



## SYS.1: Server

# SYS.1.3: Server unter Linux und Unix

## 1 Beschreibung

### 1.1 Einleitung

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 diesem Baustein werden alle Betriebssysteme der Unix-Familie betrachtet, also auch Linux als funktionelles Unix-System. Da sich die Konfiguration und der Betrieb von Linux- und Unix-Servern ähneln, werden in diesem Baustein Linux und Unix sprachlich als „Unix-Server“ bzw. „unixartig“ zusammengefasst.

Linux ist freie Software, die von der Open-Source-Gemeinschaft entwickelt wird. Das bedeutet, dass sie von jedem genutzt, kopiert, verteilt und verändert werden darf. Daneben gibt es Anbieter, die die verschiedenen Software-Komponenten zu einer Distribution zusammenfassen und pflegen sowie weitere Dienstleistungen anbieten. Für Linux-Server werden häufig die Distributionen Debian, Red Hat Enterprise Linux / CentOS, SUSE Linux Enterprise / openSUSE oder Ubuntu Server eingesetzt. Darüber hinaus gibt es für spezielle Einsatzzwecke und Geräte zugeschnittene Linux-Distributionen wie OpenWRT für Router.

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 kommt der Verfügbarkeit und Absicherung von Unix-Servern eine besondere Bedeutung zu.

### 1.2 Zielsetzung

Ziel des Bausteins ist der Schutz von Informationen, die von Unix-Servern bereitgestellt und verarbeitet werden. Die Anforderungen des Bausteins 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.

### 1.3 Abgrenzung und Modellierung

Der Baustein SYS.1.3 *Server unter Linux und Unix* ist für alle Server anzuwenden, auf denen Linux- oder Unix-basierte Betriebssysteme eingesetzt werden.

Der Baustein enthält grundsätzliche Anforderungen zur Einrichtung und zum Betrieb von Unix-Servern. Er konkretisiert und ergänzt die Aspekte, die im Baustein SYS.1.1 *Allgemeiner Server* behandelt werden, um Besonderheiten von Unix-Systemen.

Sicherheitsanforderungen möglicher Server-Funktionen wie Webserver (siehe APP.3.2 *Webserver*) oder E-Mail-Server (siehe APP.5.3 *Allgemeiner E-Mail-Client und -Server*) werden nicht in dem vorliegenden Baustein betrachtet, sondern sind Gegenstand eigener Bausteine. Eine Ausnahme ist der Unix-spezifische Server-Dienst SSH, der ebenfalls in diesem Baustein behandelt wird. Das Thema Virtualisierung wird ebenfalls nicht im vorliegenden Baustein beleuchtet, sondern im Baustein SYS.1.5 *Virtualisierung*.

## 2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein SYS.1.3 *Server unter Linux und Unix* von besonderer Bedeutung:

### 2.1 Ausspähen von System- und Benutzerinformationen

Mithilfe verschiedener Unix-Programme ist es möglich, Daten abzufragen, die das IT-System über die Benutzer speichert. Hiervon sind auch solche Daten betroffen, die Auskunft über das Leistungsprofil eines Benutzers geben können. Zu diesen Informationen zählen sowohl Informationen über weitere angemeldete Benutzer wie auch technische Informationen zur Betriebssysteminstallation und -konfiguration.

Beispielsweise kann mit einem einfachen Programm, das in einem bestimmten Zeitintervall die Informationen auswertet, die der Befehl „who“ liefert, jeder Benutzer ein genaues Nutzungsprofil für einen Account erstellen. So lassen sich auf diese Weise die Abwesenheitszeiten des oder der Systemadministratoren feststellen, um diese Zeiten für unberechtigte Handlungen zu nutzen. Des Weiteren lässt sich feststellen, welche Terminals für einen privilegierten Zugang zugelassen sind. Weitere Programme mit ähnlichen Möglichkeiten zum Datenmissbrauch sind „finger“ oder „ruser“.

### 2.2 Ausnutzbarkeit der Skriptumgebung

In Unix-Betriebssystemen werden oft Skriptsprachen genutzt. Skripte sind eine Auflistung von einzelnen Kommandos, die in einer Textdatei gespeichert und beispielsweise in der Kommandozeile aufgerufen werden. Durch den großen Funktionsumfang der Skriptumgebung können Angreifer Skripte umfangreich für ihre Zwecke missbrauchen. Darüber hinaus können aktivierte Skriptsprachen nur sehr schwer eingedämmt werden.

### 2.3 Dynamisches Laden von gemeinsam genutzten Bibliotheken

Mit der Kommandozeilenoption LD\_PRELOAD wird eine dynamische Bibliothek vor allen anderen Standardbibliotheken, die in einer Anwendung benötigt werden, geladen. Dadurch lassen sich gezielt einzelne Funktionen der Standardbibliotheken durch eigene überschreiben. Ein Angreifer könnte das Betriebssystem beispielsweise so manipulieren, dass Schadfunktionen bei der Nutzung von bestimmten Anwendungen mit ausgeführt werden.

### 2.4 Software aus Drittquellen

Bei unixartigen IT-Systemen kommt es vor, dass Benutzer Softwarequellcode selbst herunterladen und kompilieren, statt fertige Softwarepakete zu installieren. Wenn fertige Softwarepakete genutzt werden, werden diese außerdem in einigen Fällen aus Drittquellen ohne weitere Prüfung installiert, statt ausschließlich aus den vorhandenen Paketquellen des Herstellers. Jeder dieser alternativen Wege der Softwareinstallation birgt zusätzliche Risiken, da dadurch fehlerhafte oder inkompatible Software sowie Schadsoftware installiert werden kann.

### 3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.3 *Server unter Linux und Unix* 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	

#### 3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.1.3 *Server unter Linux und Unix* vorrangig erfüllt werden:

##### **SYS.1.3.A1            ENTFALLEN (B)**

Diese Anforderung ist entfallen.

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

Jeder Login-Name, jede Benutzer-ID (User-ID, UID) und jede Gruppen-ID (GID) DARF NUR einmal vorkommen. Jeder Benutzer MUSS Mitglied mindestens einer Gruppe sein. Jede in der Datei */etc/passwd* vorkommende GID MUSS in der Datei */etc/group* definiert sein. Jede Gruppe SOLLTE nur die Benutzer enthalten, die unbedingt notwendig sind. Bei vernetzten Systemen MUSS außerdem darauf geachtet werden, dass die Vergabe von Benutzer- und Gruppennamen, UID und GID im Systemverbund konsistent erfolgt, wenn beim systemübergreifenden Zugriff die Möglichkeit besteht, dass gleiche UIDs bzw. GIDs auf den Systemen unterschiedlichen Benutzer- bzw. Gruppennamen zugeordnet werden könnten.

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

Wechseldatenträger wie z. B. USB-Sticks oder CDs/DVDs DÜRFEN NICHT automatisch eingebunden werden.

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

Um die Ausnutzung von Schwachstellen in Anwendungen zu erschweren, MUSS ASLR und DEP/NX im Kernel aktiviert und von den Anwendungen genutzt werden. Sicherheitsfunktionen des Kernels und der Standardbibliotheken, wie z. B. Heap- und Stackschutz, DÜRFEN NICHT deaktiviert werden.

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

Wenn zu installierende Software aus Quellcode kompiliert werden soll, DARF diese NUR unter einem unprivilegierten Benutzeraccount entpackt, konfiguriert und übersetzt werden. Anschließend DARF die zu installierende Software NICHT unkontrolliert in das Wurzeldateisystem des Servers installiert werden.

Wird die Software aus dem Quelltext übersetzt, SOLLTEN die gewählten Parameter geeignet dokumentiert werden. Anhand dieser Dokumentation SOLLTE die Software jederzeit nachvollziehbar und reproduzierbar kompiliert werden können. Alle weiteren Installationsschritte SOLLTEN dabei ebenfalls dokumentiert werden.

### 3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.1.3 *Server unter Linux und Unix*. Sie SOLLTEN grundsätzlich erfüllt werden.

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

Zur Verwaltung von Benutzern und Gruppen SOLLTEN die entsprechenden Verwaltungswerkzeuge genutzt werden. Von einer direkten Bearbeitung der Konfigurationsdateien */etc/passwd*, */etc/shadow*, */etc/group* und */etc/sudoers* SOLLTE abgesehen werden.

#### **SYS.1.3.A7 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

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

Um eine verschlüsselte und authentifizierte, interaktive Verbindung zwischen zwei IT-Systemen aufzubauen, SOLLTE ausschließlich Secure Shell (SSH) verwendet werden. Alle anderen Protokolle, deren Funktionalität durch Secure Shell abgedeckt wird, SOLLTEN vollständig abgeschaltet werden. Für die Authentifizierung SOLLTEN Benutzer vorrangig Zertifikate anstatt eines Passwortes verwenden.

#### **SYS.1.3.A9 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

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

Dienste und Anwendungen SOLLTEN mit einer individuellen Sicherheitsarchitektur geschützt werden (z. B. mit AppArmor oder SELinux). Auch chroot-Umgebungen sowie LXC- oder Docker-Container SOLLTEN dabei berücksichtigt werden. Es SOLLTE sichergestellt sein, dass mitgelieferte Standardprofile bzw. -regeln aktiviert sind.

#### **SYS.1.3.A11 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

#### **SYS.1.3.A12 ENTFALLEN (S)**

Diese Anforderung ist entfallen.

### 3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.1.3 *Server unter Linux und Unix* 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.1.3.A13 ENTFALLEN (H)**

Diese Anforderung ist entfallen.

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

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

#### **SYS.1.3.A15 ENTFALLEN (H)**

Diese Anforderung ist entfallen.

#### **SYS.1.3.A16 Zusätzliche Verhinderung der Ausbreitung bei der Ausnutzung von Schwachstellen (H)**

Die Nutzung von Systemaufrufen SOLLTE insbesondere für exponierte Dienste und Anwendungen auf

die unbedingt notwendige Anzahl beschränkt werden. Die Standardprofile bzw. -regeln von z. B. SELinux, AppArmor SOLLTEN manuell überprüft und unter Umständen an die eigenen Sicherheitsrichtlinien angepasst werden. Falls erforderlich, SOLLTEN neue Regeln bzw. Profile erstellt werden.

#### **SYS.1.3.A17            Zusätzlicher Schutz des Kernels (H)**

Es SOLLTEN speziell gehärtete Kernels (z. B. grsecurity, PaX) und geeignete Schutzmaßnahmen wie Speicherschutz oder Dateisystemabsicherung umgesetzt werden, die eine Ausnutzung von Schwachstellen und die Ausbreitung im Betriebssystem verhindern.

## **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: Kreuzreferenztablelle zu elementaren Gefährdungen**

Die Kreuzreferenztablelle 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.1.3 Server unter Linux und Unix* von Bedeutung.

- G 0.14    Ausspähen von Informationen (Spionage)
- 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 0.28    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 0.43    Einspielen von Nachrichten
- G 0.45    Datenverlust
- G 0.46    Integritätsverlust schützenswerter Informationen