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

Sicherheitsrichtlinie "Linux und Unix Server"

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 Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300026 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Linux und Unix Server" | [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](#_Toc80531799)

[Dokumentenhistorie 3](#_Toc80531800)

[Inhaltsverzeichnis 4](#_Toc80531801)

[Allgemeine Festlegungen 5](#_Toc80531802)

[Ziel / Zweck 5](#_Toc80531803)

[Geltungsbereich 5](#_Toc80531804)

[Zuständigkeiten 6](#_Toc80531805)

[Genehmigungs- und Änderungsverfahren 6](#_Toc80531806)

[Aufbau des Dokuments 6](#_Toc80531807)

[Sicherheitsrichtlinie „Linux und Unix Server" 7](#_Toc80531808)

[Basismaßnahmen 7](#_Toc80531809)

[Allgemeiner Server 7](#_Toc80531810)

[Unix Server 9](#_Toc80531811)

[Standardmaßnahmen 10](#_Toc80531812)

[Allgemeiner Server 10](#_Toc80531813)

[Unix Server 13](#_Toc80531814)

[Maßnahmen bei erhöhtem Schutzbedarf 14](#_Toc80531815)

[Allgemeiner Server 14](#_Toc80531816)

[Unix Server 16](#_Toc80531817)

# Allgemeine Festlegungen

## Ziel / Zweck

Auf Server-Systemen werden häufig die Betriebssysteme Linux oder Unix eingesetzt. Beispiele für klassische Unix-Systeme sind die BSD-Reihe (FreeBSD, OpenBSD und NetBSD), Solaris und AIX. Linux bezeichnet hingegen kein klassisches Unix, sondern ist ein funktionelles Unix-System. Das heißt, dass der Linux-Kernel nicht auf dem ursprünglichen Quelltext basiert, aus dem sich die verschiedenen Unix-Derivate entwickelt haben. In dieser Sicherheitsrichtlinie werden alle Betriebssysteme der Unix-Familie übergreifend betrachtet, also auch Linux als funktionelles Unix-System. Da sich die Konfiguration und der Betrieb von Linux- und Unix-Servern ähneln, werden Linux und Unix sprachlich als „Unix-Server“ bzw. „unixartig“ zusammengefasst.

Die auf einem Unix-Server angebotenen Dienste sind oft zentral und daher in besonderem Maße exponiert. Aus diesem Grund sind Unix-Server nicht nur für Geschäftsprozesse oder Fachaufgaben kritisch, sondern geraten außerdem häufig in den Fokus von Angreifern. Deswegen kommen der Verfügbarkeit und Absicherung von Unix-Servern eine besondere Bedeutung zu.

Ziel der Sicherheitsrichtlinie ist der Schutz von Informationen, die von Unix-Servern bereitgestellt und verarbeitet werden. Die Anforderungen in dieser Sicherheitsrichtlinie gelten vorrangig für Linux-Server, können aber generell für Unix-Server adaptiert werden. Es werden Anforderungen formuliert, wie das Betriebssystem unabhängig vom Einsatzzweck des Servers konfiguriert und betrieben werden soll.

Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben der BSI Bausteine SYS.1.1. „Allgemeiner Server" und SYS.1.3 „Server unter Linux und Unix" beachtet. Aus diesem Grunde wurden die Anforderungen in die Abschnitte „Allgemeiner Server" und „Unix Server" zusätzlich unterteilt.

## 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 „Linux und Unix Server“ 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 „Linux und Unix Server"

## Basismaßnahmen

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

### Allgemeiner Server

#### Geeignete Aufstellung (SYS.1.1.A1)

Die Systeme sind in einem speziell dafür vorgesehenen Raum aufzustellen. Server müssen daher in Rechenzentren, Rechnerräumen oder abschließbaren Serverschränken aufgestellt beziehungsweise eingebaut werden. Besondere Infrastrukturen wie Zutrittskontrolle, Temperaturregulierung, Luftfeuchteregulierung, mehrere Stromkreise, die mit einer USV abgesichert sind, Alarm- und Löschsysteme für Feuer sowie ein Alarmsystem für Wasser, sind in diesen Räumen zu installieren. Die Server, die gesichert werden sollen, müssen geeignet von den sichernden Systemen, etwa Backup-Servern, in unterschiedlichen Brandabschnitten getrennt werden.

Es ist zu regeln, wer Zutritt zu den Räumen beziehungsweise zu den Servern selbst erhält.

#### Benutzerauthentisierung an Servern (SYS.1.1.A2)

Für die Anmeldung von Benutzern und Diensten am Server sind Authentisierungsverfahren einzusetzen, die dem Schutzbedarf der Server angemessen sind. Dieses ist in besonderem Maße für administrative Zugänge zu berücksichtigten. Soweit möglich, sind dabei zentrale, netzbasierte Authentisierungsdienste zu bevorzugen. Verwendete Passwörter müssen sicher sein.

Die Authentisierung beziehungsweise Autorisierung muss gemäß den Anforderungen für das Identitäts- und Berechtigungsmanagement erfolgen.

#### Restriktive Rechtevergabe (SYS.1.1.A3)

Zugriffsrechte auf Dateien, die auf Servern gespeichert sind, sind restriktiv zu vergeben. Jeder Benutzer darf nur auf die Dateien zugreifen können, die er für seine Aufgabenerfüllung benötigt (Need-to-know-Prinzip). Nur Mitarbeitende mit administrativen Zugriffsrechten dürfen auf die Systemverzeichnisse zugreifen.

Alle Anträge, Änderungen, Löschungen und Freigaben zu Zugriffsrechten sind geeignet zu dokumentieren. Es sollte regelmäßig überprüft werden, ob die Berechtigungen, insbesondere für Systemverzeichnisse und -dateien, den Vorgaben der <Institution> entsprechen.

#### Rollentrennung (SYS.1.1.A4)

Es ist sicherzustellen, dass Kennungen mit Administratorrechten nur für Administrationsaufgaben verwendet werden. Für alle Administratoren sind zusätzliche Benutzerkennungen einzurichten, die nur über die eingeschränkten Rechte verfügen, die die Administratoren zur Aufgabenerfüllung außerhalb der Administration benötigen. Für Arbeiten, die nicht der Administration dienen, dürfen die Administratoren nur diese Benutzerkennungen verwenden. Über die notwendigen Benutzerkennungen hinaus sollten keine weiteren Benutzer auf dem Server angelegt werden.

Die Installation, Modifikation, Änderung oder Löschung von Anwendungen und Systemkonfigurationen sollte nur durch die Administration unter Zuhilfenahme von zentralen Managementwerkzeugen erfolgen.

#### Schutz der Administrationsschnittstellen (SYS.1.1.A5)

Die Administration der Server muss über freigegebene kryptografische Protokolle und Algorithmen erfolgen. Die Tools, Methoden und die Sicherheitsvorkehrungen sind geeignet zu dokumentieren.

Die Administration der Server sollte aus einem dedizierten Sicherheitsbereich für Administration heraus erfolgen.

#### Deaktivierung nicht benötigter Dienste und Kennungen (SYS.1.1.A6)

Nach der Installation sind nur solche Module, Programme, Dienste, Benutzerkennungen und Schnittstellen aktiv, die für die Verwendung des Systems an der vorgesehenen Einsatzstelle notwendig sind. Alle nicht benötigten Komponenten bzw. Funktionen sind zu deaktivieren oder zu deinstallieren. Nicht benötigte Benutzerkennungen sind entweder zu löschen oder zumindest so zu deaktivieren, dass unter diesen Kennungen keine Anmeldungen am System weiterhin möglich sind. Vorhandene Default-Kennungen sind soweit möglich zu deaktivieren oder zumindest zu ändern. Voreingestellte Default-Passwörter und Default-Passwörter von Default-Kennungen sind zu ändern. Auf Servern sollte der Speicherplatz für die einzelnen Benutzer, aber auch für Anwendungen, geeignet beschränkt werden.

Die Konfiguration und die Veränderungen dieser Einstellungen an den Servern sind zu dokumentieren und dürfen nur mit administrativen Rechten durchgeführt werden.

#### Updates und Patches für Firmware, Betriebssystem und Anwendungen (SYS.1.1.A7)

Die verantwortlichen Administratoren müssen sich regelmäßig über bekannt gewordene Schwachstellen der Firmware, Betriebssysteme, eingesetzter Anwendungen und Dienste informieren. Die identifizierten Schwachstellen sind so schnell wie möglich zu beheben. Grundsätzlich ist darauf zu achten, dass Patches und Updates nur aus vertrauenswürdigen Quellen bezogen werden.

Solange kein entsprechender Patch zur Verfügung steht, ist abhängig vom Schweregrad (Impact) der Schwachstelle und Bedrohungen eine geeignete Maßnahme (Workaround) zum Schutz des Systems zu etablieren.

#### Regelmäßige Datensicherung (SYS.1.1.A8)

Unter Berücksichtigung der etablierten Datensicherungsverfahren sind die Server regelmäßig zu sichern. In virtuellen Umgebungen sollte geprüft werden, ob das System unter Umständen durch Snapshot-Mechanismen der Virtualisierungsumgebung gesichert werden kann.

Die Wiederherstellung einer Datensicherung ist zur Minimierung von Fehlern im Datensicherungsprozess regelmäßig zu üben. Zur Vermeidung von Fehlfunktionen ist beim Einspielen einer Datensicherung darauf zu achten, dass die Wiederherstellung von produktiv Systemen zuvor auf einem identisch eingerichteten Testsystem stattfindet. Im Rahmen des Notfallplans sind der Wiederanlauf, die Wiederherstellung und die benötigten Zeiten zu definieren. Der Notfallplan sollte durch praktische Tests validiert und kontinuierlich verbessert werden.

#### Einsatz von Virenschutz-Programmen (SYS.1.1.A9)

Bei der Auswahl des Virenschutz-Programmes sind die zu unterstützenden Betriebssysteme sowie die Service- und Supportleistungen des Herstellers zu berücksichtigen. Bei der Nutzung von Cloud-Diensten ist zu prüfen und zu dokumentieren, ob Datenschutzaspekte eventuell gegen den Einsatz sprechen. Alle Server sind in eine zentrale Infrastruktur zur Erkennung, Behandlung und Vermeidung von Malware zu integrieren.

Die Virenschutz-Programme und deren Signaturen sind nach den Vorgaben des Herstellers zu aktualisieren. Nach einem Update der Virenschutz-Programme sollten die Konfigurationseinstellungen mit den dokumentierten Vorgaben abgeglichen werden.

Es ist sicherzustellen, dass die berechtigten Administratoren oder installierten Anwendungen keine sicherheitsrelevanten Konfigurationsänderungen am Virenschutz-Programm vornehmen oder dieses deaktivieren.

#### Protokollierung (SYS.1.1.A10)

Alle sicherheitsrelevanten Ereignisse von Servern und Anwendungen sind zu protokollieren. Diese umfassen 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).

Bei der Einrichtung der Protokollierung sind die Herstellervorgaben für die jeweiligen IT-Systeme oder Anwendungen zu beachten und in einem angemessenen Rahmen anzuwenden.

Es ist in geeigneten Intervallen stichpunktartig zu überprüfen, ob die Protokollierung noch korrekt funktioniert. Die Intervalle sollten an die zu berücksichtigen Server und deren ermittelten Schutzbedarf (Verfügbarkeit, Vertraulichkeit und Integrität) angepasst werden.

Bei der Protokollierung sind die gesetzlichen Datenschutzbestimmungen einzuhalten. Dazu zählen unter anderem die gesetzlichen Anforderungen der EU-DSGVO und des BDSG-neu. Sofern wir Kunden aus dem öffentlichen Sektor betreuen, können zusätzlich landestypische Datenschutzanforderungen mit zu beachten sein. Die Protokollierungsdaten sind nach einem festgelegten Aufbewahrungsprozess zu löschen.

Seitens der <Institution> wird technisch unterbunden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden können.

### Unix Server

#### Authentisierung von Administratoren und Benutzern (SYS.1.3.A1)

Alle Benutzer müssen sich gegenüber dem Unix-Server authentisieren. Die Authentisierung über ein Netz muss verschlüsselt sein. Wenn ein Benutzerkonto auf bestimmte Dienste wird, darf dieses das Benutzerkonto nicht für andere Dienste außer den freigegeben genutzt werden können.

#### Sorgfältige Vergabe von IDs (SYS.1.3.A2)

Jeder Login-Name, jede Benutzer-ID (User-ID, UID) und jede Gruppen-ID (GID) darf auf dem Unix-Server nur einmal vorkommen. Jeder Benutzer auf dem Unix-Server muss mindestens Mitglied einer Gruppe sein. Jede in der Datei /etc/passwd vorkommende GID muss in der Datei /etc/group definiert sein. Jede Gruppe darf nur die Benutzer enthalten, die unbedingt notwendig sind. Bei vernetzten Servern muss außerdem darauf geachtet werden, dass die Vergabe von Benutzer- und Gruppennamen, UID und GID im Serververbund konsistent erfolgt.

#### Kein automatisches Einbinden von Wechsellaufwerken (SYS.1.3.A3)

Wechseldatenträger wie z. B. USB-Sticks oder CDs/DVDs dürfen nicht automatisch eingebunden werden.

#### Schutz vor Ausnutzung von Schwachstellen in Anwendungen (SYS.1.3.A4)

Alle Möglichkeiten um die Ausnutzung von Schwachstellen zu erschweren (z. B. Address Space Layout Randomization (ASLR) und Data Execution Prevention/ No-Execute (DEP/NX)) sind im Kernel zu aktivieren.

Die Sicherheitsfunktionen des Kernels und der Standardbibliotheken, wie z. B. Heap- und Stackschutz sind zu aktivieren.

#### Sichere Installation von Software-Paketen (SYS.1.3.A5)

Auf den Systemen sind nur benötigte und auf der Whitelist befindliche Anwendungen zu installieren. Die Anwendungen dürfen ausschließlich aus einer vertrauenswürdiger Quelle bezogen und die Integrität und Authentizität der zu installierenden Softwarepakete ist immer zu prüfen.

Müssen Programme vor der Installation entpackt, konfiguriert, kompiliert oder übersetzt werden, geschieht dies mit einem nicht privilegierten Benutzeraccount. Alle Aktivitäten vor und zur Installation von Anwendungssoftware sind zu dokumentieren.

## Standardmaßnahmen

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

### Allgemeiner Server

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

Jedes Server-System sollte geeignet geplant werden. Dabei sind mindestens die folgenden Punkte zu berücksichtigen 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,
* Zugriffe von Benutzern,
* Realisierung der Protokollierung,
* Realisierung der Systemaktualisierung sowie
* Einbindung ins System- und Netzmanagement, in die Datensicherung und die Schutzsysteme (Virenschutz, IDS etc.).

Alle Entscheidungen, die in der Planungsphase getroffen wurden, sind nachvollziehbar zu dokumentieren.

#### Beschaffung von Servern (SYS.1.1.A13)

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

#### Erstellung eines Benutzer- und Administrationskonzepts (SYS.1.1.A14)

Bei den eingesetzten Servern muss eine Funktionstrennung zwischen der Administration des Betriebssystemsystems und dem normalen Standardnutzer erfolgen. Nur verantwortliche Administratoren erhalten eine zusätzliche Benutzerkennung mit Administrationsrechten für das Server-System.

Die Installation, Modifikation, Änderung oder Löschung von Anwendungen und Systemkonfigurationen dürfen nur durch ein zentrales Konfigurationsmanagement und den verantwortlichen Administratoren erfolgen.

Die Rahmenbedingungen, Anforderungen und Aufgabentrennungen an die Rollen des Benutzers und der Administration sind im Standard „IT-Administration“ festgelegt.

#### Unterbrechungsfreie und stabile Stromversorgung (SYS.1.1.A15)

Jeder Server sollte an eine unterbrechungsfreie Stromversorgung (USV) angeschlossen werden. Die USV sollte eine ausreichende Leistung und Kapazität haben. Es ist erneut zu prüfen, ob die Stützzeit der verwendeten USV ausreicht, wenn Änderungen an den Verbrauchern durchgeführt wurden.

Die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV ist regelmäßig zu testen. Die USV ist in die zentralen Wartungspläne aufzunehmen. Sofern die USV zentral überwacht und verwaltet werden kann, ist diese in ein vorhandenes System- und Netzmanagement einzubinden.

#### Sichere Installation und Grundkonfiguration von Servern (SYS.1.1.A16)

Die Installation von Servern muss auf Basis eines dokumentierten Installationsprozess und ausschließlich durch die verantwortlichen Administratoren erfolgen. Soweit vorhanden, sind Installation-Templates oder zentrale Verwaltungssysteme wie bspw. Puppet, SaltStack, Chef, Ansible zu verwenden.

Die System- und Anwendungssoftware ist vertrauenswürdigen Installationsquellen zu beziehen.

Alle nicht benötigten Dienste, Prozesse und Benutzer sind zu entfernen, alle Standardpasswörter sind zu ändern.

Alle Installationsschritte sollten so dokumentiert werden, dass die Installation durch einen sachkundigen Dritten nachvollzogen und wiederholt werden kann.

#### Einsatzfreigabe für Server (SYS.1.1.A17)

Bevor Server im produktiven Betrieb eingesetzt und bevor die Server an ein produktives Netz angeschlossen werden, sollte eine Prüfung und Einsatzfreigabe erfolgen. Mittels Soll-/Ist-Vergleich zwischen der Anforderungsliste und der aktuellen Installation sowie der Prüfung, ob nur benötigte Dienste und Prozesses auf dem System laufen sollte die Einsatzfreigabe vorbereitet werden. Die Prüfung/Tests umfassen auch die Verifizierung der einwandfreien Funktion des Systems sowie der Anwendungssoftware.

Alle Ergebnisse der Prüfungen und Tests sollten geeignet dokumentiert und abgelegt werden.

Sind alle Tests und Prüfungen ohne Auffälligkeiten bestanden, ist der Server an das produktive Netzwerk anzuschließen.

#### Verschlüsselung der Kommunikationsverbindungen (SYS.1.1.A18)

Für alle vom Server angebotenen und genutzten Netzdienste ist zu prüfen, ob mit vertretbarem Aufwand eine Verschlüsselung der Kommunikationsverbindungen möglich und praktikabel ist. Ist dies der Fall, so ist die Verschlüsselung entsprechend den internen Vorgaben der <Institution> zu aktivieren.

#### Einrichtung lokaler Paketfilter (SYS.1.1.A19)

Für die lokale Kommunikationsfilterung und gestaffelte Verteidigung (Defense-in-Depth) sind bei erhöhtem Schutzbedarf neben der Segmentierung von Netzen, Zonierung und Paketfilterung durch dedizierte und aktive Firewalls eine lokale Paketfilterung zu aktivieren. Zum weiteren Schutz wird die lokale Firewall auf dem Server-System für den eingehenden und ausgehenden Datenverkehr strikt eingestellt/aktiviert. Die Identität von einem entfernten System und die Integrität der Verbindungen mit dem entfernten System sind kryptografisch abzusichern.

#### Beschränkung des Zugangs über Netze (SYS.1.1.A20)

Generell sollte das gesamte Netz durch eine entsprechende Firewall-Infrastruktur gegen unbefugte Zugänge geschützt sein. Server, die Dienste nach außen hin anbieten, sind in einer Demilitarisierten Zone (DMZ) aufzustellen.

Server dürfen nicht im selben IP-Subnetz wie die Clients platziert sein. Server sind mindestens durch ein Layer-3-Gerät (Router, L3-Switch, Firewall) von den Clients zu trennen.

#### Betriebsdokumentation für Server (SYS.1.1.A21)

Zur Betriebsdokumentation sind die Server in das zentrale Monitoring einzubinden. Alle manuellen Tätigkeiten, wie z. B. der Austausch des Speichers oder Änderungen an der Konfiguration, sind in die Serverdokumentation einzupflegen.

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

Der Server ist im Notfallmanagementprozess zu berücksichtigen. 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.

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

Das Server-System ist in ein geeignetes Systemüberwachungs- bzw. Monitoringkonzept einzubinden, das den Systemzustand und die Funktionsfähigkeit des Systems und der darauf betriebenen Dienste laufend überwacht und Fehlerzustände sowie die Überschreitung definierter Grenzwerte an die verantwortlichen Mitarbeitenden meldet.

Beim Überschreiten definierter Grenzwerte sind entsprechende Alarme auszulösen.

#### Sicherheitsprüfungen (SYS.1.1.A24)

Die Server sind regelmäßigen Sicherheitstests zu unterziehen, die überprüfen, ob alle Sicherheitsvorgaben der <Institution> eingehalten werden und ggf. vorhandene Schwachstellen identifizieren. Diese Sicherheitsprüfungen sind insbesondere auf Servern mit externen Schnittstellen durchzuführen. Um mittelbare Angriffe über infizierte Systeme 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.

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

Die Außerbetriebnahme von Servern erfolgt dokumentiert. Dabei ist auf die Sicherung aller notwendigen Daten zu achten. Die Speichermodule sind entweder sicher zu löschen oder einer zertifizierten Zerstörung zu zuführen. Alle angebrachten Beschriftungen sind zu entfernen.

### Unix Server

#### Verwaltung von Benutzern und Gruppen (SYS.1.3.A6)

Zur Verwaltung von Benutzern auf den Systemen werden entsprechende Verwaltungswerkzeuge genutzt. Eine direkte Bearbeitung der Konfigurationsdateien "/etc/passwd" und "/etc/group" und "/etc/sudoers" erfolgt nicht.

#### Verschlüsselter Zugriff über Secure Shell (SYS.1.3.A8)

Um eine verschlüsselte und authentisierte interaktive Verbindung zwischen einem Administratoren Client und einem Unix Server aufzubauen, soll ausschließlich SSH in Version 2 verwendet werden. Alle anderen Protokolle, deren Funktionalität durch Secure Shell abgedeckt wird, müssen vollständig abgeschaltet werden.

Bei der Verwendung von SSH dürfen nur die freigegebenen Versionen, Algorithmen und Verfahren eingesetzt werden.

#### Absicherung des Bootvorgangs (SYS.1.3.A9)

Beim Booten ist die Integrität vom (Pre-) Bootloader bis zum Kernel zu überprüfen. Die hierfür genutzten Schlüssel sollten bei der Ersteinrichtung überprüft werden. Es ist zu prüfen, ob hierfür Secure Boot als Teil der UEFI-Spezifikation genutzt werden kann.

#### Verhinderung der Ausbreitung bei der Ausnutzung von Schwachstellen (SYS.1.3.A10)

Alle vorinstallierten Standardprofile und Regeln sind an den definierten Schutzbedarf der <Institution> anzupassen und zu aktivieren.

Dienste und Anwendungen sind mit individuellen Sicherheitsrichtlinien bspw. mit Hilfe von AppArmor oder SELinux abzusichern. Auch chroot-Umgebungen sowie LXC- oder Docker-Container sind zu berücksichtigen.

#### Einsatz der Sicherheitsmechanismen von NFS (SYS.1.3.A11)

Die über Network File System (NFS) exportierten bzw. mountbaren Verzeichnisse sind auf das notwendige Minimum zu reduzieren. Dies bedeutet in den Dateien "/etc/exports" bzw. "/etc/dfs/fstab" sollten die mountbaren Verzeichnisse auf das notwendige Maß reduziert werden.

Die mountbaren Verzeichnisse sind nur für bestimmte IT-Systeme sowie Benutzer unter Berücksichtigung der festgelegten Berechtigungsstruktur freizugeben. Sofern NFS eingesetzt wird ist die Version 4 zu verwenden und die Benutzerauthentisierung sollte auf Basis von LDAP erfolgen.

#### Einsatz der Sicherheitsmechanismen von NIS (SYS.1.3.A12)

Network Information Service (NIS) darf nur in einer sicheren Umgebung eingesetzt werden. In "/etc/passwd" und "/etc/group" sowie allen anderen sicherheitsrelevanten Dateien darf der Eintrag "+::0:0:::" nicht enthalten sein. Der Server-Prozess ypserv darf nur Anfragen von vorher festgelegten IT-Systemen beantworten.

## 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).

### Allgemeiner Server

#### Mehr-Faktor-Authentisierung (SYS.1.1.A26 - CIA)

Bei höherem Schutzbedarf ist eine sichere Mehr-Faktor-Authentisierung für den Zugang zum Server einzurichten. Insbesondere gilt dies für alle administrativen Zugänge zum Server.

#### Hostbasierte Angriffserkennung (SYS.1.1.A27 - CA)

Hostbasierte Angriffserkennungssysteme (Host-based Intrusion Detection Systems (HIDS) bzw. Host-based Intrusion Prevention Systems (HIPS)) sollten eingesetzt werden, um das Systemverhalten des Servers auf Anomalien und Missbrauch hin zu überwachen. Sofern HIDS/HIPS-Mechanismen eingesetzt werden, sind diese geeignet auszuwählen, zu konfigurieren und ausführlich zu testen. Im Falle einer Angriffserkennung sind die Verantwortlichen für den Server in geeigneter Weise zu alarmieren.

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

#### Steigerung der Verfügbarkeit durch Redundanz (SYS.1.1.A28 - A)

Server mit hohen Verfügbarkeitsanforderungen sind gegen Ausfälle in geeigneter Weise zu schützen. Hierzu sollten mindestens geeignete Redundanzen verfügbar sein sowie Wartungsverträge mit den Lieferanten abgeschlossen werden. Es ist zu prüfen, ob bei sehr hohen Anforderungen GEO-redundante Hochverfügbarkeitsarchitekturen mit automatischem Failover erforderlich sind.

#### Einrichtung einer Testumgebung (SYS.1.1.A29 - CIA)

Um Veränderungen am System oder der Konfiguration des Servers testen zu können ohne den produktiven Betrieb zu gefährden, sind entsprechende Testsysteme (bspw. funktionale und architektonische Referenzen der produktiven Server) vorzuhalten oder bei Bedarf bereitzustellen. Für Anwendungssysteme sollten geeignete Testdaten generiert werden, die keine vertraulichen oder personenbezogenen Inhalte der produktiven Daten enthalten.

Die Ergebnisse der durchgeführten Tests sind geeignet zu dokumentieren.

#### Ein Dienst pro Server (SYS.1.1.A30 - CIA)

Abhängig von der Bedrohungslage und dem Schutzbedarf der Dienste ist auf einem Server nur jeweils ein Dienst (Service) zu betrieben.

#### Application Whitelisting (SYS.1.1.A31 - CA)

Über eine Application-Whitelist ist sicherzustellen, dass auf dem Server nur freigegebene Software installiert und ausgeführt wird. Die Anwendungssoftware wird nur in dafür vorgesehene Verzeichnisse installiert. Anwendungen außerhalb dieser Verzeichnisse können nicht ausgeführt werden.

#### Zusätzlicher Schutz von privilegierten Anmeldeinformationen (SYS.1.1.A32 - CA)

Passwörter für administrative Konten sollten in mehrere Teile zerlegt werden. Um diese Anmeldeinformationen zusätzlich zu schützen, sollte das Vier-Augen-Prinzip angewendet werden. Auch administrative Konten sollten so eingerichtet werden, dass diese nach einer vorher festgelegten Anzahl fehlerhafter Anmeldeversuche gesperrt werden.

#### Aktive Verwaltung der Wurzelzertifikate (SYS.1.1.A33 - CIA)

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 sind alle auf dem Server vorhandenen Zertifikatsspeicher in die Prüfung einzubeziehen.

#### Festplattenverschlüsselung (SYS.1.1.A34 - CI)

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 ist an einem geeigneten sicheren Ort zu speichern. Bei sehr hohen Anforderungen an die Vertraulichkeit oder Abstreitbarkeit ist eine Full Volume Encryption zu etablieren.

### Unix Server

#### Verhinderung des Ausspähens von System- und Benutzerinformationen (SYS.1.3.A14 - CI)

Die Ausgabe von Informationen über das Betriebssystem und der Zugriff auf Protokoll- und Konfigurationsdateien ist für Benutzer auf das notwendige Maß zu beschränken. Außerdem sollten bei Befehlsaufrufen keine vertraulichen Informationen als Parameter übergeben werden.

#### Zusätzliche Absicherung des Bootvorgangs (SYS.1.3.A15 - CI)

Der Bootloader und der Kernel sind durch selbstkontrolliertes Schlüsselmaterial zu signieren und nicht benötigtes Schlüsselmaterial ist zu entfernen.

#### Zusätzliche Verhinderung der Ausbreitung bei der Ausnutzung von Schwachstellen (SYS.1.3.A16 - C)

Die Nutzung von Systemaufrufen sind insbesondere für exponierte Dienste und Anwendungen auf die unbedingt notwendige Anzahl zu beschränken. Die Standardprofile bzw. -regeln von bspw. SELinux, AppArmor sollten manuell überprüft und bei Bedarf an die Sicherheitsrichtlinien der <Institution> angepasst werden. Falls erforderlich, sind neue Regeln bzw. Profile zu erstellen.

#### Zusätzlicher Schutz des Kernels (SYS.1.3.A17 - CIA)

Mit speziell gehärteten Kernels sind geeignete Schutzmechanismen wie Speicherschutz, Dateisystemabsicherung und rollenbasierte Zugriffskontrolle zu etablieren, um die Ausnutzung von Schwachstellen im Netz und die Ausbreitung von Schwachstellen im Betriebssystem zu verhindern.