



SYS.1.5 Virtualisierung

1. Beschreibung

1.1. Einleitung

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 in einem Informationsverbund. 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 des Informationsverbunds. Da durch die eingesetzte Virtualisierungstechnik unterschiedliche Bereiche und Arbeitsfelder im Informationsverbund 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.

1.2. Zielsetzung

Das Ziel dieses Bausteins ist es aufzuzeigen, wie Virtualisierungsserver im Informationsverbund sicher eingeführt und betrieben werden können.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.1.5 *Virtualisierung* ist auf jeden Virtualisierungsserver anzuwenden.

Neben dem vorliegenden Baustein müssen auch die jeweils relevanten Server- oder Client-Bausteine der Schicht *SYS IT-Systeme* auf jeden Virtualisierungsserver angewandt werden. Neben den betriebssystemspezifischen Bausteinen müssen außerdem die Bausteine SYS.1.1 *Allgemeiner Server* bzw. SYS.2.1 *Allgemeiner Client* angewendet werden, da in diesen Bausteinen die plattformunabhängigen Sicherheitsaspekte für Server bzw. Clients zusammengefasst sind.

In diesem Baustein wird nur die Virtualisierung vollständiger IT-Systeme behandelt. Andere Techniken, die teilweise ebenfalls mit dem Wort „Virtualisierung“ in Verbindung gebracht werden (z.

B. Anwendungsvirtualisierung mittels Terminalservern, Storage-Virtualisierung und Container), sind nicht Gegenstand dieses Bausteins.

Im Bereich der Software-Entwicklung werden die Begriffe „*Virtuelle Maschine*“ und „*Virtueller-Maschinen-Monitor*“ auch für Laufzeitumgebungen benutzt, z. B. wenn Java oder Microsoft .NET eingesetzt werden. Solche Laufzeitumgebungen werden in diesem Baustein ebenfalls nicht betrachtet.

Virtuelle Infrastrukturen werden in der Regel mit speziellen Managementsystemen verwaltet. Da mit diesen IT-Systemen umfassend auf die Virtualisierungsinfrastruktur zugegriffen werden kann, ist es wichtig, diese ausreichend abzusichern. Das betrifft sowohl den physischen oder virtuellen Server, auf dem die Management-Software ausgeführt wird, als auch das Produkt selber.

Virtualisierungsumgebungen werden meistens gemeinsam mit Speichernetzen (NAS oder SAN) eingesetzt. Die Anbindung und Absicherung dieser Systeme werden in diesem Baustein ebenfalls nicht betrachtet (siehe hierfür Baustein SYS.1.8 *Speicherlösungen*).

Durch die Virtualisierung müssen die Netze der Institution anders strukturiert werden. Dieses Thema wird in diesem Baustein nicht umfassend behandelt. Dafür müssen die Anforderungen des Bausteins NET.1.1 *Netzarchitektur und -design* erfüllt werden. Auch die Netzvirtualisierung wird im vorliegenden Baustein nicht in der notwendigen Tiefe beleuchtet.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein SYS.1.5 *Virtualisierung* von besonderer Bedeutung.

2.1. Fehlerhafte Planung der Virtualisierung

Ein Virtualisierungsserver ermöglicht den Betrieb virtueller IT-Systeme, integriert die IT-Systeme in das Rechenzentrum und steuert dabei deren Anbindung an weitere Infrastrukturelemente, z. B. Netze (inklusive Speichernetze). Wird nicht geplant, wie die Virtualisierungsserver technisch und organisatorisch in die bestehende Infrastruktur zu integrieren sind, kann dies dazu führen, dass die Zuständigkeiten für unterschiedliche Bereiche womöglich nicht klar definiert sind, z. B. für Anwendungen, Betriebssysteme und Netzkomponenten. Weiterhin können sich die Zuständigkeiten verschiedener Bereiche überschneiden oder es ist keine passende Rechtestruktur vorhanden, um administrative Zugriffe für die unterschiedlichen Bereiche zu trennen.

2.2. Fehlerhafte Konfiguration der Virtualisierung

Durch Virtualisierung ändert sich die Art und Weise, wie Server provisioniert werden. Ressourcen wie CPU, RAM, Netzanbindung und Speicher werden in der Regel zentral über ein Managementsystem konfiguriert und sind nicht mehr durch Hardware und Verkabelung vorgegeben. Dadurch können schnell Fehler in der Konfiguration entstehen. Wird beispielsweise ein hoch schutzbedürftiges virtuelles IT-System fälschlicherweise in einer externen demilitarisierten Zone (DMZ) platziert, ist es folglich aus dem Internet erreichbar und somit einem erhöhten Risiko ausgesetzt.

2.3. Unzureichende Ressourcen für virtuelle IT-Systeme

Virtualisierungsserver benötigen für den Betrieb der virtuellen IT-Systeme Speicherplatz, der entweder lokal im Virtualisierungsserver selbst oder in einem Speichernetz bereitgestellt wird. Werden die hierfür benötigten Speicherkapazitäten nicht ausreichend groß geplant, bestehen weitreichende Risiken für die Verfügbarkeit der virtuellen IT-Systeme und die Integrität der in ihnen verarbeiteten Informationen. Das gilt insbesondere dann, wenn spezielle Virtualisierungsfunktionen, wie Snapshots oder die Überbuchung von Speicherplatz, benutzt werden.

Engpässe können nicht nur den Speicherplatz auf Festplatten oder in Speichernetzen betreffen, sondern auch die Prozessorleistung, den Arbeitsspeicher (RAM), oder die Netzanbindung. Außerdem könnten sich durch unzureichende Ressourcen auf dem Virtualisierungsserver die virtuellen Maschinen gegenseitig in ihrem Betrieb stören und letztlich nicht mehr korrekt arbeiten oder ganz ausfallen.

2.4. Informationsabfluss oder Ressourcen-Engpass durch Snapshots

Durch einen Snapshot kann der Zustand einer virtuellen Maschine eingefroren und gesichert werden. Wird ein solcher Snapshot zu einem späteren Zeitpunkt wiederhergestellt, gehen alle in der Zwischenzeit vorgenommenen Änderungen verloren. Dadurch können auch bereits gepatchte Sicherheitslücken wieder offen sein. Weiterhin können durch offene Dateien, Dateitransfers oder Datenbanktransaktionen zum Zeitpunkt des Snapshots inkonsistente Daten entstehen.

Außerdem können Snapshots bei Angriffen dazu missbraucht werden, um unberechtigt auf die Daten eines virtuellen IT-Systems zuzugreifen. Denn wenn der Snapshot im laufenden Betrieb erstellt wurde, ist auch der Inhalt des Hauptspeichers auf der Festplatte gesichert worden und kann auf einer virtuellen Umgebung außerhalb der ursprünglichen IT-Infrastruktur wiederhergestellt und analysiert werden. Ebenso können Snapshots sehr groß werden und dadurch kann die verfügbare Speicherkapazität knapp werden.

2.5. Ausfall des Verwaltungsservers für Virtualisierungssysteme

Da über den Verwaltungsserver sämtliche Funktionen einer virtuellen Infrastruktur gesteuert und administriert werden, führt ein Ausfall dieses Verwaltungssystems dazu, dass keine Konfigurationsänderungen an der virtuellen Infrastruktur durchgeführt werden können. Der IT-Betrieb kann in dieser Zeit nicht auf auftretende Probleme wie Ressourcenengpässe oder den Ausfall einzelner Virtualisierungsserver reagieren und keine neuen Virtualisierungsserver in die Infrastruktur integrieren oder neue virtuelle IT-Systeme anlegen. Auch die Live-Migration und damit die dynamische Zuteilung von Ressourcen für einzelne Gast-Systeme ist ohne Verwaltungsserver nicht möglich.

2.6. Missbräuchliche Nutzung von Gastwerkzeugen

Gastwerkzeuge werden in den virtuellen Maschinen häufig mit sehr hohen Berechtigungen ausgeführt. Dadurch lassen sie sich beispielsweise für Denial-of-Service-Angriffe missbrauchen oder Angreifende übernehmen mit ihnen gleich den ganzen Virtualisierungsserver.

2.7. Kompromittierung der Virtualisierungssoftware

Die Virtualisierungssoftware (auch „Hypervisor“) ist die zentrale Komponente eines Virtualisierungsservers. Sie steuert alle auf diesem Server ausgeführten virtuellen Maschinen und teilt ihnen Prozessor- und Speicherressourcen zu. Wird diese Komponente erfolgreich angegriffen, führt dies auch dazu, dass alle virtuellen IT-Systeme, die auf dem Virtualisierungsserver ausgeführt werden, kompromittiert sind.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.5 *Virtualisierung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Planende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

SYS.1.5.A1 ENTFALLEN (B)

Diese Anforderung ist entfallen.

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

Jede Person, die virtuelle IT-Systeme administriert, MUSS wissen, wie sich eine Virtualisierung auf die betriebenen IT-Systeme und Anwendungen auswirkt. Die Zugriffsrechte für Administrierende auf virtuelle IT-Systeme MÜSSEN auf das tatsächlich notwendige Maß reduziert sein.

Es MUSS gewährleistet sein, dass die für die virtuellen IT-Systeme notwendigen Netzverbindungen in der virtuellen Infrastruktur verfügbar sind. Auch MUSS geprüft werden, ob die Anforderungen an die Isolation und Kapselung der virtuellen IT-Systeme sowie der darauf betriebenen Anwendungen hinreichend erfüllt sind. Weiterhin MÜSSEN die eingesetzten virtuellen IT-Systeme den Anforderungen an die Verfügbarkeit und den Datendurchsatz genügen. Im laufenden Betrieb MUSS die Performance der virtuellen IT-Systeme überwacht werden.

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

Gast-Systeme DÜRFEN NICHT auf Geräte und Schnittstellen des Virtualisierungsservers zugreifen. Ist eine solche Verbindung jedoch notwendig, MUSS diese exklusiv zugeteilt werden. Sie DARF NUR für die notwendige Dauer von den Administrierenden des Host-Systems hergestellt werden. Dafür MÜSSEN verbindliche Regelungen festgelegt werden.

Virtuelle IT-Systeme SOLLTEN nach den Sicherheitsrichtlinien der Institution konfiguriert und geschützt werden.

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

Es MUSS sichergestellt werden, dass bestehende Sicherheitsmechanismen (z. B. Firewalls) und Monitoring-Systeme nicht über virtuelle Netze umgangen werden können. Auch MUSS ausgeschlossen sein, dass über virtuelle IT-Systeme, die mit mehreren Netzen verbunden sind, unerwünschte Netzverbindungen aufgebaut werden können.

Netzverbindungen zwischen virtuellen IT-Systemen und physischen IT-Systemen sowie für virtuelle Firewalls SOLLTEN gemäß den Sicherheitsrichtlinien der Institution konfiguriert werden.

SYS.1.5.A5 Schutz der Administrationsschnittstellen (B)

Alle Administrations- und Management-Zugänge zum Managementsystem und zu den Host-Systemen MÜSSEN eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht-vertrauenswürdigen Netzen heraus nicht auf die Administrationsschnittstellen zugegriffen werden kann.

Um die Virtualisierungsserver oder die Managementsysteme zu administrieren bzw. zu überwachen, SOLLTEN als sicher geltende Protokolle eingesetzt werden. Sollte dennoch auf unsichere Protokolle

zurückgegriffen werden, MUSS für die Administration ein eigenes Administrationsnetz genutzt werden.

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

Betriebszustand, Auslastung und Netzanbindungen der virtuellen Infrastruktur MÜSSEN laufend protokolliert werden. Werden Kapazitätsgrenzen erreicht, SOLLTEN virtuelle Maschinen verschoben werden. Zudem SOLLTE eventuell die Hardware erweitert werden. Auch MUSS überwacht werden, ob die virtuellen Netze den jeweiligen virtuellen IT-Systemen korrekt zugeordnet sind.

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

Die Systemzeit aller produktiv eingesetzten virtuellen IT-Systeme MUSS immer synchron sein.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.5.A8 Planung einer virtuellen Infrastruktur (S) [Planende]

Der Aufbau der virtuellen Infrastruktur SOLLTE detailliert geplant werden. Dabei SOLLTEN die geltenden Regelungen und Richtlinien für den Betrieb von IT-Systemen, Anwendungen und Netzen (inklusive Speichernetzen) berücksichtigt werden. Wenn mehrere virtuelle IT-Systeme auf einem Virtualisierungsserver betrieben werden, SOLLTEN KEINE Konflikte hinsichtlich des Schutzbedarfs der IT-Systeme auftreten. Weiterhin SOLLTEN die Aufgaben der einzelnen Gruppen, die für die Administration zuständig sind, festgelegt und klar voneinander abgegrenzt werden. Es SOLLTE auch geregelt werden, wer für den Betrieb welcher Komponente verantwortlich ist.

SYS.1.5.A9 Netzplanung für virtuelle Infrastrukturen (S) [Planende]

Der Aufbau des Netzes für virtuelle Infrastrukturen SOLLTE detailliert geplant werden. Auch SOLLTE geprüft werden, ob für bestimmte Virtualisierungsfunktionen (wie z. B. die Live-Migration) ein eigenes Netz aufgebaut und genutzt werden muss. Es SOLLTE geplant werden, welche Netzsegmente aufgebaut werden müssen (z. B. Managementnetz, Speichernetz). Es SOLLTE festgelegt werden, wie die Netzsegmente sich sicher voneinander trennen und schützen lassen. Dabei SOLLTE sichergestellt werden, dass das produktive Netz vom Managementnetz getrennt ist (siehe SYS.1.5.A11 *Administration der Virtualisierungsinfrastruktur über ein gesondertes Managementnetz*). Auch die Verfügbarkeitsanforderungen an das Netz SOLLTEN erfüllt werden.

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

Für Virtualisierungsserver und virtuelle IT-Systeme SOLLTEN Prozesse für die Inbetriebnahme, die Inventarisierung, den Betrieb und die Außerbetriebnahme definiert und etabliert werden. Die Prozesse SOLLTEN dokumentiert und regelmäßig aktualisiert werden.

Wenn der Einsatz von virtuellen IT-Systemen geplant wird, SOLLTE festgelegt werden, welche Virtualisierungsfunktionen die virtuellen IT-Systeme benutzen dürfen. Test- und Entwicklungsumgebungen SOLLTEN NICHT auf demselben Virtualisierungsserver betrieben werden wie produktive virtuelle IT-Systeme.

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

Die Virtualisierungsinfrastruktur SOLLTE ausschließlich über ein separates Managementnetz administriert werden (siehe NET.1.1 *Netzarchitektur und -design*). Die verfügbaren Sicherheitsmechanismen der eingesetzten Managementprotokolle zur Authentisierung, Integritätssicherung und Verschlüsselung SOLLTEN aktiviert werden. Alle unsicheren Managementprotokolle SOLLTEN deaktiviert werden (siehe NET.1.2 *Netzmanagement*).

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

Anhand der in der Planung definierten Aufgaben und Rollen (siehe SYS.1.5.A8 *Planung einer virtuellen Infrastruktur*) SOLLTE für die Administration der virtuellen IT-Systeme und Netze sowie der Virtualisierungsserver und der Managementumgebung ein Rechte- und Rollenkonzept erstellt und umgesetzt werden. Alle Komponenten der virtuellen Infrastruktur SOLLTEN in ein zentrales Identitäts- und Berechtigungsmanagement eingebunden werden. Administrierende von virtuellen Maschinen und Administrierende der Virtualisierungsumgebung SOLLTEN unterschieden werden. Sie SOLLTEN mit unterschiedlichen Zugriffsrechten ausgestattet werden.

Weiterhin SOLLTE die Managementumgebung virtuelle Maschinen zur geeigneten Strukturierung gruppieren können. Die Rollen der Administrierenden SOLLTEN entsprechend zugeteilt werden.

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

Die verwendete Hardware SOLLTE kompatibel mit der eingesetzten Virtualisierungslösung sein. Dabei SOLLTE darauf geachtet werden, dass das herstellende Unternehmen der Virtualisierungslösung über den geplanten Einsatzzeitraum auch Support für die betriebene Hardware anbietet.

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

Für die eingesetzten virtuellen IT-Systeme SOLLTEN einheitliche Konfigurationsstandards definiert werden. Die virtuellen IT-Systeme SOLLTEN nach diesen Standards konfiguriert werden. Die Konfigurationsstandards SOLLTEN regelmäßig überprüft werden. Sie SOLLTEN, falls erforderlich, angepasst werden.

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

Falls virtuelle IT-Systeme mit unterschiedlichem Schutzbedarf gemeinsam auf einem Virtualisierungsserver betrieben werden, SOLLTE dabei sichergestellt sein, dass die virtuellen IT-Systeme ausreichend gekapselt und voneinander isoliert sind. Auch SOLLTE dann die Netztrennung in der eingesetzten Virtualisierungslösung ausreichend sicher sein. Ist das nicht der Fall, SOLLTEN weitergehende Sicherheitsmaßnahmen identifiziert und umgesetzt werden.

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

Die Funktionen „Kopieren“ und „Einfügen“ von Informationen zwischen virtuellen Maschinen SOLLTEN deaktiviert sein.

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

Der Betriebszustand der virtuellen Infrastruktur SOLLTE überwacht werden. Dabei SOLLTE unter anderem geprüft werden, ob noch ausreichend Ressourcen verfügbar sind. Es SOLLTE auch geprüft werden, ob es eventuell Konflikte bei gemeinsam genutzten Ressourcen eines Virtualisierungsservers gibt.

Weiterhin SOLLTEN die Konfigurationsdateien der virtuellen IT-Systeme regelmäßig auf unautorisierte Änderungen überprüft werden.

Wird die Konfiguration der Virtualisierungsinfrastruktur geändert, SOLLTEN die Änderungen geprüft und getestet werden, bevor sie umgesetzt werden.

SYS.1.5.A18 ENTFALLEN (S)

Diese Anforderung ist entfallen.

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

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 Auditergebnisse SOLLTEN nachvollziehbar dokumentiert werden. Abweichungen SOLLTEN behoben werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

SYS.1.5.A20 Verwendung von hochverfügbaren Architekturen (H) [Planende]

Die virtuelle Infrastruktur SOLLTE hochverfügbar ausgelegt werden. Alle Virtualisierungsserver SOLLTEN in Clustern zusammengeschlossen werden.

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

Für virtuelle IT-Systeme SOLLTEN Überbuchungsfunktionen für Ressourcen deaktiviert werden.

SYS.1.5.A22 Härtung des Virtualisierungsservers (H)

Der Virtualisierungsserver SOLLTE gehärtet werden. Um virtuelle IT-Systeme voneinander und gegenüber dem Virtualisierungsserver zusätzlich zu isolieren und zu kapseln, SOLLTEN Mandatory Access Controls (MACs) eingesetzt werden. Ebenso SOLLTE das IT-System, auf dem die Management-Software installiert ist, gehärtet werden.

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

Alle Schnittstellen und Kommunikationskanäle, die es einem virtuellen IT-System erlauben, Informationen über das Host-System auszulesen und abzufragen, SOLLTEN deaktiviert sein oder unterbunden werden. Weiterhin SOLLTE ausschließlich der Virtualisierungsserver auf seine Ressourcen zugreifen können. Virtuelle IT-Systeme SOLLTEN NICHT die sogenannten Pages des Arbeitsspeichers teilen.

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

Für alle virtuellen IT-Systeme SOLLTE die Snapshot-Funktion deaktiviert werden.

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

Direkte Zugriffe auf die emulierten Konsolen virtueller IT-Systeme SOLLTEN auf ein Mindestmaß reduziert werden. Die virtuellen IT-Systeme SOLLTEN möglichst über das Netz gesteuert werden.

SYS.1.5.A26 Einsatz einer PKI (H) [Planende]

Für die mit Zertifikaten geschützte Kommunikation zwischen den Komponenten der IT-Infrastruktur SOLLTE eine Public-Key-Infrastruktur (PKI) eingesetzt werden.

SYS.1.5.A27 Einsatz zertifizierter Virtualisierungssoftware (H)

Es SOLLTE zertifizierte Virtualisierungssoftware der Stufe EAL 4 oder höher eingesetzt werden.

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

Alle virtuellen IT-Systeme SOLLTEN verschlüsselt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das BSI gibt in seiner Veröffentlichung zur Cyber-Sicherheit BSI-CS 113: „Server-Virtualisierung“ Empfehlungen zum Einsatz von Virtualisierung.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel SYS.1.3 - Virtual Servers - Vorgaben für den Betrieb von virtuellen Servern.

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800-125 „Guide to Security for Full Virtualization Technologie“ Empfehlungen zum Einsatz von Virtualisierung.