|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Virtualisierung"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300027 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc80532656)

[Dokumentenhistorie 3](#_Toc80532657)

[Inhaltsverzeichnis 4](#_Toc80532658)

[Allgemeine Festlegungen 6](#_Toc80532659)

[Ziel / Zweck 6](#_Toc80532660)

[Geltungsbereich 6](#_Toc80532661)

[Zuständigkeiten 6](#_Toc80532662)

[Genehmigungs- und Änderungsverfahren 7](#_Toc80532663)

[Aufbau des Dokuments 7](#_Toc80532664)

[Sicherheitsrichtlinie „Virtualisierung" 8](#_Toc80532665)

[Basismaßnahmen 8](#_Toc80532666)

[Einspielen von Aktualisierungen und Sicherheitsupdates (SYS.1.5.A1) 8](#_Toc80532667)

[Sicherer Einsatz virtueller IT-Systeme (SYS.1.5.A2) 8](#_Toc80532668)

[Sichere Konfiguration virtueller IT-Systeme (SYS.1.5.A3) 8](#_Toc80532669)

[Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen (SYS.1.5.A4) 8](#_Toc80532670)

[Schutz der Administrationsschnittstellen (SYS.1.5.A5) 9](#_Toc80532671)

[Protokollierung in der virtuellen Infrastruktur (SYS.1.5.A6) 9](#_Toc80532672)

[Zeitsynchronisation in virtuellen IT-Systemen (SYS.1.5.A7) 9](#_Toc80532673)

[Standardmaßnahmen 9](#_Toc80532674)

[Planung einer virtuellen Infrastruktur (SYS.1.5.A8) 9](#_Toc80532675)

[Netzplanung für virtuelle Infrastrukturen (SYS.1.5.A9) 10](#_Toc80532676)

[Einführung von Verwaltungsprozessen für virtuelle IT-Systeme (SYS.1.5.A10) 10](#_Toc80532677)

[Administration der Virtualisierungsinfrastruktur über ein gesondertes Managementnetz (SYS.1.5.A11) 10](#_Toc80532678)

[Rechte- und Rollenkonzept für die Administration einer virtuellen Infrastruktur (SYS.1.5.A12) 10](#_Toc80532679)

[Auswahl geeigneter Hardware für Virtualisierungsumgebungen (SYS.1.5.A13) 11](#_Toc80532680)

[Einheitliche Konfigurationsstandards für virtuelle IT-Systeme (SYS.1.5.A14) 11](#_Toc80532681)

[Betrieb von Gast-Betriebssystemen mit unterschiedlichem Schutzbedarf (SYS.1.5.A15) 11](#_Toc80532682)

[Kapselung der virtuellen Maschinen (SYS.1.5.A16) 11](#_Toc80532683)

[Überwachung des Betriebszustands und der Konfiguration der virtuellen Infrastruktur (SYS.1.5.A17) 11](#_Toc80532684)

[Schulung der Administratoren virtueller Umgebungen (SYS.1.5.A18) 12](#_Toc80532685)

[Regelmäßige Audits der Virtualisierungsinfrastruktur (SYS.1.5.A19) 12](#_Toc80532686)

[Maßnahmen bei erhöhtem Schutzbedarf 12](#_Toc80532687)

[Verwendung von hochverfügbaren Architekturen (SYS.1.5.A20 - A) 12](#_Toc80532688)

[Sichere Konfiguration virtueller IT-Systeme bei erhöhtem Schutzbedarf (SYS.1.5.A21 - A) 12](#_Toc80532689)

[Härtung des Virtualisierungsservers (SYS.1.5.A22 - CIA) 13](#_Toc80532690)

[Rechte-Einschränkung der virtuellen Maschinen (SYS.1.5.A23 - CA) 13](#_Toc80532691)

[Deaktivierung von Snapshots virtueller IT-Systeme (SYS.1.5.A24 -CIA) 13](#_Toc80532692)

[Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme (SYS.1.5.A25 - CIA) 13](#_Toc80532693)

[Einsatz einer PKI (SYS.1.5.A26 - CIA) 13](#_Toc80532694)

[Einsatz zertifizierter Virtualisierungssoftware (SYS.1.5.A27 - CIA) 13](#_Toc80532695)

[Verschlüsselung von virtuellen IT-Systemen (SYS.1.5.A28 - IA) 13](#_Toc80532696)

# Allgemeine Festlegungen

## Ziel / Zweck

Bei der Virtualisierung von IT-Systemen werden ein oder mehrere virtuelle IT-Systeme auf einem physischen IT-System ausgeführt. Ein solches physisches IT-System wird als „Virtualisierungsserver“ bezeichnet. Mehrere Virtualisierungsserver können zu einer virtuellen Infrastruktur zusammengefasst werden. Darin können die Virtualisierungsserver selbst und die auf ihnen betriebenen virtuellen IT-Systeme gemeinsam verwaltet werden.

Die Virtualisierung von IT-Systemen bietet viele Vorteile für den IT-Betrieb so können beispielsweise Kosten für Hardwarebeschaffung, Strom und Klimatisierung eingespart werden, wenn die Ressourcen der physischen IT-Systeme effizienter genutzt werden. Allerdings ist die Virtualisierung auch eine Herausforderung für den Betrieb. Da durch die eingesetzte Virtualisierungstechnik unterschiedliche Bereiche und Arbeitsfelder berührt werden, müssen Wissen und Erfahrungen aus diesen Bereichen zusammengeführt werden. Zudem können sich Probleme auf einem Virtualisierungsserver auch auf alle anderen virtuellen IT-Systeme, die auf demselben Virtualisierungsserver betrieben werden, auswirken. Ebenso können sich virtuelle IT-Systeme gegenseitig in ihrem Betrieb stören.

Das Ziel dieser Sicherheitsrichtlinie ist es aufzuzeigen, wie Virtualisierungsserver sicher durch die <Institution> eingeführt und betrieben werden können. Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben des BSI Bausteines SYS.1.5 "Virtualisierung" beachtet.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „Virtualisierung“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Virtualisierung"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Einspielen von Aktualisierungen und Sicherheitsupdates (SYS.1.5.A1)

Das Host-Betriebssystem, die Management-Software und die Firmware der zugrundeliegenden physischen Hardware sind regelmäßig zu aktualisieren.

Die Verantwortlichen für den Support der Virtualisierungsinfrastruktur müssen bekannt gewordene Schwachstellen zeitnah in Abhängigkeit vom Schutzbedarf und der Kritikalität beheben. Vorab ist auf Testsystemen zu überprüfen, ob die Sicherheitsupdates kompatibel sind und keine Fehler für produktive Systeme verursachen.

### Sicherer Einsatz virtueller IT-Systeme (SYS.1.5.A2)

Jeder Administrator von virtuellen IT-Systemen muss über geeignete Kenntnisse und Erfahrungen im Rahmen der Virtualisierung verfügen. Die Zugriffsrechte für Administratoren auf virtuelle IT-Systeme sind auf das tatsächlich notwendige Maß (Need-to-know-Prinzip) zu reduzieren.

Die für die virtuellen IT-Systeme notwendigen Netzverbindungen in der virtuellen Infrastruktur sind entsprechend den Anforderungen aus dem Dokument ISMS-E3-00032-DE zur Verfügung zu stellen. Die Anforderungen an die Isolation und Härtung der virtuellen IT-Systeme sowie der darauf/darin betriebenen Anwendungen sind hinreichend gemäß den festgelegten bzw. ererbten Schutzbedarf zu erfüllen. Alle eingesetzten virtuellen IT-Systeme müssen den Anforderungen an die Verfügbarkeit und den Datendurchsatz genügen. Im laufenden Betrieb ist die Performance der virtuellen IT-Systeme durchgehend zu überwachen.

### Sichere Konfiguration virtueller IT-Systeme (SYS.1.5.A3)

Gast-Systeme dürfen nicht auf Host-Systeme und Schnittstellen des Virtualisierungsservers zugreifen. Ist eine solche Verbindung jedoch notwendig, darf diese nur exklusiv und nur für die notwendige Dauer vom Administrator des Host-Systems hergestellt werden. Alle Bedingungen für die Ausschaltung und Abschaltung der Verbindung sind je Einzelfall unter Berücksichtigung der Sicherheitsbedingungen zu definieren. Jede Verbindungsherstellung ist in diesem Fall zu protokollieren.

Virtuelle IT-Systeme sind nach den Sicherheitsrichtlinien der <Institution> zu konfigurieren und zu schützen.

### Sichere Konfiguration eines Netzes für virtuelle Infrastrukturen (SYS.1.5.A4)

Es ist sicherzustellen, dass bestehende Sicherheitsmechanismen und Monitoring-Systeme nicht durch virtuelle Netze umgangen werden (siehe auch Dokument ISMS-E3-00032-DE). Ebenfalls ist sicherzustellen, dass über virtuelle IT-Systeme, die mit mehreren Netzen (Multi-Homed) verbunden sind, keine unerwünschte Netzverbindungen aufgebaut werden können.

Netzverbindungen zwischen virtuellen IT-Systemen und physischen IT-Systemen sowie für virtuelle Firewalls/IDS/IPS/WAFs sind gemäß den geltenden Sicherheitsrichtlinien der <Institution> zu konfigurieren.

### Schutz der Administrationsschnittstellen (SYS.1.5.A5)

Alle Administrations- und Management-Zugänge zum Management-System selbst und zu den Host-Systemen sind restriktiv einzuschränken (Need-to-know-Prinzip). Es muss sichergestellt sein, dass aus nicht-vertrauenswürdigen Netzen heraus nicht auf die Administrationsschnittstellen zugegriffen werden kann (siehe Dokument ISMS-E3-00032-DE).

Um die Virtualisierungsserver oder die Management-Systeme zu administrieren bzw. zu überwachen, sind die freigegebenen kryptographischen Protokolle (siehe Dokument ISMS-E4-00001-DE) einzusetzen. Sollte dennoch auf unsichere Protokolle zurückgegriffen werden, muss für die Administration ein eigenes Administrationsnetz genutzt werden.

### Protokollierung in der virtuellen Infrastruktur (SYS.1.5.A6)

Der Betriebszustand, die Auslastung und Netzanbindungen der virtuellen Infrastruktur sind fortlaufend zu protokollieren. Virtuelle Maschinen sollten automatisch zu verschieben oder eventuelle Hardwareerweiterungen vorzunehmen, sobald die hinterlegten Schwellwerte (Kapazitätsgrenzen) erreicht werden. Die Protokollierungsdaten sind regelmäßig proaktiv auszuwerten und sollten ebenfalls an ein SIEM übergeben werden.

### Zeitsynchronisation in virtuellen IT-Systemen (SYS.1.5.A7)

Zum Zwecke einer übergreifenden Auswertung von Ereignissen muss die Zeit-Synchronisation mit den freigegebenen Zeitquellen der <Institution> erfolgen.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Planung einer virtuellen Infrastruktur (SYS.1.5.A8)

Der Aufbau der virtuellen Infrastruktur sollte detailliert geplant werden. Dabei sind die geltenden internen Regelungen und Richtlinien für den Betrieb von IT-Systemen, Anwendungen, Netzen (inklusive Speichernetzen) zu berücksichtigen. Wenn mehrere virtuelle IT-Systeme auf einem Virtualisierungsserver betrieben werden, sollten keine Konflikte hinsichtlich des Schutzbedarfs (Verfügbarkeit, Vertraulichkeit und Integrität) der IT-Systeme auftreten. Die Vererbung der Schutzbedarfe für die virtuellen IT-Systeme sind basierend auf dem Maximum-Prinzip bei der Planung der virtuellen Infrastrukturen zu bewerten und dementsprechend zu behandeln.

Weiterhin sind die Aufgaben der einzelnen Gruppen von Administratoren festzulegen und klar voneinander abzugrenzen. Es sollte auch geregelt werden, welcher Mitarbeitenden für den Betrieb welcher Komponente verantwortlich sind und die getroffene Regelung in der Betriebsdokumentation festgehalten. Die Administratoren für die virtuellen Infrastrukturen besitzen durch Ihre langjährige Erfahrung und entsprechender Weiterbildung ausreichende Fachkenntnisse.

### Netzplanung für virtuelle Infrastrukturen (SYS.1.5.A9)

Der Aufbau des Netzes für virtuelle Infrastrukturen ist detailliert zu planen. Bei der Planung sind die Anforderungen aus dem Dokument ISMS-E3-00032-DE zu beachten. Es ist zu planen, welche Netzsegmente aufgebaut werden müssen und wie sie sich sicher voneinander trennen und schützen lassen. Dabei ist sicherzustellen, dass das produktive Netz vom Managementnetz getrennt ist. Auch die Verfügbarkeitsanforderungen (SLA/OLA) an die virtuellen Netze und deren Übergänge in die physische Netz-Infrastruktur sind zu berücksichtigen und in die Umsetzung einzuplanen.

In der Netzplanung für virtuelle Infrastrukturen ist zu prüfen, ob bestimmte Virtualisierungsfunktionen eigenständige Netze erforderlich machen. Sofern dies erkannt wurde, sind diese Netze unter Berücksichtigung der Anforderungen aus dem Dokument ISMS-E3-00032-DE zu etablieren.

### Einführung von Verwaltungsprozessen für virtuelle IT-Systeme (SYS.1.5.A10)

Für Virtualisierungsserver und virtuelle IT-Systeme sind Prozesse für die Inbetriebnahme, die Inventarisierung, den Betrieb und die Außerbetriebnahme zu definieren und zu etablieren. Die Prozesse sollten dokumentiert und regelmäßig gemäß PDCA-Zyklus aktualisiert werden.

Wenn der Einsatz geplant ist, sollte festgelegt, welche Virtualisierungsfunktionen die virtuellen IT-Systeme benutzen dürfen.

Bevor ein virtuelles IT-System betrieben wird, ist in einer Test- und Entwicklungsumgebung zu prüfen, ob es für den Produktiveinsatz geeignet ist. Die Test- und Entwicklungsumgebungen sollte getrennt von der Produktivumgebung auf differenzierten Virtualisierungsservern betrieben werden.

### Administration der Virtualisierungsinfrastruktur über ein gesondertes Managementnetz (SYS.1.5.A11)

Die Virtualisierungsinfrastruktur ist ausschließlich über ein separates Managementnetz zu administrieren. Die verfügbaren Sicherheitsmechanismen der eingesetzten Managementprotokolle zur Authentisierung, Integritätssicherung und Verschlüsselung sind zu aktivieren und alle unsicheren Managementprotokolle zu deaktivieren.

### Rechte- und Rollenkonzept für die Administration einer virtuellen Infrastruktur (SYS.1.5.A12)

Anhand der in der Planung definierten Aufgaben und Rollen sollte für die Administration der virtuellen IT-Systeme und Netze sowie der Virtualisierungsserver und der Management-Umgebung ein Rechte- und Rollenkonzept erstellt und umgesetzt werden. Alle Komponenten der virtuellen Infrastruktur sind in ein zentrales Identitäts- und Berechtigungsmanagement einzubinden.

Administratoren von virtuellen Maschinen und Administratoren der Virtualisierungsumgebung sollten durch die verwendeten Benutzernamen unterschieden und mit unterschiedlichen Zugriffsrechten ausgestattet werden.

Um eine geeignete Strukturierung mit einer entsprechenden Administratoren-Rollenzuteilung einführen zu können, sollte die Management-Umgebung virtuelle Maschinen gruppieren können.

### Auswahl geeigneter Hardware für Virtualisierungsumgebungen (SYS.1.5.A13)

Die verwendete Hardware ist kompatibel zur eingesetzten Virtualisierungslösung auszuwählen. Dabei ist zu berücksichtigen, dass der Hersteller der Virtualisierungslösung bzw. der Dienstleister für die Virtualisierungslösung über den geplanten Einsatzzeitraum auch Support für die betriebene Hardware anbietet.

### Einheitliche Konfigurationsstandards für virtuelle IT-Systeme (SYS.1.5.A14)

Für die eingesetzten virtuellen IT-Systeme sind einheitliche Konfigurationsstandards zu definieren und anzuwenden. Die Konfigurationsstandards sind regelmäßig zu überprüfen und falls erforderlich anzupassen.

### Betrieb von Gast-Betriebssystemen mit unterschiedlichem Schutzbedarf (SYS.1.5.A15)

Falls virtuelle IT-Systeme mit unterschiedlichem Schutzbedarf gemeinsam auf einem Virtualisierungsserver betriebenen werden, ist sicherzustellen, dass die virtuellen IT-Systeme ausreichend gekapselt und voneinander isoliert sind. Zusätzlich ist auch die Netztrennung in der eingesetzten Virtualisierungslösung ausreichend abzusichern. Ist das nicht der Fall, werden weitergehende Sicherheitsmaßnahmen wie bspw. Mikro-Segmentierung oder PVLAN oder VXLAN identifiziert und umgesetzt.

### Kapselung der virtuellen Maschinen (SYS.1.5.A16)

Die Funktionen "Kopieren" und "Einfügen" von Informationen zwischen virtuellen Maschinen ist zu deaktivieren.

### Überwachung des Betriebszustands und der Konfiguration der virtuellen Infrastruktur (SYS.1.5.A17)

Der Betriebszustand der virtuellen Infrastruktur ist geeignet zu überwachen. In der Überwachung ist zu prüfen, ob noch ausreichend Ressourcen verfügbar sind und ob es eventuell Konflikte bei gemeinsam benutzten Ressourcen eines Virtualisierungsservers gibt. Sofern dies erkannt wird sollte auf Basis von Schwellwerten eine automatische Anpassung der Ressourcen erfolgen.

Weiterhin werden die Konfigurationsdateien der virtuellen IT-Systeme regelmäßig auf unautorisierte Änderungen überprüft. Auch wird überwacht, ob die virtuellen Netze den jeweiligen virtuellen IT-Systemen korrekt zugeordnet sind.

Sofern Konfigurationsänderungen an der Virtualisierungsinfrastruktur vorgenommen werden, ist zu prüfen bzw. zu testen, bevor die Konfigurationsänderungen umgesetzt werden.

### Schulung der Administratoren virtueller Umgebungen (SYS.1.5.A18)

Alle Administratoren der virtuellen Umgebung sind regelmäßig und ausreichend entsprechend des abgestimmten schulungsplanes bezüglich der Virtualisierung zu sensibilisieren und weiterzubilden. In der Schulung sollte vermittelt werden, wie virtuelle Infrastrukturen sicher aufgebaut und betrieben werden können.

### Regelmäßige Audits der Virtualisierungsinfrastruktur (SYS.1.5.A19)

Es sollte regelmäßig auditiert werden, ob der Ist-Zustand der virtuellen Infrastruktur dem in der Planung festgelegten Zustand entspricht. Auch sollte regelmäßig auditiert werden, ob die Konfiguration der virtuellen Komponenten die vorgegebene Standardkonfiguration einhält. Die Ergebnisse des Audits sind nachvollziehbar zu dokumentieren. Festgestellte Abweichungen sind angemessen und zeitnah im Rahmen eines Maßnahmenbehandlungsplans zu beheben.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Verwendung von hochverfügbaren Architekturen (SYS.1.5.A20 - A)

Sofern die Verfügbarkeitsanforderungen (SLA/OLA) an die virtuelle Infrastruktur mit erhöhten Schutzbedarf ausgelegt ist, sind alle Virtualisierungsserver im Rahmen der Hochverfügbarkeitsarchitektur in Clustern zusammenzuschließen.

### Sichere Konfiguration virtueller IT-Systeme bei erhöhtem Schutzbedarf (SYS.1.5.A21 - A)

Für virtuelle IT-Systeme ist bei einem erhöhten Schutzbedarf die Überbuchungsfunktion für Ressourcen zu deaktivieren.

### Härtung des Virtualisierungsservers (SYS.1.5.A22 - CIA)

Die Virtualisierungsserver sind zu härten. Um virtuelle IT-Systeme voreinander und gegenüber dem Virtualisierungsserver zusätzlich zu isolieren und zu kapseln, sollte die Funktion Mandatory-Access-Controls (MACs) eingesetzt werden. Ebenfalls ist das IT-System zu härten, auf dem die Management-Software installiert ist.

### Rechte-Einschränkung der virtuellen Maschinen (SYS.1.5.A23 - CA)

Alle Schnittstellen und Kommunikationskanäle die es einem virtuellen IT-System erlauben, Informationen über das Host-System auszulesen und abzufragen sind zu deaktivieren oder zu unterbinden. Weiterhin sollte im Sinne der Rechte-Einschränkung der virtuellen Maschinen sichergestellt sein, dass ausschließlich der Virtualisierungsserver auf seine eigenen Ressourcen zugreifen kann. Außerdem sollte es nicht möglich sein, dass sich virtuelle IT-Systeme sogenannte Pages des Arbeitsspeichers teilen.

### Deaktivierung von Snapshots virtueller IT-Systeme (SYS.1.5.A24 -CIA)

Für alle virtuellen IT-Systeme sind bei erhöhtem Schutzbedarf die Snapshot-Funktion zu deaktivieren.

### Minimale Nutzung von Konsolenzugriffen auf virtuelle IT-Systeme (SYS.1.5.A25 - CIA)

Direkte Zugriffe auf die emulierten Konsolen virtueller IT-Systeme sind bei erhöhtem Schutzbedarf auf ein Mindestmaß zu reduzieren. Die virtuellen Systeme sollten möglichst über das Netz gesteuert werden.

### Einsatz einer PKI (SYS.1.5.A26 - CIA)

Die Kommunikation zwischen den Komponenten der IT-Infrastruktur mithilfe von Zertifikaten abgesichert wird, ist bei einem erhöhten Schutzbedarf eine Public-Key-Infrastruktur (PKI) einzusetzen.

### Einsatz zertifizierter Virtualisierungssoftware (SYS.1.5.A27 - CIA)

Es sollte zertifizierte Virtualisierungssoftware der Common Criteria Stufe EAL 4 oder höher eingesetzt werden.

### Verschlüsselung von virtuellen IT-Systemen (SYS.1.5.A28 - IA)

Alle virtuellen IT-Systeme sollten bei erhöhtem Schutzbedarf verschlüsselt werden.