Bundesamt
für Sicherheit in der
Informationstechnik

APP.2.1 Allgemeiner Verzeichnisdienst

1. Beschreibung

1.1. Einleitung

Ein Verzeichnisdienst stellt in einem Datennetz Informationen über beliebige Objekte in einer definierten Art zur Verfügung. In einem Objekt können zugehörige Attribute gespeichert werden, zum Beispiel können zu einer Kennung der Name und Vorname des oder der Benutzenden, die Personalnummer und der Name des IT-Systems abgelegt werden. Diese Daten können dann gleichermaßen von verschiedenen Applikationen verwendet werden. Der Verzeichnisdienst und seine Daten werden in der Regel von zentraler Stelle aus verwaltet.

Einige typische Anwendungsgebiete von Verzeichnisdiensten sind:

- Verwaltung von Adressbüchern, z. B. für Telefonnummern, E-Mail-Adressen und Zertifikate für elektronische Signaturen
- Benutzendenverwaltung, z. B. zur Verwaltung von Konten und Berechtigungen
- Bereitstellung eines Backend-Dienstes für Authentifizierungsfunktionen, z. B. zur Anmeldung an Betriebssystemen oder Anwendungen

Verzeichnisdienste sind auf Lesezugriffe hin optimiert, da Daten aus dem Verzeichnisdienst typischerweise vorwiegend abgerufen werden. Schreibzugriffe, bei denen Einträge erstellt, geändert oder gelöscht werden, sind seltener notwendig.

Wenn ein Verzeichnisdienst eingesetzt wird, können manche Verwaltungsaufgaben innerhalb des Netzes, wie z. B. Kontenerstellung, Passwortänderungen und Zuweisungen von Rollen und Gruppen, an zentraler Stelle durchgeführt werden.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, allgemeine Verzeichnisdienste sicher zu betreiben sowie die damit verarbeiteten Informationen angemessen zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* ist für alle verwendeten Verzeichnisdienste anzuwenden.

Dieser Baustein betrachtet allgemeine Sicherheitsaspekte von Verzeichnisdiensten unabhängig vom eingesetzten Produkt. Für produktspezifische Sicherheitsaspekte gibt es im IT-Grundschutz-Kompendium weitere Bausteine, die zusätzlich auf den jeweiligen Verzeichnisdienst anzuwenden sind. Bausteine zu Server-Betriebssystemen, auf denen Verzeichnisdienste üblicherweise betrieben werden, sind in der Schicht SYS.1 *Server* des IT-Grundschutz-Kompendiums aufgeführt. Grundlegende Anforderungen an Software-Produkte finden sich in APP.6 *Allgemeine Software* und sind ebenfalls zu beachten.

Verzeichnisdienste sollten 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,* OPS.1.2.5 *Fernwartung* 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.2.1 *Allgemeiner Verzeichnisdienst* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Planung des Einsatzes von Verzeichnisdiensten

Die Sicherheit von Verzeichnisdiensten stützt sich stark auf die Sicherheit des Basisbetriebssystems und dabei vor allem auf die Dateisystemsicherheit. Verzeichnisdienste lassen sich auf vielen Betriebssystemen installieren und betreiben, wodurch sich eine große Vielfalt der vorzunehmenden Sicherheitseinstellungen ergeben kann. Diese Vielfalt erhöht die Anforderungen an die Planung und setzt entsprechende Kenntnisse über das jeweilige Betriebssystem voraus. Sollte die entstehende Gesamtlösung sehr heterogen oder komplex sein, kann ein nicht ausreichend geplanter Einsatz des Verzeichnisdienstes im Wirkbetrieb zu Sicherheitslücken führen.

2.2. Fehlerhafte oder unzureichende Planung der Partitionierung und Replizierung im Verzeichnisdienst

Durch eine Partitionierung können die Verzeichnisdaten eines Verzeichnisdienstes in einzelne Teilbereiche (Partitionen) aufgeteilt werden. Um für eine bessere Lastverteilung zu sorgen, werden Partitionen des Verzeichnisdienstes häufig auf weitere Instanzen repliziert. Außerdem wird durch die redundante Datenhaltung die Ausfallsicherheit verbessert und somit die Verfügbarkeit erhöht. Von entscheidender Bedeutung ist deshalb auch hier eine geeignete Planung, da Partitions- und Replikationseinstellungen zwar nachträglich geändert werden können, dies aber Probleme verursachen kann. Es kann etwa zu Datenverlusten sowie Inkonsistenzen in der Datenhaltung, zu einer mangelhaften Verfügbarkeit des Verzeichnisdienstes und zu einer insgesamt schlechten Systemperformance bis hin zu Ausfällen führen.

2.3. Fehlerhafte Administration von Zugangs- und Zugriffsrechten

Zugangsrechte zu einem IT-System und Zugriffsrechte auf gespeicherte Daten und IT-Anwendungen dürfen nur in dem Umfang eingeräumt werden, wie sie für die durchzuführenden Aufgaben

erforderlich sind. Dies gilt auch für die Berechtigungen, die über einen Verzeichnisdienst verwaltete Benutzende und Gruppen erhalten, auch wenn diese für die Informationen *im* Verzeichnisdienst selbst gelten. Werden diese Rechte fehlerhaft administriert, kann einerseits der Betrieb gestört werden, falls erforderliche Rechte nicht zugewiesen wurden. Andererseits können Sicherheitslücken entstehen, falls über die notwendigen Rechte hinaus weitere Rechte vergeben werden. Wenn die Zugriffsrechte im Verzeichnisdienst falsch oder inkonsistent vergeben werden, ist dadurch die Sicherheit des Gesamtsystems erheblich gefährdet. Ein besonders kritischer Punkt sind auch die Administrationsrechte. Werden diese Rechte falsch vergeben, kann das gesamte Administrationskonzept unterlaufen oder unter Umständen sogar die Administration des Verzeichnissystems selbst verhindert oder eine unberechtigte Nutzung ermöglicht werden.

2.4. Fehlerhafte Konfiguration des Zugriffs auf Verzeichnisdienste

In vielen Fällen müssen weitere Applikationen wie Internet- oder Intranet-Anwendungen auf den Verzeichnisdienst zugreifen. Eine Fehlkonfiguration kann dazu führen, dass Zugriffsrechte falsch vergeben werden. Es kann auch passieren, dass unautorisiert auf den Verzeichnisdienst zugegriffen werden kann oder dass Daten zur Authentisierung im Klartext übermittelt werden. In diesem Fall können Informationen während der Übertragung ausgespäht werden.

2.5. Ausfall von Verzeichnisdiensten

Durch technisches Versagen aufgrund von Hardware- oder Software-Problemen können Verzeichnisdienste oder Teile davon ausfallen. Als Folge sind die Daten im Verzeichnis temporär nicht mehr zugänglich. Im Extremfall können auch Daten verloren gehen oder Anmeldungen an vom Verzeichnisdienst bedienten IT-Systemen nicht mehr möglich sein. Dadurch können Geschäftsprozesse und interne Arbeitsabläufe behindert werden. Sind funktionsfähige Kopien der ausgefallenen Systemteile vorhanden, so ist der Zugriff zwar weiterhin möglich, jedoch je nach gewählter Netztopologie nur mit eingeschränkter Leistungsfähigkeit.

2.6. Kompromittierung von Verzeichnisdiensten durch unbefugten Zugriff

Wenn es Angreifenden gelungen ist, eine notwendige Authentisierung gegenüber dem Verzeichnisdienst erfolgreich durchzuführen oder zu umgehen, können sie danach unbefugt auf eine Vielzahl von Daten zugreifen. Somit kann potentiell der gesamte Verzeichnisdienst kompromittiert werden. Dadurch könnte das gesamte betroffene System beeinträchtigt oder gar zerstört werden.

Die Sicherheit eines Verzeichnisdienstes kann ebenfalls gefährdet werden, wenn anonyme Benutzende zugelassen werden. Dadurch, dass deren Identität nicht überprüft wird, können anonyme Benutzende zunächst beliebige Abfragen an den Verzeichnisdienst richten, durch die sie zumindest Teilinformationen über dessen Struktur und Inhalt erlangen. Wenn anonyme Zugriffe zugelassen werden, sind außerdem DoS-Attacken auf den Verzeichnisdienst leichter durchzuführen, da Angreifende mehr Zugriffsmöglichkeiten haben, die nur schlecht kontrollierbar sind.

2.7. Fehlerhafte Konfiguration von Verzeichnisdiensten

Verzeichnisdienste verfügen über zahlreiche Funktionen, sodass der Verzeichnisdienst von Anwendenden mit sehr unterschiedlichen Bedürfnissen genutzt werden kann. Eine Fehlkonfiguration dieser zahlreichen Funktionen kann dazu führen, dass unautorisiert auf den Verzeichnisdienst zugegriffen werden kann. Wenn beispielsweise die Standardkonfiguration nicht ausreichend geprüft und angepasst wird, können die Informationen zur Authentisierung im Klartext oder unzureichend abgesichert übermittelt und damit ausgespäht werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.2.1 *Allgemeiner Verzeichnisdienst* 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	Fachverantwortliche, Datenschutzbeauftragte

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.2.1.A1 Erstellung einer Sicherheitsrichtlinie für Verzeichnisdienste (B)

Es MUSS eine Sicherheitsrichtlinie für den Verzeichnisdienst erstellt werden. Diese SOLLTE mit dem übergreifenden Sicherheitskonzept der gesamten Institution abgestimmt sein.

APP.2.1.A2 Planung des Einsatzes von Verzeichnisdiensten (B) [Datenschutzbeauftragte, Fachverantwortliche]

Der Einsatz von Verzeichnisdiensten MUSS sorgfältig geplant werden. Die konkrete Nutzung des Verzeichnisdienstes MUSS festgelegt werden. Es MUSS sichergestellt sein, dass der Verzeichnisdienst und alle ihn verwendenden Anwendungen kompatibel sind. Zudem MUSS ein Konzept für eine Struktur aus Objektklassen und Attributtypen entwickelt werden, dass den Ansprüchen der vorgesehenen Nutzungsarten genügt. Bei der Planung eines Verzeichnisdienstes, der personenbezogene Daten beinhaltet, MÜSSEN Personalvertretung und Datenschutzbeauftragte beteiligt werden. Es MUSS ein bedarfsgerechtes Berechtigungskonzept zum Verzeichnisdienst entworfen werden. Generell SOLLTE die geplante Verzeichnisdienststruktur vollständig dokumentiert und die Dokumentation bei Änderungen fortgeschrieben werden. Maßnahmen SOLLTEN geplant und umgesetzt werden, die es unterbinden, aus dem Verzeichnisdienst unbefugt Daten sammeln zu können.

APP.2.1.A3 Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste (B) [Fachverantwortliche]

Die Administration des Verzeichnisdienstes selbst und die eigentliche Verwaltung der Daten MÜSSEN getrennt werden. Alle administrativen Aufgabenbereiche und Berechtigungen SOLLTEN ausreichend dokumentiert werden.

Bei einer eventuellen Zusammenführung mehrerer Verzeichnisdienstbäume MÜSSEN die daraus resultierenden effektiven Rechte kontrolliert werden.

APP.2.1.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.2.1.A5 Sichere Konfiguration und Konfigurationsänderungen von Verzeichnisdiensten (B)

Der Verzeichnisdienst MUSS sicher konfiguriert werden. Für die sichere Konfiguration einer Verzeichnisdienste-Infrastruktur MÜSSEN neben dem Server auch die Clients (IT-Systeme und Anwendungen) einbezogen werden.

Wird die Konfiguration des Verzeichnisdienstes oder der mit ihm vernetzten IT-Systeme geändert, SOLLTEN die Benutzenden rechtzeitig über Wartungsarbeiten informiert werden.

APP.2.1.A6 Sicherer Betrieb von Verzeichnisdiensten (B)

Die Sicherheit des Verzeichnisdienstes MUSS im Betrieb permanent aufrechterhalten werden. Alle den Betrieb eines Verzeichnisdienst-Systems betreffenden Richtlinien, Regelungen und Prozesse SOLLTEN nachvollziehbar dokumentiert und aktuell gehalten werden. Sofern der Verzeichnisdienst zur Verwaltung von Anmeldedaten verwendet wird, MÜSSEN dedizierte Clients bei der Fernwartung eingesetzt werden. Der Zugriff auf alle Administrationswerkzeuge MUSS für normale Benutzende unterbunden werden.

APP.2.1.A17 Absicherung von schutzbedürftigen Anmeldeinformationen (B)

Für Attribute, die schutzbedürftige Anmeldeinformationen wie beispielsweise Passwörter enthalten, MUSS der Zugriff stark eingeschränkt 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.2.1.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.1.A8 Planung einer Partitionierung im Verzeichnisdienst (S)

Sofern eine Partitionierung geplant ist, SOLLTE sich diese an den Schutzzielen des Verzeichnisdienstes orientieren und diese geeignet unterstützen. Eine Partitionierung SOLLTE so geplant werden, dass sie die Schadensauswirkungen bei Sicherheitsvorfällen begrenzt, die unabhängige Administration verschiedener Partitionen ermöglicht und organisatorischen bzw. Sicherheitsgrenzen folgt.

APP.2.1.A9 Geeignete Auswahl von Komponenten für Verzeichnisdienste (S) [Fachverantwortliche]

Für den Einsatz eines Verzeichnisdienstes SOLLTEN geeignete Komponenten identifiziert werden. Es SOLLTE unter Berücksichtigung von APP.6 *Allgemeine Software* ein Anforderungskatalog erstellt werden, nach dem die Komponenten für den Verzeichnisdienst ausgewählt und beschafft werden. Im Rahmen der Planung und Konzeption des Verzeichnisdienstes SOLLTEN passend zum Einsatzzweck Anforderungen an dessen Sicherheit formuliert werden. Insbesondere SOLLTE bereits bei der Produktauswahl berücksichtigt werden, wie weitere Sicherheitsanforderungen unter Einsatz der jeweiligen Komponente umgesetzt werden können.

APP.2.1.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.1.A11 Einrichtung des Zugriffs auf Verzeichnisdienste (S)

Der Zugriff auf den Verzeichnisdienst SOLLTE entsprechend der Sicherheitsrichtlinie konfiguriert werden. Wird der Verzeichnisdienst als Server im Internet eingesetzt, SOLLTE er entsprechend durch ein Sicherheitsgateway geschützt werden.

APP.2.1.A12 Überwachung von Verzeichnisdiensten (S)

Verzeichnisdienste SOLLTEN gemeinsam mit dem Server beobachtet und protokolliert werden, auf dem sie betrieben werden. Insbesondere Änderungen innerhalb des Verzeichnisdienstes sowie Konfigurationsänderungen des Verzeichnisdienstes SOLLTEN vorrangig protokolliert werden.

APP.2.1.A13 Absicherung der Kommunikation mit Verzeichnisdiensten (S)

Werden vertrauliche Informationen übertragen, SOLLTE die gesamte Kommunikation mit dem Verzeichnisdienst über ein sicheres Protokoll entsprechend der Technischen Richtlinie TR-02102 des BSI (z. B. TLS) verschlüsselt werden. Der Datenaustausch zwischen Client und Verzeichnisdienst-Server SOLLTE abgesichert werden. Es SOLLTE definiert werden, auf welche Daten zugegriffen werden darf.

APP.2.1.A14 Geregelte Außerbetriebnahme eines Verzeichnisdienstes (S) [Fachverantwortliche]

Bei einer Außerbetriebnahme des Verzeichnisdienstes SOLLTE sichergestellt sein, dass weiterhin benötigte Rechte bzw. Informationen in ausreichendem Umfang zur Verfügung stehen. Alle anderen Rechte und Informationen SOLLTEN gelöscht werden. Zudem SOLLTEN die Benutzenden darüber informiert werden, wenn ein Verzeichnisdienst außer Betrieb genommen wird. Bei der Außerbetriebnahme einzelner Partitionen eines Verzeichnisdienstes SOLLTE darauf geachtet werden, dass dadurch andere Partitionen nicht beeinträchtigt werden.

APP.2.1.A15 Migration von Verzeichnisdiensten (S)

Bei einer geplanten Migration von Verzeichnisdiensten SOLLTE vorab ein Migrationskonzept erstellt werden. In dem Migrationskonzept SOLLTE berücksichtigt werden, ob das Berechtigungsmanagement von altem und neuem Verzeichnisdienst analog funktioniert oder ob neue Berechtigungsstrukturen erforderlich sind. Die Schema-Änderungen, die am Verzeichnisdienst vorgenommen wurden, SOLLTEN vor der Migration analysiert und dokumentiert werden. Weitreichende Berechtigungen, die dazu verwendet wurden, die Migration des Verzeichnisdienstes durchzuführen, SOLLTEN wieder zurückgesetzt werden. Bei der Migration SOLLTE berücksichtigt werden, dass IT-Systeme, die auf den Verzeichnisdienst zugreifen, gegebenenfalls lokale Caches vorhalten oder aus anderen Gründen dort eine Aktualisierung der migrierten Verzeichnisdienstinhalte initiiert werden muss.

APP.2.1.A18 Planung einer Replikation im Verzeichnisdienst (S)

Bei jeder Replikation MUSS festgelegt werden, welches Ziel diese Replikation verfolgt. Dafür SOLLTEN eine Replikationstopologie und -strategie gewählt werden, die zum Ziel bzw. Einsatzszenario passen. Bei Replikationen, die nicht der Hochverfügbarkeit des Dienstes dienen, MUSS der replizierte Inhalt des Verzeichnisdienstes auf die erforderlichen Objekte beschränkt werden. Um die Replikationen zeitgerecht ausführen zu können, SOLLTE eine ausreichende Bandbreite sichergestellt werden.

APP.2.1.A19 Umgang mit anonymen Zugriffen auf Verzeichnisdienste (S)

Sollen anonymen Benutzenden auf einzelne Teilbereiche des Verzeichnisbaums Zugriffe eingeräumt werden, so SOLLTE hierfür ein Proxy-Dienst vorgelagert werden. Dieser Proxy-Dienst SOLLTE über ein gesondertes Konto, einen sogenannten Proxy-User, auf den eigentlichen Verzeichnisdienst zugreifen. Die Zugriffsrechte für diesen Proxy-User SOLLTEN hinreichend restriktiv vergeben werden. Sie SOLLTEN zudem wieder komplett entzogen werden, wenn der Account nicht mehr gebraucht wird. Damit nicht versehentlich schutzbedürftige Informationen herausgegeben werden, SOLLTE die Suchfunktion des Verzeichnisdienstes dem Einsatzzweck angemessen eingeschränkt 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.

APP.2.1.A16 Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes (H)

Im Rahmen der Notfallvorsorge SOLLTE es eine bedarfsgerechte Notfallplanung für Verzeichnisdienste geben. Für den Ausfall wichtiger Verzeichnisdienst-Systeme SOLLTEN Notfallpläne vorliegen. Alle Notfall-Prozeduren für die gesamte Systemkonfiguration der Verzeichnisdienst-Komponenten SOLLTEN dokumentiert werden.

APP.2.1.A20 Absicherung der Replikation (H)

Replikationen von vertraulichen Inhalten SOLLTEN zusätzlich zu einer Verschlüsselung auf Applikations- oder Transportebene durch z. B. IPsec gesichert werden. Für die Authentisierung im Rahmen der Replikation SOLLTEN möglichst starke Authentisierungsverfahren verwendet werden.

APP.2.1.A21 Hochverfügbarkeit des Verzeichnisdienstes (H)

Es SOLLTE eine geeignete Strategie zur Hochverfügbarkeit gewählt werden. Hierbei SOLLTE entschieden werden, ob eine Master-Master-Replikation oder Master-Replica-Replikation (früher als Master-Slave-Replikation bezeichnet) geeigneter ist. Es SOLLTEN auch Randbedingungen wie verteilte Standorte oder Verhalten bei Inkonsistenzen berücksichtigt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein APP.2.1 *Allgemeiner Verzeichnisdienst* sind keine weiterführenden Informationen vorhanden.