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

Sicherheitsrichtlinie "Verzeichnisdienst"

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 | ISMS300048 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [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](#_Toc82448242)

[Dokumentenhistorie 3](#_Toc82448243)

[Inhaltsverzeichnis 4](#_Toc82448244)

[Allgemeine Festlegungen 5](#_Toc82448245)

[Ziel / Zweck 5](#_Toc82448246)

[Geltungsbereich 6](#_Toc82448247)

[Zuständigkeiten 6](#_Toc82448248)

[Genehmigungs- und Änderungsverfahren 7](#_Toc82448249)

[Aufbau des Dokuments 7](#_Toc82448250)

[Sicherheitsrichtlinie „Verzeichnisdienst" 8](#_Toc82448251)

[Basismaßnahmen 8](#_Toc82448252)

[Allgemeiner Verzeichnisdienst 8](#_Toc82448253)

[Active-Directory 9](#_Toc82448254)

[OpenLDAP 14](#_Toc82448255)

[Standardmaßnahmen 16](#_Toc82448256)

[Allgemeiner Verzeichnisdienst 16](#_Toc82448257)

[Active-Directory 17](#_Toc82448258)

[OpenLDAP 19](#_Toc82448259)

[Maßnahmen bei erhöhtem Schutzbedarf 20](#_Toc82448260)

[Allgemeiner Verzeichnisdienst 21](#_Toc82448261)

[Active-Directory 21](#_Toc82448262)

[OpenLDAP 21](#_Toc82448263)

# Allgemeine Festlegungen

## Ziel / Zweck

**Allgemeiner Verzeichnisdienst**

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 Benutzerkennung der Name und Vorname des Benutzers, die Personalnummer und der Rechnername 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
* Ressourcen-Verwaltung, z. B. für IT-Systeme, Drucker, Scanner und andere Peripherie-Geräte
* Benutzerverwaltung, z. B. zur Verwaltung von Benutzerkonten und Benutzerberechtigungen
* Authentisierung, z. B. zur Anmeldung an Betriebssystemen oder Anwendungen

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

**Microsoft Active-Directory (AD)**

Die Firma Microsoft entwickelte einen eigenen Verzeichnisdienst "Active-Directory (AD)". Dieses wurde mit dem Betriebssystem Windows 2000 Server erstmalig eingeführt wurde. Ausgehend von den Active-Directory-Funktionen des Betriebssystems Microsoft Windows 2000 Server wurden dem Active-Directory-Dienst mit jedem Release der Windows-Server-Familie weitere Schlüsselfunktionen hinzugefügt. Ein AD speichert Informationen über Objekte innerhalb eines Netzes, z. B. über Benutzer oder IT-Systeme. Es erleichtert es Anwendern und Administratoren, diese Informationen bereitzustellen, zu organisieren, zu nutzen und zu überwachen. Als ein objektbasierter Verzeichnisdienst ermöglicht Active-Directory die Verwaltung von Objekten und deren Beziehung untereinander, was die eigentliche Netzumgebung auszeichnet. Das AD stellt zentrale Steuerungs- und Kontrollmöglichkeiten des jeweiligen Netzes bereit. Ohne einen Verzeichnisdienst könnte nicht mehr gewährleistet werden, dass lokal vorzunehmende Einstellungen, wie z. B. die Vorgaben aus Sicherheitsrichtlinien, aufgrund des hohen Aufwandes zuverlässig erledigt werden. Verwaltungsaufgaben innerhalb des Netzes wie z. B. Passwortänderungen, Kontenerstellung und Zugriffsrechte können effizienter durchgeführt werden, wenn ein Verzeichnisdienst eingesetzt wird.

**OpenLDAP**

OpenLDAP ist ein frei verfügbarer Verzeichnisdienst, der in einem Datennetz Informationen über beliebige Objekte, beispielsweise Benutzer oder IT-Systeme, in einer 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 Benutzerverwaltungen.

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.

Ziel dieser Sicherheitsrichtlinie ist es, Verzeichnisdienste wie ein Active-Directory oder openLDAP im Regelbetrieb sicher zu betreiben sowie die damit verarbeiteten Informationen angemessen zu schützen. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben der BSI Bausteine APP.2.1 "Allgemeiner Verzeichnisdienst", APP.2.2 "Active Directory" und APP.2.3 "OpenLDAP" zurückgegriffen.

## 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 „Verzeichnisdienst“ 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 „Verzeichnisdienst"

## Basismaßnahmen

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

### Allgemeiner Verzeichnisdienst

#### Planung des Einsatzes von Verzeichnisdiensten (APP.2.1.A2)

Der Einsatz von Verzeichnisdiensten wird gemäß der Sicherheitsstrategie der <Institution> sorgfältig geplant. Neben der Festlegung der Nutzung des Verzeichnisdienstes wird ein Modell aus Objektklassen und Attributtypen entwickelt, dass den Ansprüchen der vorgesehenen Nutzungsarten genügt.

Bei jeder Neuplanung oder Migration von Verzeichnisdiensten werden die Verantwortlichen der Departments, der <Informationssicherheitsbeauftragter> und der <Datenschutzbeauftragter> koordinativ beteiligt. Für jeden Verzeichnisdienst wird ein bedarfsgerechtes Berechtigungskonzept erstellt und evaluiert. Generell wird die geplante Verzeichnisdienststruktur vollständig dokumentiert. Es wird technisch und organisatorisch unterbunden, dass Unbefugt Daten aus dem Verzeichnisdienst sammeln können.

#### Einrichtung von Zugriffsberechtigungen auf Verzeichnisdienste (APP.2.1.A3)

Die administrativen Aufgaben für die Administration des Verzeichnisdienstes selbst sowie für die eigentliche Verwaltung der Daten wird strikt getrennt. Die administrativen Tätigkeiten an den Verzeichnisdiensten werden so koordiniert und delegiert, dass sich möglichst keine Überschneidungen ergeben. Alle Vorgaben für die administrativen Aufgabenbereiche und Berechtigungen werden für Dritte nachvollziehbar in den Betriebsdokumenten des Verzeichnisdienstes dokumentiert.

Die Zugriffsrechte der Benutzer- und Administratorengruppen werden anhand der den internen Vorgaben der <Institution> konfiguriert und somit etabliert. Bei einer eventuellen Zusammenführung mehrerer Verzeichnisdienstbäume werden die resultierenden effektiven Rechte kontrolliert und eine minimale Rechtevergabe (Need-to-know-Prinzip) weiterhin sichergestellt.

#### Sichere Installation von Verzeichnisdiensten (APP.2.1.A4)

Administrations- und Zugriffsberechtigungen werden bereits bei der Installation des Verzeichnisdienstes konfiguriert und beruhen auf dem Need-to-know-Prinzip. Zusätzlich wird sichergestellt, dass lediglich die benötigten Dienste vom darunterliegenden Betriebssystem aktiviert sind.

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

Alle Verzeichnisdienste werden sicher und geeignet konfiguriert. Für die sichere Konfiguration einer Verzeichnisdienst-Infrastruktur werden auch die IT-Systeme und Komponenten (z. B. Server, Clients und Betriebssysteme sowie kryptografische Vorgaben) einbezogen.

Administrative Zugänge zum Verzeichnisdienst werden geschützt und sind entsprechend den etablierten Sicherheitsbereichen in die Infrastruktur integriert. Bei der Durchführung von Konfigurationsänderungen der vernetzten IT-Systeme mit Auswirkung auf den Service an sich, werden die Benutzer dieses Service rechtzeitig über Wartungsarbeiten informiert.

Die Hierarchie der Organisationseinheiten (OU) sollte die folgenden Anforderungen erfüllen:

* Einfache Verwaltbarkeit der in den Organisationseinheiten enthaltenen Objekte
* Eindeutige Zuweisung von Richtlinienobjekten
* Eindeutige Berechtigungsvergabe zur Administration für Objekte in einer Organisationseinheit

Es sind einheitliche Namenskonventionen anhand eines Namenskonzeptes anzuwenden für:

* Computer (Clients, Server)
* Benutzerobjekte (User, technische Benutzerkonten, Administratorenkonten, Ressourcen)
* Benutzergruppen
* OU’s
* Standorte

Vor Konfigurationsänderungen oder bei Patchen und Updates werden von allen betroffenen Dateien und Verzeichnissen Datensicherungen gemäß den internen Vorgaben der <Institution> angefertigt.

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

Die Sicherheit der Verzeichnisdienste wird im laufenden Betrieb permanent aufrechterhalten. Alle für den Betrieb eines Verzeichnisdienst-Systems betreffenden Richtlinien, Regelungen und Prozesse sind dokumentiert.

Besitzer von Administratorkonten dürfen diese nicht für die gewöhnliche tägliche Arbeit verwenden. Server-Administrator-Konten dürfen nicht auf Workstations im Rahmen der klassischen Anmeldung verwendet werden.

Jedes personalisierte Benutzerkonto muss sich eindeutig einem Mitarbeitenden zuordnen lassen. Pro technischen Benutzerkonto muss mindestens ein verantwortlicher Ansprechpartner benannt sein.

Die Anzahl der Dienste-Administratoren und der Datenadministratoren des Active-Directory muss auf das notwendige Minimum vertrauenswürdiger Personen reduziert sein. Ihre Konten müssen entsprechend den Empfehlungen im Umgang mit Passwörtern angemessen abgesichert sein.

Alltägliche, nichtadministrative Aufgaben sind mit unprivilegierten personalisierten Benutzerkonten durchzuführen.

### Active-Directory

#### Planung des Active-Directory (APP.2.2.A1)

Unter Berücksichtigung des Cloud-Strategie der <Institution> ist der Einsatz einer Active-Directory Infrastruktur und AzureAD-Infrastruktur zu planen.

Bei der Planung der Nutzung der Konten für Dienste und Computer ist darauf zu achten, dass die Konten für Dienste und Computer niemals Mitglieder der Gruppe „Protected Users" sind.

Die Nutzung von Builtin Gruppen für privilegierte Accounts ist zu vermeiden, da die Builtin Gruppen einerseits bereits über hohe Privilegien verfügen. So haben die Mitglieder der Gruppe „Account Operators“ sowohl Schreib- und Änderungsrechte auf alle User und Group Objekte inkl. der Domain Admins, Enterprise Admins und Schema Admins Gruppen. In die Planung sollte auch mit einfließen, da sich viele Administratoren über die Rechte von Builtin Gruppen nicht vollumfänglich bewusst sind.

Stattdessen ist ein granulares, aber übersichtliches Rollen-basiertes Admin-Konzept mit eigenen Gruppen nach dem Least-Privilege Prinzip zu etablieren und zu betreiben.

Das Active-Directory Berechtigungskonzept ist grundsätzlich nach dem Need-to-know-Prinzip und den aktuellen Empfehlungen des Herstellers Microsoft und führenden Sicherheitsexperten zu etablieren. Administrative Delegationen sind mit restriktiven und bedarfsgerechten Berechtigungen auszustatten. Im Rahmen der Planung einer Active-Directory-Infrastruktur ist zu prüfen, ob die folgenden Einstellungen für privilegierte und hoch privilegierte Accounts aktiviert werden:

* Aktivieren der Option „Account is sensitive an cannot be delegated“
* Aktivieren der Option „Smart card is required for interactive logon“
* Hinzufügen aller privilegierten Accounts zur Gruppe „Protected Users“

Die geplante Active-Directory Struktur einschließlich etwaiger Schema-Änderungen ist geeignet und nachvollziehbar zu dokumentieren.

#### Planung der Active-Directory-Administration (APP.2.2.A2)

Für Domain Administratoren ist zwischen 3 Arten von Benutzerkonten zu unterscheiden:

* Der nicht privilegierte Account: Mit diesem Account muss sich ein Administrator an seiner physischen bzw. virtuellen Arbeitsstation anmelden. Dieser Account besitzt keine privilegierten Rechte, sondern dient wie bei jedem anderen Mitarbeiter der <Institution> der täglichen Arbeit für bspw. den Zugriff auf die Mailbox, die Office-Programme und sonstige bereitgestellte Standardsoftware.
* Der privilegierte Account: Mit diesem Account sind die alltäglichen administrativen Tätigkeiten durchzuführen, z.B. Administration einzelner Server, Arbeitsstationen oder Services.
* Der hoch privilegierte Account: Dieser Account dient ausschließlich zu administrativen Zwecken im Active-Directory selbst. Nur dieser Account ist Mitglied der Domain Admins Gruppe und kann die Domain administrieren.

In der Active-Directory Struktur sind die nicht privilegierten Accounts von den privilegierten Accounts hierarchisch strikt zu trennen und zu dokumentieren. Die administrativen Aufgaben sind im Active-Directory nach einem Delegationsmodell überschneidungsfrei zu verteilen. Hieraus ableitend ist zu prüfen, in wie weit die folgenden Einstellungen zur Absicherung der Accounts und deren Rechte innerhalb der <Institution> umsetzbar sind.

Für Gruppen mit privilegierten Accounts (Role-based Admin Gruppen) sollte per GPO eine Beschränkung auf Member Servern und/oder Member Clients mit dem Ziel etabliert werden, dass sich ein privilegierter Account ausschließlich lokal über ein Konsolen Login an Member Servern und/oder Member Clients anmelden kann. Des Weiteren sollte eine Beschränkung der Gruppen mit privilegierten Accounts per GPO auf Domain Controllern mit dem Ziel etabliert werden, dass sich ein privilegierter Account überhaupt nicht mehr an Domain Controllern anmelden kann.

Per GPO sollte sichergestellt werden, dass sich ein hoch privilegierter Account überhaupt nicht an einem Member Server und Member Client anmelden kann. Für Gruppen mit hoch privilegierten Accounts (Enterprise Administrator, Domain Administrator und Schema Administrator) muss eine Reduzierung der Gruppenmitglieder sichergestellt sein. Dies bedeutet für die nachfolgend aufgeführten Gruppen:

* Enterprise Admins: Die Gruppe sollte keine Mitglieder besitzen. Ein Mitglied darf lediglich bei Bedarf und zeitlich begrenzt hinzugefügt werden.
* Domain Admins: Die Gruppe sollte lediglich den Built-in Administrator beinhalten. Werden zusätzliche hoch privilegierte Accounts hinzugefügt, sollte deren Anzahl so minimal wie möglich gehalten werden.
* Schema Admins: Die Gruppe sollte im besten Fall keine Mitglieder haben. Ein Mitglied sollte lediglich bei Bedarf und zeitlich begrenzt hinzugefügt werden.

#### Planung der Gruppenrichtlinien unter Windows (APP.2.2.A3)

Die Verwendung von Gruppenrichtlinien ist unter Windows geeignet einzurichten. Aus der Betriebsdokumentation zu den Windows Systemen gehen die eingesetzten Gruppenrichtlinien hervor. Gruppenrichtlinienobjekte sind getrennt nach Objektklasse (User und Computer) anzulegen und anzuwenden. Bei der Planung der Gruppenrichtlinien sind die Sicherheitsziele der <Institution> sowie die Best Practice Ansätze zur Vermeidung von Sicherheitsvorfällen zu berücksichtigen.

Die Default-Domänenrichtlinie sollte nur die folgenden Einstellungen enthalten:

* Password Policy
* Account Lockout Policy
* Kerberos Policy

Die Default Domain Controller Policy sollte nur die folgenden Einstellungen enthalten:

* User Rights Assignment
* Security Options (aber nicht alle)

Die Hierarchie der Organisationseinheiten (OU) sollte die folgenden Anforderungen erfüllen:

* Einfache Verwaltbarkeit der in den Organisationseinheiten enthaltenen Objekte
* Eindeutige Zuweisung von Gruppenrichtlinienobjekten
* Eindeutige Berechtigungsvergabe zur Administration für Objekte in einer Organisationseinheit

Es sind einheitliche Namenskonventionen anhand eines Namenskonzeptes anzuwenden für:

* Computer (Clients, Server)
* Benutzerobjekte (User, Servicekonten, Administratorkonten, Ressourcen)
* Benutzergruppen
* Gruppenrichtlinien
* OU’s
* Standorte

Mehrfachüberdeckungen sind beim Gruppenrichtlinienkonzept möglichst zu vermeiden. Durch die Dokumentation des Gruppenrichtlinienkonzepts werden Ausnahmeregelungen erkannt. Alle Gruppenrichtlinienobjekte sind durch restriktive Zugriffsrechte zu schützen. Für die Parameter in allen Gruppenrichtlinienobjekten sind sichere Vorgaben festzulegen.

Änderungen an Gruppenrichtlinien sind durch geeignete Werkzeuge zu versionieren und zu genehmigen.

#### Schulung zur Active-Directory-Verwaltung (APP.2.2.A4)

Die verantwortlichen Administratoren sind mit allen Sicherheitsmechanismen und -aspekten von Active-Directory in ihrem Tätigkeitsbereich vertraut. Sie werden für die Arbeit mit Active-Directory vor der Einrichtung und anschließend regelmäßig sensibilisiert und geschult.

#### Härtung des Active-Directory (APP.2.2.A5)

Es muss geprüft werden, ob es die Netz-Infrastruktur der <Institution> zulässt, die Domain-Controller in einem eigenen Netzwerk-Segment zu betreiben. Die Netz-Segmente der Domain-Controller müssen durch die etablierte Firewall-Infrastruktur bzw. Micro-Segmentierung separiert werden. Grundsätzlich sind ausschließlich die für den Betrieb benötigten Ports und ggf. Ports für die Remote Verwaltung freizuschalten. An Außenstandorten, an denen die geforderte physische Sicherheit unter Umständen nicht gegeben ist, sollten ausschließlich Read-only Domain Controller (RODCs) etabliert und betrieben werden.

Der „Software-Footprint“ eines Domain-Controllers muss möglichst klein gehalten werden. Daher sollte der Domain-Controller als Server Core installiert werden. Eine direkte Anmeldung am Desktop eines Domain-Controllers sollte nicht erfolgt.

Da das Pagefile durchaus sensible Daten enthält, sollte zu Gunsten der Informationssicherheit die Verschlüsselung des Pagefiles aktiviert werden.

Die meisten Monitoring Produkte benötigen einen Agenten, welcher mit privilegierten Service Accounts betrieben werden muss. Auf Domain-Controllern sollte auf ein Agent-basiertes Monitoring zur Reduzierung des Kompromittierungsvektors verzichtet werden. Für ein risikoarmes Monitoring sollten die wichtigsten Systemparameter und Services per WMI oder WinRM abgefragt werden.

Externe Produkte zum Erstellen eines Backups benötigen meist einen privilegierten Service Account. Unter der Berücksichtigung der Empfehlung der Firma Microsoft sollte keine Wiederherstellung (Restore) eines Domain-Controllers durchgeführt werden. Zur Erfüllung der benötigten Service Level Agreements (SLA) sollten die Informationen verteilt über mehrere Domain-Controller vorgehalten werden. Sollte ein einzelner Domain-Controller Probleme im Betrieb aufzeigen, sollte nach den folgenden Schritten vorgegangen werden:

* den betroffenen Domain-Controller herunterstufen,
* den betroffenen Domain-Controller anschließend löschen,
* den zuvor gelöschten Domain-Controller neu installieren und
* den neuen Domain-Controller zum Abschluss der Arbeiten wieder heraufstufen.

Der Active-Directory-Restore-Modus ist durch ein geeignetes Passwort zu schützen. Insofern sich entschieden wurde den Active-Directory-Restore-Modus zu verwenden, erfolgen alle Tätigkeiten nur unter Einhaltung des Vier-Augen-Prinzips.

Als Notfallvorsorge sollte unter zur Hilfenahme von Bordmittel der System State inkl. Datenbank gesichert werden.

Der Hypervisor von VMware inklusive der VMware Tools, als auch Citrix mit den XenServer Tools benötigen eine eigene Installation, um Treiber und Management Funktionen bereitzustellen. Während die XenServer Tools auf .NET basieren, basieren die VMware Tools auf Visual C++ und installieren aus diesem Grunde eine Vielzahl an Visual C++ Redistributable Versionen, die bekanntermaßen eine große Angriffsfläche bieten. Um die potentielle Angriffsfläche zu reduzieren, sollten virtualisierte Domain-Controller möglichst auf Microsoft Hyper-V installiert und betrieben werden. Denn die benötigten Treiber und Tools sind bereits „Builtin“ integraler Bestandteil des Betriebssystems.

Für den Betrieb eines Domain-Controllers kein Internet Zugang benötigt. Daher muss jeder direkte Zugang zum Internet gesperrt werden.

Die Built-in-Accounts sind mit komplexen Passwörtern zu versehen und ausschließlich als Notfallkonten einzusetzen.

Für alle Domänen-Controller sind restriktive Zugriffsrechte auf Betriebssystemebene zu vergeben.

Die Berechtigungen für die Gruppe "Jeder" sind zu beschränken. Alle Domänencontroller sind gegen unautorisierte Neustarts zu schützen.

Die Domänenrichtlinien umfassen sichere Einstellungen für Kennworte, Kontensperrung, Kerberos-Authentisierung, Benutzerrechte und Überwachung. Es ist eine ausreichende Größe für das Sicherheitsprotokoll des Domänen-Controllers einzustellen. Bei externen Vertrauensstellungen zu anderen Domänen sind Autorisierungsdaten der Mitarbeitenden zu filtern und zu anonymisieren.

#### Aufrechterhaltung der Betriebssicherheit von Active-Directory (APP.2.2.A6)

Alle Vertrauensbeziehungen im Active-Directory werden regelmäßig auf einen weiteren Bedarf evaluiert.

Die Dienste-Administratoren auf dem Domänencontroller besitzen nur die notwendigen Rechte (Need-to-Know-Prinzip). Diese Rechte sind in regelmäßigen Abständen zu überprüfen. Die Gruppe der Domänen-Administratoren ist möglichst klein zu halten. Nicht mehr verwendete personalisierte Konten sind im Active-Directory zu deaktivieren und nach 90 Tagen zu löschen. Nicht mehr benötigte technische Benutzerkonten sind sofort zu löschen.

Alle notwendigen Parameter des Active-Directorys sind als Basisinformationen aktuell und nachvollziehbar festzuhalten.

#### Umsetzung sicherer Verwaltungsmethoden für Active-Directory (APP.2.2.A7)

Besitzer von Administratorkonten dürfen diese nicht für die gewöhnliche tägliche Arbeit verwenden. Serveradministrator-Konten dürfen nicht auf Workstations im Rahmen der klassischen Anmeldung verwendet werden. Domänenadministrator-Konten dürfen nicht auf Workstations oder Servern im Rahmen der klassischen Benutzer-Anmeldung am System genutzt werden.

Jedes personalisierte Benutzerkonto muss sich eindeutig einem Mitarbeitenden zuordnen lassen. Pro technischen Benutzerkonto muss mindestens ein verantwortlicher Ansprechpartner benannt sein.

Die Anzahl der Dienste-Administratoren und der Daten-Administratoren des Active-Directorys ist auf das notwendige Minimum vertrauenswürdiger Personen zu reduzieren. Ihre Konten sind entsprechend den Empfehlungen im Umgang mit Passwörtern angemessen abzusichern.

Das Standardkonto "Administrator" muss umbenannt und sollte in eine nicht privilegierte Benutzergruppe verschoben werden. Alltägliche, nichtadministrative Aufgaben sind mit nicht privilegierten personalisierten Benutzerkonten durchzuführen.

Es ist sicherzustellen, dass die Verwaltung von Dienste-Administratorkonten ausschließlich von Mitgliedern der Dienste-Administratorgruppe erfolgt. Die Gruppe "Kontenoperatoren" ist auf das notwendige Minimum vertrauenswürdiger Personen zu reduzieren.

Administratoren dürfen der Gruppe "Schema-Admins" nur temporär für den Zeitraum der Schema-Änderungen zugewiesen werden. Für die Gruppen "Organisations-Admins" und "Domänen-Admins" zur Administration der Stammdomäne sollte ein Vier-Augen-Prinzip etabliert sein.

Die Arbeitsplätze zur Administration des Active-Directorys sind ausreichend abzusichern. Bei Remoteadministration der Domänen-Controller muss der Datenverkehr entsprechend den freigegebenen Verfahren verschlüsselt sein.

Der Einsatz von domänenlokalen Gruppen für die Steuerung der Leseberechtigung für Objektattribute sollte vermieden werden.

Der Papierkorb des Active-Directorys muss aktiviert werden.

Mit Hilfe einer Enterprise Identity Management-Lösung sollte sichergestellt werden, dass die Rechte aller Anwender definierten Vorgaben der <Institution> entsprechen.

### OpenLDAP

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

Der Einsatz von OpenLDAP ist innerhalb der <Institution> sorgfältig zu planen. Sofern OpenLDAP gemeinsam mit anderen Anwendungen verwendet werden soll, ist die Planung, Konfiguration und Installation der Anwendungen mit OpenLDAP aufeinander abzustimmen. Für die zur Datenhaltung ausgewählte Datenbank ist sicherzustellen, dass die eingesetzte Version kompatibel ist. Bei der Auswahl des Datenbank-Backends ist zu beachten, das slapd mit einer Vielzahl verschiedener Datenbank-Backends ausgeliefert wird. Dazu gehören

* MDB, ein hierarchisches transaktionales Hochleistungsdatenbank-Backend
* BDB, ein transaktionales Hochleistungsdatenbank-Backend (veraltet)
* HDB, ein hierarchisches transaktionales Hochleistungs-Backend (veraltet)
* SHELL, eine Backend-Schnittstelle zu beliebigen Shell-Skripten und
* PASSWD, eine einfache Backend-Schnittstelle zur passwd-Datei

Das MDB-Backend verwendet LMDB, einen hochleistungsfähigen Ersatz für Berkeley DB der Oracle Corporation.

Des Weiteren sind Backends und Overlays für OpenLDAP restriktiv zu selektieren. Hierzu ist sicherzustellen, dass die OpenLDAP-Overlays in der korrekten Reihenfolge eingesetzt werden. Bei der Planung von OpenLDAP sind auch die auszuwählenden und unterstützten Client-Anwendungen zu berücksichtigen.

#### Sichere Installation von OpenLDAP (APP.2.3.A2)

Es ist zu überprüfen, ob alle Anwendungen, die auf OpenLDAP zugreifen sollen, mit der zu installierenden OpenLDAP-Version kompatibel sind. Die Versionen der OpenLDAP-Installationspakete sind sorgfältig auszuwählen. Die Integrität der OpenLDAP-Installationspakete ist zu überprüfen. Alle Installationsschritte und die Herkunft der OpenLDAP-Installationspakete sollten dokumentiert werden.

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

Für die sichere Konfiguration von OpenLDAP muss der slapd-Server korrekt konfiguriert werden. Es müssen ebenfalls 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 an die Bedürfnisse der <Institution> 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.

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

Die Zugriffsrechte für neu angelegte Datenbankdateien sind auf die Benutzerkennung zu beschränken, in deren Kontext der slapd-Server betrieben wird. Sofern die BDB- und HDB-Backends auf Basis der BerkeleyDB eingesetzt werden, sind die Standard-Einstellungen der von OpenLDAP genutzten BerkeleyDB anzupassen.

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

Es ist ein Berechtigungskonzept zu erstellen. Die dort getroffenen Regelungen sind in OpenLDAP technisch umzusetzen. Die in OpenLDAP geführten globalen und datenbankspezifischen Access Control Lists sind beim Einsatz von OpenLDAP korrekt zu berücksichtigen. Datenbank-Direktiven besitzen Vorrang vor globalen Direktiven.

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

Wenn der Verzeichnisdienst zwischen verschiedenen Benutzern unterscheiden soll, sind sich diese geeignet zu authentisieren. Die Authentisierung zwischen dem slapd-Server und den Kommunikationspartnern muss verschlüsselt erfolgen. Es dürfen nur die Hashwerte von Passwörtern auf den Clients und Servern abgespeichert werden. Es muss ein geeigneter Hashing-Algorithmus verwendet werden.

## Standardmaßnahmen

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

### Allgemeiner Verzeichnisdienst

#### Erstellung eines Sicherheitskonzepts für den Einsatz von Verzeichnisdiensten (APP.2.1.A7)

Es werden für die Verzeichnisdienste sämtliche sicherheitsbezogene Themenbereiche geregelt und dokumentiert. Die daraus entwickelten Sicherheitsvorgaben werden hinsichtlich der etablierten internen Service Level Agreements (SLA) bzw. Operational Level Agreement (OLA) validiert. Die Benutzer werden bezüglich des erforderlichen Umfangs zu den Regelungen der eingesetzten Verzeichnisdienste sensibilisiert und geschult.

#### Planung einer Partitionierung und Replikation im Verzeichnisdienst (APP.2.1.A8)

Bei einer Partitionierung wird auf die Verfügbarkeit und den Schutzbedarf des Verzeichnisdienstes geachtet. Sofern die Partitionierung des Verzeichnisdienstes zum Einsatz kommt, wird diese schriftlich dokumentiert, sodass sie manuell wieder rekonstruierbar ist. Um die Replikationen zeitgerecht ausführen zu können, wird eine ausreichende Bandbreite sichergestellt.

#### Geeignete Auswahl von Komponenten für Verzeichnisdienste (APP.2.1.A9)

Für den Einsatz von Verzeichnisdiensten sollten ausschließlich geeignete Komponenten mittels Anforderungskatalog identifiziert und eingesetzt werden. Der Anforderungskatalog ist maßgebend für die Beschaffung von Verzeichnisdiensten und deren Komponenten. Im Rahmen der Planung und Konzeption von Verzeichnisdiensten werden Anforderungen an dessen Sicherheit in Abhängigkeit vom Einsatzzweck formuliert.

#### Schulung zu Administration und Betrieb von Verzeichnisdiensten (APP.2.1.A10)

Die Administratoren bzw. externen Dienstleister sind mit allen Sicherheitsmechanismen und -aspekten von Verzeichnisdiensten in ihrem Tätigkeitsbereich vertraut. Zur Förderung und Aufrechterhaltung des Wissens der Administratoren werden regelmäßige Sensibilisierungen und Schulungen zum Thema ermöglicht.

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

Der Zugriff auf den Verzeichnisdienst wird entsprechend den internen Vorgaben der <Institution> konfiguriert. Sofern der Verzeichnisdienst als Server mit Anbindung an öffentliche Netze eingesetzt wird, ist der Verzeichnisdienst in die etablierte Firewall-Infrastruktur und dem zu Grunde liegenden Modell für die Etablierung von Sicherheitsbereichen und Sicherheitszonen zu integrieren und zu schützen.

Sollten anonyme Benutzer auf einzelne Teilbereiche des Verzeichnisbaums weitergehende Zugriffe benötigen, werden gesonderte Benutzerkonten (Proxy-User) für den anonymen Zugriff eingerichtet. Des Weiteren werden die Zugriffsrechte für die Proxy-User hinreichend restriktiv (Need-to-know-Prinzip) vergeben. Die Zugriffsrechte werden komplett entzogen, sobald der Account nicht mehr benötigt wird.

Um die unnötige Herausgabe von vertraulichen Informationen zu verhindern, werden die Suchfunktion der Verzeichnisdienste dem Einsatzzweck angemessen eingeschränkt.

#### Überwachung von Verzeichnisdiensten (APP.2.1.A12)

Die Verzeichnisdienste werden gemäß den internen Vorgaben der <Institution> überwacht. Für die Verzeichnisdienste spezifische Ereignisse sowie Ereignisse des eingesetzten Betriebssystems werden beobachtet, protokolliert und proaktiv ausgewertet.

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

Der Datenaustausch zwischen den Clients und Verzeichnisdienst-Server wird sowohl bei Innen- und Außenanbindungen kryptographisch abgesichert. Auf welche Daten zugegriffen werden darf, ist klar zu definieren. Beim Einsatz einer serviceorientierten Architektur (SOA) werden zum Schutz von Service-Einträgen in einer Service-Registry sämtliche Anfragen an die Registratur auf Gültigkeit des Benutzers überprüft.

#### Geregelte Außerbetriebnahme eines Verzeichnisdienstes (APP.2.1.A14)

Die Außerbetriebnahme der Verzeichnisdienste erfolgt auf Basis der internen Anforderungen der <Institution>. Bei Außerbetriebnahmen der Verzeichnisdienste wird sichergestellt, dass weiterhin benötigte Rechte beziehungsweise Informationen für Verfahren der der <Institution> in ausreichendem Umfang zur Verfügung stehen. Alle nicht mehr benötigten Rechte und Informationen werden gelöscht.

Die betroffenen Benutzer (personalisierte Konten) bzw. Kontenverantwortlichen (technische Benutzerkonten) werden über die Außerbetriebnahmen der Verzeichnisdienste informiert. Bei der Außerbetriebnahme einzelner Partitionen von Verzeichnisdiensten wird darauf geachtet, dass dadurch andere Partitionen nicht beeinträchtigt werden.

#### Migration von Verzeichnisdiensten (APP.2.1.A15)

Für alle Migrationen von Verzeichnisdiensten werden vorab Migrationskonzepte erstellt. Alle Änderungen an den Verzeichnisdiensten z. B. Schemaänderungen beim Active-Directory von Microsoft werden dokumentiert.

Weitreichende Berechtigungen, die zur Durchführung der Migration des Verzeichnisdienstes verwendet wurden, sind im Rahmen der Finalisierung der Migration wieder zurückzusetzen.

Die Zugriffsrechte für Verzeichnisdienst-Objekte bei Systemen, die von Vorgängerversionen aktualisiert beziehungsweise von anderen Verzeichnissystemen übernommen wurden, werden mit migriert.

### Active-Directory

#### Konfiguration des sicheren Kanals unter Windows (APP.2.2.A8)

Der Sichere Kanal unter Windows ist entsprechend den Sicherheitsanforderungen und den lokalen Gegebenheiten der <Institution> zu konfigurieren. Dabei werden alle relevanten Gruppenrichtlinienparameter berücksichtigt.

#### Schutz der Authentisierung beim Einsatz von Active-Directory (APP.2.2.A9)

In der Umgebung des Active-Directorys sind konsequent die von der der <Institution> freigegebenen Authentisierungsprotokolle einzusetzen. Sofern aus Kompatibilitätsgründen übergangsweise noch NTLMv2 eingesetzt wird, ist die Migration auf die freigegebenen Authentisierungsprotokolle der der <Institution> zu planen und zu terminieren. Die LM-Authentisierung ist grundsätzlich zu deaktivieren und der SMB-Datenverkehr sollte authentisiert und signiert werden.

Anonyme Zugriffe auf Domänencontroller sind geeignet zu unterbinden.

#### Sicherer Einsatz von DNS für Active-Directory (APP.2.2.A10)

Integrierte DNS-Zonen beziehungsweise die sichere dynamische Aktualisierung der DNS-Informationen sind zu verwenden, um DNS-Clientabfragen durch unautorisierte Systeme zu vermeiden. Der Zugriff auf die Konfigurationsdaten des DNS-Servers ist nur von administrativen Konten zu erlauben.

Der DNS-Cache auf den DNS-Servern ist vor unberechtigten Änderungen zu schützen. Der Zugriff auf den DNS-Dienst der Domänen-Controller ist auf das notwendige Maß zu beschränken.

Die Netzaktivitäten in Bezug auf DNS-Anfragen sind gemäß den internen Vorgaben der <Institution> zu überwachen. Der Zugriff auf die DNS-Daten im Active-Directory ist mittels ACLs auf Administratoren zu beschränken. Insofern sekundäre DNS-Zonen eingesetzt werden, sind die Zonen-Dateien vor unbefugten Zugriffen zu schützen.

Beim Einsatz von IPSec oder DNS over TLS zur Absicherung der DNS-Kommunikation ist ein ausreichender Datendurchsatz im Netz der <Institution> bzw. des beauftragten Dienstleisters zu gewährleisten.

#### Überwachung der Active-Directory-Infrastruktur (APP.2.2.A11)

Die Active-Directory-Infrastruktur ist anhand der systemeigenen Ereignisse zu überwachen und zu protokollieren. Die Ergebnisse der Sicherheitsüberwachung des Active-Directorys sind proaktiv durch ein SIEM auszuwerten. Die Verfügbarkeit und Systemressourcen der Domänen-Controller sind geeignet durch eine übergreifende zentrale Monitoring-Infrastruktur zu überwachen. Änderungen auf Domänen-Ebene und an der Gesamtstruktur des Active Directory sind zu überwachen, zu protokollieren und auszuwerten. Hierfür sind mindestens die folgenden Log-Events automatisiert auszuwerten und auf das Überschreiten von zuvor festgelegten Schwellwerten zu überprüfen.

| **EventID** | **Beschreibung** |
| --- | --- |
| 4720 | Created |
| 4722 | Enabled |
| 4723 | User changed password |
| 4724 | Privileged user changed this user’s password |
| 4725 | Disabled |
| 4726 | Deleted |
| 4738 | Changed |
| 4740 | Locked out |
| 4767 | Unlocked |
| 4781 | Name changed |

Zusätzlich ist zu verifizieren, welcher Logon-Fehler-Code zurückgegeben wird. Hierfür ist auf die in der nachfolgenden Tabelle aufgeführten Codes zurück zu greifen.

| **Failure Code** | **Beschreibung** |
| --- | --- |
| 0xC0000064 | User name does not exist |
| 0xC000006A | User name is correct but the password is wrong |
| 0xC0000234 | User is currently locked out |
| 0xC0000072 | Account is currently disabled |
| 0xC000006F | User tried to logon outside his day of week or time of day restrictions |
| 0xC0000070 | Workstation restriction |
| 0xC00000193 | Account expiration |
| 0xC0000071 | Expired password |
| 0xC0000133 | Clocks between DC and other computer too far out of sync |
| 0xC0000224 | User is required to change password at next logon |
| 0xC0000225 | Evidently a bug in Windows and not a risk |
| 0xC000015b | The user has not been granted the requested logon type (aka logon right) at this machine |

#### Datensicherung für Domänen-Controller (APP.2.2.A12)

Es ist eine Datensicherungs- und Wiederherstellungsrichtlinie für Domänen-Controller zu etablieren. Insofern nicht auf die Boardmittel der Firma Microsoft zurückgegriffen wird, muss die eingesetzte Sicherungssoftware explizit vom Hersteller für die Datensicherung von Domänen-Controllern freigegeben sein. Die Anzahl der Mitglieder der Gruppe „Sicherungs-Operatoren“ ist auf das notwendige Maß zu begrenzen. Der Zugriff auf das AdminSDHolder-Objekt ist zum Schutz der Berechtigungen besonders zu schützen.

Die Daten der Domänen-Controller sollten in regelmäßigen Abständen gesichert werden. Dabei ist ein Sicherungsverfahren einzusetzen, das veraltete Objekte weitgehend vermeidet.

Die Sicherungsmedien sollten an einem geeigneten Standort aufbewahrt werden. Der korrekte Ablauf und das Wiedereinspielen von Datensicherungen der Domänen-Controller sollte in regelmäßigen Abständen überprüft werden.

### OpenLDAP

#### Schulung von Administratoren von OpenLDAP (APP.2.3.A7)

Es sind alle verantwortlichen Administratoren zu OpenLDAP und den zugehörigen Sicherheitsthemen entsprechend des vereinbarten Schulungsplans fortzubilden.

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

Anhand von Overlays sind die Attribute in OpenLDAP einzuschränken. Die Konfigurationen in OpenLDAP sollten 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. Diese Restriktionen sind auf Nutzerdaten anzuwenden.

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

OpenLDAP sollte in Teilbäume auf verschiedene Server aufgeteilt (partitioniert) werden. Dabei sollten Veränderungen an den Daten durch Replikation zwischen den Servern ausgetauscht werden. Der Replikationsmodus ist in Abhängigkeit von Netzverbindungen und Verfügbarkeitsanforderungen zu wählen.

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

Die OpenLDAP-Software sollte bei neu erscheinenden Releases, die sicherheitsrelevante Änderungen enthalten oder Schwachstellen beheben, so schnell wie möglich aktualisiert werden. Dabei ist insbesondere darauf zu achten, ob diese Änderungen von der <Institution> eingesetzte Backends oder Overlays sowie Softwareabhängigkeiten betreffen. Sofern von der der <Institution> eigene Skripte eingesetzt werden, sind die Skripte daraufhin zu überprüfen, ob sie mit der aktualisierten Version von OpenLDAP fehlerfrei und ohne Sicherheitsimpact zusammenarbeiten. Die Konfiguration und die Zugriffsrechte sind nach einer Aktualisierung sorgfältig zu prüfen.

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

Der slapd-Server ist auf ein Laufzeitverzeichnis einzuschränken. Hierfür sollte das Laufzeitverzeichnis alle Konfigurationsdateien und Datenbanken beinhalten.

#### Protokollierung und Überwachung von OpenLDAP (APP.2.3.A12)

Alle relevanten Aktivitäten in OpenLDAP sind zu protokollieren und zu überwachen. Der laufende Betrieb des slapd-Server sollte mit geeigneten Werkzeugen überwacht werden. Die angefallenen Protokolldaten sind regelmäßig und proaktiv auszuwerten. Die Protokollierung und Überwachung von OpenLDAP muss auch den Server miteinschließen, auf dem OpenLDAP betrieben wird.

#### Datensicherung von OpenLDAP (APP.2.3.A13)

Die Daten des OpenLDAP-Servers samt seiner Verzeichnisdienstobjekte und Konfigurationseinstellungen sind in die seitens der <Institution> etablierten Datensicherungsprozesse zu integrieren. Zudem sollten bei der Datensicherung alle Partitionen des OpenLDAP-Servers berücksichtigt werden. Für die Wiederherstellung der Datenbestände sollte ein geeignetes Werkzeug eingesetzt werden.

## 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 Verzeichnisdienst

#### Erstellung eines Notfallplans für den Ausfall eines Verzeichnisdienstes (APP.2.1.A16 - CIA)

Im Rahmen der Notfallvorsorge wird eine bedarfsgerechte Notfallplanung für Verzeichnisdienste entsprechend dem Dokument ISMS-E3-00033-DE durchgeführt. Für den Ausfall wichtiger Verzeichnisdienst-Systeme liegen Notfallpläne für den Wiederanlauf bzw. die Wiederherstellung vor.

Alle Notfall-Prozeduren für die gesamte Systemkonfiguration der Verzeichnisdienst-Komponenten werden dokumentiert und können im Notfall den verantwortlichen Administratoren zur Verfügung gestellt werden.

#### Einsatz von zwei-Faktor-Authentisierung (APP.2.1.bd.A1 - CIA)

Privilegierte Konten im Bereich des Verzeichnisdienstes sollten mittels Zwei-Faktor-Authentisierung geschützt werden.

### Active-Directory

#### Einsatz von Zwei-Faktor-Authentifizierung (APP.2.2.A13 - CIA)

Privilegierte Konten im Bereich des Active-Directorys sind mittels Zwei-Faktor-Authentisierung zu schützen.

#### Verwendung dedizierter privilegierter Administrationssysteme (APP.2.2.A14 - CIA)

Die Administration des Active Directory ist auf dedizierte Administrationssysteme einzuschränken. Diese dedizierte Administrationssysteme sollten durch die eingeschränkte Aufgabenstellung besonders stark gehärtet sein.

#### Trennung von Administrations- und Produktionsumgebung (APP.2.2.A15 - CIA)

Die Architektur der erweiterten Sicherheitsadministratorumgebung (ESA - Red-Forest) ist als Ansatz zu etablieren, um eine sichere Umgebung für Windows Server Active Directory-Administratoren (AD) zu bieten. Insofern die Etablierung eines Red-Forest nicht durch die <Institution> umgesetzt wird, ist zur Absicherung der privilegierten Zugriffe, der Microsoft Plan zur schnellen Modernisierung zu realisieren ((Rapid Modernization Plan, RAMP).

### OpenLDAP

#### Trennung von Administrations- und Produktionsumgebung (APP.2.3.bd.A1 - CIA)

Besonders kritische Systeme wie die OpenLDAP-Server und Systeme zur Administration der SaaS-Lösung der <Institution> sollten in einen eigenen OpenLDAP-Server und zugehöriger Domain ausgegliedert werden, der einen einseitigen Trust in Richtung des Produktionsdomain besitzt.