Bundesamt
für Sicherheit in der
Informationstechnik

APP.2.2 Active Directory

1. Beschreibung

1.1. Einleitung

Active Directory (AD) ist ein von Microsoft entwickelter Verzeichnisdienst, der 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.

Active Directory wird hauptsächlich in Netzen mit Microsoft-Komponenten eingesetzt. 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. Active Directory stellt zentrale Steuerungs- und Kontrollmöglichkeiten des jeweiligen Netzes bereit.

1.2. Zielsetzung

Das Ziel dieses Bausteins ist es, Active Directory im Regelbetrieb einer Institution abzusichern, die AD zur Verwaltung ihrer Infrastruktur von Windows-Systemen (Client und Server) einsetzt.

1.3. Abgrenzung und Modellierung

Der Baustein APP.2.2 *Active Directory* ist für alle verwendeten Verzeichnisdienste anzuwenden, die auf Microsoft Active Directory basieren.

In diesem Baustein werden die für Active Directory spezifischen Gefährdungen und Anforderungen betrachtet. Allgemeine Sicherheitsempfehlungen zu Verzeichnisdiensten finden sich im Baustein APP.2.1 *Allgemeiner Verzeichnisdienst*. Die dort beschriebenen allgemeinen Anforderungen werden im vorliegenden Baustein konkretisiert und ergänzt. Dieser Baustein wiederholt nicht die Anforderungen zur Absicherung der Betriebssysteme der Server und Clients, die für den Betrieb und die Verwaltung des AD genutzt werden, wie z. B. SYS.1.2.2 *Windows Server 2012* oder SYS.2.2.3 *Clients unter Windows 10*. Dieser Baustein geht auch nicht erneut auf die Anforderungen der zugrundeliegenden Netzinfrastruktur ein.

Active Directory sollte grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement,* CON.3 *Datensicherungskonzept*, OPS.1.1.2 *Archivierung*, OPS.1.1.5 *Protokollierung,* sowie OPS.1.1.2 *Ordnungsgemäße IT-Administration* mit berücksichtigt werden.

2. Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein *APP.2.2 Active Directory* von besonderer Bedeutung.

2.1. Unzureichende Planung der Sicherheitsgrenzen

Eine AD-Instanz erzeugt einen Wald (Forest) als Container auf höchster Ebene für alle Domänen dieser Instanz. Ein Wald kann einen oder mehrere Domänen-Containerobjekte enthalten, die über eine gemeinsame logische Struktur, einen Global Catalog, ein Schema und automatische transitive Vertrauensbeziehungen verfügen. Der Wald stellt also die Sicherheitsgrenze dar, innerhalb derer Informationen standardmäßig im AD weitergegeben werden, nicht ein einzelner Baum. Werden diese Grenzen nicht bewusst und strukturiert geplant, können Informationen ungewollt abfließen und das Sicherheitskonzept der Institution kann versagen. Daher kann es notwendig sein, weitere Forests aufzubauen, wenn für Teile der Infrastruktur unterschiedliche Sicherheitsanforderungen gelten. Dies macht das Einrichten und Verwalten jedoch zusätzlich komplexer.

2.2. Zu viele oder nachlässige Vertrauensbeziehungen

Werden die Vertrauensbeziehungen zwischen Wäldern und Domänen nicht regelmäßig daraufhin evaluiert, ob sie weiterhin benötigt werden und gerechtfertigt sind, können Probleme mit Berechtigungen auftreten und Informationen abfließen. Auch muss regelmäßig überprüft werden, ob sie den korrekten Typ haben, d. h. vor allem, ob eine zweiseitige Vertrauensbeziehung wirklich notwendig ist, und ob die Sicherheitskontrollen rund um diese Vertrauensbeziehungen ausreichend sind. Insbesondere wenn die standardmäßig aktive SID-(Security Identifier)-Filterung deaktiviert wird, können komplexe, schwer zu durchschauende Schwachstellen auftreten. Gleiches gilt, wenn auf Selective Authentication bei Vertrauensbeziehungen zwischen Forests verzichtet wird.

2.3. Fehlende Sicherheitsfunktionen durch ältere Betriebssysteme und Domain Functional Level

Jede neue Generation des Betriebssystems Windows Server bringt zusätzliche Sicherheitsfunktionen und -erweiterungen auch in Bezug auf AD mit. Außerdem werden in der Regel die Standardeinstellungen mit jedem neuen Release immer sicherer gesetzt. Einige davon sind verwendbar, sobald das neue System installiert ist, andere erst dann, wenn das Domänen- bzw. Forest-Functional-Level angehoben wurde. Werden ältere Betriebssysteme als (primärer) Domänencontroller bzw. veraltete Domain Functional Level eingesetzt, können zeitgemäße Sicherheitsfunktionen nicht genutzt werden. Dies erhöht die Gefahr unsicherer Standardeinstellungen. Eine unsicher konfigurierte Domäne gefährdet die darin verarbeiteten Informationen und erleichtert Angriffe durch Dritte.

2.4. Betrieb weiterer Rollen und Dienste auf Domänencontrollern

Werden neben dem AD auf einem Domänencontroller noch weitere Dienste betrieben, erhöht dies die Angriffsfläche dieser zentralen Infrastrukturkomponenten durch mögliche zusätzliche Schwachstellen und Fehlkonfigurationen. Solche Dienste können bewusst oder unbewusst missbraucht werden, um z. B. Informationen unberechtigt zu kopieren oder zu verändern.

2.5. Unzureichende Überwachung und Dokumentation von delegierten Rechten

Wenn die Bildung unternehmensspezifischer Gruppen und die Delegation von Rechten an diese Gruppen nicht systematisch geplant und umgesetzt wird, kann die Delegation nur noch schwer kontrolliert werden.

Sie könnte dann etwa viel mehr Zugriffe einräumen als vorgesehen, was durch Dritte missbraucht werden kann. Eine fehlende regelmäßige Auditierung der Gruppen und ihrer Zugriffsrechte kann das Problem zusätzlich verschärfen. Auch wenn Standardgruppen genutzt und ihre Rechte an eigene Gruppen delegiert werden, etwa bei der Delegation von „Account Operators“ an Helpdesk-Mitarbeiter, werden in der Regel mehr Rechte gewährt als tatsächlich benötigt werden.

2.6. Unsichere Authentisierung

Sogenannte „Legacy“- (also historische) Authentisierungsmechanismen im Bereich AD wie LAN Manager (LM) und NT LAN Manager (NTLM) v1 gelten heute als unsicher und können von Angreifern unter bestimmten Bedingungen leicht umgangen werden. Dadurch kann ein Angreifer Rechte erhalten und missbrauchen, ohne Benutzerpasswörter zu kennen, zu erraten oder anderweitig zu brechen und so die Domäne oder Teile von ihr kompromittieren.

2.7. Zu mächtige oder schwach gesicherte Dienstkonten

Anbieter von Anwendungssoftware setzen manchmal DA-Rechte für Dienstkonten voraus, um ihre Produkte einfacher testen und ausbringen zu können, obwohl für den Betrieb deutlich weniger Rechte notwendig wären. Die zusätzlichen Rechte des Dienstkontos können von Angreifern missbraucht werden, um sich in der Domäne weiterzubewegen. Da die Credentials eines Dienstes, der im Kontext eines Dienstkontos ausgeführt wird, im geschützten Speicher des Local Security Authority Subsystem (LSASS) vorgehalten werden, kann der Angreifer diese dort extrahieren. So kann ein einzelner schwach gesicherter Serviceaccount dazu führen, dass die gesamte Domäne kompromittiert wird.

Insbesondere gilt dies, wenn das Dienstkonto mit einem schwachen Passwort gesichert ist. Denn ein Angreifer kann, wenn er Kerberos-Authentisierung einsetzt, ohne weiteres ein TGS-(Ticket Granting Service)-Ticket anfordern, in dem das Passwort des Dienstaccounts verarbeitet ist. Letzteres kann er dann offline per Brute-Force brechen.

2.8. Nutzung desselben lokalen Administratorpassworts auf mehreren IT-Systemen

Lokale Konten können sich auf einem IT-System anmelden, auch wenn es nicht mit der Domäne verbunden ist. Werden dieselben Credentials auf mehreren IT-Systemen verwendet, kann der Administrator sich auf den anderen IT-Systemen ebenfalls anmelden. Damit steigt die Gefahr, dass ein Angreifer auf einem der IT-Systeme Domänencredentials mit höheren Rechten findet und diese missbrauchen kann, um die Domäne zu kompromittieren.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.2.2 *Active Directory* aufgeführt. Grundsätzlich ist IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein APP.2.2 *Active Directory* vorrangig erfüllt werden:

APP.2.2.A1 Planung des Active Directory [Fachverantwortliche] (B)

Es MUSS ein geeignetes, möglichst hohes Domain Functional Level gewählt werden. Die Begründung SOLLTE geeignet dokumentiert werden. Ein bedarfsgerechtes Active-Directory-Berechtigungskonzept MUSS entworfen werden. Administrative Delegationen MÜSSEN mit restriktiven und bedarfsgerechten Berechtigungen ausgestattet sein. Die geplante Active-Directory-Struktur einschließlich etwaiger Schema-Änderungen SOLLTE nachvollziehbar dokumentiert sein.

APP.2.2.A2 Planung der Active-Directory-Administration [Fachverantwortliche] (B)

In großen Domänen MÜSSEN die administrativen Benutzer bezüglich Diensteverwaltung und Datenverwaltung des Active Directory aufgeteilt werden. Zusätzlich MÜSSEN hier die administrativen Aufgaben im Active Directory nach einem Delegationsmodell überschneidungsfrei verteilt sein.

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

Es MUSS ein Konzept zur Einrichtung von Gruppenrichtlinien vorliegen. Mehrfachüberdeckungen MÜSSEN beim Gruppenrichtlinienkonzept möglichst vermieden werden. In der Dokumentation des Gruppenrichtlinienkonzepts MÜSSEN Ausnahmeregelungen erkannt werden können. Alle Gruppenrichtlinienobjekte MÜSSEN durch restriktive Zugriffsrechte geschützt sein. Für die Parameter in allen Gruppenrichtlinienobjekten MÜSSEN sichere Vorgaben festgelegt sein.

APP.2.2.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.2.2.A5 Härtung des Active Directory (B)

Built-in-Accounts MÜSSEN mit komplexen Passwörtern versehen werden. Sie DÜRFEN NUR als Notfallkonten dienen. Privilegierte Accounts MÜSSEN Mitglieder der Gruppe „Protected Users“ sein. Für Dienstkonten MÜSSEN (Group) Managed Service Accounts verwendet werden.

Für alle Domänen-Controller MÜSSEN restriktive Zugriffsrechte auf Betriebssystemebene vergeben sein. Der Active-Directory-Restore-Modus MUSS durch ein geeignetes Passwort geschützt sein. Arbeiten in diesem Modus SOLLTEN nur erfolgen, wenn das Vier-Augen-Prinzip eingehalten wird.

Ein Abbild des Domänencontrollers SOLLTE regelmäßig erstellt werden. Die Berechtigungen für die Gruppe „Jeder“ MUSS beschränkt werden. Der Domänencontroller MUSS gegen unautorisierte Neustarts geschützt sein.

Die Richtlinien für Domänen und Domänencontroller MÜSSEN sichere Einstellungen für Kennworte, Kontensperrung, Kerberos-Authentisierung, Benutzerrechte und Überwachung umfassen. Es MUSS eine ausreichende Größe für das Sicherheitsprotokoll des Domänen-Controllers eingestellt sein. Bei externen Vertrauensstellungen zu anderen Domänen MÜSSEN die Autorisierungsdaten der Benutzer gefiltert und anonymisiert werden.

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

Alle Vertrauensbeziehungen im AD MÜSSEN regelmäßig evaluiert werden.

Die Gruppe der Domänenadministratoren MUSS leer oder möglichst klein sein. Nicht mehr verwendete Konten MÜSSEN im AD deaktiviert werden. Sie SOLLTEN nach Ablauf einer angemessenen Aufbewahrungsfrist gelöscht werden.

Alle notwendigen Parameter des Active Directory SOLLTEN aktuell und nachvollziehbar festgehalten werden.

APP.2.2.A7 Umsetzung sicherer Verwaltungsmethoden für Active Directory [Fachverantwortliche] (B)

Jeder Account MUSS sich eindeutig einem Mitarbeiter zuordnen lassen.

Die Anzahl der Dienste-Administratoren und der Daten-Administratoren des Active Directory MUSS auf das notwendige Minimum vertrauenswürdiger Personen reduziert sein.

Das Standardkonto „Administrator“ SOLLTE umbenannt werden. Es SOLLTE ein unprivilegiertes Konto mit dem Namen „Administrator“ erstellt werden.

Es MUSS sichergestellt sein, dass die Dienste-Administratorkonten ausschließlich von Mitgliedern der Dienste-Administratorgruppe verwaltet werden. Die Gruppe „Kontenoperatoren“ SOLLTE leer sein.

Administratoren SOLLTEN 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.

Es MUSS sichergestellt sein, dass die Gruppen „Administratoren“ bzw. „Domänenadministratoren“ auch die Besitzer des Domänenstammobjektes der jeweiligen Domäne sind.

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

Der Papierkorb des AD SOLLTE aktiviert werden.

In großen Institutionen SOLLTE mit einer Enterprise-Identity-Management-Lösung sichergestellt werden, dass die Rechte aller Anwender den definierten Vorgaben entsprechen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein APP.2.2 *Active Directory*. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.2.2.A8 Konfiguration des „Sicheren Kanals“ unter Windows (S)

Der „Sichere Kanal“ unter Windows SOLLTE entsprechend den Sicherheitsanforderungen und den lokalen Gegebenheiten konfiguriert sein. Dabei SOLLTEN alle relevanten Gruppenrichtlinienparameter berücksichtigt werden.

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

In der Umgebung des Active Directory SOLLTE konsequent das Authentisierungsprotokoll Kerberos eingesetzt werden. Wenn aus Kompatibilitätsgründen übergangsweise NTLMv2 eingesetzt wird, SOLLTE die Migration auf Kerberos geplant und terminiert werden. Die LM-Authentisierung SOLLTE deaktiviert sein. Der SMB-Datenverkehr SOLLTE signiert sein. Anonyme Zugriffe auf Domänencontroller SOLLTEN unterbunden sein.

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

Integrierte DNS-Zonen bzw. die sichere dynamische Aktualisierung der DNS-Daten SOLLTEN verwendet werden. Der Zugriff auf die Konfigurationsdaten des DNS-Servers SOLLTE nur von administrativen Konten erlaubt sein. Der DNS-Cache auf den DNS-Servern SOLLTE vor unberechtigten Änderungen geschützt sein. Der Zugriff auf den DNS-Dienst der Domänen-Controller SOLLTE auf das notwendige Maß beschränkt sein. Die Netzaktivitäten in Bezug auf DNS-Anfragen SOLLTEN überwacht werden. Der Zugriff auf die DNS-Daten im Active Directory SOLLTE mittels ACLs auf Administratoren beschränkt sein.

Sekundäre DNS-Zonen SOLLTEN vermieden werden. Zumindest SOLLTE die Zonen-Datei vor unbefugtem Zugriff geschützt werden.

Wird IPsec eingesetzt, um die DNS-Kommunikation abzusichern, SOLLTE ein ausreichender Datendurchsatz im Netz gewährleistet sein.

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

Änderungen auf Domänen-Ebene und an der Gesamtstruktur des Active Directory SOLLTEN überwacht, protokolliert und ausgewertet werden.

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

Es SOLLTE eine Datensicherungs- und Wiederherstellungsrichtlinie für Domänen-Controller existieren. Die eingesetzte Sicherungssoftware SOLLTE explizit vom Hersteller für die Datensicherung von Domänen-Controllern freigegeben sein. Für die Domänen-Controller SOLLTE ein separates Datensicherungskonto mit Dienste-Administratorenrechten eingerichtet sein. Die Anzahl der Mitglieder der Gruppe „Sicherungs-Operatoren" SOLLTE auf das notwendige Maß begrenzt sein. Der Zugriff auf das AdminSDHolder-Objekt SOLLTE zum Schutz der Berechtigungen besonders geschützt sein.

Die Daten der Domänen-Controller SOLLTEN in regelmäßigen Abständen gesichert werden. Dabei SOLLTE ein Verfahren eingesetzt werden, das veraltete Objekte weitgehend vermeidet.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein APP.2.2 *Active Directory* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

APP.2.2.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.2.2.A14 Verwendung dedizierter privilegierter Administrationssysteme (H)

Die Administration des Active Directory SOLLTE auf dedizierte Administrationssysteme eingeschränkt werden. Diese SOLLTEN durch die eingeschränkte Aufgabenstellung besonders stark gehärtet sein.

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

Besonders kritische Systeme wie Domaincontroller und Systeme zur Administration der Domain SOLLTEN in einen eigenen Forest ausgegliedert werden, der einen einseitigen Trust in Richtung des Produktions-Forests besitzt.

4. Weiterführende Informationen

4.1. Wissenswertes

Die Website „Active Directory Security" (https://adsecurity.org) enthält viele weiterführende Informationen zu AD-Sicherheit.

Der Hersteller Microsoft bietet weitergehende Informationen zu Active Directory und dessen Sicherheitsaspekten:

- Enhanced Security Administrative Environment: https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access
- Privileged Access Workstations: http://download.microsoft.com/download/9/3/9/9392A4D2-D530-4344-8447-4A7CF1C01AEE/Privileged%20Access%20Workstation_Datasheet.pdf
- Einstiegspunkt Active Directory für Windows Server 2012 (R2): https://technet.microsoft.com/en-us/library/dn283324.aspx
- Einstiegspunkt Active Directory für Windows Server 2008 R2: https://technet.microsoft.com/en-us/library/dd378801.aspx

5. Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein APP.2.2 *Active Directory* von Bedeutung.

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktion von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.42 Social Engineering

G 0.43 Einspielen von Nachrichten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen