SYS.1.1: Allgemeiner Server

1 Beschreibung

1.1 Einleitung

Als „Allgemeiner Server“ werden IT-Systeme mit einem beliebigen Betriebssystem bezeichnet, die Benutzern und anderen IT-Systemen Dienste bereitstellen. Diese Dienste können Basisdienste für das lokale oder externe Netz sein, oder auch den E-Mail-Austausch ermöglichen oder Datenbanken und Druckerdienste anbieten. Server-IT-Systeme haben eine zentrale Bedeutung für die Informationstechnik und damit für funktionierende Arbeitsabläufe einer Institution. Oft erfüllen Server Aufgaben im Hintergrund, ohne dass Benutzer direkt mit ihnen im Austausch stehen. Auf der anderen Seite gibt es Serverdienste, die direkt mit den Benutzern interagieren und nicht auf den ersten Blick als Serverdienst wahrgenommen werden. Ein bekanntes Beispiel sind X-Server unter Unix.

1.2 Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die auf Servern verarbeitet, angeboten oder darüber übertragen werden, sowie der Schutz der damit zusammenhängenden Dienste.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.1.1 *Allgemeiner Server* ist für alle Server-IT-Systeme mit beliebigem Betriebssystem anzuwenden.

In der Regel werden Server-Systeme unter Betriebssystemen betrieben, bei denen jeweils spezifische Sicherheitsanforderungen zu berücksichtigen sind. Für verbreitete Server-Betriebssysteme sind im IT-Grundschutz-Kompendium eigene Bausteine vorhanden, die auf dem vorliegenden Baustein aufbauen. Der Baustein SYS.1.1 *Allgemeiner Server* bildet die Grundlage für die Bausteine der konkreten Server-Betriebssysteme. Sofern für ein betrachtetes IT-System ein konkreter Baustein existiert, ist dieser zusätzlich zum Baustein SYS.1.1 *Allgemeiner Server* anzuwenden. Falls für eingesetzte Server-Systeme kein spezifischer Baustein existiert, müssen die Anforderungen des vorliegenden Bausteins geeignet konkretisiert werden.

Die jeweils spezifischen Dienste, die vom Server angeboten werden, sind nicht Bestandteil dieses Bausteins. Für diese Serverdienste müssen zusätzlich zu diesem Baustein noch weitere Bausteine umgesetzt werden, gemäß den Ergebnissen der Modellierung nach IT-Grundschutz. Falls für ein Server-System im Einzelfall auch eine interaktive Nutzung durch Benutzer vorgesehen ist (z. B. Terminalserver), sind die damit verbundenen Sicherheitsaspekte ebenfalls zu berücksichtigen.

Grundsätzlich sind die Anforderungen an das Rollen- und Berechtigungskonzept aus dem Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* zu berücksichtigen. Ebenfalls zu berücksichtigen sind

Anforderungen aus dem Baustein DER.4 *Notfallmanagement*.

Server sollten grundsätzlich beim Konzept zum Schutz vor Schadsoftware berücksichtigt werden. Anforderungen dazu finden sich im Baustein OPS.1.1.4 *Schutz vor Schadprogrammen*.

Bei Servern gibt es besondere Anforderungen an die Administratoren sowie den Umgang mit Patches und Änderungen. Deswegen sind die Anforderungen der Bausteine OPS.1.1.2 *Ordnungsgemäße IT-Administration* und OPS1.1.3 *Patch- und Änderungsmanagement* zu beachten.

Server bieten häufig Dienste für eine Vielzahl von Clients an, oft auch über das Internet. Aus diesem Grund sind sie besonders vom übrigen Netz der Institution zu trennen. Anforderungen dazu gibt es im Baustein NET.1.1 *Netzarchitektur und -design*.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein SYS.1.1 *Allgemeiner Server* von besonderer Bedeutung:

2.1 Datenverlust

Der Verlust von Daten kann besonders bei Servern erhebliche Auswirkungen auf Geschäftsprozesse bzw. Fachaufgaben und damit auf die gesamte Institution haben. Sehr viele IT-Systeme wie Clients oder andere Server sind in der Regel darauf angewiesen, dass die dort zentral gespeicherten Daten immer verfügbar sind.

Wenn institutionsrelevante Informationen, egal welcher Art, zerstört oder verfälscht werden, können dadurch Geschäftsprozesse und Fachaufgaben verzögert oder sogar deren Ausführung verhindert werden. Insgesamt kann der Verlust gespeicherter Daten, neben dem Ausfall und den Kosten für die Wiederbeschaffung der Daten, vor allem zu langfristigen Konsequenzen wie Vertrauenseinbußen bei Kunden und Partnern, zu juristischen Auswirkungen sowie zu einem negativen Eindruck in der Öffentlichkeit führen. In vielen Institutionen existieren Regelungen, dass keine Daten auf den lokalen Clients gespeichert werden dürfen, sondern stattdessen zentrale Ablagen auf den Servern dazu genutzt werden müssen. Ein Verlust dieser zentral abgelegten Daten hat in einem solchen Fall gravierende Auswirkungen. Durch die verursachten direkten und indirekten Schäden können Institutionen sogar in ihrer Existenz bedroht sein.

2.2 Denial-of-Service-Angriffe

Ein Angriff auf die Verfügbarkeit von Datenbeständen, der „Denial of Service“ genannt wird, zielt darauf ab, die Benutzer daran zu hindern, benötigte und normalerweise verfügbare Funktionen oder Geräte zu verwenden. Dieser Angriff steht häufig im Zusammenhang mit verteilten Ressourcen, indem ein Angreifer diese Ressourcen sehr stark in Anspruch nimmt, können andere Benutzer nicht mehr darauf zugreifen. In der Regel sind IT-Systeme auch stark voneinander abhängig. Somit sind von der Verknappung der Ressourcen eines Servers schnell weitere Server betroffen. Es können zum Beispiel CPU-Zeit, Speicherplatz oder Bandbreite künstlich verknappt werden. Dies kann dazu führen, dass Dienste oder Ressourcen überhaupt nicht mehr genutzt werden können.

2.3 Bereitstellung unnötiger Betriebssystemkomponenten und Applikationen

Schon bei der Installation des Server-Betriebssystems ist es möglich, mitgelieferte Applikationen und Dienste zu installieren, von denen einige unter Umständen gar nicht genutzt werden. Auch im späteren Betrieb wird oft Software installiert, die kurz getestet, aber danach nicht mehr benötigt wird. Oft ist Mitarbeitern gar nicht bekannt, dass diese nicht genutzten Anwendungen und Dienste vorhanden sind. Auf diese Weise befinden sich zahlreiche Applikationen und Dienste auf den Servern, die nicht eingesetzt werden und die ihn so unnötig belasten.

Außerdem können diese nicht genutzten Anwendungen und Dienste Schwachstellen enthalten, etwa

wenn sie nicht mehr aktualisiert werden. Sind die installierten Anwendungen und Dienste unbekannt, ist der Institution gar nicht bewusst, dass diese ebenfalls aktualisiert werden müssen. Auf diese Weise können sie leicht zum Einfallstor für Angreifer werden.

2.4 Überlastung von Servern

Wenn Server nicht ausreichend dimensioniert sind, ist irgendwann der Punkt erreicht, an dem sie den Anforderungen der Institution nicht mehr gerecht werden. Je nach Art der betroffenen Systeme kann dies eine Vielzahl von negativen Auswirkungen haben. So können die Server oder Dienste beispielsweise vorübergehend nicht verfügbar sein oder es können Datenverluste auftreten. Die Überlastung eines einzelnen Servers kann bei komplexen IT-Landschaften außerdem dazu führen, dass bei weiteren Servern Probleme oder Ausfälle auftreten.

Auslöser für die Überlastung von Informationssystemen kann sein, dass

- installierte Dienste oder Anwendungen falsch konfiguriert sind und so unnötig viel Speicher beanspruchen,
- vorhandene Speicherplatzkapazitäten überschritten werden,
- zahlreiche Anfragen zur gleichen Zeit ein System überbeanspruchen,
- zu viel Rechenleistung von den Diensten beansprucht wird oder
- eine zu große Anzahl an Nachrichten zur gleichen Zeit versendet wird.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.1 *Allgemeiner Server* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Haustechnik

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.1.1 *Allgemeiner Server* vorrangig erfüllt werden:

SYS.1.1.A1 Geeignete Aufstellung (B)

Server MÜSSEN an Orten betrieben werden, zu denen nur berechtigte Personen Zutritt haben. Server MÜSSEN daher in Rechenzentren, Rechnerräumen oder abschließbaren Serverschränken aufgestellt beziehungsweise eingebaut werden (siehe hierzu die entsprechenden Bausteine der Schicht INF *Infrastruktur*). Server DÜRFEN NICHT als Arbeitsplatzrechner genutzt werden. Als Arbeitsplatz genutzte IT-Systeme DÜRFEN NICHT als Server genutzt werden.

SYS.1.1.A2 Benutzerauthentisierung an Servern (B)

Für die Anmeldung von Benutzern und Diensten am Server MÜSSEN Authentisierungsverfahren eingesetzt werden, die dem Schutzbedarf der Server angemessen sind. Dies SOLLTE in besonderem Maße für administrative Zugänge berücksichtigt werden. Soweit möglich, SOLLTE dabei auf zentrale,

netzbasierte Authentisierungsdienste zurückgegriffen werden.

SYS.1.1.A3 ENTFALLEN (B)
Diese Anforderung ist entfallen.

SYS.1.1.A4 ENTFALLEN (B)
Diese Anforderung ist entfallen.

SYS.1.1.A5 Schutz von Schnittstellen (B)
Es MUSS gewährleistet werden, dass nur dafür vorgesehene Wechselspeicher und sonstige Geräte an die Server angeschlossen werden können. Alle Schnittstellen, die nicht verwendet werden, MÜSSEN deaktiviert werden.

SYS.1.1.A6 Deaktivierung nicht benötigter Dienste (B)
Alle nicht benötigten Dienste und Anwendungen MÜSSEN deaktiviert oder deinstalliert werden, vor allem Netzdienste. Auch alle nicht benötigten Funktionen in der Firmware MÜSSEN deaktiviert werden. Auf Servern SOLLTE der Speicherplatz für die einzelnen Benutzer, aber auch für Anwendungen, geeignet beschränkt werden.

Die getroffenen Entscheidungen SOLLTEN so dokumentiert werden, dass nachvollzogen werden kann, welche Konfiguration und Softwareausstattung für die Server gewählt wurden.

SYS.1.1.A7 ENTFALLEN (B)
Diese Anforderung ist entfallen.

SYS.1.1.A8 ENTFALLEN (B)
Diese Anforderung ist entfallen.

SYS.1.1.A9 Einsatz von Virenschutz-Programmen auf Servern (B)
Abhängig vom installierten Betriebssystem, den bereitgestellten Diensten und von anderen vorhandenen Schutzmechanismen des Servers MUSS geprüft werden, ob Viren-Schutzprogramme eingesetzt werden sollen und können. Soweit vorhanden, MÜSSEN konkrete Aussagen, ob ein Virenschutz notwendig ist, aus den betreffenden Betriebssystem-Bausteinen des IT-Grundschutz-Kompendiums berücksichtigt werden.

SYS.1.1.A10 Protokollierung (B)
Generell MÜSSEN alle sicherheitsrelevanten Systemereignisse protokolliert werden, dazu gehören mindestens:

- Systemstarts und Reboots,
- erfolgreiche und erfolglose Anmeldungen am System (Betriebssystem und Anwendungssoftware),
- fehlgeschlagene Berechtigungsprüfungen,
- blockierte Datenströme (Verstöße gegen ACLs oder Firewallregeln),
- Einrichtung oder Änderungen von Benutzern, Gruppen und Berechtigungen,
- sicherheitsrelevante Fehlermeldungen (z. B. Hardwaredefekte, Überschreitung von Kapazitätsgrenzen) sowie
- Warnmeldungen von Sicherheitssystemen (z. B. Virenschutz).

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.1.1 *Allgemeiner Server*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.1.A11 Festlegung einer Sicherheitsrichtlinie für Server (S)
Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an

Server in einer separaten Sicherheitsrichtlinie konkretisiert werden. Diese Richtlinie SOLLTE allen Administratoren und anderen Personen, die an der Beschaffung und dem Betrieb der Server beteiligt sind, bekannt und Grundlage für deren Arbeit sein. Die Umsetzung der in der Richtlinie geforderten Inhalte SOLLTE regelmäßig überprüft werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

SYS.1.1.A12 Planung des Server-Einsatzes (S)

Jedes Server-System SOLLTE geeignet geplant werden. Dabei SOLLTEN mindestens folgende Punkte berücksichtigt werden:

- Auswahl der Hardwareplattform, des Betriebssystems und der Anwendungssoftware,
- Dimensionierung der Hardware (Leistung, Speicher, Bandbreite etc.),
- Art und Anzahl der Kommunikationsschnittstellen,
- Leistungsaufnahme, Wärmelast, Platzbedarf und Bauform,
- Realisierung administrativer Zugänge (siehe SYS.1.1.A5 *Schutz der Administrationsschnittstellen*),
- Zugriffe von Benutzern,
- Realisierung der Protokollierung (siehe SYS.1.1.A10 *Protokollierung*),
- Realisierung der Systemaktualisierung (siehe SYS.1.1.A7 *Updates und Patches für Betriebssystem und Anwendungen*) sowie
- Einbindung ins System- und Netzmanagement, in die Datensicherung und die Schutzsysteme (Virenschutz, IDS etc.).

Alle Entscheidungen, die in der Planungsphase getroffen wurden, SOLLTEN so dokumentiert werden, dass sie zu einem späteren Zeitpunkt nachvollzogen werden können.

SYS.1.1.A13 Beschaffung von Servern (S)

Bevor ein oder mehrere Server beschafft werden, SOLLTE eine Anforderungsliste erstellt werden, anhand derer die am Markt erhältlichen Produkte bewertet werden.

SYS.1.1.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.1.A15 Unterbrechungsfreie und stabile Stromversorgung [Haustechnik] (S)

Jeder Server SOLLTE an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden.

SYS.1.1.A16 Sichere Grundkonfiguration von Servern (S)

Die Grundeinstellungen von Servern SOLLTEN überprüft und falls erforderlich entsprechend den Vorgaben der Sicherheitsrichtlinie angepasst werden. Erst nachdem die Installation und die Konfiguration abgeschlossen sind, SOLLTE der Server mit dem Internet verbunden werden.

SYS.1.1.A17 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.1.A18 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.1.A19 Einrichtung lokaler Paketfilter (S)

Vorhandene lokale Paketfilter SOLLTEN über ein Regelwerk so ausgestaltet werden, dass die eingehende und ausgehende Kommunikation auf die erforderlichen Kommunikationspartner, Kommunikationsprotokolle bzw. Ports und Schnittstellen beschränkt wird. Die Identität von Remote-Systemen und die Integrität der Verbindungen mit diesen SOLLTE kryptografisch abgesichert sein.

SYS.1.1.A20 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.1.A21 Betriebsdokumentation für Server (S)

Betriebliche Aufgaben, die an einem Server durchgeführt werden, SOLLTEN nachvollziehbar dokumentiert werden (Wer?, Wann?, Was?). Aus der Dokumentation SOLLTEN insbesondere Konfigurationsänderungen nachvollziehbar sein. Sicherheitsrelevante Aufgaben, z. B. wer befugt ist, neue Festplatten einzubauen, SOLLTEN dokumentiert werden. Alles, was automatisch dokumentiert werden kann, SOLLTE auch automatisch dokumentiert werden. Die Dokumentation SOLLTE gegen unbefugten Zugriff und Verlust geschützt werden.

SYS.1.1.A22 Einbindung in die Notfallplanung (S)

Der Server SOLLTE im Notfallmanagementprozess berücksichtigt werden. Dazu SOLLTEN die Notfallanforderungen an das System ermittelt und geeignete Notfallmaßnahmen umgesetzt werden, z. B. indem Wiederanlaufpläne erstellt oder Passwörter und kryptografische Schlüssel sicher hinterlegt werden.

SYS.1.1.A23 Systemüberwachung und Monitoring von Servern (S)

Das Server-System SOLLTE in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept eingebunden werden. Hierbei SOLLTEN der Systemzustand und die Funktionsfähigkeit des Systems und der darauf betriebenen Dienste laufend überwacht werden. Fehlerzustände sowie die Überschreitung definierter Grenzwerte SOLLTEN hierüber an das Betriebspersonal meldet werden.

SYS.1.1.A24 Sicherheitsprüfungen für Server (S)

Server SOLLTEN regelmäßigen Sicherheitstests unterzogen werden, die überprüfen, ob alle Sicherheitsvorgaben eingehalten werden und ggf. vorhandene Schwachstellen identifizieren. Diese Sicherheitsprüfungen SOLLTEN insbesondere auf Servern mit externen Schnittstellen durchgeführt werden. Um mittelbare Angriffe über infizierte Systeme im eigenen Netz zu vermeiden, SOLLTEN jedoch auch interne Server in festgelegten Zyklen entsprechend überprüft werden. Es SOLLTE geprüft werden, ob die Sicherheitsprüfungen automatisiert, z. B. mittels geeigneter Skripte, realisiert werden können.

SYS.1.1.A25 Geregelte Außerbetriebnahme eines Servers (S)

Bei der Außerbetriebnahme eines Servers SOLLTE sichergestellt werden, dass keine wichtigen Daten, die eventuell auf den verbauten Datenträgern gespeichert sind, verloren gehen und dass keine schutzbedürftigen Daten zurückbleiben. Es SOLLTE einen Überblick darüber geben, welche Daten wo auf dem Server gespeichert sind. Es SOLLTE außerdem sichergestellt sein, dass vom Server angebotene Dienste durch einen anderen Server übernommen werden, wenn dies erforderlich ist.

Es SOLLTE eine Checkliste erstellt werden, die bei der Außerbetriebnahme eines Servers abgearbeitet werden kann. Diese Checkliste SOLLTE mindestens Aspekte zur Datensicherung, Migration von Diensten und dem anschließenden sicheren Löschen aller Daten umfassen.

SYS.1.1.A35 Erstellung und Pflege eines Betriebshandbuchs (S)

Es SOLLTE ein Betriebshandbuch erstellt werden. Darin SOLLTEN alle erforderlichen Regelungen, Anforderungen und Einstellungen dokumentiert werden, die erforderlich sind, um Server zu betreiben. Für jede Art von Server SOLLTE es ein spezifisches Betriebshandbuch geben. Das Betriebshandbuch SOLLTE regelmäßig aktualisiert werden. Das Betriebshandbuch SOLLTE vor unberechtigtem Zugriff geschützt werden. Das Betriebshandbuch SOLLTE in Notfällen zur Verfügung stehen.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.1.1 *Allgemeiner Server* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

SYS.1.1.A26 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.1.A27 Hostbasierte Angriffserkennung (H)

Hostbasierte Angriffserkennungssysteme (Host-based Intrusion Detection Systems, IDS bzw. Intrusion Prevention Systems, IPS) SOLLTEN eingesetzt werden, um das Systemverhalten auf Anomalien und Missbrauch hin zu überwachen. Die eingesetzten IDS/IPS-Mechanismen SOLLTEN geeignet ausgewählt, konfiguriert und ausführlich getestet werden. Im Falle einer Angriffserkennung SOLLTE das Betriebspersonal in geeigneter Weise alarmiert werden.

Über Betriebssystem-Mechanismen oder geeignete Zusatzprodukte SOLLTEN Veränderungen an Systemdateien und Konfigurationseinstellungen überprüft, eingeschränkt und gemeldet werden.

SYS.1.1.A28 Steigerung der Verfügbarkeit durch Redundanz (H)

Server mit hohen Verfügbarkeitsanforderungen SOLLTEN gegen Ausfälle in geeigneter Weise geschützt sein. Hierzu SOLLTEN mindestens geeignete Redundanzen verfügbar sein sowie Wartungsverträge mit den Lieferanten abgeschlossen werden. Es SOLLTE geprüft werden, ob bei sehr hohen Anforderungen Hochverfügbarkeitsarchitekturen mit automatischem Failover, gegebenenfalls über verschiedene Standorte hinweg, erforderlich sind.

SYS.1.1.A29 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.1.A30 Ein Dienst pro Server (H)

Abhängig von der Bedrohungslage und dem Schutzbedarf der Dienste SOLLTE auf jedem Server jeweils nur ein Dienst betrieben werden.

SYS.1.1.A31 Application Whitelisting (H)

Es SOLLTE bei erhöhtem Schutzbedarf über Application Whitelisting sichergestellt werden, dass nur erlaubte Programme ausgeführt werden. Zum einen SOLLTEN vollständige Pfade bzw. Verzeichnisse festgelegt werden, aus denen diese Programme ausgeführt werden dürfen. Zum anderen SOLLTE alternativ einzelnen Anwendungen explizit die Ausführung gestattet werden.

SYS.1.1.A32 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.1.1.A33 Aktive Verwaltung der Wurzelzertifikate (H)

Im Zuge der Beschaffung und Installation des Servers SOLLTE dokumentiert werden, welche Wurzelzertifikate für den Betrieb des Servers notwendig sind. Auf dem Server SOLLTEN lediglich die für den Betrieb notwendigen und vorab dokumentierten Wurzelzertifikate enthalten sein. Es SOLLTE regelmäßig überprüft werden, ob die vorhandenen Wurzelzertifikate noch den Vorgaben der Institution entsprechen. Es SOLLTEN alle auf dem IT-System vorhandenen Zertifikatsspeicher in die Prüfung einbezogen werden.

SYS.1.1.A34 Festplattenverschlüsselung (H)

Bei erhöhtem Schutzbedarf sollten die Datenträger des Servers mit einem als sicher geltenden Produkt bzw. Verfahren verschlüsselt werden. Dies SOLLTE auch für virtuelle Maschinen mit produktiven Daten gelten. Es SOLLTE nicht nur ein TPM allein als Schlüsselschutz dienen. Das Wiederherstellungspasswort SOLLTE an einem geeigneten sicheren Ort gespeichert werden. Bei sehr hohen Anforderungen z. B. an die Vertraulichkeit SOLLTE eine Full Volume oder Full Disk Encryption erfolgen.

SYS.1.1.A36 Absicherung des Bootvorgangs (H)

Bootloader und Betriebssystem-Kern SOLLTEN durch selbstkontrolliertes Schlüsselmaterial signiert beim Systemstart in einer vertrauenswürdigen Kette geprüft werden (Secure Boot). Nicht benötigtes Schlüsselmaterial SOLLTE entfernt werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Das National Institute of Standards and Technology (NIST) stellt das Dokument „Guide to General Server Security: NIST Special Publication 800-123“, Juli 2008 zur Verfügung.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein SYS.1.1 *Allgemeiner Server* von Bedeutung.

G 0.8 Ausfall oder Störung der Stromversorgung

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.43 Einspielen von Nachrichten

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen