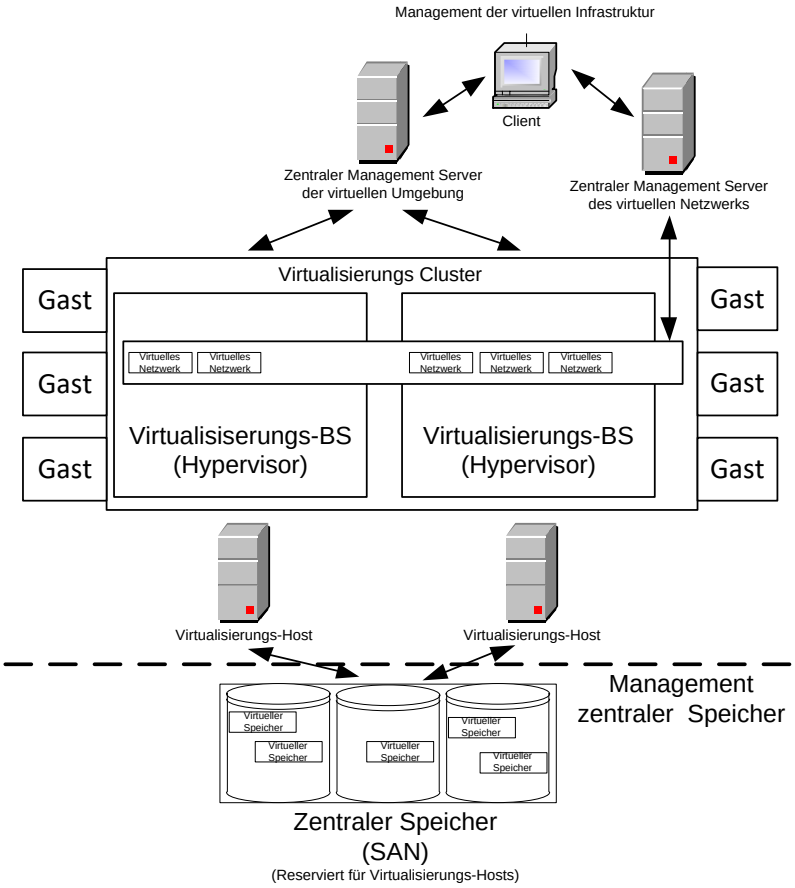

Abbildung 1 - Virtualisierte Umgebung für Sever und Desktops

Abbildung 2 gibt einen Überblick über eine virtualisierte Applikationsumgebung.

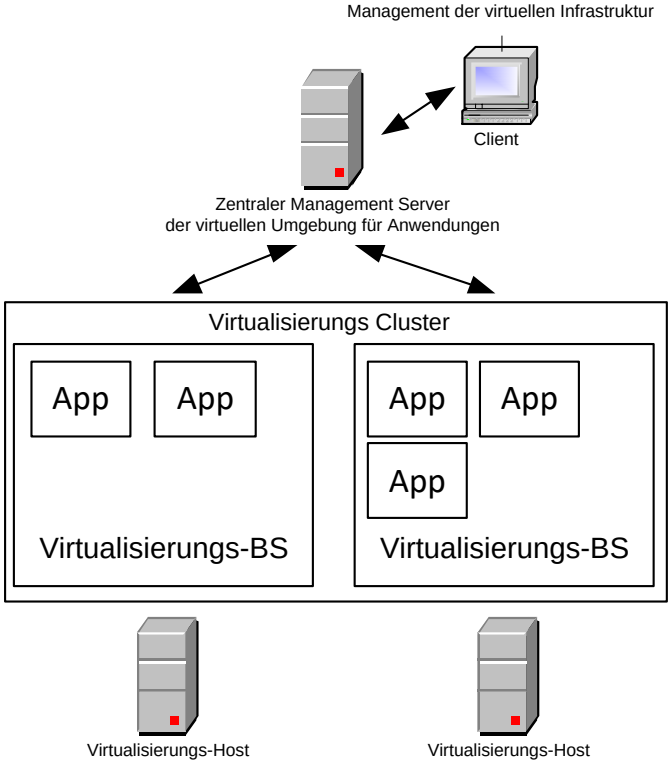

Abbildung 2 - virtualisierte Applikationsumgebung (App)

Wie aus den vorangegangenen Abbildungen ersichtlich, bestehen virtualisierte Umgebungen im Wesentlichen aus

- Virtualisierungs-Hosts,
- Virtualisierungs-Betriebssystemen / Hypervisor / Virtualisierungs-Software
- Virtualisierten Systemen / Gästen (Server und Desktops),
- Virtuellen Anwendungen (Apps, Remote-Anwendungen, Anwendungs-Virtualisierung
- Virtualisiertem Speicher (nicht bei Anwendungs-Virtualisierung),
- Virtualisiertem Netzwerk (nicht bei Anwendungs-Virtualisierung)[1],
- und dem Management der virtualisierten Umgebung

Wie in Abbildung 1 dargestellt, nutzen Desktop- und Server-Virtualisierung zentralen Speicher und stellen diesen ihren Gästen über die Virtualisierungs-Schicht zur Verfügung. Das Management der zentralen Speicherumgebung ist aber nicht Bestandteil dieser Regelung.

[1] Netzwerkkomponenten (z.B. Switche, und Firewalls) können im Hypervisor virtualisiert (emuliert) werden. Virtualisierte Netzwerkkomponenten sollten nicht mit VLANs verwechselt werden. VLANs teilen einen Switch in verschiedene logische Switche auf. Diese Trennung kann auf physikalischen und logischen Switchen genutzt werden.

2. Virtualisierte Systeme und Anwendungen im Allgemeinen

2.1. Ziel

Dieses Kapitel definiert die Anforderungen allgemein für alle Arten von Virtualisierung gelten. Diese sind:

- Virtualisierte Server und Netzwerke
- Virtualisierte Desktops
- Virtualisierter (Platten-)Speicher
- Virtualisierte Anwendungen

2.2. Verantwortlichkeiten

Für jede Komponente in einer virtuellen Infrastruktur muss eine verantwortliche Person oder eine Gruppe verantwortlicher Personen definiert werden, die für die Installation und den Betrieb der Umgebung gemäß den Regelungen verantwortlich ist. Komponenten der virtualisierten Infrastruktur sind:

- Virtualisierungs-Host / Hypervisor für Server, Desktops und Anwendungen,
- virtualisierte Maschinen / Gäste, Server
- virtualisierte Desktops / Gäste
- virtualisierte Anwendungen,
- virtualisierte Speicher,
- virtualisierte Netzwerkkomponenten,
- und die zu diesen Systemen notwendigen Managementsystemen

Die benannten Personen sind verantwortlich für die sichere Konfiguration der virtualisierten Infrastruktur und das zentrale Management der Virtualisierungsumgebung. Dies umfasst z. B. folgende Aufgaben:

- Die Administration und Bereitstellung von virtualisiertem Speicher für den Gast.
- Das Patch Management aller virtualisierten Infrastrukturkomponenten, insbesondere der Virtualisierungs-Hosts.
- Das Härten aller virtualisierten Infrastrukturkomponenten, insbesondere der Virtualisierungs-Hosts.
- Das Bereitstellen eines Virenschutzes.
- Das Aufsetzen von virtualisierten Maschinen, Desktops und Anwendungen.
- Die Administration von Benutzerkennungen für alle virtualisierten Infrastrukturkomponenten, insbesondere für die Virtualisierungs-Hosts und die zentralen Management-Systeme der Virtualisierungs-Infrastruktur.

2.3. Rollenkonzept

Ein Rollenkonzept ist notwendig, damit die Trennung zwischen einzelnen Funktionen, wie z.B. zwischen der Administration des Virtualisierungs-Hosts und des virtualisierten Netzwerks, gewährleistet ist. Welche der unten aufgeführten Rollen getrennt werden

müssen, hängt von der Sicherheitsklassifizierung der zu verarbeitenden Daten ab und ist individuell zu ermitteln. Es sind mindestens Rollen für die folgenden Funktionen zu definieren:

- Administration und Wartung der Virtualisierungs-Hosts für **Server**, inklusive der Zuweisung von virtualisiertem Plattenspeicher an die Gäste
- Administration und Wartung der Virtualisierungs-Hosts für **Desktops**, inklusive der Zuweisung von virtualisiertem Plattenspeicher an die Gäste
- Administration und Wartung der Virtualisierungs-Hosts für Anwendungen
- Administration und Wartung des virtualisierten Netzwerks
- Protokollierung hinsichtlich der virtualisierten Infrastruktur, um administrative Tätigkeiten nachweisen zu können
- Betrieb der Virtualisierungs-Hosts
- Betrieb von virtualisierten Netzwerkkomponenten

Die Administration der Virtualisierungs-Hosts für Server und Desktops umfasst auch das Anbinden von zentralem Speicher an den Virtualisierungs-Host. Dieser muss allerdings vorher durch die Administration der zentralen Speicher-Infrastruktur den Virtualisierungs-Hosts dediziert zugewiesen worden sein.

Sollten Speichernetzwerke (z. B. NAS) über herkömmliche LAN-Komponenten betrieben werden, muss die Administration, Wartung und der Betrieb dieser Netzwerke für Nicht-NAS und NAS getrennt sein (siehe auch Kapitel 4.3).

Das Rollenkonzept muss eine Aufteilung der Pflichten (Segregation of duties) sicherstellen (z.B. eingeschränkter Zugriff auf Log-Nachrichten, Einführung von Sub-Administratoren, zusätzliche Audits und Kontrollmechanismen für Super-Administratoren). Die Rollen müssen regelmäßig auditiert werden.

2.4. Prozesse

Etablierte Prozesse und Anforderungen für die physikalische Infrastruktur gelten auch für virtualisierte Umgebungen. Erweiterungen zu diesen Prozessen und Anforderungen sind in den folgenden Kapiteln für die verschiedenen Virtualisierungstypen beschrieben.

2.5. Härtung

Alle virtualisierten Komponenten müssen gehärtet werden. Für die virtualisierten Gäste gelten die Regelungen für die jeweiligen Betriebssysteme[2]. Zusätzlich sind die Herstellerempfehlungen zu beachten.

[2] Siehe Anhang A.1.2, A.1.9, A.1.10 und Kapitel 3.6, 4.7

2.6. Management der virtualisierten Infrastruktur

Das Management der virtualisierten Infrastruktur muss auf Basis des "Need-to-Know"-Prinzips erfolgen. Daher müssen neben dem Rollenkonzept[3] und den Vorgaben der Regelung Access- und Identitymanagement[4] folgende weitere Regeln eingehalten werden:

- Die Management-Konsolen müssen auf die notwendigen Dienste eingeschränkt werden.
- Die Management-Konsolen müssen auf die notwendigen Netzwerkadressen eingeschränkt werden.
- Die Management-Konsolen müssen in einem eigenen VLAN betrieben werden.
- Die Authentifizierung an die zentralen Management Systeme hat über einen zentralen Authentifizierungsdienst zu erfolgen.[5]

2.7. Monitoring und Protokollierung

- Die virtualisierte Umgebung muss gemäß den Regelungen für Monitoring[6] und Protokollierung[7] überwacht und protokolliert werden.
- In einer virtualisierten Umgebung müssen zusätzliche Ereignisse protokolliert werden. Diese sind:
  - Zugriff, erfolgreich und erfolglos, von privilegierten Benutzerkennungen auf das Management bzw. die Management-Konsolen der virtualisierten Infrastruktur.
  - Alle sicherheitsrelevanten Aktionen, die durch diese Benutzerkennungen in der virtualisierten Infrastruktur durchgeführt werden.
- Protokollierungsdateien der Virtualisierungs-Hosts müssen gemäß der "Monitoring und Protokollierung" Regelung[8] zentral gespeichert und ausgewertet werden.
- Diese Auswertung[9] muss unter anderem gewährleisten, dass die Pflichtentrennung bei administrativen Tätigkeiten in der virtualisierten Umgebung gemäß dieser Regelung durchgesetzt ist und dem Rollenkonzept entsprechen.
- Auf allen virtualisierten Systemen ist die Zeitsynchronisation zu gewährleiten.

2.8. Notfallplanung und Datensicherung[10]

- Virtualisierte Umgebungen konzentrieren IT-Dienste auf wenige Hochleistungskomponenten, die durch eine große Anzahl von Benutzern verwendet werden. Auch um das Schutzziel Verfügbarkeit in virtualisierten Umgebungen erreichen zu können, müssen bestehende Konzepte und Notfallpläne an die virtuellen

[3] Siehe Kapitel 2.3

[4] Siehe Anhang A.1.11

[5] Siehe Anhang A.1.13

[6] Siehe Anhang A.1.3

[7] Siehe Anhang A.1.3

[8] Siehe Anhang A.1.3

[9] Siehe Anhang A.1.11

[10] Siehe Anhang A.1.12

Gegebenheiten angepasst werden. Das gilt insbesondere auch für Datensicherungskonzepte[11].

[11] Siehe Anhang A.1.4

3. Virtualisierte Server und Netzwerke, virtuelle Desktops und Remote-Anwendungen

3.1. Ziel

In diesem Kapitel werden Regeln für den sicheren Betrieb von virtualisierten Servern und Netzwerken, sowie virtuellen Desktops (auch bekannt als virtuelle Desktop-Infrastruktur oder Desktop-Virtualisierung) als auch Remote-Anwendungen definiert.

3.2. Abgrenzung

3.2.1 Server- und Netzwerk-Virtualisierung

Virtualisierte Server sind ähnlich zu virtualisierten Desktops. Bei beiden werden auf dem Virtualisierungs-Host-Betriebssystem virtualisiert. Hierbei spielt es für den Virtualisierungs-Host keine große Rolle, ob es ein Server- oder ein Workstation-Betriebssystem virtualisieren muss. Unterschiedlich ist allerdings die Nutzung. Bei virtualisierten Desktops wird dem konsumierenden Client der Bildschirminhalt des virtualisierten Desktops übertragen, bei der Virtualisierung von Servern ist dies gegebenenfalls sogar unerwünscht. Hier werden die Dienste, die ein Server zur Verfügung stellt, von Desktops und anderen Diensten genutzt.

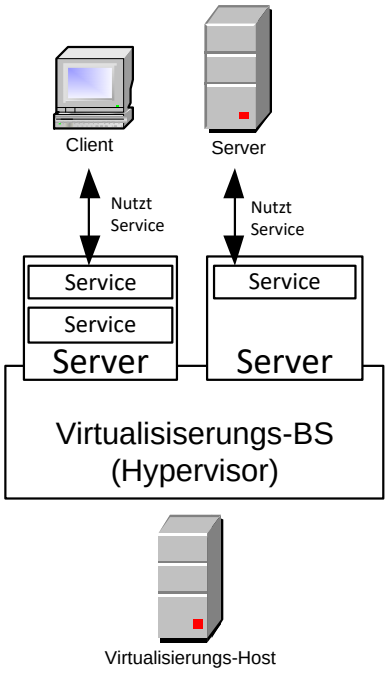

Abbildung 3 - Virtualisierte Server

3.2.2 Virtualisierter Desktop (Infrastruktur, Desktop Virtualisierung)

Virtualisierte Desktops sind in Teilen virtualisierten Servern sehr ähnlich, nur anstatt Servern werden auf den Virtualisierungs-Hosts Desktops für Benutzer, teilweise dynamisch erst bei Anfrage durch den Client, zur Verfügung gestellt. Hier sind je nach Hersteller zahlreiche Varianten möglich. Dies reicht von zentralen virtualisierten Desktops, die einem Nutzer autark zur Verfügung stehen, bis hin zu replizierten virtualisierten Desktops, wo sich mehrere Benutzer eine Basis teilen müssen. Bei Desktop-Virtualisierung erfolgt der Zugriff über Clients, die nur den Bildschirminhalt vom Virtualisierungs-Host und die Tastatur- und Mauseingaben zum Virtualisierungs-Host bzw. zum virtualisierten Desktop übertragen.

Clients für diese Funktionen können auf normalen Desktops, auf Thin Clients oder auch auf Smartphones installiert und genutzt werden. Auch Offline-Fähigkeit oder das Einbeziehen von Anwendungs-Virtualisierung sind mit der Desktop-Virtualisierung möglich.

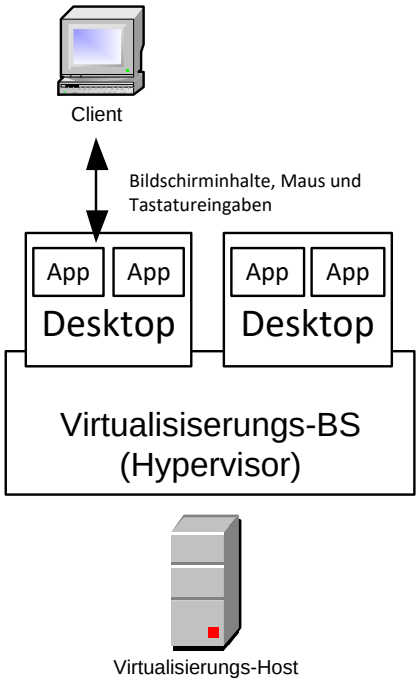

Abbildung 4 - Desktop - Virtualisierung

3.2.3 Remote-Anwendungen

Virtualisierte Anwendungen sind in Teilen ähnlich virtualisierten Desktops. Sowohl virtualisierte Anwendungen als auch virtualisierte Desktops werden auf Virtualisierungs-Hosts betrieben. Bei beiden Verfahren wird nur der Bildschirminhalt zum Client hin übermittelt. Bei der Anwendungs-Virtualisierung muss sich allerdings der Benutzer das darunterliegende Betriebssystem (z.B. Terminal Server) mit anderen Benutzern teilen, was bei der Desktop-Virtualisierung gewöhnlich nicht der Fall ist. Als Clients können neben normalen Desktops auch Thin Clients oder Smartphones verwendet werden. Auch eine Offline-Fähigkeit von virtualisierten Anwendungen ist möglich.

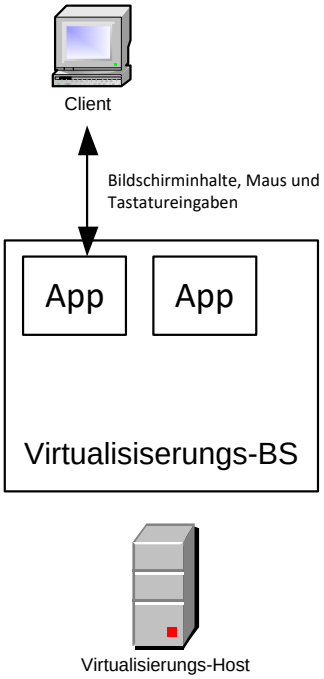

Abbildung 5 - Virtualisierte Anwendungen

3.3. Virtualisierungs-Host und Betriebssystem

Es sollte ein schlankes Virtualisierungs-Betriebssystem genutzt werden, dass nur die notwendigen Komponenten enthält, die für den Betrieb freigegeben sind.

Die Virtualisierungs-Hosts müssen für die notwendigen Sicherheitsklassen[12] freigegeben sein. Für jede Klasse muss ein separates virtuelles Netzwerk mit einem eigenen internen VLAN exklusiv verwendet werden. Die Kommunikation zwischen Sicherheitsstufen muss in einem Sicherheitskonzept dokumentiert werden. Die höchste Sicherheit kann erreicht werden, wenn pro Virtualisierungs-Host nur eine Sicherheitsklasse zugelassen ist.

Alle Gäste (Server und Desktops) und Remote-Anwendungen eines Virtualisierungs-Hosts müssen Mitglied der zugelassen Sicherheitsklasse bzw. -klassen sein.

Alle Virtualisierung-Hosts müssen ein internes VLAN für die Kommunikation zwischen den Virtualisierung-Host exklusiv verwenden.

Das Servermanagement der Virtualisierungs-Hosts muss ein dediziertes VLAN verwenden.

Die Zugriffsberechtigungen auf das Virtualisierungs-Host-Betriebssystem mittels der Management-Konsole müssen gemäß des "Need-to-know"-Prinzips eingeschränkt und der Zugriff auf Netzwerkebene z.B. durch Firewalls abgesichert werden.

Generell müssen auch die Regelungen zur Zonierung[13] eingehalten werden.

---

[12] Siehe Anhang A.1.5

[13] Siehe Kapitel 3.10

Erweiterte Virtualisierungsmöglichkeiten wie Fehlertoleranz, Hochverfügbarkeit oder das Migrieren von Gästen im Betrieb von einem Virtualisierungs-Host auf einen anderen oder der Betrieb von Remote-Anwendungen auf verschiedenen Virtualisierungs-Host, müssen wie vom Hersteller empfohlen implementiert werden und in einem Virtualisierungs-Konzept detailliert dargestellt werden.

Um eine ausreichende Ausfallsicherheit gewährleisten zu können, sind die Virtualisierungs-Hosts in redundanten Rechenzentren zu betreiben.

Ein Einsatz von zertifizierten Hypervisoren (z.B. Common Criteria mindestens EAL 4) sollte bei hoher Vertraulichkeit vorgeschrieben werden.

Virtualisierte Server und Desktops müssen auf getrennten Virtualisierungs-Hosts betrieben werden.

3.4. Virtualisierte Server (Gäste), virtualisierte Desktops (Gäste) und Remote-Anwendungen

Virtualisierte Server, virtualisierte Desktops und Remote-Anwendungen müssen einer Sicherheitsklasse zugeordnet werden. Ausnahmen können für spezielle Management-Server gemacht werden, die virtualisierte Switche verwalten und dadurch mehreren Sicherheitsklassen angehören können.

Jeder Gast bzw. jede Remote-Anwendung muss einer Sicherheitsklasse des Virtualisierungs-Hosts entsprechen. Die Kommunikation des Gastes muss für diejenige Netzwerkzone limitiert werden, die für die Sicherheitsklasse der Gäste entsprechend spezifiziert wurde.

Eine Kommunikation von Gast zu Gast ausschließlich über den Hypervisor unter Nutzung eines virtualisierten Netzwerkes ist für virtuelle Desktops verboten und nur dann erlaubt, wenn die virtualisierten Server über dasselbe VLAN kommunizieren.

Die direkte Gast-zu-Gast-Kommunikation unter Umgehung von LANs und VLANs (z.B. mit VMwares Virtual Machine Communication Interface (VMCI)) ist untersagt.

Werden virtualisierte Gäste zwischen Virtualisierungs-Hosts verschoben, muss die Gast-Klassifizierung stets der Klassifizierung des Virtualisierungs-Hosts entsprechen.

Gäste, die zur Verwaltung der Virtualisierungsumgebung dienen, dürfen auf den Virtualisierungs-Hosts betrieben werden, selbst wenn sie zu unterschiedlichen Netzwerkzonen mit unterschiedlichen Klassifizierungen verbunden werden müssen.

Werden virtualisierte Desktops dynamisch auf Virtualisierungs-Hosts gestartet, muss die Gast-Klassifizierung stets der Virtualisierungs-Host-Klassifizierung entsprechen.

Für den Einsatz von Remote-Anwendungen muss ein Konzept erstellt werden, das abhängig von der Sicherheitsklasse folgende Aspekte regelt:

- Detaillierte Härtungsmaßnahmen (siehe auch Kapitel 3.6) und notwendige Sicherheitskonfigurationen
- Verschlüsselung der Kommunikation
- Erlaubte Clients

- Erlaubte Dienste am Client (z.B. Laufwerksverbindungen, Zwischenablage zwischen Client und Virtualisierungs-Host)
- Welche Dienste müssen auf welchen Servern betrieben werden, insbesondere welche Dienste
  - sind erlaubt oder verboten (z.B. Shadowing von Sessions)
  - sind als kritisch zu bewerten (z.B. Lizenzierung, Konfigurations-Datenbank).
  - müssen auf getrennten Servern betrieben werden (z.B. Benutzer- / Server-spezifische oder kritische / unkritische Dienste)
- Notwendige Protokollierungsmaßnahmen

Der anonymisierte Zugriff auf virtualisierte Anwendungen muss unterbunden werden.

3.5. Prozesse

Für virtualisierte Umgebungen ist sicher zu stellen, dass

- Server- und Desktop-Gäste, als auch Remote-Anwendungen der korrekten Sicherheitsklasse[14] zugeordnet werden,
- Server-Gäste untereinander über den Hypervisor und das Netzwerk kommunizieren
- Desktop-Gäste nicht untereinander kommunizieren
- die die Trennung der Rollen gemäß Kapitel 2.3 eingehalten wird.

Der Einfluss und das Risiko, dass von einem Sicherheitsvorkommnis auf einem Server- oder Desktop-Gast auf andere Gäste desselben VLANs bzw. Virtualisierungs-Hosts ausgeht muss vor der Implementierung bewertet werden. Entsprechende Maßnahmen müssen abgeleitet werden (z.B. kann ein Virenfund auf einem Gast Full-Scan auf allen anderen Gästen des Vitualisierungs-Hosts notwendig machen).

Dem Patch-Management-Prozess[15] muss gegebenenfalls für virtualisierte Systeme erweitert werden und zusätzlich folgende virtualisierte Infrastrukturkomponenten betrachten:

- Virtualisierungs-Host/-Hypervisor für Server, Desktops und Remote-Anwendungen
- Jede(n) virtualisierte(n) Maschine/Gast/Server/Remote-Anwendungen
- Software mit dem der Client auf die virtualisierte Anwendung zugreift
- Virtualisierte Netzwerkkomponenten
- Alle dazu notwendigen Managementsysteme
- Weitere Systeme bzw. Dienste, die für den Betrieb der Virtualisierungs-Infrastruktur wie z.B. Applikation Server, Lizenz Server, Broker und Master Image Server notwendig sind,.

3.6. Härtung

Folgende Server-Virtualisierungskomponenten müssen gehärtet werden:

- Hypervisor (Betriebssystem des Virtualisierungs-Hosts)

[14] Siehe Anhang A.1.5

[15] Siehe Anhang A.1.7

- Betriebssystem des Virtualisierungs-Hosts für Remote-Anwendungen
- Virtualisierte Netzwerkkomponenten (z.B. software-emulierte Switche oder Firewalls)
- Virtualisierte Management-Server und Konsolen für den Hypervisor und das virtualisierte Netzwerk
- Weitere Systeme bzw. Dienste, die für den Betrieb der Virtualisierungs-Infrastruktur wie z.B. Applikation Server, Lizenz Server, Broker und Master Image Server notwendig sind.
- Software mit dem der Client auf die virtualisierte Anwendung zugreift

Sollte die Virtualisierungs-Software (Hypervisor) auf einem weiteren Betriebssystem installiert sein, so muss dieses zusätzlich gehärtet werden.

Virtualisierte Gäste müssen ebenfalls gehärtet werden[16].

Das Ausbrechen aus virtualisierten Anwendungen und somit der Zugriff auf beliebige anderer Serveranwendungen ist auf nicht gehärteten Anwendungs-Virtualisierungssystemen, relativ leicht zu bewerkstelligen. Als wirksamer Schutz z.B. unter dem Betriebssystem Windows Server 2008, muss der Einsatz von Software Restriction Policies bzw. AppLocker in Erwägung gezogen werden. Auch das Einschränken von Zugriffsrechten im Dateisystem muss als Schutzmaßnahem in Betracht gezogen werden. Besonders berücksichtigt werden müssen dabei Anwendungen, die für das Management der Anwendungs-Virtualisierungs-Umgebung notwendig sind.

Die Härtungshinweise des Herstellers der Virtualisierungs-Software müssen berücksichtigt werden.

Details zu Härtung können der Regelung System Security entnommen werden.[17]

3.7. Virenschutz

Ein Virenschutz muss entsprechend der in der Regelung System Security beschriebenen Anforderungen implementiert werden.[18]

3.8. Image und Snapshot Management

- Der Zugriff auf Virtualisierungs-Dateien (wie z.B. Swap, Sleep Mode, Disk, Image und Snapshot Dateien) muss beschränkt werden wie im Rollenkonzept[19] definiert.
- Der Zugriff auf Backups von Virtualisierungs-Dateien (wie z.B. Swap, Sleep Mode, Disk, Image und Snapshot Dateien) muss beschränkt werden.
- Snapshots können zwar für den Backup von Gästen hilfreich sein, sie sind aber für sich selbst genommen kein Ersatz für einen Backup.

[16] Für weitere Informationen siehe Anhang A.1.2

[17] Siehe Anhang A.1.2

[18] Siehe Anhang A.1.2

[19] Siehe Kapitel 2.3

3.9. Monitoring und Protokollierung

In einer virtualisierten Serverumgebung müssen zusätzliche Ereignisse protokolliert werden. Diese sind:

- Starten, Stoppen, das In-den-Ruhezustand-bringen und das Herunterfahren von virtualisierten Servern
- Ändern, neu zur Verfügung stellen und Außerdienststellen von virtualisierten Master-Desktops
- Snapshots und Wiederherstellung von Snapshots von virtualisierten Servern
- Konfigurationsänderungen an Virtualisierungs-Hosts und virtualisierten Netzwerken sowie an anderen Servern, die für den Betrieb der Virtualisierungs-Infrastruktur notwendig sind
- Der regelungskonforme Netzwerkanschluss aller Virtualisierungs-Hosts und Gäste entsprechend der Festlegungen in dieser Regelung
- Änderungen an wichtigen Dateien des Betriebssystems des Virtualisierung-Hosts.

Leistungseigenschaften von virtualisierten Servern müssen überwacht werden, damit auf Engpässe zeitnah reagiert werden kann.

3.10. Netzwerkvirtualisierung und Zonierung

Die Segmentierung von Netzwerken trägt unter Anderem zur Erhöhung der Verfügbarkeit, der Integrität und der Vertraulichkeit bei. Die Einteilung einer IT-Infrastruktur in verschiedene Sicherheitszonen muss basierend auf dem Architekturstandard des Konzerns zu „sicheren Umgebungen“[20] und den entsprechenden spezifischen, dokumentierten Implementierungs-konzepten für den Konzern erfolgen. Die Zuweisung von Systemen zu Sicherheitszonen muss nach einem standardisierten Prozess erfolgen, der die Sicherheitsanforderungen und Datenklassifizierung[21] berücksichtigt[22].

Die verwendeten Infrastrukturkomponenten müssen dem Book of Standards folgen[23].

3.10.1 Logische Segmentierung

Logische Netzwerksegmentierung ist zulässig, wenn die folgenden Bedingungen erfüllt werden:

- Die physischen Netzwerkkomponenten verarbeiten nur internen Verkehr oder nur externen Verkehr. Es ist nicht zulässig, dass eine Netzwerkkomponente sowohl internen als auch externen Verkehr verarbeitet.

[20] Siehe Anhang A.1.6

[21] Siehe Anhang A.1.5

[22] Siehe Anhang A.1.14

[23] Siehe Anhang A.1.15

- Verkehr von oder zu Sicherheitszonen wird gemäß der Datenklassifizierung und dem Implementierungskonzept mindestens von einem Filter (host- oder netzwerkbasiert) kontrolliert.

3.10.2 Physikalische Segmentierung

Physikalische Segmentierung ist zwischen externen Bereichen (wie Partnernetzwerken oder Internet) und internen Bereichen erforderlich.

Physikalische Segmentierung ist notwendig, um internen und externen Verkehr zu trennen.

Nur Sicherheitsgateways dürfen auf einem Gerät interne und externe Verkehrsströme verarbeiten[24].

[24] Zum Anschluss der Infrastruktur einer Instanz zum CBB (entsprechend Modul 12 Secure Environments) kann die Funktion des Sicherheitsgateways durch den CBB Router übernommen werden.

4. Virtueller Speicher

4.1. Ziel

In diesem Kapitel werden die Anforderungen an virtualisierten Speicher definiert. Das Management einer zentralen Speicherumgebung ist nicht Teil dieser Regelung[25].

4.2. Abgrenzung

Virtualisierter Speicher basiert auf physikalischen Speichersystemen. Eine virtuelle Speichereinheit kann sich aus verschiedenen physikalischen Speicherplätzen auf verschiedenen Speichersystemen zusammensetzen (siehe Abbildung 6). Speichersysteme sind mit den Servern (z.B. Virtualisierungs-Hosts) durch Storage Area Networks (SAN) verbunden. Der Speicher wird den Gästen durch den Virtualisierungs-Host zugewiesen, den dieser wiederum über Speichernetzwerke auf zentralen Speichersystemen zur Verfügung gestellt bekommt.

[25] Für weitergehende Informationen siehe A.1.4

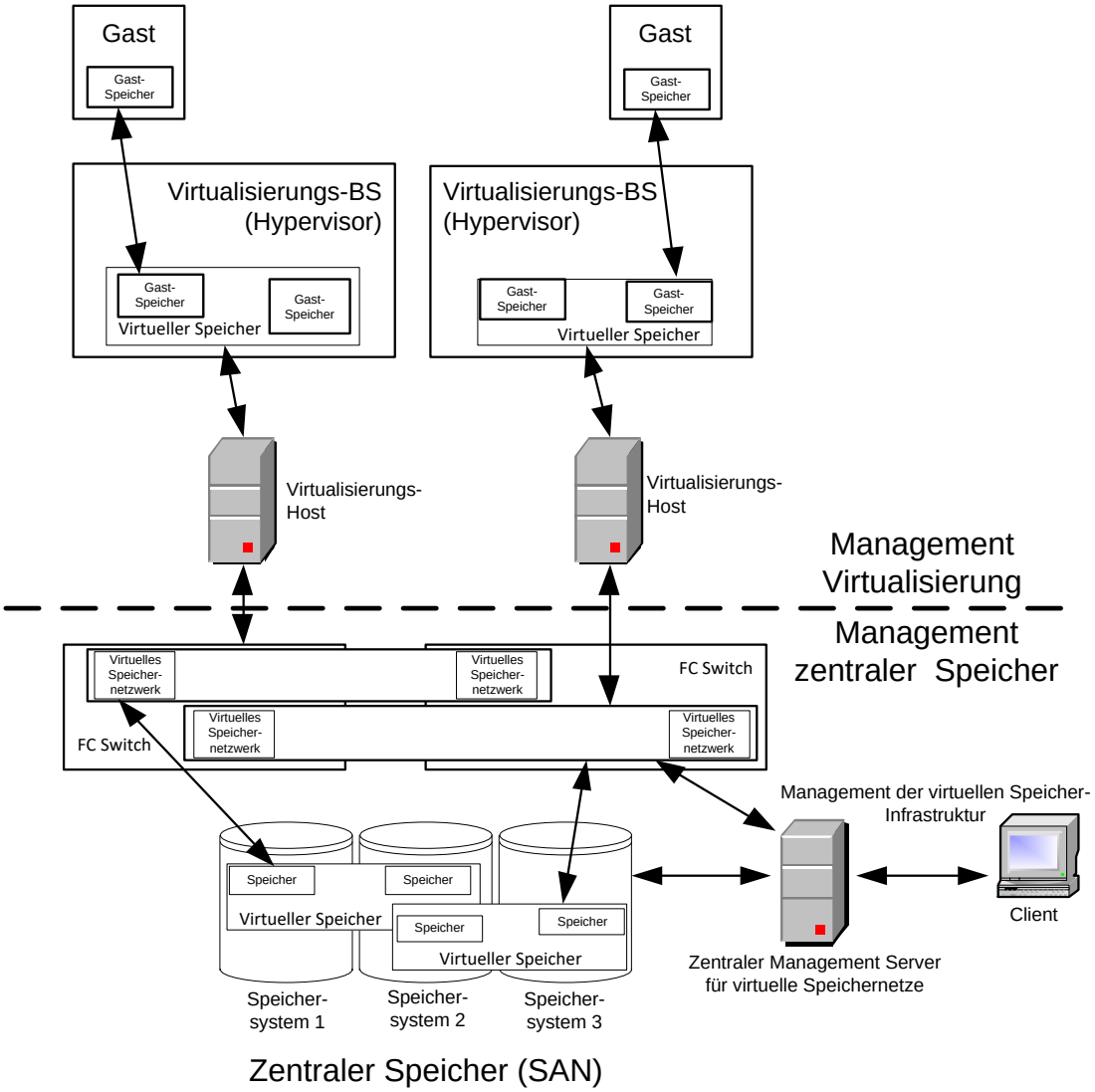

Abbildung 6 - Speichervirtualisierung

Wie in Abbildung 6 dargestellt, nutzen Virtualisierungs-Hosts zentralen Speicher und stellen diesen ihren Gästen virtualisiert zur Verfügung.

4.3. Plattenspeicher für die Virtualisierungs-Hosts

Die Administration des zentralen Speichers legt mit Hilfe des Speicher-Managements fest, welche Speicher-Pools den Virtualisierungs-Hosts zugewiesen werden. Die Zuweisung hat nach dem "Need-to-Know"-Prinzip zu erfolgen.

Die Sicherheitsklassen[26] des Virtualisierungs-Hosts müssen auf den durch die Virtualisierungs-Hosts verwendeten Speichersystemen und Speichernetzen zugelassen sein. Die höchste Sicherheit kann erreicht werden, wenn pro Speichersystem und Speichernetzwerk nur eine Sicherheitsklasse zugelassen ist.

[26] Siehe Anhang A.1.5

In einem Konzept für die zentrale Speicher-Infrastruktur muss abhängig von der Sicherheitsklasse festgelegt werden, welche Maßnahmen hinsichtlich der Authentifizierung und der Verschlüsselung bei der Nutzung von Speichersystemen und Speichernetzen notwendig sind und inwieweit verschiedene Sicherheitsklassen auf physischen oder virtualisierten Umgebungen kombiniert oder separiert werden müssen.

Plattenplatz auf Speichersystemen für unterschiedliche Konsumenten müssen voneinander isoliert werden. d.h. das Speichernetzwerk muss so konfiguriert sein, dass

- der Virtualisierungs-Host nur auf den Speicherbereich zugreifen kann, den dieser auch nutzen soll und
- kein anderes System auf diesen Speicherbereich zugreifen darf, außer es ist konzeptionell notwendig. (z.B. bei Clusterlösungen, Backup, etc.).

Weiter muss die Regelung zur Datensicherung berücksichtigt[27] werden.

Es wird empfohlen SAN-basierten Speicher zu verwenden. NAS ist nur erlaubt, wenn

- die Netzwerke für Nicht-NAS und NAS physikalisch getrennt sind und
- die Pflichten für die Administration, Wartung und Betrieb von Netzwerken für Nicht-NAS-Speicher und NAS getrennt sind (siehe auch Kapitel 2.3, Rollenkonzept und Kapitel 4.5, Rollen).

4.4. Gast-Plattenspeicher

Der Virtualisierungs-Host legt fest, welche Speicher-Pools den Gästen zugewiesen werden. Die Zuweisung hat nach dem "Need-to-Know"-Prinzip zu erfolgen.

4.5. Rollen

Die Rollen, die die zentrale Speicher-Infrastruktur benötigt, gehen über die bereits in Kapitel 2.3 erwähnten Rollen hinaus. Die zusätzlichen Rollen werden für die Speicher-Infrastruktur benötigt. Werden Speicher-Infrastrukturen basierend auf NAS eingesetzt, sind die Anmerkungen in Kapitel 4.3 zu beachten. Diese Rollen sind nicht im Geltungsbereich dieser Richtlinie. Die entsprechenden Regeln werden in der Richtlinie für zentrale Speicher-Infrastrukturen behandelt.

4.6. Prozesse

Es muss sichergestellt werden, dass Virtualisierungs-Hosts und Gästen nur derjenige Plattenplatz zugeordnet werden kann, der für den jeweiligen Virtualisierungs-Host bzw. Gast zulässig ist.

4.7. Härtung

Die entsprechenden Regeln werden in der Richtlinie für zentrale Speicher-Infrastrukturen[28] behandelt.

[27] Siehe Anhang A.1.4

[28] Siehe Anhang A.1.4

4.8. Virenschutz

Das Virenschutzkonzept für virtualisierte Umgebungen muss kompatibel zum eingesetzten zentralen Plattenspeicher sein. Gegebenenfalls muss geprüft werden, ob statt eines Gäste- oder Virtualisierungs-Host-basiertem Virenschutzes ein Speichersystem-basierter Virenschutz zum Einsatz kommen soll.

4.9. Management der virtualisierten Speicher-Infrastruktur

Soweit der Virtualisierungs-Host den zugewiesen virtualisierten Speicher verwaltet, ist dies Bestandteil des Virtualisierungs-Managements. Das Management der zentralen Speichersysteme hat hiervon getrennt zu erfolgen (siehe Abbildung 6) und muss in einer eigenen Richtlinie für zentrale Speicher-Infrastrukturen[29] festgelegt werden.

Das Management der virtualisierten Speicher-Infrastruktur muss auf Basis des "Need-to-Know"-Prinzips durchgeführt werden.

4.10. Monitoring und Protokollierung

In einer virtualisierten Serverumgebung müssen folgende Parameter überwacht werden

- Leistungseigenschaften des zentralen Plattenspeichers, der den Virtualisierungs-Hosts zugewiesen wurde
- virtualisierter Plattenspeicher, der den einzelnen Gästen zugewiesen wurde.

Dies erlaubt die zeitnahe Reaktion auf Engpässe.

[29] Siehe Anhang A.1.4

II. Verantwortlichkeiten

II.I Kapitel 1: Überblick

Diese Regelung ist von allen Betreibern von virtualisierten Umgebungen anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.II Kapitel 2: Virtualisierte Systeme und Anwendungen im Allgemeinen

Diese Regelung ist von allen Betreibern von virtualisierten Umgebungen anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.III Kapitel 3: Virtualisierte Server und Netzwerke, virtuelle Desktops und Remote-Anwendungen

Diese Regelung ist von allen Betreibern von virtualisierten Servern und Netzwerken anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

II.IV Kapitel 4: Virtueller Speicher

Diese Regelung ist von allen Betreibern von virtualisierten Umgebungen anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

.

Anhang

A. Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheit Regelung Nr. 03.01.16 Dienstleistung durch Dritte

A.1.2 Informationssicherheit Regelung Nr. 03.01.01 Anti Malware & Systemschutz

A.1.3 Informationssicherheit Regelung Nr. 03.01.04 Sicherheitsprotokollierung und -monitoring

A.1.4 Informationssicherheit Regelung Nr. 03.01.06 Backup und Archivierung

A.1.5 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

A.1.6 Sichere Umgebungen, TAP03: http://it-apf.vw.vwg/

A.1.7 Informationssicherheit Regelung Nr. 03.01.08 Change- und Patch-Management

A.1.8 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.9 Informationssicherheit Regelung Nr. 03.03.01 Server

A.1.10 Informationssicherheit Regelung Nr. 03.03.02 Clients

A.1.11 Informationssicherheitshandlungsleitlinien für Systembetreiber und Administratoren

A.1.12 Informationssicherheit Regelung Nr. 03.01.14 IT Service Continuity Management

A.1.13 Informationssicherheit Regelung Nr. 03.01.05 Authentifizierung und IAM

A.1.14 sADM-Prozess (innerhalb der Volkswagen AG)

A.1.15 Book of Standards

A.2 Referenzen zu Standards

Die folgende Tabelle zeigt die Referenzen zu den Standards ISO/IEC 27001:2013, ISO/IEC 27001:2005 und VDA.

Thema	Kapitel	ISO 27001:2013	ISO 27001:2005	VDA
		-	-	-

A.3 Anlagen

A.3.1 Anlage 1 Feedbackformular

Das Feedbackformular für Änderungsvorschläge zu Regelungen kann von der MyNet-Webseite Gesellschaften → Audi Brussels → Organisation → Finanz (B/F) → IT (B/FP) → IT-Sicherheit → Regelwerk heruntergeladen werden.

Das Feedback-Formular ist folgendermaßen auszufüllen:

Die Spalten 2 bis 6 müssen für jede vorgeschlagene Änderung ausgefüllt werden. Änderungen, für die nicht alle Spalten 2 bis 6 ausgefüllt sind, werden automatisch ohne weitere Prüfung abgelehnt.

Spalte 3: Folgende Kommentararten sind möglich: a=allgemein, f=fachlich, r=redaktionell

Spalte 4: Bitte bisherigen Text, Tabelle oder Bild einfügen

Spalte 5: Bitte vollständig umformulierten Text, geänderte Tabelle oder geändertes Bild einfügen

Spalte 6: Bitte begründen Sie die gewünschte Änderung möglichst ausführlich.

Bitte senden Sie das ausgefüllte Formular an: it-security.audibx@audi.de

A.4 Quellen und Referenzen

A.4.1 Bundesamt für Sicherheit in der Informationstechnik, BSI IT-Grundschutz Kataloge, 13. Ergänzungslieferung 2013.

A.4.2 Gefährdungen und Gegenmaßnahmen beim Einsatz von VCE Vblock für das Bundesamt für Sicherheit in der Informationstechnik von EMC², VMware und Cisco, Dezember 2011.

A.4.3 Guide to Security for Full Virtualization, NIST SP 800-125, January 2011.

A.5 Abkürzungen und Definitionen

Abkürzung	Definition
Virtualisierungs-Host	Die Hardware auf dem das Virtualisierungs-Betriebssystem installiert wird
Hypervisor	Das Virtualisierungs-Betriebssystem, das es für Server-, Desktop- und Anwendungs-Virtualisierung gibt.
Virtualisierte Maschine	Allgemeiner Begriff für virtualisierte Server. Allgemein auch Gast genannt.
Virtualisierter Desktop	Allgemein auch Gast genannt
Virtualisierte Anwendung	Anwendungen, die zentral auf dem Virtualisierungs-Host zur Verfügung gestellt werden.
Virtualisierter Speicher	Speicher der durch das Virtualisierungs-Betriebssystem dem Gast zugewiesen wird
Virtualisierte Netzwerkkomponenten	Virtualisierte Netzwerkkomponenten, die entweder komplett im Hypervisor virtualisiert werden oder die über ein oder mehrere externe Netzwerkkomponenten gebildet werden.
Virtualisiertes LAN (VLAN)	Trennt die Ports eines Switches (Layer2) in Domänen voneinander. Der Hypervisor stellt diese Trennung mit Hilfe virtueller Switches (vSwitch) dar.
EAL	Evaluation Assurance Level
ESX und ESXi	Virtualisierungs Software von VMware
FC	Fibre Channel
NAS	Network-Attached Storage (dt. netzgebundener Speicher)
NIST	National Institute of Standards and Technology
SAN	Storage Area Network
VCE Vblock	Virtualisierte Einheit von VMware, Cisco und EMC²
Sicherheitsgateway	Ein Sicherheitsgateway ist ein System aus Software- und Hardwarekomponenten zur sicheren Verbindung von IT-Netzwerken (z. B. einige IT-Systeme mit verschiedenen Aufgaben wie Paketfilterung, Virenschutz oder Überwachung von Netzwerkverkehr).
Sicherheitszone	Eine Sicherheitszone ist ein IP-Netzwerk, das aus Sicherheitsgründen von anderen

	Netzwerken der IT-Infrastruktur eines Standorts des Audi Konzerns getrennt ist. Kommunikation von und/oder zu einer Sicherheitszone wird durch Sicherheitsmaßnahmen kontrolliert und ist möglicherweise an einem sogenannten Zugriffspunkt für die Sicherheitszone eingeschränkt. Es besteht keine Verpflichtung dazu, dass jede Sicherheitszone einen dedizierten Zugriffspunkt verwendet. Ein Zugriffspunkt kann eine beliebige Anzahl von Sicherheitszonen bereitstellen. Dies ermöglicht die Erstellung zentraler Zugriffspunkte, z. B. über zentralisierte, standortspezifische Sicherheitsgateways. Geräte innerhalb einer Sicherheitszone können miteinander vollständig auf Netzwerkebene kommunizieren.

A.6 Gültigkeit

Diese Regelung ist mit der Veröffentlichung sofort gültig.

Bereits bestehende Ausnahmeregelungen sind spätestens bei der nächsten Änderung (z.B. Verlängerung, Änderung der Auflagen) an diese Regelung anzupassen.

Nächster Überprüfungstermin: 06.08.2021

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[30].

A.7 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht

[30] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Überblick

-

B.2 Kapitel 2: Virtualisierte Systeme und Anwendungen im Allgemeinen

-

B.3 Kapitel 3: Virtualisierte Server und Netzwerke, virtuelle Desktops und Remote-Anwendungen

-

B.4 Kapitel 4: Virtueller Speicher

-