Bundesamt
für Sicherheit in der
Informationstechnik

APP.3.4 Samba

1. Beschreibung

1.1. Einleitung

Samba ist ein frei verfügbarer und vollwertiger Active Directory Domain Controller (ADDC), der Authentisierungs-, Datei- und Druckdienste bereitstellen kann und dadurch die Interoperabilität zwischen der Windows- und der Unix-Welt ermöglicht. Samba führt viele unterschiedliche Protokolle und Techniken zusammen. Dazu gehört beispielsweise das Server-Message-Block (SMB)-Protokoll. Als Samba-Server werden Server bezeichnet, auf denen Samba betrieben wird. In der Regel sind das Unix-Server.

Wurde der Einsatz von Samba korrekt konzipiert und geeignet konfiguriert, interagiert Samba mit einem Windows-Client oder -Server, als ob es selbst ein Windows-System wäre.

1.2. Zielsetzung

Ziel des Bausteins ist es darzustellen, wie Samba in Institutionen sicher eingesetzt werden kann und wie sich die durch Samba bereitgestellten Informationen schützen lassen.

1.3. Abgrenzung und Modellierung

Der Baustein APP.3.4.*Samba* ist auf jeden Samba-Server des betrachteten Informationsverbunds anzuwenden.

Dieser Baustein betrachtet Samba als Authentisierungs-, Datei- und Druckdienst. Da Samba in der Regel auf Unix-Servern eingesetzt wird und dort aus der Windows-Server-Welt bekannte Dienste bereitstellt, sind die Sicherheitsaspekte der Bausteine SYS.1.1 *Allgemeiner Server* und SYS.1.3 *Server unter Linux und Unix* zu berücksichtigen.

Ein wichtiger Schwerpunkt bei der Absicherung eines Samba-Servers ist es, Zugriffsrechte auf Dateien nur restriktiv zu vergeben. Vertiefende Informationen zum Identitäts- und Berechtigungsmanagement sind nicht in diesem Baustein, sondern in ORP.4 *Identitäts- und Berechtigungsmanagement* zu finden.

Generelle Sicherheitsanforderungen für Drucker, Fileserver oder Verzeichnisdienste sind nicht Bestandteil dieses Bausteins. Diese werden in den Bausteinen SYS.4.1 *Drucker, Kopierer und Multifunktionsgeräte*, APP.3.3 *Fileserver* und APP.2.1 *Allgemeiner Verzeichnisdienst* sowie APP.2.3 *OpenLDAP* beschrieben.

2. Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein APP.3.4 *Samba* von besonderer Bedeutung:

2.1. Abhören ungeschützter Kommunikationsverbindungen von Samba

Wenn Angreifer ungeschützte Kommunikationsverbindungen von Samba abhören, können vertrauliche Informationen abgefangen und missbraucht werden. Beim Dateitransfer zwischen Unix-Servern, Windows-Servern und Clients werden oftmals Protokolle ohne umfangreiche Sicherheitseigenschaften eingesetzt, sodass sowohl Authentisierungs- als auch Nutzerdaten für Dritte zugänglich sind und von Unberechtigten missbraucht werden könnten. Das kann dazu führen, dass schützenswerte Informationen der Institution in die falschen Hände gelangen.

2.2. Unsichere Standardeinstellungen auf Samba-Servern

Um einige Fähigkeiten des Samba-Servers zu zeigen und um den Administratoren einen schnellen Einstieg zu ermöglichen, wird während der Installation des Samba-Servers die Konfigurationsdatei smb.conf mit Standardeinstellungen erzeugt. Mit den in dieser Datei voreingestellten Optionen kann der Samba-Server im Anschluss gestartet werden. Wird diese Datei unbedacht ohne weitere Anpassungen benutzt, kann das zu erheblichen Sicherheitslücken führen. Werden die beispielhaft vorgenommenen Dateifreigaben nicht auskommentiert, können in diesen unerwünschten Freigaben sensible Informationen eingesehen werden.

2.3. Unberechtigte Nutzung oder Administration von Samba

Unbefugte können durch die Nutzung von Anwendungen oder IT-Systemen an vertrauliche Informationen gelangen, diese manipulieren oder Störungen verursachen. So ist es möglich, dass sie Samba unberechtigt administrieren können. Besonders kritisch ist es, wenn veraltete und nicht mehr aktualisierte Konfigurationswerkzeuge eingesetzt werden, wie z. B. das Samba Web Administration Tool (SWAT).

2.4. Fehlerhafte Administration von Samba

Sind die Administratoren mit den umfangreichen Komponenten, Funktionen, Optionen und Konfigurationseinstellungen von Samba zu wenig vertraut, kann dies zu weitreichenden Komplikationen führen. So können Fehlkonfigurationen des DNS oder des Benutzer- und Rechtemanagements dazu führen, dass Unbefugte auf Ressourcen zugreifen können. Des Weiteren kann dies zu Betriebsunterbrechungen führen oder es können schützenswerte Informationen offengelegt werden.

2.5. Datenverlust bei Samba

Ein Datenverlust wirkt sich erheblich auf den IT-Einsatz aus. Wenn institutionsrelevante Informationen zerstört oder verfälscht werden, können dadurch Geschäftsprozesse und Fachaufgaben verzögert oder gar nicht mehr ausgeführt werden. Bei Samba ist beispielsweise zu beachten, dass sich die Eigenschaften der Dateisysteme unter Windows und Unix erheblich voneinander unterscheiden. Deswegen ist nicht immer sichergestellt, dass die Zugriffsrechte unter Windows aufrechterhalten bleiben, unter Umständen können so wichtige Dateieigenschaften verloren gehen. Auch können dadurch Informationen zu sogenannten Alternate Data Streams (ADS) und DOS-Attributen verloren gehen.

2.6. Integritätsverlust schützenswerter Informationen bei Samba

Samba selbst legt wichtige Betriebsdaten in Datenbanken im Trivial-Database-(TDB)-Format ab. Sollten diese Datenbanken vom Betriebssystem nicht ausreichend leistungsfähig und konsistent behandelt werden, können sie Probleme verursachen, wenn Samba-Dienste genutzt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.4 *Samba* aufgeführt. Grundsätzlich ist der 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 Umsetzung 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	

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein APP.3.4 *Samba* vorrangig erfüllt werden:

APP.3.4.A1 Planung des Einsatzes eines Samba-Servers (B)

Der IT-Betrieb MUSS die Einführung eines Samba-Servers sorgfältig planen und regeln. Sie MUSS abhängig vom Einsatzszenario definieren, welche Aufgaben der Samba-Server zukünftig erfüllen soll und in welcher Betriebsart er betrieben wird. Außerdem MUSS festgelegt werden, welche Komponenten von Samba und welche weiteren Komponenten dafür erforderlich sind.

Soll die Cluster-Lösung CTDB (Cluster Trivia Data Base) eingesetzt werden, MUSS der IT-Betrieb diese Lösung sorgfältig konzeptionieren. Falls Samba die Active-Directory-(AD)-Dienste auch für Linux- und Unix-Systeme bereitstellen soll, MÜSSEN diese Diente ebenfalls sorgfältig geplant und getestet werden. Des Weiteren MUSS das Authentisierungsverfahren für das AD sorgfältig konzipiert und implementiert werden. Die Einführung und die Reihenfolge, in der die Stackable-Virtual-File-System-(VFS)-Module ausgeführt werden, MUSS sorgfältig konzipiert werden. Die Umsetzung SOLLTE dokumentiert werden.

Soll IPv6 unter Samba eingesetzt werden, MUSS auch dies sorgfältig geplant werden Zudem MUSS in einer betriebsnahen Testumgebung überprüft werden, ob die Integration fehlerfrei funktioniert.

APP.3.4.A2 Sichere Grundkonfiguration eines Samba-Servers (B)

Der IT-Betrieb MUSS den Samba-Server sicher konfigurieren. Hierfür MÜSSEN unter anderem die Einstellungen für die Zugriffskontrollen angepasst werden. Das gleiche SOLLTE auch für Einstellungen gelten, welche die Leistungsfähigkeit des Servers beeinflussen.

Samba MUSS vom IT-Betrieb so konfiguriert werden, dass Verbindungen nur von sicheren Hosts und Netzen entgegengenommen werden. Änderungen an der Konfiguration SOLLTEN sorgfältig dokumentiert werden, sodass zu jeder Zeit nachvollzogen werden kann, wer aus welchem Grund was geändert hat. Dabei MUSS nach jeder Änderung überprüft werden, ob die Syntax der Konfigurationsdatei noch korrekt ist.

Zusätzliche Softwaremodule wie SWAT DÜRFEN NICHT installiert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein APP.3.4 *Samba*. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.3.4.A3 Sichere Konfiguration eines Samba-Servers (S)

Datenbanken im Trivial-Database-(TDB)-Format SOLLTEN NICHT auf einer Partition gespeichert werden, die ReiserFS als Dateisystem benutzt. Wird eine netlogon-Freigabe konfiguriert, SOLLTEN unberechtigte Benutzer KEINE Dateien in dieser Freigabe modifizieren können.

Das Betriebssystem eines Samba-Servers SOLLTE Access Control Lists (ACLs) in Verbindung mit dem eingesetzten Dateisystem unterstützen. Zusätzlich SOLLTE sichergestellt werden, dass das Dateisystem mit den passenden Parametern eingebunden wird.

Die Voreinstellungen von SMB Message Signing SOLLTEN beibehalten werden, sofern sie nicht im Widerspruch zu den existierenden Sicherheitsrichtlinien im Informationsverbund stehen.

APP.3.4.A4 Vermeidung der NTFS-Eigenschaften auf einem Samba-Server (S)

Wird eine Version von Samba eingesetzt, die im New Technology File System (NTFS) keine ADS abbilden kann und sollen Dateisystemobjekte über Systemgrenzen hinweg kopiert oder verschoben werden, SOLLTEN Dateisystemobjekte KEINE ADS mit wichtigen Informationen enthalten.

APP.3.4.A5 Sichere Konfiguration der Zugriffssteuerung bei einem Samba-Server (S)

Die von Samba standardmäßig verwendeten Parameter, mit denen DOS-Attribute auf das Unix-Dateisystem abgebildet werden, SOLLTEN NICHT verwendet werden. Stattdessen SOLLTE Samba so konfiguriert werden, dass es DOS-Attribute und die Statusindikatoren zur Vererbung (Flag) in Extended Attributes speichert. Die Freigaben SOLLTEN ausschließlich über die Samba-Registry verwaltet werden.

Ferner SOLLTEN die effektiven Zugriffsberechtigungen auf die Freigaben des Samba-Servers regelmäßig überprüft werden.

APP.3.4.A6 Sichere Konfiguration von Winbind unter Samba (S)

Für jeden Windows-Domänenbenutzer SOLLTE im Betriebssystem des Servers ein Benutzerkonto mit allen notwendigen Gruppenmitgliedschaften vorhanden sein. Falls das nicht möglich ist, SOLLTE Winbind eingesetzt werden. Dabei SOLLTE Winbind Domänen-Benutzernamen in eindeutige Unix-Benutzernamen umsetzen. Beim Einsatz von Winbind SOLLTE sichergestellt werden, dass Kollisionen zwischen lokalen Unix-Benutzern und Domänen-Benutzern verhindert werden.

Des Weiteren SOLLTEN die PAM (Pluggable Authentication Modules) eingebunden werden.

APP.3.4.A7 Sichere Konfiguration von DNS unter Samba (S)

Wenn Samba als DNS-Server eingesetzt wird, SOLLTE die Einführung sorgfältig geplant und die Umsetzung vorab getestet werden. Da Samba verschiedene AD-Integrationsmodi unterstützt, SOLLTE der IT-Betrieb die DNS-Einstellungen entsprechend dem Verwendungsszenario von Samba vornehmen.

APP.3.4.A8 Sichere Konfiguration von LDAP unter Samba (S)

Werden die Benutzer unter Samba mit LDAP verwaltet, SOLLTE die Konfiguration sorgfältig vom IT-Betrieb geplant und dokumentiert werden. Die Zugriffsberechtigungen auf das LDAP SOLLTEN mittels ACLs geregelt werden.

APP.3.4.A9 Sichere Konfiguration von Kerberos unter Samba (S)

Zur Authentisierung SOLLTE das von Samba implementierte Heimdal Kerberos Key Distribution Center (KDC) verwendet werden. Es SOLLTE darauf geachtet werden, dass die von Samba vorgegebene Kerberos-Konfigurationsdatei verwendet wird. Es SOLLTEN nur sichere Verschlüsselungsverfahren für Kerberos-Tickets benutzt werden.

Wird mit Kerberos authentisiert, SOLLTE der zentrale Zeitserver lokal auf dem Samba-Server installiert werden. Der NTP-Dienst SOLLTE so konfiguriert werden, dass nur autorisierte Clients die Zeit abfragen können.

APP.3.4.A10 Sicherer Einsatz externer Programme auf einem Samba-Server (S)

Vom IT-Betrieb SOLLTE sichergestellt werden, dass Samba nur auf schadhafte Funktionen überprüfte und vertrauenswürdige externe Programme aufruft.

APP.3.4.A11 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.4.A12 Schulung der Administratoren eines Samba-Servers (S)

Administratoren SOLLTEN zu den genutzten spezifischen Bereichen von Samba wie z. B. Benutzerauthentisierung, Windows- und Unix-Rechtemodelle, aber auch zu NTFS ACLs und NTFS ADS geschult werden.

APP.3.4.A13 Regelmäßige Sicherung wichtiger Systemkomponenten eines Samba-Servers (S)

Es SOLLTEN alle Systemkomponenten in das institutionsweite Datensicherungskonzept eingebunden werden, die erforderlich sind, um einen Samba-Server wiederherzustellen. Auch die Kontoinformationen aus allen eingesetzten Backends SOLLTEN berücksichtigt werden. Ebenso SOLLTEN alle TDB-Dateien gesichert werden. Des Weiteren SOLLTE die Samba-Registry mit gesichert werden, falls sie für Freigaben eingesetzt wurde.

APP.3.4.A14 ENTFALLEN (S)

Diese Anforderung ist entfallen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein APP.3.4 *Samba* 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.3.4.A15 Verschlüsselung der Datenpakete unter Samba (H)

Um die Sicherheit der Datenpakete auf dem Transportweg zu gewährleisten, SOLLTEN die Datenpakete mit den ab SMB Version 3 integrierten Verschlüsselungsverfahren verschlüsselt werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein APP.3.4 *Samba* sind keine weiterführenden Informationen vorhanden.

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.3.4 *Samba* von Bedeutung.

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

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 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen