Bundesamt
für Sicherheit in der
Informationstechnik

APP.2.3 OpenLDAP

1. Beschreibung

1.1. Einleitung

OpenLDAP ist ein frei verfügbarer Verzeichnisdienst, der in einem Datennetz Informationen über beliebige Objekte, beispielsweise Konten, IT-Systeme oder Konfigurationen, in einer standardisierten und definierten Art zur Verfügung stellt. Die Informationen können einfache Attribute wie die Namen oder Nummern von Objekten oder auch komplexe Formate wie Fotos oder Zertifikate für elektronische Signaturen umfassen. Typische Einsatzgebiete sind zum Beispiel Adressbücher oder Kontenverwaltungen, aber auch Konfigurationen.

OpenLDAP stellt eine Referenz-Implementierung für einen Server-Dienst im Rahmen des Lightweight Directory Access Protocols (LDAP) dar. Als Open-Source-Software kann OpenLDAP auf einer Vielzahl von Betriebssystemen installiert werden und gilt als einer der am meisten verbreiteten Verzeichnisdienste. Zur Besonderheit von OpenLDAP gehören die *Overlays*. Overlays erweitern den Funktionsumfang von OpenLDAP um zahlreiche Funktionen und werden auch für grundlegende Funktionen wie Protokollierung, Replikation und die Wahrung der Integrität verwendet.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, auf OpenLDAP basierende Verzeichnisdienste sicher zu betreiben sowie die damit verarbeiteten Informationen geeignet zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.2.3 *OpenLDAP* ist auf jedes OpenLDAP-Verzeichnis anzuwenden.

In diesem Baustein werden die für OpenLDAP spezifischen Gefährdungen und Anforderungen betrachtet. Dabei wird die Version 2.4 von OpenLDAP zugrunde gelegt. Allgemeine Sicherheitsempfehlungen zu Verzeichnisdiensten gibt es im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst.* Diese müssen zusätzlich berücksichtigt werden. Die dort beschriebenen Anforderungen werden im vorliegenden Baustein konkretisiert und ergänzt.

OpenLDAP sollte grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement,* CON.3 *Datensicherungskonzept*, OPS.1.2.2 *Archivierung*, OPS.1.1.5 *Protokollierung* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* mitberücksichtigt 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 APP.2.3 *OpenLDAP* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Planung von OpenLDAP

OpenLDAP kann in Verbindung mit zahlreichen anderen Anwendungen genutzt werden. Diese Anwendungen können auf die Informationen des Verzeichnisdienstes zugreifen und diese in der Regel auch ändern. Wird der Einsatz von OpenLDAP nicht oder unzureichend geplant, können folgende Probleme auftreten:

- Werden die Backends und die zugehörigen Direktiven und Parameter falsch ausgewählt, beeinflussen diese ungewollt die Funktionen, die OpenLDAP anbieten kann. Wird beispielsweise das Backend „back-ldif“ zur Datenspeicherung verwendet, um die Installation einer zusätzlichen Datenbank zu umgehen, stehen nur rudimentäre Funktionen des Verzeichnisdienstes zur Verfügung. Eine große Menge von Benutzenden oder anderen Objekten kann dann nicht geeignet verwaltet werden.
- Wenn der Einsatz von Overlays mangelhaft geplant wird, können in OpenLDAP nicht benötigte Operationen ausgeführt oder sonstige Funktionen beeinträchtigt werden. Beispielsweise werden Zugriffe auf den Verzeichnisdienst nicht oder falsch protokolliert, wenn die Debug-Funktion des slapd-Servers selbst und die Overlays „auditlog“ und „accesslog“ unzureichend geplant werden.
- OpenLDAP kann in einer ungeeigneten Systemumgebung ausgeführt werden. Wird ein verteiltes Dateisystem wie Network File System (NFS) verwendet, um die OpenLDAP-Daten abzuspeichern, könnten Dateifunktionen von OpenLDAP nicht verwendet werden. Ein Beispiel dafür ist die von vielen Datenbanken verwendete Locking-Funktion, die es ermöglicht, die Datenbank des Verzeichnisdienstes zu sperren, wenn mehrere Benutzende parallel schreibend auf die Datenbank zugreifen möchten.
- Es könnten inkompatible Versionen einer oder mehrerer Anwendungen auf die von OpenLDAP verwendeten Datenbanken zugreifen. Beispielsweise werden die Spezifikationen des Protokolls LDAPv3 nicht von OpenLDAP ohne zusätzliche Erweiterungen erfüllt. Zudem können auch Verbindungsprobleme mit den Anwendungen entstehen, wenn die falsche Version eines oder mehrerer Programme eingesetzt wird, die mit OpenLDAP nicht kompatibel sind.

2.2. Unzureichende Trennung von Offline- und Online-Zugriffen auf OpenLDAP

Auf die durch OpenLDAP verwalteten Daten (Objekte im Verzeichnisdienst ebenso wie Konfigurationseinstellungen) kann über verschiedene Möglichkeiten zugegriffen werden. Die Offline- und Online-Zugriffe erfüllen dabei ganz oder teilweise identische Funktionen. Bei einem Online-Zugriff wird über das Protokoll LDAP und den slapd auf die Daten zugegriffen. Beim Offline-Zugriff wird direkt auf die Datenbankdateien zugegriffen, bzw. es wird ein ldif-Export des Verzeichnisses editiert und anschließend wieder zurück in die Datenbank geladen. Werden diese Möglichkeiten vermischt oder wird die jeweilige Wirkungsweise vom Offline- oder Online-Zugriff fehlinterpretiert, können zahlreiche Fehler auftreten. In der Folge ist die resultierende Datenbank für OpenLDAP inkonsistent und kann somit nicht mehr fehlerfrei genutzt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.2.3 *OpenLDAP* 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	Keine

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.

APP.2.3.A1 Planung und Auswahl von Backends und Overlays für OpenLDAP (B)

Der Einsatz von OpenLDAP in einer Institution MUSS sorgfältig geplant werden. Soll OpenLDAP gemeinsam mit anderen Anwendungen verwendet werden, so MÜSSEN die Planung, Konfiguration und Installation der Anwendungen mit OpenLDAP aufeinander abgestimmt werden. Für die zur Datenhaltung verwendete Datenbank MUSS sichergestellt werden, dass die verwendete Version kompatibel ist. Backends und Overlays für OpenLDAP MÜSSEN restriktiv selektiert werden. Dazu MUSS sichergestellt werden, dass die OpenLDAP-Overlays in der korrekten Reihenfolge eingesetzt werden. Bei der Planung von OpenLDAP MÜSSEN die auszuwählenden und unterstützten Client-Anwendungen berücksichtigt werden.

APP.2.3.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.2.3.A3 Sichere Konfiguration von OpenLDAP (B)

Für die sichere Konfiguration von OpenLDAP MUSS der slapd-Server korrekt konfiguriert werden. Es MÜSSEN auch die verwendeten Client-Anwendungen sicher konfiguriert werden. Bei der Konfiguration von OpenLDAP MUSS darauf geachtet werden, dass im Betriebssystem die Berechtigungen korrekt gesetzt sind. Die Vorgabewerte aller relevanten Konfigurationsdirektiven von OpenLDAP MÜSSEN geprüft und gegebenenfalls angepasst werden. Die Backends und Overlays von OpenLDAP MÜSSEN in die Konfiguration einbezogen werden. Für die Suche innerhalb von OpenLDAP MÜSSEN angemessene Zeit- und Größenbeschränkungen festgelegt werden. Die Konfiguration am slapd-Server MUSS nach jeder Änderung geprüft werden.

APP.2.3.A4 Konfiguration der durch OpenLDAP verwendeten Datenbank (B)

Die Zugriffsrechte für neu angelegte Datenbankdateien MÜSSEN auf die Kennung beschränkt werden, in deren Kontext der slapd-Server betrieben wird. Die Standard-Einstellungen der von OpenLDAP genutzten Datenbank MÜSSEN angepasst werden.

APP.2.3.A5 Sichere Vergabe von Zugriffsrechten auf dem OpenLDAP (B)

Die in OpenLDAP geführten globalen und datenbankspezifischen Zugriffskontrolllisten (Access Control Lists) MÜSSEN beim Einsatz von OpenLDAP korrekt berücksichtigt werden. Datenbank-Direktiven MÜSSEN Vorrang vor globalen Direktiven haben.

APP.2.3.A6 Sichere Authentisierung gegenüber OpenLDAP (B)

Wenn der Verzeichnisdienst zwischen verschiedenen Benutzenden unterscheiden soll, MÜSSEN sich diese geeignet authentisieren. Die Authentisierung zwischen dem slapd-Server und den Kommunikationsbeteiligten MUSS verschlüsselt werden. Es SOLLTEN NUR die Hashwerte von Passwörtern auf den Clients und Servern abgespeichert werden. Es MUSS ein geeigneter Hashing-Algorithmus verwendet 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.

APP.2.3.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.3.A8 Einschränkungen von Attributen bei OpenLDAP (S)

Anhand von Overlays SOLLTEN die Attribute in OpenLDAP eingeschränkt werden. OpenLDAP SOLLTE so angepasst werden, dass Werte im Verzeichnisdienst nur einem bestimmten regulären Ausdruck entsprechen. Zudem SOLLTE mit Hilfe von Overlays sichergestellt werden, das ausgesuchte Werte nur einmal im Verzeichnisbaum vorhanden sind. Solche Restriktionen SOLLTEN ausschließlich auf Daten von Nutzenden angewendet werden.

APP.2.3.A9 Partitionierung und Replikation bei OpenLDAP (S)

Bei einer Partitionierung oder Replikation von OpenLDAP SOLLTE die Aufteilung geeignet für die Sicherheitsziele ausgewählt werden. Dabei SOLLTEN Veränderungen an den Daten durch Replikation zwischen den Servern ausgetauscht werden. Ein Replikationsmodus SOLLTE in Abhängigkeit von Netzverbindungen und Verfügbarkeitsanforderungen gewählt werden.

APP.2.3.A10 Sichere Aktualisierung von OpenLDAP (S)

Bei Updates SOLLTE darauf geachtet werden, ob die Änderungen eingesetzte Backends oder Overlays sowie Softwareabhängigkeiten betreffen. Beim Update auf neue Releases SOLLTE geprüft werden, ob die verwendeten Overlays und Backends in der neuen Version weiterhin zur Verfügung stehen. Ist dies nicht der Fall, SOLLTEN geeignete Migrationspfade ausgewählt werden.

Setzen Administrierende eigene Skripte ein, SOLLTEN sie daraufhin überprüft werden, ob sie mit der aktualisierten Version von OpenLDAP problemlos zusammenarbeiten. Die Konfiguration und die Zugriffsrechte SOLLTEN nach einer Aktualisierung sorgfältig geprüft werden.

APP.2.3.A11 Einschränkung der OpenLDAP-Laufzeitumgebung (S)

Die Laufzeitumgebung des slapd-Servers SOLLTE, möglichst mit Mitteln des Betriebssystems, auf die minimal benötigten Dateien, Verzeichnisse und vom Betriebssystem bereitgestellten Funktionen eingeschränkt werden. Werden hierfür Containerisierungstechniken eingesetzt, SOLLTEN diese unter Berücksichtigung von SYS.1.6 *Containerisierung* genutzt werden. Wird der slapd-Server als exklusiver Dienst auf einem dedizierten Server betrieben, SOLLTE dieser ausreichend gehärtet sein.

APP.2.3.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.3.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Für diesen Baustein sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein APP.2.3 *OpenLDAP* sind keine weiterführenden Informationen vorhanden.