



APP.3.3 Fileserver

1. Beschreibung

1.1. Einleitung

Ein Fileserver (oder auch Dateiserver) ist ein Server in einem Netz, der Dateien von (internen) Festplatten oder Netzfestplatten für alle zugriffsberechtigten Personen sowie Clients zentral bereitstellt. Die Datenbestände können von den Zugriffsberechtigten genutzt werden, ohne sie z. B. auf Wechseldatenträgern zu transportieren oder per E-Mail zu verteilen. Dadurch, dass die Daten zentral vorgehalten werden, können sie strukturiert und in verschiedenen Verzeichnissen und Dateien bereitgestellt werden. Bei Fileservern können Zugriffsrechte auf die Dateien zentral vergeben werden. Auch die Datensicherung kann vereinfacht werden, wenn sich alle Informationen an einer zentralen Stelle befinden.

Ein Fileserver verwaltet meistens Massenspeicher, die mit ihm über Schnittstellen wie SCSI (Small Computer System Interface) oder SAS (Serial Attached SCSI) verbunden sind. Die Speicher befinden sich entweder direkt im Gehäuse des Fileservers oder sind extern angeschlossen. Letzteres wird oft als Directly Attached Storage (DAS) bezeichnet. Ein Fileserver kann auf herkömmlicher Server-Hardware oder einer dedizierten Appliance betrieben werden. Oft können bei großen Datenmengen auch zentrale Storage-Area-Network (SAN)-Speicher über Host-Bus-Adapter (HBA) im Server und an SAN-Switches angebunden werden.

1.2. Zielsetzung

In diesem Baustein werden wesentliche, für einen Fileserver spezifischen Gefährdungen und die sich daraus ergebenden Anforderungen für einen sicheren Einsatz beschrieben.

1.3. Abgrenzung und Modellierung

Der Baustein APP.3.3.*Fileserver* ist auf jeden Fileserver im Informationsverbund einmal anzuwenden.

Der vorliegende Baustein enthält grundsätzliche Anforderungen, die beim Einsatz von Fileservern zu beachten und zu erfüllen sind. Allgemeine und betriebssystemspezifische Aspekte eines Servers sind nicht Gegenstand des vorliegenden Bausteins, sondern werden im Baustein SYS.1.1 *Allgemeiner Server* bzw. in den entsprechenden betriebssystemspezifischen Bausteinen der Schicht SYS *IT-Systeme* behandelt, z. B. in SYS.1.3 *Server unter Linux und Unix* oder SYS.1.2.3 *Windows Server*. Es werden keine Anforderungen an netzbasierte Speichersysteme bzw. Speichernetze beschrieben. Diese sind im Baustein SYS.1.8 *Speicherlösungen* zu finden. Auch wird nicht auf dedizierte Dienste eingegangen, mit

denen ein Fileserver betrieben werden kann, wie z. B. Samba. Der Dienst Samba wird im Baustein APP.3.4 *Samba* behandelt.

Ein wichtiger Schwerpunkt bei der Absicherung eines Fileservers ist es, Zugriffsrechte auf Dateien nur restriktiv zu vergeben. Weitergehende Anforderungen hierzu sind in dem Baustein ORP.4 *Identitäts- und Berechtigungsmanagement* zu finden. Auch die Sicherung der auf einem Fileserver abgelegten Informationen wird in diesem Baustein nicht behandelt. Hierzu sind die Anforderungen des Bausteins CON.3 *Datensicherungskonzept* zu erfüllen.

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.3.3 *Fileserver* von besonderer Bedeutung.

2.1. Ausfall eines Fileservers

Fällt ein Fileserver aus, kann der gesamte Informationsverbund davon betroffen sein und damit auch wichtige Geschäftsprozesse und Fachaufgaben der Institution. Nicht nur Benutzende, sondern auch Anwendungen können auf Daten vom Fileserver angewiesen sein, um ordnungsgemäß zu funktionieren. Ist die Verfügbarkeit von Daten und Diensten nicht gegeben, können z. B. Fristen nicht eingehalten oder essenzielle Geschäftsprozesse unterbrochen werden. Ist zudem kein Notfallmanagementkonzept vorhanden, können sich Wiederanlaufzeiten weiter erhöhen. In vielen Fällen führt dies zu finanziellen Einbußen. Außerdem kann sich der Ausfall auf andere Institutionen auswirken.

2.2. Unzureichende Dimensionierung des Fileservers

Ist die Leitungsanbindung oder die Speicherkapazität des Fileservers unzureichend, können sich die Zugriffszeiten erhöhen oder Speicherengpässe können auftreten. Dadurch können beispielsweise Mitarbeitende aufgrund der längeren Wartezeiten frustriert werden und damit beginnen, Daten lokal zu speichern. So kann nicht mehr nachvollzogen werden, wo Daten gespeichert sind und wer im Besitz der Daten ist. Auch Applikationen, die auf eine korrekte (Zwischen-)Speicherung von Informationen angewiesen sind, können nicht mehr zuverlässig funktionieren.

2.3. Unzureichende Überprüfung von abgelegten Dateien

Ist ein Fileserver unzureichend in das Konzept zum Schutz vor Schadprogrammen der Institution einbezogen, kann es passieren, dass unbemerkt Schadsoftware auf dem Fileserver abgelegt wird. Alle IT-Systeme und Anwendungen, die auf die Daten des Fileservers zugreifen, können mit der Schadsoftware infiziert werden, wodurch sich die Schadsoftware sehr schnell in der gesamten Institution ausbreitet.

2.4. Fehlendes oder unzureichendes Zugriffsberechtigungskonzept

Werden Zugriffsberechtigungen und Freigaben nicht ordnungsgemäß konzipiert und vergeben, können eventuell Dritte unbefugt auf Daten zugreifen. Dadurch können Unberechtigte Daten verändern, löschen oder kopieren.

2.5. Unstrukturierte Datenhaltung

Wird die Speicherstruktur nicht vorgegeben bzw. halten sich die Mitarbeitenden nicht daran, können Daten unübersichtlich und unkoordiniert auf dem Fileserver gespeichert werden. Das führt zu

verschiedenen Problemen, wie zum Beispiel Speicherplatzverschwendung durch das mehrmalige Ablegen derselben Datei. Auch können unterschiedliche Versionen einer Datei abgelegt werden. Außerdem sind unbefugte Zugriffe möglich, wenn sich z. B. Dateien in Verzeichnissen oder Dateisystemen befinden, die Dritten zugänglich gemacht werden.

2.6. Verlust von auf Fileservern abgespeicherten Daten

Fällt ein Fileserver komplett aus oder sind einzelne Komponenten defekt, können ohne eine Dateisynchronisierung oder ein funktionierendes Backup wichtige Informationen verloren gehen. Das gleiche gilt, wenn Mitarbeitende Dateien unbeabsichtigt löschen. Sollte zudem keine ausreichende Redundanz, etwa durch ein geeignetes Redundant Array of Independent Disks (RAID), eingesetzt werden, können weitere Probleme folgen. So wirkt sich der Ausfall eines einzelnen Datenträgers direkt auf den laufenden Betrieb aus, da die Dateien nicht mehr verfügbar sind.

2.7. Ransomware

Eine spezielle Form von Schadprogrammen ist Ransomware, bei der Daten auf den infizierten IT-Systemen verschlüsselt werden. Angreifende verlangen im Nachgang die Zahlung eines Lösegelds, damit das Opfer die Daten wieder entschlüsseln kann. Es ist jedoch auch nach der Zahlung eines Lösegelds nicht gewährleistet, dass die Daten wiederhergestellt werden können.

Nicht nur die lokalen Daten des infizierten IT-Systems werden hierbei verschlüsselt. Viele Ausprägungen von Ransomware suchen nach Netzlaufwerken mit Schreibzugriff, auf denen alle Daten ebenfalls verschlüsselt werden.

Damit können alle verschlüsselten Informationen seit der letzten Datensicherung verloren sein, auch wenn ein Lösegeld gezahlt wurde. Nicht nur das ursprünglich infizierte IT-System wäre hiervon betroffen, sondern auch zentral abgelegte Informationen, auf die viele IT-Systeme zugreifen dürfen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.3.3 *Fileserver* 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	Benutzende

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.3.3.A1 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.3.A2 Einsatz von RAID-Systemen (B)

Der IT-Betrieb MUSS festlegen, ob im Fileserver ein RAID-System eingesetzt werden soll. Eine Entscheidung gegen ein solches System MUSS nachvollziehbar dokumentiert werden. Falls ein RAID-System eingesetzt werden soll, MUSS der IT-Betrieb entscheiden:

- welches RAID-Level benutzt werden soll,
- wie lang die Zeitspanne für einen RAID-Rebuild-Prozess sein darf und
- ob ein Software- oder ein Hardware-RAID eingesetzt werden soll.

In einem RAID SOLLTEN Hotspare-Festplatten vorgehalten werden.

APP.3.3.A3 Einsatz von Viren-Schutzprogrammen (B)

Alle Daten MÜSSEN durch ein Viren-Schutzprogramm auf Schadsoftware untersucht werden, bevor sie auf dem Fileserver abgelegt werden.

APP.3.3.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.3.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.3.3.A15 Planung von Fileservern (B)

Bevor eine Institution einen oder mehrere Fileserver einführt, SOLLTE sie entscheiden, wofür die Fileserver genutzt und welche Informationen darauf verarbeitet werden. Die Institution SOLLTE jede benutzte Funktion eines Fileservers einschließlich deren Sicherheitsaspekte planen. Arbeitsplatzrechner DÜRFEN NICHT als Fileserver eingesetzt werden.

Der Speicherplatz des Fileservers MUSS ausreichend dimensioniert sein. Auch ausreichende Speicherreserven SOLLTEN vorgehalten werden. Es SOLLTE ausschließlich Massenspeicher verwendet werden, der für einen Dauerbetrieb ausgelegt ist. Die Geschwindigkeit und die Anbindung der Massenspeicher MUSS für den Einsatzzweck angemessen sein.

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.3.3.A6 Beschaffung eines Fileservers und Auswahl eines Dienstes (S)

Die Fileserver-Software SOLLTE geeignet ausgewählt werden. Der Fileserver-Dienst SOLLTE den Einsatzzweck des Fileservers unterstützen, z. B. Einbindung von Netzlaufwerken in den Clients, Streaming von Multimedia-Inhalten, Übertragung von Boot-Images von festplattenlosen IT-Systemen oder ausschließliche Dateiübertragung über FTP. Die Leistung, die Speicherkapazität, die Bandbreite sowie die Anzahl der Benutzenden, die den Fileserver nutzen, SOLLTEN bei der Beschaffung des Fileservers berücksichtigt werden.

APP.3.3.A7 Auswahl eines Dateisystems (S)

Der IT-Betrieb SOLLTE eine Anforderungsliste erstellen, nach der die Dateisysteme des Fileservers bewertet werden. Das Dateisystem SOLLTE den Anforderungen der Institution entsprechen. Das Dateisystem SOLLTE eine Journaling-Funktion bieten. Auch SOLLTE es über einen Schutzmechanismus verfügen, der verhindert, dass mehrere Benutzende oder Anwendungen gleichzeitig schreibend auf eine Datei zugreifen.

APP.3.3.A8 Strukturierte Datenhaltung (S) [Benutzende]

Es SOLLTE eine Struktur festgelegt werden, nach der Daten abzulegen sind. Die Benutzenden SOLLTEN regelmäßig über die geforderte strukturierte Datenhaltung informiert werden. Die Dateien SOLLTEN ausschließlich strukturiert auf den Fileserver abgelegt werden. Es SOLLTE schriftlich festgelegt werden, welche Daten lokal und welche auf dem Fileserver gespeichert werden dürfen. Programm- und Arbeitsdaten SOLLTEN in getrennten Verzeichnissen gespeichert werden. Die Institution SOLLTE regelmäßig überprüfen, ob die Vorgaben zur strukturierten Datenhaltung eingehalten werden.

APP.3.3.A9 Sicheres Speichermanagement (S)

Der IT-Betrieb SOLLTE regelmäßig überprüfen, ob die Massenspeicher des Fileservers noch wie vorgesehen funktionieren. Es SOLLTEN geeignete Ersatzspeicher vorgehalten werden.

Wurde eine Speicherhierarchie (Primär-, Sekundär- bzw. Tertiärspeicher) aufgebaut, SOLLTE ein (teil-)automatisiertes Speichermanagement verwendet werden. Werden Daten automatisiert verteilt, SOLLTE regelmäßig manuell überprüft werden, ob dies korrekt funktioniert.

Es SOLLTEN mindestens nicht-autorisierte Zugriffsversuche auf Dateien und Änderungen von Zugriffsrechten protokolliert werden.

APP.3.3.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

APP.3.3.A11 Einsatz von Speicherbeschränkungen (S)

Der IT-Betrieb SOLLTE bei mehreren Benutzenden auf dem Fileserver prüfen, Beschränkungen des Speicherplatzes für einzelne Benutzende (Quotas) einzurichten. Alternativ SOLLTEN Mechanismen des verwendeten Datei- oder Betriebssystems genutzt werden, um die Benutzenden bei einem bestimmten Füllstand der Festplatte zu warnen oder in diesem Fall nur noch dem IT-Betrieb Schreibrechte einzuräumen.

APP.3.3.A14 Einsatz von Error-Correction-Codes (S)

Der IT-Betrieb SOLLTE ein fehlererkennendes bzw. fehlerkorrigierendes Dateisystem einsetzen. Hierfür SOLLTE genügend Speicherplatz vorgehalten werden. Der IT-Betrieb SOLLTE beachten, dass, je nach eingesetztem Verfahren, Fehler nur mit einer gewissen Wahrscheinlichkeit erkannt und auch nur in begrenzter Größenordnung behoben werden können.

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.3.3.A12 Verschlüsselung des Datenbestandes (H)

Die Massenspeicher des Fileservers SOLLTEN auf Dateisystem- oder Hardwareebene verschlüsselt werden. Falls Hardwareverschlüsselung eingesetzt wird, SOLLTEN Produkte verwendet werden, deren Verschlüsselungsfunktion zertifiziert wurde. Es SOLLTE sichergestellt werden, dass der Virenschutz die verschlüsselten Daten auf Schadsoftware prüfen kann.

APP.3.3.A13 Replikation zwischen Standorten (H)

Für hochverfügbare Fileserver SOLLTE eine angemessene Replikation der Daten auf mehreren Massenspeichern stattfinden. Daten SOLLTEN zudem zwischen unabhängigen Fileservern repliziert werden, die sich an unabhängigen Standorten befinden. Dafür SOLLTE vom IT-Betrieb ein geeigneter

Replikationsmechanismus ausgewählt werden. Damit die Replikation wie vorgesehen funktionieren kann, SOLLTEN hinreichend genaue Zeitdienste genutzt und betrieben werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für den Baustein APP.3.3 *Fileserver* sind keine weiterführenden Informationen vorhanden.