Bundesamt
für Sicherheit in der
Informationstechnik

SYS.2.3 Clients unter Linux und Unix

1. Beschreibung

1.1. Einleitung

Neben Windows werden auf immer mehr Clients Linux- oder seltener Unix-basierte Betriebssysteme installiert. Beispiele für klassische Unix-Systeme sind die BSD-Reihe (FreeBSD, OpenBSD und NetBSD), Solaris und AIX. Linux bezeichnet hingegen kein klassisches, sondern ein funktionelles Unix-System, da der Linux-Kernel nicht auf dem ursprünglichen Quelltext basiert, aus dem sich die verschiedenen Unix-Derivate entwickelt haben. Da sich die Konfiguration und der Betrieb von Linux- und Unix-Clients ähneln, werden in diesem Baustein Linux und Unix sprachlich als „Unix-Client“ bzw. „unixartig“ zusammengefasst.

Linux ist freie Software, die von der Open-Source-Gemeinschaft entwickelt wird. Das bedeutet, dass sie frei genutzt, kopiert, verteilt und verändert werden darf. Daneben gibt es Unternehmen, die den Linux-Kernel und die verschiedenen Software-Komponenten zu einer Distribution zusammenfassen und pflegen sowie weitere Dienstleistungen anbieten. Häufig werden Derivate der Distributionen Debian, Fedora / Red Hat Enterprise Linux oder openSUSE / SUSE Linux Enterprise eingesetzt. Darüber hinaus gibt es für spezielle Einsatzzwecke und Geräte zugeschnittene Linux-Distributionen. Dazu gehören z. B. Qubes OS, das versucht, ein hohes Maß an Sicherheit durch Virtualisierung zu erreichen, LibreElec für den Einsatz eines Home Theater PCs (HTPC) oder Kali Linux, eine auf Sicherheit, Computerforensik und Penetrationstests spezialisierte Distribution. Außerdem können Clients auch Live-Distributionen starten, ohne dass das auf dem Client installierte Betriebssystem verändert wird. Der Marktanteil des Betriebssystems Linux auf Clients hat in den letzten Jahren zugenommen. In speziellen Einsatzumgebungen werden weiterhin „klassische“ Unix-Systeme in verschiedenen Derivaten eingesetzt. Typischerweise ist ein solches IT-System vernetzt und wird als Client in einem Client-Server-Netz betrieben.

Durch die Menge der vorausgewählten Softwarepakete einer Standardinstallation der gängigen Linux-Distributionen beziehungsweise der Unix-Derivate erhöht sich einerseits die Angriffsfläche. Gleichzeitig bieten unixartige Betriebssysteme aber auch umfangreiche Schutzmechanismen.

1.2. Zielsetzung

Ziel dieses Bausteins ist der Schutz von Informationen, die auf Linux- und Unix-Clients erstellt, bearbeitet, gespeichert oder versendet werden. Die Anforderungen des Bausteins gelten vorrangig für Linux-Clients, können aber generell für Unix-Clients adaptiert werden.

1.3. Abgrenzung und Modellierung

Der Baustein SYS.2.3 *Clients unter Linux und Unix* ist für alle Clients anzuwenden, auf denen Linux- oder Unix-basierte Betriebssysteme eingesetzt werden.

Dieser Baustein enthält grundsätzliche Anforderungen zum Betrieb von unixartigen Clients. Er konkretisiert und ergänzt die Aspekte, die im Baustein SYS.2.1 *Allgemeiner Client* behandelt werden, um Besonderheiten von Unix-Systemen. Dementsprechend sind die beiden Bausteine immer gemeinsam anzuwenden.

Auch wenn es sich bei macOS von Apple um ein unixartiges Betriebssystem handelt, wird dieses Betriebssystem nicht in diesem Baustein behandelt. Empfehlungen hierzu sind im Baustein SYS.2.4 *Clients unter macOS* zu finden.

Der Baustein umfasst nur das eigentliche Betriebssystem, das in der Regel bei einer Basisinstallation einer Distribution installiert wird. Darauf aufbauende Software, wie E-Mail-Clients oder Office-Software, wird in diesem Baustein nicht berücksichtigt. Anforderungen hierzu sind z. B. in den Bausteinen der Schicht APP.1 *Client-Anwendungen* des IT-Grundschutz-Kompendiums zu finden.

Dieser Client-Baustein setzt voraus, dass neben Administrierenden dauerhaft nur eine unveränderte Person mit einem interaktiven Konto aktiv ist. Clients, die von mehreren Personen nacheinander oder gleichzeitig genutzt werden, erfordern zusätzliche Maßnahmen, die im Rahmen dieses Bausteins nicht behandelt werden.

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.2.3 *Clients unter Linux und Unix* von besonderer Bedeutung.

2.1. Software aus Drittquellen

Bei unixartigen IT-Systemen kommt es vor, dass Benutzende 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 herstellenden Unternehmens. Jeder dieser alternativen Wege der Softwareinstallation birgt zusätzliche Risiken, da dadurch fehlerhafte oder inkompatible Software sowie Schadsoftware installiert werden kann.

2.2. Ausnutzbarkeit der Skriptumgebung

Oft werden in unixartigen Betriebssystemen 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 Skriptumgebungen können Angreifende 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. Angreifende könnten das Betriebssystem beispielsweise so manipulieren, dass Schadfunktionen bei der Nutzung von bestimmten Anwendungen mit ausgeführt werden.

2.4. Fehlerhafte Konfiguration

Schon in einer Standardinstallation werden bei unixartigen Betriebssystemen zahlreiche Anwendungen installiert, die separat konfiguriert werden müssen. Auch nachinstallierte Anwendungen müssen separat konfiguriert werden, so dass sich schließlich unzählige Konfigurationsdateien auf dem Betriebssystem befinden.

Da viele Anwendungen unabhängig voneinander konfiguriert werden, können die Konfigurationsoptionen im Widerspruch zueinander stehen, ohne dass dies aus den einzelnen Einstellungen ersichtlich ist. Beispielsweise könnte ein Dienst für eine Fernadministration auf einem Port lauschen, der von Paketfilterregeln blockiert wird. Auf diese Weise können die Anwendungen zusätzliche Funktionen bereitstellen, die nicht gewünscht sind, oder wichtige Funktionen nicht anbieten. Das kann dazu führen, dass bestimmte Aufgaben am Client erschwert oder gar nicht erfüllt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.2.3 *Clients unter Linux und Unix* 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	Benutzende

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.2.3.A1 Authentisierung von Administrierenden und Benutzenden (B) [Benutzende]

Personen mit Adminstrationsrechten DÜRFEN sich NICHT im Normalbetrieb als „root“ anmelden. Für die Systemadministrationsaufgaben SOLLTE „sudo“ oder eine geeignete Alternative mit einer geeigneten Protokollierung genutzt werden. Es SOLLTE verhindert werden, dass sich mehrere Benutzende auf einem Client gleichzeitig einloggen können.

SYS.2.3.A2 Auswahl einer geeigneten Distribution (B)

Auf Grundlage der Sicherheitsanforderungen und des Einsatzzwecks MUSS ein geeignetes Unix-Derivat bzw. eine geeignete Linux-Distribution ausgewählt werden. Es MUSS für die geplante Einsatzdauer des Betriebssystems Support verfügbar sein. Alle benötigten Anwendungsprogramme SOLLTEN als Teil der Distribution direkt verfügbar sein. Sie SOLLTEN NUR in Ausnahmefällen aus Drittquellen bezogen werden. Distributionen, bei denen das Betriebssystem selbst kompiliert wird, SOLLTEN NICHT in Produktivumgebungen eingesetzt werden.

SYS.2.3.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.2.3.A4 Kernel-Aktualisierungen auf unixartigen Systemen (B)

Der Client MUSS zeitnah neu gebootet werden, nachdem der Kernel des Betriebssystems aktualisiert wurde. Ist dies nicht möglich, MUSS alternativ Live-Patching des Kernels aktiviert werden.

SYS.2.3.A5 Sichere Installation von Software-Paketen (B)

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

Wird die Software aus dem Quelltext übersetzt, dann 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 diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.2.3.A6 Kein automatisches Einbinden von Wechsellaufwerken (S) [Benutzende]

Wechsellaufwerke SOLLTEN NICHT automatisch eingebunden werden. Die Einbindung von Wechsellaufwerken SOLLTE so konfiguriert sein, dass alle Dateien als nicht ausführbar markiert sind (Mount-Option „noexec“).

SYS.2.3.A7 Restriktive Rechtevergabe auf Dateien und Verzeichnisse (S)

Es SOLLTE sichergestellt werden, dass Dienste und Anwendungen nur die ihnen zugeordneten Dateien erstellen, verändern oder löschen dürfen. Auf Verzeichnissen, in denen alle Konten Schreibrechte haben (z. B. „/tmp“), SOLLTE das Sticky Bit gesetzt werden.

SYS.2.3.A8 Einsatz von Techniken zur Rechtebeschränkung von Anwendungen (S)

Zur Beschränkung der Zugriffsrechte von Anwendungen auf Dateien, Geräte und Netze SOLLTE App-Armor oder SELinux eingesetzt werden. Es SOLLTEN die von dem jeweiligen Unix-Derivat bzw. der Linux-Distribution am besten unterstützten Lösungen eingesetzt werden. Rechte SOLLTEN grundsätzlich entzogen sein und wo nötig über Positivlisten explizit erteilt werden.

Erweiterungen zur Rechtebeschränkung SOLLTEN im Zwangsmodus (Enforcing Mode) oder mit geeigneten Alternativen verwendet werden.

SYS.2.3.A9 Sichere Verwendung von Passwörtern auf der Kommandozeile (S) [Benutzende]

Passwörter SOLLTEN NICHT als Parameter an Programme übergeben werden.

SYS.2.3.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.2.3.A11 Verhinderung der Überlastung der lokalen Festplatte (S)

Es SOLLTEN Quotas für Konten bzw. Dienste eingerichtet werden, die ausreichend Freiraum für das Betriebssystem lassen. Generell SOLLTEN unterschiedliche Partitionen für Betriebssystem und Daten genutzt werden. Alternativ SOLLTEN auch Mechanismen des verwendeten Dateisystems genutzt werden, die ab einem geeigneten Füllstand nur noch dem Konto „root“ Schreibrechte einräumen.

SYS.2.3.A12 Sicherer Einsatz von Appliances (S)

Es SOLLTE sichergestellt werden, dass Appliances ein ähnliches Sicherheitsniveau wie Clients auf Standard-IT-Systemen erfüllen. Es SOLLTE dokumentiert werden, wie entsprechende Sicherheitsanforderungen mit einer eingesetzten Appliance erfüllt werden. Wenn die Anforderungen nicht zweifelsfrei erfüllt werden können, SOLLTE eine Konformitätserklärung von den herstellenden Unternehmen angefordert 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.2.3.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.2.3.A14 Absicherung gegen Nutzung unbefugter Peripheriegeräte (H)

Peripheriegeräte SOLLTEN nur nutzbar sein, wenn sie explizit freigegeben sind. Kernelmodule für Peripheriegeräte SOLLTEN nur geladen und aktiviert werden, wenn das Gerät freigegeben ist.

SYS.2.3.A15 Zusätzlicher Schutz vor der Ausführung unerwünschter Dateien (H)

Partitionen und Verzeichnisse, in denen Benutzende Schreibrechte haben, SOLLTEN so gemountet werden, dass keine Dateien ausgeführt werden können (Mountoption „noexec“).

SYS.2.3.A16 ENTFALLEN (H)

Diese Anforderung ist entfallen.

SYS.2.3.A17 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 (z. B. durch seccomp). Die vorhandenen Standardprofile bzw. -regeln von SELinux, AppArmor sowie alternativen Erweiterungen SOLLTEN manuell überprüft und gegebenenfalls an die eigene Sicherheitsrichtlinie angepasst werden. Falls erforderlich, SOLLTEN neue Regeln bzw. Profile erstellt werden.

SYS.2.3.A18 Zusätzlicher Schutz des Kernels (H)

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

SYS.2.3.A19 Festplatten- oder Dateiverschlüsselung (H)

Festplatten oder die darauf abgespeicherten Dateien SOLLTEN verschlüsselt werden. Die dazugehörigen Schlüssel SOLLTEN NICHT auf dem IT-System gespeichert werden. Es SOLLTEN AEAD-Verfahren (Authenticated Encryption with Associated Data) bei der Festplatten- und Dateiverschlüsselung eingesetzt werden. Alternativ SOLLTE „dm-crypt“ in Kombination mit „dm-verity“ genutzt werden.

SYS.2.3.A20 Abschaltung kritischer SysRq-Funktionen (H)

Es SOLLTE festgelegt werden, welche SysRq-Funktionen von den Benutzenden ausgeführt werden dürfen. Generell SOLLTEN keine kritischen SysRq-Funktionen von den Benutzenden ausgelöst werden können.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein SYS.2.3 *Clients unter Linux und Unix* sind keine weiterführenden Informationen vorhanden.