Bundesamt
für Sicherheit in der
Informationstechnik

APP.2.2 Active Directory Domain Services

1. Beschreibung

1.1. Einleitung

Active Directory (AD) ist ein Sammelbegriff für verschiedene von Microsoft für Windows Server entwickelte Serverrollen. Die Serverrolle Active Directory Domain Services (AD DS) aggregiert sowohl Funktionalitäten eines Verzeichnis-, als auch Authentifizierungs- und Autorisierungsdienstes sowie einer zentralen Konfigurationsverwaltung für Windows-Infrastrukturen.

Active Directory Domain Services wird hauptsächlich in Netzen eingesetzt, die vorrangig von Microsoft-basierten Betriebssystemen geprägt sind. Ein AD DS speichert und verwaltet Informationen zu Netzressourcen (z. B. Benutzende, Computer und Geräte). Bei Bedarf können diese Informationen, wie in LDAP-Verzeichnisdiensten üblich, auch um anwendungsspezifische Daten erweitert werden. Es dient Anwendenden und Administrierenden dazu, diese Informationen in einer hierarchischen Struktur zu organisieren, bereitzustellen und zu nutzen. Dabei strukturiert AD DS die Objekte in Namensräumen, die als Gesamtstrukturen, Domänen und Organisationseinheiten bezeichnet werden. Eine Gesamtstruktur bildet eine hierarchische Sammlung von Domänen, die jeweils mehrere Organisationseinheiten enthalten können. Die erste und damit in der Hierarchie oben angeordnete Domäne, die in einer Gesamtstruktur angelegt wird, übernimmt systembedingt die Rolle der „Gesamtstruktur Stammdomäne“ (englisch „forest root domain“) und beinhaltet die administrativen Gruppen, die für gesamtstrukturweite Verwaltungsaufgaben wie beispielsweise das Hinzufügen weiterer Domänen oder Schemaänderungen zuständig sind. Alle Domänen innerhalb einer Gesamtstruktur sind implizit durch bidirektionale, transitive Vertrauensstellungen miteinander verknüpft, so dass die Gesamtstruktur eine logische Sicherheitsgrenze darstellt.

Als Authentisierungsprotokoll nutzt AD DS im Standard Kerberos v5 (in einer durch Microsoft erweiterten Implementierung). Zusätzlich steht weiterhin auch noch das Protokoll NTLM (New Technology LAN Manager) zur Verfügung. NTLM kann dabei einfacher von Angreifenden ausgenutzt werden. Windows Server mit der Serverrolle AD DS werden als Domänencontroller bezeichnet. Aus Verfügbarkeitsgründen werden häufig mehrere Domänencontroller verteilt eingesetzt. Das AD DS bietet außerdem die Möglichkeit eines „Read-Only-Betriebs“ eines Domänencontrollers, der für Standorte mit erhöhtem Risiko für die physische Sicherheit vorgesehen ist.

1.2. Zielsetzung

Das Ziel dieses Bausteins ist es, Active Directory Domain Services im Regelbetrieb einer Institution abzusichern, die AD DS zur Verwaltung von Windows-Systemen (Client und Server) sowie zur zentralen Authentifizierung und Autorisierung einsetzt.

1.3. Abgrenzung und Modellierung

Der Baustein APP.2.2 *Active Directory Domain Services* ist für alle verwendeten Verzeichnisdienste anzuwenden, die auf Microsoft Active Directory Domain Services basieren. Er kann zusätzlich für die Modellierung von Active Directory Lightweight Directory Services (AD LDS), die einen reduzierten Funktionsumfang von AD DS bieten, in Teilen verwendet werden.

In diesem Baustein werden die für Active Directory Domain Services 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 DS genutzt werden, wie z. B. SYS.1.2.3 *Windows Server* oder SYS.2.2.3 *Clients unter Windows*. Dieser Baustein geht auch nicht erneut auf die Anforderungen der zugrundeliegenden Netzinfrastruktur ein.

Active Directory Domain Services sollte nicht losgelöst von den Bausteinen 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,* OPS.1.2.5 *Fernwartung*, DER.1 *Detektion von sicherheitsrelevanten Ereignissen,* DER.2 *Security Incident Management,* DER.4 *Notfallmanagement* und APP.3.6 *DNS-Server* modelliert werden. Es ist davon auszugehen, dass sich die Anforderungen dieser Bausteine wechselseitig beeinflussen.

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.2.2 *Active Directory Domain Services* von besonderer Bedeutung.

2.1. Unzureichende Planung der Sicherheitsgrenzen

In AD DS existieren verschiedene Arten von Grenzen. Diese Grenzen definieren die Gesamtstruktur (englisch Forest), die Domäne, die Standorttopologie und die Zuweisung von Rechten. Eine AD-DS-Instanz erzeugt zunächst eine Gesamtstruktur (engl. Forest) als Container auf höchster Ebene für alle Domänen dieser Instanz. Eine Gesamtstruktur kann ein oder mehrere Domänen-Containerobjekte enthalten, die über eine gemeinsame logische Struktur, einen Global Catalog, ein Schema und automatische bidirektionale, transitive Vertrauensbeziehungen verfügen. Dies bedeutet, dass zwischen Domänen innerhalb einer Gesamtstruktur sowohl das Vertrauen zueinander, also auch der Zugriff aufeinander, beidseitig möglich ist. Die Gesamtstruktur stellt also systembedingt die Sicherheitsgrenze dar, innerhalb derer Informationen standardmäßig im AD DS weitergegeben werden. Eine Domäne bildet dabei nur eine Verwaltungsgrenze. Werden Sicherheitsgrenzen nicht entlang der Gesamtstrukturgrenzen realisiert, kann eine Kompromittierung ein höheres Schadensausmaß als erwartet erzeugen, da sie zu einer Kompromittierung aller IT-Systeme in der Gesamtstruktur führen kann. Diese Gefährdung ist eine Besonderheit beim AD DS, da sich die Planung einer Partitionierung im Verzeichnisdienst produktbedingt nicht vollständig umsetzen lässt. Eine vollständige Kompromittierung einer Gesamtstruktur bedeutet, dass Angreifende Kontrolle über alle Objekte, die

zu den enthaltenen Domänen gehören, also unter anderem alle Konten und alle IT-Systeme, haben. Damit haben diese potentiell auch Kontrolle über die zugehörigen IT-Systeme und Dienste.

2.2. Zu viele oder nachlässige Vertrauensbeziehungen

Vertrauensbeziehungen zwischen Domänen und zwischen Gesamtstrukturen ermöglichen es, Konten einer anderen Domäne oder Gesamtstruktur Zugriff auf Ressourcen innerhalb der eigenen Domäne oder Gesamtstruktur zu gewähren. Werden die Vertrauensbeziehungen zwischen Gesamtstrukturen und zwischen Domänen nicht initial und regelmäßig daraufhin evaluiert, ob sie benötigt werden und ob die Sicherheitskontrollen rund um diese Vertrauensbeziehungen ausreichend sind, können Probleme mit Berechtigungen auftreten und Informationen abfließen. Insbesondere wenn die standardmäßig aktive SID-(Security Identifier)-Filterung deaktiviert wird, können komplexe, schwer zu durchschauende Konfigurationsfehler, die zu einer missbräuchlich Nutzung der Vertrauensstellung und zu weitreichenden Zugriffsrechten führen können, auftreten. Gleiches gilt, wenn auf „Selective Authentication“ bei Vertrauensbeziehungen zwischen Gesamtstrukturen verzichtet wird.

2.3. Fehlende Sicherheitsfunktionen durch ältere Betriebssysteme und Domänen- und Gesamtstruktur-Funktionsebenen

Bis einschließlich Windows Server 2016 bringt jede neue Generation des Betriebssystems Windows Server zusätzliche Sicherheitsfunktionen und -erweiterungen in Bezug auf AD DS in Form von Domänen- bzw. Gesamtstruktur-Funktionsebenen mit. Werden ältere Betriebssysteme als Domänencontroller bzw. veraltete Domänen- oder Gesamtstruktur-Funktionsebenen eingesetzt, können zeitgemäße Sicherheitsfunktionen nicht genutzt werden. Dies erhöht die Gefahr unsicherer Standardeinstellungen. Eine unsicher konfigurierte Gesamtstruktur oder Domäne gefährdet die darin verarbeiteten Informationen und erleichtert Angriffe durch Dritte.

2.4. Betrieb weiterer Rollen und Dienste auf Domänencontrollern

Werden neben AD DS auf einem Domänencontroller noch weitere Dienste betrieben, erhöht dies, neben den durch AD DS sowieso schon stark kumulierten Diensten, zusätzlich die Angriffsfläche dieser zentralen Komponente durch mögliche zusätzliche Schwachstellen und Fehlkonfigurationen. Solche Dienste können bewusst oder unbewusst missbraucht werden, um z. B. Informationen unberechtigt zu kopieren, zu verändern oder, im Fall von Schwachstellen oder Fehlkonfigurationen, die zur Kompromittierung des Domänencontrollers führen, die Domäne oder Gesamtstruktur zu übernehmen.

2.5. Unzureichende Überwachung und Dokumentation von delegierten Rechten

Wenn die Bildung unternehmensspezifischer Gruppen und die Delegation von Rechten an diese Gruppen- oder an einzelne Benutzendenobjekte 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 Zugriffsrechte von Gruppen- und einzelnen Benutzendenobjekte kann das Problem zusätzlich verschärfen. Auch wenn Standardgruppen genutzt und ihre Rechte an eigene Gruppen delegiert werden, etwa bei der Delegation von „Account Operators“ / „Konten-Operatoren“ an Helpdesk-Mitarbeitende, werden in der Regel mehr Rechte gewährt als tatsächlich benötigt werden.

2.6. Unsichere Authentisierung

Sogenannte „Legacy"- (also historische) Authentisierungsmechanismen im Bereich AD DS wie LAN Manager (LM) und NT LAN Manager (NTLM) v1 sind unsicher und können bei Angriffen unter bestimmten Bedingungen missbraucht werden. Angreifende können beispielsweise ohne Kenntnis der Klartextpasswörter Rechte erhalten und missbrauchen und so Teile der Domäne, die Domäne selbst oder sogar die Gesamtstruktur kompromittieren.

2.7. Zu mächtige oder schwach gesicherte Konten

Anwendungssoftware setzt manchmal Rechte hochprivilegierter Gruppen (beispielsweise von sogenannten *Domänenadministratoren*) für Dienstkonten voraus, um die Produkte einfacher testen und ausbringen zu können, obwohl für den Betrieb deutlich weniger Rechte notwendig sind. Ein besonderes Risiko besteht, wenn diese Dienstkonten mit schwachen Passwörtern gesichert sind. Auch Konten, die nicht Mitglied einer hoch privilegierten Gruppe sind, können administrative Berechtigungen beispielsweise auf einer großen Anzahl von Servern und Clients zugewiesen sein. Damit besitzen sie ähnlich umfangreiche Rechte wie Mitglieder hoch privilegierten Gruppen im AD DS. Die weitreichenden Rechte dieser Konten können von Angreifenden missbraucht werden, um sich in der Domäne weiterzubewegen.

2.8. Nutzung desselben lokalen Administrierendenpassworts auf mehreren IT-Systemen

Auch bei Domänenzugehörigkeit eines IT-Systems ist eine Anmeldung mit lokalen Konten an diesem IT-System weiterhin möglich. Werden dieselben lokalen Anmeldeinformationen auf mehreren IT-Systemen verwendet, kann eine Anmeldung mit diesen unter anderem mit dem lokalen Built-In-Konto *Administrator* auf mehreren IT-Systemen erfolgen. Dies erleichtert Angreifenden die laterale Bewegung und damit die Ausbreitung in der Infrastruktur. Damit steigt das Risiko, dass Angreifende auf einem der IT-Systeme Anmeldeinformationen eines Domänenkontos mit höheren Rechten finden und diese missbrauchen können, um die Domäne und potentiell die Gesamtstruktur zu kompromittieren.

2.9. Unsichere Speicherung von Passwörtern

Die Speicherung der Passwörter erfolgt in der zentralen AD-DS-Datenbank (*ntds.dit*) auf dem Domänencontroller produktbedingt unter anderem mittels MD4-Hashfunktion ohne Salt. Diese Hashfunktion erfüllt nicht die Anforderungen der Technischen Richtlinie TR-02102-1 „Kryptografische Verfahren: Empfehlungen und Schlüssellängen" des BSI. Unautorisierte lesende Zugriffe auf die gespeicherten Passwörter sind daher besonders kritisch. Aufgrund der weiten Verbreitung von AD DS existieren viele Werkzeuge, um die Hashes der Passwörter zu extrahieren. Die AD-DS-Datenbank kann beispielsweise unter Verwendung weiterer auf dem Domänencontroller hinterlegter Schlüssel offline entschlüsselt werden und den Zugriff auf die Hashes ermöglichen. Zudem ist durch die schwache Hashfunktion ein Ermitteln der Klartextpasswörter möglich.

2.10. Unzureichende Absicherung von Domänencontrollern

Jeder (Read-Write)-Domänencontroller einer Domäne hält ein vollständiges Replikat der zentralen AD-DS-Datenbank (*ntds.dit*) vor, in der die Passwörter unsicher gespeichert sind. Neben dem unzureichenden Schutz vor Zugriff durch Dritte auf die Domänencontroller im Betrieb kann auch ein ungeeignetes Backupverfahren zum Abgreifen der zentralen AD-DS-Datenbank und in Folge zum Abfluss von Informationen und der Kompromittierung der Domäne und potentiell der Gesamtstruktur führen. Auch der Betrieb von virtualisierten Domänencontrollern gemeinsam mit weniger schützenswerten virtuellen Maschinen auf einem physischen Virtualisierungshost kann zu

einer Kompromittierung des AD DS führen. Dies gilt auch, wenn die administrativen Konten des Virtualisierungshosts, die durch ihre administrativen Tätigkeiten Vollzugriff auf AD DS besitzen, nicht angemessen geschützt werden.

2.11. Hinterlassen von hochprivilegierten Anmeldeinformationen auf Domänenmitgliedsservern und -clients

Erfolgt eine Anmeldung oder Dienstnutzung mit hochprivilegierten Konten auf einem Server oder Client der Domäne, so werden die zugehörigen Anmeldeinformationen auf diesem zwischengespeichert (z. B. im Speicher des Local Security Authority Subsystem / LSASS). Im Fall einer Kompromittierung können Angreifende diese dort extrahieren. Dadurch kann die Kompromittierung eines einzelnen Servers oder Clients der Domäne dazu führen, dass die gesamte Domäne und potentiell die Gesamtstruktur kompromittiert wird.

2.12. Hinzufügen nicht vertrauenswürdiger IT-Systemen zur Windows-Domäne

In den voreingestellten Konfigurationen dürfen alle im AD DS authentifizierten Benutzenden bis zu zehn IT-Systeme zu der Domäne hinzufügen, auch, wenn sie keine administrativen Berechtigungen im AD DS besitzen. Dadurch können sie IT-Systeme in die Domäne hinzufügen, auf denen sie hohe Privilegien besitzen. Diese Privilegien können als Ausgangspunkt für weitere Angriffe verwendet werden. Da das Hinzufügen von IT-Systemen zu einer Domäne eine Verwaltungsaufgabe ist, die typischerweise in einen IT-Prozess eingebettet ist, können hier schwer vorhersehbare Seiteneffekt entstehen, wenn IT-Systeme unkontrolliert der Domäne beitreten, ohne diesen Prozess korrekt zu durchlaufen.

2.13. Vermaschung von administrativen Privilegien durch Integration von weiteren Anwendungen

Werden Anwendungen mit einer Integration in AD DS eingesetzt (beispielsweise Microsoft Exchange), können den durch diese Anwendungen angelegten AD-DS-Konten administrative Berechtigungen in AD DS zugewiesen sein. Dadurch können Sicherheitslücken in diesen Anwendungen dazu führen, dass Angreifende weitreichende Administrationsrechte bei IT-Systemen innerhalb der Gesamtstruktur erhalten. Ein Beispiel hierfür ist die Sicherheitslücke CVE-2019-0686 (PrivExchange) in Microsoft Exchange.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.2.2 *Active Directory Domain Services* 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

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.2.2.A1 Planung von Active Directory Domain Services (B) [Fachverantwortliche]

Es MUSS eine Funktionsebene für die Domäne(n) und die Gesamtstruktur von mindestens Windows Server 2016 gewählt werden. Ein bedarfsgerechtes Berechtigungskonzept für die Domäne(n) und die Gesamtstruktur MUSS entworfen werden. Dabei MUSS berücksichtigt werden, dass zwischen den einzelnen Domänen einer Gesamtstruktur produktbedingt keine Sicherheitsgrenzen bestehen und daher keine sichere Begrenzung der administrativen Bereiche innerhalb einer Gesamtstruktur möglich ist. Administrative Delegationen MÜSSEN mit restriktiven und bedarfsgerechten Berechtigungen ausgestattet sein. Die geplante Struktur einschließlich etwaiger Schema-Änderungen MUSS nachvollziehbar dokumentiert sein.

APP.2.2.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

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 Absicherung des Domänencontrollers (B)

Aufgrund der zentralen Rolle und der Schadensauswirkung bei Kompromittierung des AD DS für die Infrastruktur SOLLTE eine Risikobetrachtung durchgeführt werden. Der Notfallzugriff auf den Domänencontroller mit dem lokalen Restore-Konto DSRM (Directory Services Restore Mode) MUSS im Rahmen des Notfallmanagements geplant werden.

Auf dem Domänencontroller MUSS eine ausreichende Größe für das Sicherheitsprotokoll auf Grundlage des in DER.1 *Detektion von sicherheitsrelevanten Ereignissen* festgelegten Zeitraums eingestellt sein. Aufgrund der zentralen Bedeutung des Domänencontrollers SOLLTEN auf diesem Server keine weiteren Dienste betrieben werden, sofern diese nicht zwingend auf dem *gleichen* Server zum Betrieb des AD DS erforderlich sind.

APP.2.2.A6 Sichere Konfiguration von Vertrauensbeziehungen (B)

Alle Vertrauensbeziehungen zwischen Domänen und zwischen Gesamtstrukturen MÜSSEN regelmäßig auf ihre Notwendigkeit und Absicherungsmaßnahmen evaluiert werden. Dabei MUSS geprüft werden, ob eine bidirektionale Vertrauensbeziehung notwendig ist. Wenn eine Domäne keine bidirektionale Vertrauensbeziehung zu anderen Domänen in der Gesamtstruktur benötigt, SOLLTE diese Domäne in eine eigene Gesamtstruktur ausgelagert werden, da innerhalb einer Gesamtstruktur produktbedingt keine Anpassung der Vertrauensbeziehungen möglich ist.

Die SID-(Security Identifier)-Filterung bei Vertrauensstellungen zwischen Gesamtstrukturen DARF NICHT deaktiviert werden. Die voreingestellten SIDs DÜRFEN NICHT entfernt werden. Hat der in der Gesamtstruktur abgebildete Informationsverbund, dem vertraut wird, kein ausreichendes

Sicherheitsniveau, MUSS für die Vertrauensbeziehung zu dieser Gesamtstruktur „Selective Authentication“ verwendet werden.

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

Es MUSS sichergestellt sein, dass die Konten von Dienste-Administrierenden ausschließlich von Mitgliedern der Gruppe der Dienste-Administrierenden verwaltet werden. Bevor Konten vordefinierten AD-DS-Gruppen hinzugefügt werden, SOLLTE geprüft werden, ob alle der Gruppe zugehörigen Rechte für die mit den Konten verbundenen Tätigkeiten erforderlich sind. Den Gruppen „Schema-Admins“ / „Schema-Administratoren“ sowie der Gruppe „Enterprise Admins“ / „Organisations-Administratoren“ und „Domain Admins“ / „Domänen-Administratoren“ SOLLTEN neben dem AD-DS-Built-In-Konto für Administrierende weitere administrative Konten nur temporär für den Zeitraum zugewiesen werden, in dem sie diese Berechtigungen benötigen.

APP.2.2.A16 Härtung der AD-DS-Konten (B)

Built-in-AD-DS-Konten MÜSSEN mit komplexen Passwörtern versehen werden. Sie DÜRFEN NUR als Notfallkonten dienen. Das Built-in „Guest“- / „Gast“-Konto MUSS deaktiviert werden. Die Berechtigungen für die Gruppe „Everyone“ / „Jeder“ MUSS beschränkt werden. Privilegierte Konten MÜSSEN Mitglied der Gruppe „Protected Users“ / „Geschütze Benutzer“ sein. Für Dienstkonten MÜSSEN (Group) Managed Service Accounts verwendet werden. Vor dem Löschen nicht mehr verwendeter Konten MUSS geprüft werden, nach welcher Aufbewahrungsfrist diese gelöscht werden können. Dabei MÜSSEN die Auswirkungen auf die Detektion und gesetzliche Aufbewahrungs- und Löschfristen berücksichtigt werden. Der Zugriff auf das AdminSDHolder-Objekt SOLLTE zum Schutz der Berechtigungen besonders geschützt sein.

APP.2.2.A17 Anmelderestriktionen für hochprivilegierte Konten der Gesamtstruktur auf Clients und Servern (B)

Die Anmeldung von hochpriviligierten Domänen- und Gesamtstruktur-Konten und Gruppen MUSS technisch auf die minimal notwendigen IT-Systeme einschränkt werden. Insbesondere die Anmeldung von Mitgliedern der Gruppen „Schema Admins“ / „Schema-Administratoren“, „Enterprise Admins“ / „Enterprise-Administratoren“ und „Domain Admins“ / „Domänen-Administratoren“ SOLLTE technisch auf den Domänencontroller beschränkt werden, eine Anmeldung an anderen IT-Systemen ist für diese Gruppen also zu unterbinden.

APP.2.2.A18 Einschränken des Hinzufügens neuer Computer-Objekte zur Domäne (B)

Die Berechtigung, in der Domäne neue Computer-Objekte hinzuzufügen, MUSS auf die notwendigen administrativen Konten beschränkt 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.2.2.A8 Absicherung des „Sicheren Kanals“ (S)

Der „Sichere Kanal“ SOLLTE so konfiguriert sein, dass alle übertragenen Daten immer verschlüsselt und signiert werden.

APP.2.2.A9 Schutz der Authentisierung beim Einsatz von AD DS (S)

In der Gesamtstruktur SOLLTE konsequent das Authentisierungsprotokoll Kerberos eingesetzt werden. Dabei SOLLTE für die Absicherung AES128_HMAC_SHA1 oder AES256_HMAC_SHA1 verwendet werden. Wenn aus Kompatibilitätsgründen übergangsweise NTLMv2 eingesetzt wird, SOLLTE die Migration auf Kerberos geplant und terminiert werden. Die LM-Authentisierung und NTLMv1

MÜSSEN deaktiviert sein. Der SMB-Datenverkehr MUSS signiert sein. SMBv1 MUSS deaktiviert sein. Anonyme Zugriffe auf Domänencontroller SOLLTEN unterbunden sein. LDAP-Sitzungen SOLLTEN nur signiert und mit konfiguriertem Channel Binding Token (CBT) erfolgen.

APP.2.2.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.2.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.2.2.A12 Datensicherung für Domänencontroller (S)

Aufgrund der besonderen Gefährdung der unsicher gespeicherten Passwörter SOLLTE der Zugriff auf die Backups des Domänencontrollers vergleichbar dem Zugriff auf den Domänencontroller selbst abgesichert sein.

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.2.2.A13 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.2.2.A14 ENTFALLEN (H)

Diese Anforderung ist entfallen.

APP.2.2.A15 Auslagerung der Administration in eine eigene Gesamtstruktur (H)

Besonders kritische IT-Systeme und Konten zur Administration der Domänen oder der Gesamtstruktur SOLLTEN in eine eigene Gesamtstruktur (häufig als „Red Forest“ bezeichnet) ausgegliedert werden, zu der von der zu verwaltenden Gesamtstruktur eine einseitige Vertrauensstellung besteht. Dies SOLLTE im Rahmen des Notfallmanagements bei der Erstellung des Notfallhandbuchs besonders berücksichtigt werden.

APP.2.2.A19 Betrieb von virtualisierten Domänencontrollern (H)

Virtualisierte Domänencontroller SOLLTEN nicht gemeinsam mit weiteren virtuell betriebenen IT-Systemen auf dem gleichen physischen Host betrieben werden. Bei der Absicherung der administrativen Konten für den Zugriff über die Virtualisierungsschicht SOLLTE berücksichtigt werden, dass diese Vollzugriffe auf den Domänencontroller haben und dieser dann vergleichbar mit dem der Gruppe „Domain Admins“ / „Domänen-Administratoren“ ist. Der Virtualisierungshost, die IT-Systeme, die am Virtualisierungsmanagement beteiligt sind sowie die Administrationskonten für die Virtualisierungsschicht SOLLTEN NICHT zur Gesamtstruktur gehören, zu der der virtualisierte Domänencontroller gehört.

APP.2.2.A20 Trennung von Organisationseinheiten (H)

Organisationseinheiten, die aus IT-Sicherheitsgründen oder sonstigen Gründen Unabhängigkeit voneinander gewährleisten müssen, SOLLTEN sich nicht in der gleichen Gesamtstruktur befinden.

APP.2.2.A21 Konfiguration eines Schichtenmodells (H)

Die Berechtigungsstruktur innerhalb der Gesamtstruktur SOLLTE in Schichten, die sich am Schutzbedarf der Konten, IT-Systeme und Anwendungen orientieren, entworfen werden. Bei dieser

Strukturierung SOLLTEN alle Konten, IT-Systeme und Anwendungen innerhalb einer Gesamtstruktur eindeutig einer Schicht zugeordnet werden können. Konten einer höheren Schicht SOLLTEN sich nicht auf Ressourcen einer niedrigeren Schicht anmelden können. Konten einer niedrigeren Schicht SOLLTEN keine Kontrollmöglichkeit über Konten und Ressourcen höherer Schichten besitzen.

APP.2.2.A22 Zeitlich befristete Berechtigungen für die Administration (H)

Konten, die für die Administration verwendet werden, SOLLTEN nur bei Bedarf auf das benötigte Zeitfenster befristetet die für die administrative Aufgabe notwendigen Berechtigungen zugewiesen werden.

APP.2.2.A23 Regelmäßige Analyse von Berechtigungen und resultierenden Angriffspfaden (H)

Aufgrund der Komplexität von Berechtigungen, die nicht immer unmittelbar ersichtlich sind, SOLLTE eine regelmäßige Analyse der Berechtigungsstrukturen im AD DS vorgenommen werden. Insbesondere Berechtigungen, die durch die Integration von Anwendungen in AD DS entstehen (beispielsweise Microsoft Exchange) SOLLTEN kritisch auf ihre Notwendigkeit hin geprüft und auf die minimal notwendigen Berechtigungen reduziert werden. Aktualisierungen können ebenfalls auch Berechtigungsstrukturen im AD DS ändern, daher SOLLTE die Analyse auch nach entsprechenden Aktualisierungen durchgeführt werden. Mögliche Angriffspfade über die Berechtigungen der AD-DS-Konten, die beispielsweise bei Kompromittierung von Konten zur Kompromittierung der Domäne bzw. der vollständigen Gesamtstruktur führen, SOLLTEN möglichst gering sein. Die Aktivitäten der verbleibenden, als kritisch identifizierten Konten SOLLTEN besonders überwacht werden.

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:

- Einstiegspunkt Active Directory Domain Services https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-domain-services
- Dokumentation zum “Implementieren von Verwaltungsmodellen der geringsten Rechte” https://docs.microsoft.com/de-de/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models
- Übersicht zu Domänen und Gesamtstrukturen https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2003/cc759073(v=ws.10)
- Sicherheitsaspekte bei Vertrauensstellungen https://docs.microsoft.com/de-de/previous-versions/windows/it-pro/windows-server-2003/cc755321(v=ws.10)
- Dokumentation zum Schichtenmodell https://web.archive.org/web/20171205072455/https:/docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material