SYS.1: Server

SYS.1.8: Speicherlösungen

1 Beschreibung

1.1 Einleitung

Das stetige Wachstum digitaler Informationen und die zunehmende Menge unstrukturierter Informationen führen dazu, dass innerhalb von Institutionen zentrale Speicherlösungen eingesetzt werden. Dabei unterliegen die Anforderungen an solche Speicherlösungen einem stetigen Wandel, der sich beispielsweise an folgenden Aspekten beobachten lässt:

- Die Daten einer Institution sollen jederzeit, an jedem Ort und für unterschiedliche Anwendungsszenarien verfügbar sein. Dadurch gelten für moderne Speicherlösungen häufig gestiegene Verfügbarkeitsanforderungen.
- Die zunehmende Digitalisierung sämtlicher Informationen in einer Institution macht es notwendig, dass weitreichende rechtliche Vorgaben (Compliance-Anforderungen) beachtet und eingehalten werden müssen.
- Speicherlösungen sollen dynamisch an die sich stetig ändernden Anforderungen anpassbar sein und Speicherplatz zentral bereitstellen können.

In der Vergangenheit wurden Speicherlösungen oft umgesetzt, indem Speichermedien direkt an einen Server angeschlossen wurden. Diese sogenannten Direct-Attached-Storage-(DAS)-Systeme können die aktuellen und zukünftigen Anforderungen jedoch oft nicht mehr erfüllen. Daher sind die heute weitverbreiteten zentralen Speicherlösungen und deren Bestandteile notwendig, die sich wie folgt unterscheiden lassen:

- Speicherlösungen: Eine Speicherlösung besteht aus einem oder mehreren Speichernetzen sowie mindestens einem Speichersystem.
- Speichernetze: Speichernetze ermöglichen einerseits den Zugriff auf die Speichersysteme, andererseits die Replikation von Daten zwischen Speichersystemen.
- Speichersysteme: Als Speichersystem wird die zentrale Instanz bezeichnet, die für andere IT-Systeme Speicherplatz zur Verfügung stellt. Ein Speichersystem erlaubt außerdem den zeitgleichen Zugriff mehrerer IT-Systeme auf den vorhandenen Speicherplatz.

1.2 Zielsetzung

Das Ziel dieses Bausteins ist es, aufzuzeigen, wie zentrale Speicherlösungen sicher geplant, umgesetzt, betrieben und ausgesondert werden.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.1.8 *Speicherlösungen* ist immer dann anzuwenden, wenn zentrale Speicherlösungen

eingesetzt werden. Somit kann er auf Network-Attached-Storage-(NAS)-Systeme, Storage-Area-Networks-(SAN)-Systeme, Hybrid Storage, Objekt Storage oder Cloud Storage angewendet werden. Dabei muss jedoch Folgendes beachtet werden:

- **Network Attached Storage (NAS)** stellt beispielsweise über die Protokolle NFS (Network File System), AFP (Apple Filing Protocol) und CIFS (Common Internet File System) Zugriffe auf die Speichersysteme zur Verfügung. Der Hauptanwendungsfall besteht darin, Fileserver-Dienste zur Verfügung zu stellen. Für NAS-Systeme sind daher auch zusätzlich zu diesem Baustein die Bausteine SYS.1.1 *Allgemeiner Server* sowie APP.3.3 *Fileserver* anzuwenden.
- **Storage Area Networks (SAN)** werden in der Regel durch ein dediziertes Speichernetz zwischen Speichersystemen und angeschlossenen IT-Systemen geschaffen. Für SAN-Systeme ist daher der Baustein NET.1.1 *Netzarchitektur und -design* geeignet zu berücksichtigen.Speichersysteme, die sowohl über NAS als auch SAN Daten zur Verfügung stellen können, werden oft unter der Bezeichnung **Hybrid-Storage** oder kombiniertes Speichersystem (Unified Storage) geführt. Für Hybrid-Systeme sind daher auch zusätzlich die Bausteine SYS.1.1 *Allgemeiner Server* sowie APP.3.3 *Fileserver* anzuwenden. Darüber hinaus ist der Baustein NET.1.1 *Netzarchitektur und -design* geeignet zu berücksichtigen.
- **Objekt-Storage** (oftmals auch als **Object-based Storage** bezeichnet) ermöglicht gegenüber den traditionellen blockbasierten und dateibasierten Zugriffsmethoden einen objektbasierten Zugriff auf Daten. Der Zugriff auf einen objektbasierenden Speicher erfolgt über eine führende Anwendung. Die Anwendung greift hierbei über eine spezielle Schnittstelle (Application Programming Interface (API)) und deren mögliche Kommandos oder direkt per IP auf den Objekt-Storage zu. Für objektbasierende Speicherlösungen ist daher auch zusätzlich der Baustein SYS.1.1 *Allgemeiner Server* anzuwenden. Darüber hinaus müssen Sicherheitsanforderungen mitberücksichtigt werden, die sich dadurch ergeben, dass Webservices eingesetzt werden. Webservices werden im vorliegenden Baustein nicht betrachtet.
- Im Zusammenhang mit Weiterentwicklungen im Speicherumfeld etabliert sich zunehmend auch der Begriff des **Cloud Storage**. Hierunter sind Speicherlösungen als Basis für Cloud-Services zu verstehen. Die Speicherlösung an sich bleibt dabei weitgehend unverändert, jedoch liegt eine von den klassischen SAN- oder NAS-Architekturen abweichende Art des Zugriffs auf die gespeicherten Daten vor. Dieser wird in der Regel mittels Web-Service-Schnittstelle (via Representional State Transfer (REST) und Simple Object Access Protocol (SOAP)) realisiert.

Datensicherungsgeräte, die an das Speichersystem oder an das Speichernetz angeschlossen sind, werden hier nicht betrachtet, sondern im Baustein OPS.1.2.2 *Archivierung* behandelt. Konzeptionelle Aspekte der Datensicherung werden im Baustein CON.3 *Datensicherungskonzept* erläutert.

Oft kann eine Vielzahl von Benutzerkonten auf Speicherlösungen zugreifen. Deswegen sollten Speicherlösungen geeignet im Rollen- und Rechtekonzept mit berücksichtigt werden. Anforderungen dazu finden sich im Baustein ORP.4 *Identitäts- und Berechtigungsmanagement*.

Falls auf externe Dienstleister zurückgegriffen wird, um eine Speicherlösung zu betreiben, müssen die Anforderungen des Bausteins OPS.2.1 *Outsourcing für Kunden* gesondert berücksichtigt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein SYS.1.8 *Speicherlösungen* von besonderer Bedeutung.

2.1 Unsichere Default-Einstellungen bei Speicherkomponenten

Häufig werden Speicherkomponenten mit einer Default-Konfiguration ausgeliefert, damit die Geräte schnell und mit möglichst umfassenden Funktionen in Betrieb genommen werden können. So sind in vielen Geräten nicht benötigte Protokolle aktiviert, wie z. B. HTTP, Telnet und unsichere SNMP-Versionen. Werden Speicherkomponenten mit unsicheren Werkseinstellungen produktiv eingesetzt, kann einfacher unberechtigt auf sie zugegriffen werden. Das kann dazu führen, dass z. B. Dienste nicht

mehr verfügbar sind oder dass unerlaubt auf vertrauliche Informationen der Institution zugegriffen wird.

2.2 Manipulation von Daten über das Speichersystem

Über ein mangelhaft konfiguriertes Storage Area Network (SAN) können sich ungewollt Netze verbinden. Ist beispielsweise ein Server mit SAN-Anschluss aus dem Internet erreichbar und so von außen kompromittierbar, kann dieser als Einstiegspunkt für Angreifer genutzt werden, um unberechtigt auf schützenswerte Informationen zuzugreifen, die im SAN gespeichert sind. Da auf diese Weise alle Sicherheits- und Überwachungsmaßnahmen, wie Firewalls oder Intrusion Detection Systeme (IDS), in den Netzen einer Institution umgangen werden können, ist das Schadenspotenzial groß.

2.3 Verlust der Vertraulichkeit durch storagebasierte Replikationsmethoden

Storagebasierte Replikationsmethoden haben den Zweck, gespeicherte oder archivierte Daten in Echtzeit über ein Speichernetz zu duplizieren und diese damit zusätzlich redundant abzuspeichern. Hierdurch sollen Datenverluste vermieden werden. Die automatisierte Replikation unverschlüsselter Daten birgt allerdings sowohl im eigenen Netz als auch bei der Nutzung öffentlicher Netze Risiken. So kann unberechtigt auf Replikationsverkehr zugegriffen werden, beispielsweise mittels FC-Analysern (FC-Replikation) oder Sniffern (IP-Replikation).

2.4 Zugriff auf Informationen anderer Mandanten durch WWN-Spoofing

Geräte in einem FC-SAN werden intern über World Wide Names (WWNs) verwaltet und zugeordnet. Sie entsprechen in gewisser Weise den MAC-Adressen von Ethernet-Netzadaptern. Mittels Programmen, die durch den Hersteller der Host Bus Adapter (HBA) zur Verfügung gestellt werden, kann der WWN eines HBAs geändert werden. Dadurch kann ein Angreifer auf Daten zugreifen, für die er keine Berechtigung besitzt. Die Manipulation von WWNs, auch als WWN-Spoofing bezeichnet, birgt für eine Institution erhebliches Gefahrenpotenzial. Insbesondere im Zusammenhang mit mandantenfähigen Speichersystemen können Unberechtigte auf die Informationen anderer Mandanten zugreifen.

2.5 Überwindung der logischen Netzseparierung

Werden die Netzstrukturen unterschiedlicher Mandanten nicht durch physisch getrennte Netze, sondern durch virtuelle Storage Area Networks (VSANs) separiert, kann hierdurch die Informationssicherheit der Institution gefährdet werden. Gelingt es einem Angreifer, in das Netz eines anderen Mandanten einzudringen, kann er sowohl auf das virtuelle SAN dieses Mandanten als auch auf die übertragenen Nutzdaten zugreifen.

2.6 Ausfall von Komponenten einer Speicherlösung

Komplexe netzbasierte Speicherlösungen bestehen oft aus vielen Komponenten (z. B. FC-Switches, Storage Controller, Virtualisierungs-Appliance). Fallen einzelne Komponenten einer Speicherlösung aus, kann dies dazu führen, dass wichtige Anwendungen nicht mehr korrekt arbeiten und somit Datenverluste drohen.

2.7 Erlangung physischen Zugangs auf SAN-Switches

Existieren in einer Institution unzureichende Zutritts- und Zugangskontrollen zu den Komponenten eines Speichersystems oder fehlen diese gänzlich, kann es einem Angreifer gelingen, sich physischen Zugang zu vorhandenen Switches zu verschaffen bzw. zusätzliche FC-SAN-Switches an das Netz anzuschließen. Ziel des Angreifers könnte es sein, auf die verteilte Zoning-Datenbank zuzugreifen, um diese so zu verändern, dass er auf die Speichersysteme zugreifen kann.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.1.8 *Speicherlösungen* 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 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	Haustechnik

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.1.8 *Speicherlösungen* vorrangig erfüllt werden:

SYS.1.8.A1 Geeignete Aufstellung von Speichersystemen [Haustechnik] (B)

Die IT-Komponenten von Speicherlösungen MÜSSEN in verschlossenen Räumen aufgestellt werden. Zu diesen Räumen DÜRFEN NUR Berechtigte Zutritt haben. Zudem MUSS eine sichere Stromversorgung sichergestellt sein. Die Herstellervorgaben zur empfohlenen Umgebungstemperatur und Luftfeuchte MÜSSEN eingehalten werden.

SYS.1.8.A2 Sichere Grundkonfiguration von Speicherlösungen (B)

Bevor eine Speicherlösung produktiv eingesetzt wird, MUSS sichergestellt sein, dass alle eingesetzten Softwarekomponenten und die Firmware aktuell sind. Danach MUSS eine sichere Grundkonfiguration hergestellt werden.

Nicht genutzte Schnittstellen des Speichersystems MÜSSEN deaktiviert werden. Die Dateien zur Default-Konfiguration, zur vorgenommenen Grundkonfiguration und zur aktuellen Konfiguration SOLLTEN redundant und geschützt aufbewahrt werden.

SYS.1.8.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.1.8.A4 Schutz der Administrationsschnittstellen (B)

Alle Administrations- und Management-Zugänge der Speichersysteme MÜSSEN eingeschränkt werden. Es MUSS sichergestellt sein, dass aus nicht-vertrauenswürdigen Netzen heraus nicht auf die Administrationsschnittstellen zugegriffen werden kann.

Es SOLLTEN als sicher geltende Protokolle eingesetzt werden. Sollten dennoch unsichere Protokolle verwendet werden, MUSS für die Administration ein eigenes Administrationsnetz (siehe NET.1.1 *Netzarchitektur und -design*) genutzt werden.

SYS.1.8.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.1.8 *Speicherlösungen*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.1.8.A6 Erstellung einer Sicherheitsrichtlinie für Speicherlösungen (S)

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTE eine spezifische Sicherheitsrichtlinie für Speicherlösungen erstellt werden. Darin SOLLTEN nachvollziehbar Vorgaben beschrieben sein, wie Speicherlösungen sicher geplant, administriert, installiert, konfiguriert und betrieben werden können.

Die Richtlinie SOLLTE allen für Speicherlösungen zuständigen Administratoren bekannt und grundlegend für ihre Arbeit sein. Wird die Richtlinie verändert oder wird von den Vorgaben abgewichen, SOLLTE dies mit dem ISB abgestimmt und dokumentiert werden. Es SOLLTE regelmäßig überprüft werden, ob die Richtlinie noch korrekt umgesetzt ist. Gegebenenfalls SOLLTE sie aktualisiert werden. Die Ergebnisse SOLLTEN sinnvoll dokumentiert werden.

SYS.1.8.A7 Planung von Speicherlösungen (S)

Bevor Speicherlösungen in einer Institution eingesetzt werden, SOLLTE eine Anforderungsanalyse durchgeführt werden. In der Anforderungsanalyse SOLLTEN unter anderem die Themen Performance und Kapazität betrachtet werden. Auf Basis der ermittelten Anforderungen SOLLTE dann eine detaillierte Planung für Speicherlösungen erstellt werden. Darin SOLLTEN folgende Punkte berücksichtigt werden:

- Auswahl von Herstellern und Lieferanten,
- Entscheidung für oder gegen zentrale Verwaltungssysteme (Management-Systeme),
- Planung des Netzanschlusses,
- Planung der Infrastruktur sowie
- Integration in bestehende Prozesse.

SYS.1.8.A8 Auswahl einer geeigneten Speicherlösung (S)

Die technischen Grundlagen unterschiedlicher Speicherlösungen SOLLTEN detailliert beleuchtet werden. Die Auswirkungen dieser technischen Grundlagen auf den möglichen Einsatz in der Institution SOLLTEN geprüft werden. Die Möglichkeiten und Grenzen der verschiedenen Speichersystemarten SOLLTEN für die Verantwortlichen der Institution transparent dargestellt werden. Die Entscheidungskriterien für eine Speicherlösung SOLLTEN nachvollziehbar dokumentiert werden. Ebenso SOLLTE die Entscheidung für die Auswahl einer Speicherlösung nachvollziehbar dokumentiert werden.

SYS.1.8.A9 Auswahl von Lieferanten für eine Speicherlösung (S)

Anhand der spezifizierten Anforderungen an eine Speicherlösung SOLLTE ein geeigneter Lieferant ausgewählt werden. Die Auswahlkriterien und die Entscheidung für einen Lieferanten SOLLTEN nachvollziehbar dokumentiert werden. Außerdem SOLLTEN Aspekte der Wartung und Instandhaltung schriftlich in sogenannten Service-Level-Agreements (SLAs) festgehalten werden. Die SLAs SOLLTEN eindeutig und quantifizierbar sein. Es SOLLTE genau geregelt werden, wann der Vertrag mit dem Lieferanten endet.

SYS.1.8.A10 Erstellung und Pflege eines Betriebshandbuchs (S)

Es SOLLTE ein Betriebshandbuch erstellt werden. Darin SOLLTEN alle Regelungen, Anforderungen und Einstellungen dokumentiert werden, die erforderlich sind, um Speicherlösungen zu betreiben. Das Betriebshandbuch SOLLTE regelmäßig aktualisiert werden.

SYS.1.8.A11 Sicherer Betrieb einer Speicherlösung (S)

Das Speichersystem SOLLTE hinsichtlich der Verfügbarkeit der internen Anwendungen, der Systemauslastung sowie kritischer Ereignisse überwacht werden. Weiterhin SOLLTEN für Speicherlösungen feste Wartungsfenster definiert werden, in denen Änderungen durchgeführt werden können. Insbesondere Firmware- oder Betriebssystemupdates von Speichersystemen oder den Netzkomponenten einer Speicherlösung SOLLTEN ausschließlich innerhalb eines solchen Wartungsfensters durchgeführt werden.

SYS.1.8.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.1.8.A13 Überwachung und Verwaltung von Speicherlösungen (S)

Speicherlösungen SOLLTEN überwacht werden. Dabei SOLLTEN alle erhobenen Daten (Nachrichten) vorrangig daraufhin geprüft werden, ob die Vorgaben des Betriebshandbuchs eingehalten werden.

Die wesentlichen Nachrichten SOLLTEN mit Nachrichtenfilter herausgefiltert werden. Einzelne Komponenten der Speicherlösung und des Gesamtsystems SOLLTEN zentral verwaltet werden.

SYS.1.8.A14 Absicherung eines SANs durch Segmentierung (S)

Ein SAN SOLLTE segmentiert werden. Es SOLLTE ein Konzept erarbeitet werden, das die SAN-Ressourcen den jeweiligen Servern zuordnet. Hierfür SOLLTE anhand der Sicherheitsanforderungen und des Administrationsaufwands entschieden werden, welche Segmentierung in welcher Implementierung (z. B. FC-SANs oder iSCSI-Speichernetze) eingesetzt werden soll. Die aktuelle Ressourcenzuordnung SOLLTE mithilfe von Verwaltungswerkzeugen einfach und übersichtlich erkennbar sein. Weiterhin SOLLTE die aktuelle Zoning-Konfiguration dokumentiert werden. Die Dokumentation SOLLTE auch in Notfällen verfügbar sein.

SYS.1.8.A15 Sichere Trennung von Mandanten in Speicherlösungen (S)

Es SOLLTE definiert und nachvollziehbar dokumentiert werden, welche Anforderungen die Institution an die Mandantenfähigkeit einer Speicherlösung stellt. Die eingesetzten Speicherlösungen SOLLTEN diese dokumentierten Anforderungen erfüllen.

Im Block-Storage-Umfeld SOLLTE *LUN Masking* eingesetzt werden, um Mandanten voneinander zu trennen. In Fileservice-Umgebungen SOLLTE es möglich sein, mit virtuellen Fileservern zu agieren. Dabei SOLLTE jedem Mandanten ein eigener Fileservice zugeordnet werden.

Beim Einsatz von IP oder iSCSI SOLLTEN die Mandanten über eine Segmentierung im Netz voneinander getrennt werden. Wird Fibre Channel eingesetzt, SOLLTE mithilfe von VSANs und Soft-Zoning separiert werden.

SYS.1.8.A16 Sicheres Löschen in SAN-Umgebungen (S)

In mandantenfähigen Speichersystemen SOLLTE sichergestellt werden, dass Logical Unit Numbers (LUNs), die einem bestimmten Mandanten zugeordnet sind, gelöscht werden.

SYS.1.8.A17 Dokumentation der Systemeinstellungen von Speichersystemen (S)

Alle Systemeinstellungen von Speichersystemen SOLLTEN dokumentiert werden. Die Dokumentation SOLLTE die technischen und organisatorischen Vorgaben sowie alle spezifischen Konfigurationen der Speichersysteme der Institution enthalten.

Sofern die Dokumentation der Systemeinstellungen vertrauliche Informationen beinhaltet, SOLLTEN diese vor unberechtigtem Zugriff geschützt werden. Die Dokumentation SOLLTE regelmäßig überprüft werden. Sie SOLLTE immer aktuell sein.

SYS.1.8.A18 Sicherheitsaudits und Berichtswesen bei Speichersystemen (S)

Alle eingesetzten Speichersysteme SOLLTEN regelmäßig auditiert werden. Dafür SOLLTE ein entsprechender Prozess eingerichtet werden. Es SOLLTE geregelt werden, welche Sicherheitsreports mit welchen Inhalten regelmäßig zu erstellen sind. Zudem SOLLTE auch geregelt werden, wie mit Abweichungen von Vorgaben umgegangen wird und wie oft und in welcher Tiefe Audits durchgeführt werden.

SYS.1.8.A19 Aussonderung von Speicherlösungen (S)

Werden ganze Speicherlösungen oder einzelne Komponenten einer Speicherlösung nicht mehr benötigt, SOLLTEN alle darauf vorhandenen Daten auf andere Speicherlösungen übertragen werden. Hierfür SOLLTE eine Übergangsphase eingeplant werden. Anschließend SOLLTEN alle Nutzdaten und Konfigurationsdaten sicher gelöscht werden. Aus allen relevanten Dokumenten SOLLTEN alle Verweise

auf die außer Betrieb genommene Speicherlösung entfernt werden.

SYS.1.8.A20 Notfallvorsorge und Notfallreaktion für Speicherlösungen (S)

Es SOLLTE ein Notfallplan für die eingesetzte Speicherlösung erstellt werden. Der Notfallplan SOLLTE genau beschreiben, wie in bestimmten Notfallsituationen vorzugehen ist. Auch SOLLTEN Handlungsanweisungen in Form von Maßnahmen und Kommandos enthalten sein, die die Fehleranalyse und Fehlerkorrektur unterstützen. Um Fehler zu beheben, SOLLTEN geeignete Werkzeuge eingesetzt werden.

Regelmäßige Übungen und Tests SOLLTEN anhand des Notfallplans durchgeführt werden. Nach den Übungen und Tests sowie nach einem tatsächlichen Notfall SOLLTEN die dabei erzeugten Daten sicher gelöscht werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.1.8 *Speicherlösungen* 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.

SYS.1.8.A21 Einsatz von Speicherpools zur Mandantentrennung (H)

Mandanten SOLLTEN Speicherressourcen aus unterschiedlichen sogenannten Speicherpools zugewiesen werden. Dabei SOLLTE ein Speichermedium immer nur einem einzigen Pool zugewiesen werden. Die logischen Festplatten (LUNs), die aus einem solchen Pool generiert werden, SOLLTEN nur einem einzigen Mandanten zugeordnet werden.

SYS.1.8.A22 Einsatz einer hochverfügbaren SAN-Lösung (H)

Eine hochverfügbare SAN-Lösung SOLLTE eingesetzt werden. Die eingesetzten Replikationsmechanismen SOLLTEN den Verfügbarkeitsanforderungen der Institution an die Speicherlösung entsprechen. Auch die Konfiguration der Speicherlösung SOLLTE den Verfügbarkeitsanforderungen gerecht werden. Außerdem SOLLTE ein Test- und Konsolidierungssystem vorhanden sein.

SYS.1.8.A23 Einsatz von Verschlüsselung für Speicherlösungen (H)

Alle in Speicherlösungen abgelegten Daten SOLLTEN verschlüsselt werden. Es SOLLTE festgelegt werden, auf welchen Ebenen (Data-in-Motion und Data-at-Rest) verschlüsselt wird. Dabei SOLLTE beachtet werden, dass die Verschlüsselung auf dem Transportweg auch bei Replikationen und Backup-Traffic relevant ist.

SYS.1.8.A24 Sicherstellung der Integrität der SAN-Fabric (H)

Um die Integrität der SAN-Fabric sicherzustellen, SOLLTEN Protokolle mit zusätzlichen Sicherheitsmerkmalen eingesetzt werden. Bei den folgenden Protokollen SOLLTEN deren Sicherheitseigenschaften berücksichtigt und entsprechende Konfigurationen verwendet werden:

- Diffie Hellman Challenge Handshake Authentication Protocol (DH-CHAP),
- Fibre Channel Authentication Protocol (FCAP) und
- Fibre Channel Password Authentication Protocol (FCPAP).

SYS.1.8.A25 Mehrfaches Überschreiben der Daten einer LUN (H)

In SAN-Umgebungen SOLLTEN Daten gelöscht werden, indem die zugehörigen Speichersegmente einer LUN mehrfach überschrieben werden.

SYS.1.8.A26 Absicherung eines SANs durch Hard-Zoning (H)

Um SANs zu segmentieren, SOLLTE Hard-Zoning eingesetzt werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27040:2015 „Information technology – Security techniques – Storage security“ Vorgaben für die Absicherung von Speicherlösungen.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel SY1.4 Network Storage Systems Vorgaben für die Absicherung von Speicherlösungen.

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 SYS.1.8 *Speicherlösungen* von Bedeutung.

G 0.2 Ungünstige klimatische Bedingungen

G 0.8 Ausfall oder Störung der Stromversorgung

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.15 Abhören

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

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 0.44 Unbefugtes Eindringen in Räumlichkeiten

G 0.45 Datenverlust

G 0.46 Integritätsverlust schützenswerter Informationen