|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Speicherlösungen"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300028 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc80550944)

[Dokumentenhistorie 3](#_Toc80550945)

[Inhaltsverzeichnis 4](#_Toc80550946)

[Allgemeine Festlegungen 6](#_Toc80550947)

[Ziel / Zweck 6](#_Toc80550948)

[Geltungsbereich 6](#_Toc80550949)

[Zuständigkeiten 7](#_Toc80550950)

[Genehmigungs- und Änderungsverfahren 7](#_Toc80550951)

[Aufbau des Dokuments 7](#_Toc80550952)

[Sicherheitsrichtlinie „Speicherlösungen" 8](#_Toc80550953)

[Basismaßnahmen 8](#_Toc80550954)

[Geeignete Aufstellung von Speichersystemen (SYS.1.8.A1) 8](#_Toc80550955)

[Sichere Grundkonfiguration von Speicherlösungen (SYS.1.8.A2) 8](#_Toc80550956)

[Restriktive Rechtevergabe (SYS.1.8.A3) 8](#_Toc80550957)

[Schutz der Administrationsschnittstellen (SYS.1.8.A4) 8](#_Toc80550958)

[Protokollierung bei Speichersystemen (SYS.1.8.A5) 8](#_Toc80550959)

[Standardmaßnahmen 9](#_Toc80550960)

[Planung von Speicherlösungen (SYS.1.8.A7) 9](#_Toc80550961)

[Auswahl einer geeigneten Speicherlösung (SYS.1.8.A8) 9](#_Toc80550962)

[Auswahl von Lieferanten für eine Speicherlösung (SYS.1.8.A9) 9](#_Toc80550963)

[Erstellung und Pflege eines Betriebshandbuchs (SYS.1.8.A10) 9](#_Toc80550964)

[Sicherer Betrieb einer Speicherlösung (SYS.1.8.A11) 10](#_Toc80550965)

[Schulung der Administratoren (SYS.1.8.A12) 10](#_Toc80550966)

[Überwachung und Verwaltung von Speicherlösungen (SYS.1.8.A13) 10](#_Toc80550967)

[Absicherung eines SANs durch Segmentierung (SYS.1.8.A14) 10](#_Toc80550968)

[Sichere Trennung von Mandanten in Speicherlösungen (SYS.1.8.A15) 10](#_Toc80550969)

[Sicheres Löschen in SAN-Umgebungen (SYS.1.8.A16) 11](#_Toc80550970)

[Dokumentation der Systemeinstellungen von Speichersystemen (SYS.1.8.A17) 11](#_Toc80550971)

[Sicherheits-Audits und Berichtswesen bei Speichersystemen (SYS.1.8.A18) 11](#_Toc80550972)

[Aussonderung von Speicherlösungen (SYS.1.8.A19) 11](#_Toc80550973)

[Notfallvorsorge und Notfallreaktion für Speicherlösungen (SYS.1.8.A20) 11](#_Toc80550974)

[Maßnahmen bei erhöhtem Schutzbedarf 12](#_Toc80550975)

[Einsatz von Speicher-Pools zur Mandantentrennung (SYS.1.8.A21 - CIA) 12](#_Toc80550976)

[Einsatz einer hochverfügbaren SAN-Lösung (SYS.1.8.A22 - A) 12](#_Toc80550977)

[Einsatz von Verschlüsselung für Speicherlösungen (SYS.1.8.A23 - CI) 12](#_Toc80550978)

[Sicherstellung der Integrität der SAN-Fabric (SYS.1.8.A24 - CI) 12](#_Toc80550979)

[Mehrfaches Überschreiben der Daten einer LUN (SYS.1.8.A25 - CI) 13](#_Toc80550980)

[Absicherung eines SANs durch Hard-Zoning (SYS.1.8.A25 - CI) 13](#_Toc80550981)

# Allgemeine Festlegungen

## Ziel / Zweck

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

* Die Daten sollen jederzeit, an jedem Ort und für unterschiedliche Anwendungsszenarien verfügbar sein. Dadurch gelten für moderne Speicherlösungen häufig gestiegene Verfügbarkeitsanforderungen.
* Die zunehmende Digitalisierung sämtlicher Informationen macht es notwendig, dass weitreichende rechtliche Vorgaben (Anforderungen an die Compliance) 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.

Das Ziel dieser Sicherheitsrichtlinie ist es auf Basis der Vorgaben aus dem BSI Baustein SYS.1.8 "Speicherlösungen" aufzuzeigen, wie zentrale Speicherlösungen für die <Institution> sicher geplant, betrieben und ausgesondert werden.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Die Sicherheitsrichtlinie „Speicherlösungen“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Speicherlösungen"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Geeignete Aufstellung von Speichersystemen (SYS.1.8.A1)

Die Speichersysteme in der Verantwortung der <Institution> sind in gesicherten Räumen mit besonderen Zutrittsregelungen aufgestellt. Zusätzlich wird eine sichere Stromversorgung und den Herstellervorgaben entsprechend empfohlene Umgebungstemperatur und Luftfeuchtigkeit sichergestellt.

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

Es werden nur aktuelle Software- und Firmwarestände der Speicherlösungen produktiv eingesetzt. Eine sichere Grundkonfiguration wird sichergestellt.

Nicht benötigte Benutzerkonten sind zu löschen oder deaktivieren. Zusätzlich sind alle Standard-Passwörter gemäß der Passwortrichtlinie zu ändern beziehungsweise neue Accounts anzulegen.

Alle nicht genutzten Schnittstellen des Speichersystems sind zu deaktivieren. Die Default-Konfiguration, die vorgenommene Grundkonfiguration und die aktuelle Konfiguration werden redundant und geschützt aufbewahrt.

### Restriktive Rechtevergabe (SYS.1.8.A3)

Innerhalb der <Institution> wurde ein Rechte- und Rollenkonzept etabliert. Alle auf der jeweiligen Speicherlösung eingerichteten Benutzerkonten entsprechen diesem Konzept. Alle Benutzerkonten werden entsprechend dem Need-to-know Prinzip eingerichtet.

### Schutz der Administrationsschnittstellen (SYS.1.8.A4)

Alle Administrations- und Management-Zugänge der Speichersysteme wurden eingeschränkt. Es wird sichergestellt, dass auf die Administrationsschnittstellen nur aus einem speziell bereitgestellten Sicherheitsbereich für die Administration zugegriffen werden kann.

Der Zugang zu der Speicherlösung wird so konfiguriert, dass dieser ausschließlich verschlüsselte Kommunikationsverbindungen zu lässt. Die dazu eingesetzten kryptografischen Verfahren und Protokolle müssen den internen Vorgaben der <Institution> entsprechen. Sofern die kryptografischen Verfahren und Protokolle derzeit noch nicht freigegeben sind, sind diese zu beantragen und durch den <Informationssicherheitsbeauftragter> der <Institution> freizugeben.

### Protokollierung bei Speichersystemen (SYS.1.8.A5)

Die interne Protokollierung der Speichersysteme ist so zu konfigurieren, dass die Informationen protokolliert werden, die dazu dienen, Probleme früh zu erkennen.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Planung von Speicherlösungen (SYS.1.8.A7)

Für die detaillierte Planung von Speicherlösungen wird eine Anforderungsanalyse, unter anderem hinsichtlich Performance und Kapazität, durchgeführt. Die Planung berücksichtigt folgende Punkte:

* Auswahl geeigneter Hardware,
* Auswahl von Herstellern und Lieferanten,
* Entscheidung für oder gegen zentrale Managementsysteme,
* Planung des Netzanschlusses,
* Planung der Infrastruktur,
* Integration in bestehende Prozesse.

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

Für die Auswahl einer geeigneten Speicherlösung, werden technische Grundlagen unterschiedlicher Speicherlösungen detailliert untersucht und deren Auswirkungen auf den möglichen Einsatz in der IaaS und PaaS der <Institution> geprüft. Die Möglichkeiten und Grenzen der verschiedenen Speichersystemarten werden für die Verantwortlichen der <Institution> transparent dargestellt. Sowohl die Entscheidungskriterien als auch die Entscheidung für die Auswahl werden nachvollziehbar dokumentiert.

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

Anhand der spezifizierten Anforderungen werden geeignete Lieferanten idealerweise aus Rahmenverträgen ausgewählt. Die Auswahlkriterien und die Entscheidung für einen Lieferanten werden nachvollziehbar dokumentiert. Die Service-Level-Agreements (SLAs) werden mit jedem Lieferanten innerhalb eines Vertrages schriftlich festgehalten. Diese sind eindeutig und quantifizierbar und erfüllen die vereinbarten internen Operational-Level Agreement (OLAs). Die Beendigung der Verträge wird genau geregelt. Speichermedien verbleiben im Garantiefall und nach Beendigung des Vertrages Eigentum der <Institution>.

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

Innerhalb der <Institution> wird ein Betriebshandbuch pro Speicherlösung erstellt. Darin sind alle erforderlichen Regelungen, Anforderungen und Einstellungen dokumentiert, die erforderlich sind, um Speicherlösungen zu betreiben. Das Betriebshandbuch ist in den etablierten Dokumentenlenkungsprozess integriert.

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

Das Speichersystem wird hinsichtlich der Verfügbarkeit der internen Anwendungen, der Systemauslastung sowie kritischer Ereignisse überwacht. Zusätzlich werden feste Wartungsfenster definiert, in denen Änderungen durchgeführt werden können. Insbesondere Firmware- oder Betriebssystemupdates von Speichersystemen oder den Netzkomponenten einer Speicherlösung werden ausschließlich innerhalb eines solchen Wartungsfensters durchgeführt. Alle Änderungen werden über das Änderungsmanagement aktiviert und mit allen beteiligten Verantwortlichen innerhalb der <Institution> abgestimmt.

### Schulung der Administratoren (SYS.1.8.A12)

Die zuständigen Administratoren werden ausreichend geschult. Innerhalb der <Institution> werden zielgruppenorientierte Schulungen durchgeführt. Diese vermitteln Kenntnisse zu Vorgehensweisen, Techniken und Werkzeugen der Speichersysteme sowie Einrichtung und sicheren Betrieb der zugehörigen Komponenten. Zusätzlich werden herstellerspezifische Aspekte zu einzelnen Produkten und Komponenten thematisiert. Werden neue Produkte eingesetzt, erfolgen speziell hierzu Nachschulungen.

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

Alle Speicherlösungen der <Institution> werden überwacht. Dabei werden alle erhobenen Daten vorrangig daraufhin geprüft, ob die Vorgaben des Betriebshandbuchs eingehalten werden.

Einzelne Komponenten der Speicherlösung und des Gesamtsystems werden zentral verwaltet. Die wesentlichen Nachrichten werden herausgefiltert, um diese besser darzustellen.

Wird eine Speicherlösung durch den externen Dienstleister betrieben, wird die Überwachung der vereinbarten SLAs definiert und dokumentiert.

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

Innerhalb der <Institution> ist ein Konzept zu etablieren, welches die SAN-Ressourcen den jeweiligen Servern zuordnet. Hierfür wurde anhand der Sicherheitsanforderungen und des Administrationsaufwands entschieden, welche Segmentierung in welchem Einsatzszenario eingesetzt werden soll. Die aktuelle Ressourcenzuordnung ist mithilfe von Verwaltungswerkzeugen einfach und übersichtlich erkennbar. Die aktuelle Zoning-Konfiguration wurde dokumentiert. Diese steht auch in Notfällen zur Verfügung.

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

Die Anforderungen an die Mandantenfähigkeit einer Speicherlösung sind zu definieren und schriftlich zu dokumentieren. Alle eingesetzten Speicherlösungen innerhalb der <Institution> erfüllen diese Anforderungen.

Um Mandanten sicher voneinander zu trennen, sollte im Block-Storage-Umfeld LUN Masking eingesetzt werden. In Fileservice-Umgebungen ist es möglich mit virtuellen Fileservern zu agieren. Hierbei wird jedem Mandanten ein eigener Fileservice zugeordnet.

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

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

Die Verfahren zum Löschen von Informationen sind festzulegen. In mandantenfähigen Speichersystemen wird sichergestellt, dass Logical Unit Numbers (LUNs), die einem bestimmten Mandanten zugeordnet sind, gelöscht werden.

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

Alle Systemeinstellungen von Speichersystemen sind dokumentiert worden. Die Dokumentation beinhaltet die technischen und organisatorischen Vorgaben sowie alle spezifischen Konfigurationen der Speichersysteme. Es findet eine regelmäßige Überprüfung statt. Insbesondere wird auf die Aktualität der Rechtevergabe geachtet. Die Dokumentation wird vor unberechtigtem Zugriff geschützt. Ebenfalls wird sichergestellt, dass die Dokumentation in allen Notfallszenarien verfügbar ist.

### Sicherheits-Audits und Berichtswesen bei Speichersystemen (SYS.1.8.A18)

Es finden regelmäßige Audits aller eingesetzten Speichersysteme statt. Hierfür wurde in der <Institution> ein entsprechender Prozess etabliert. Zusätzlich ist geregelt, welche Sicherheitsreports, mit welchen Inhalten regelmäßig zu erstellen sind. Weiterhin wurde definiert, wie mit Abweichungen von Vorgaben umgegangen wird und wie oft und in welcher Tiefe Audits durchgeführt werden.

### Aussonderung von Speicherlösungen (SYS.1.8.A19)

Für die Aussonderung von Speicherlösungen wird eine Übergangsphase geplant. Werden ganze Speicherlösungen oder einzelne Komponenten einer Speicherlösung nicht mehr benötigt, werden alle darauf vorhandenen Daten auf andere Speicherlösungen übertragen. Es werden alle Nutzdaten und Konfigurationsdaten von ausgesonderten Speicherlösungen sicher gelöscht. Aus allen relevanten Dokumenten werden alle Verweise auf die außer Betrieb genommene Speicherlösung entfernt.

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

Für die eingesetzten Speicherlösungen wurde ein Notfallplan etabliert. Dieser beschreibt detailliert, wie in bestimmten Notfallsituation vorzugehen ist. Der Notfallplan enthält Handlungsanweisungen in Form von Maßnahmen und Kommandos, die die Fehleranalyse und Fehlerkorrektur unterstützen. Für die Fehlerbehebung werden geeignete Werkzeuge eingesetzt.

Es finden regelmäßige Übungen und Tests des Notfallplans statt. Die dabei erzeugten Daten werden sicher gelöscht.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Einsatz von Speicher-Pools zur Mandantentrennung (SYS.1.8.A21 - CIA)

Die Speicherressourcen werden den Mandanten aus unterschiedlichen Speicher-Pools zugewiesen. Hierbei ist darauf zu achten, dass ein Speichermedium immer nur einem einzigen Pool zugewiesen wird. Die logischen Festplatten (LUNs), die aus einem solchen Pool generiert werden, werden nur einem einzigen Mandanten zugeordnet.

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

Es wird eine hochverfügbare SAN-Lösung eingesetzt. Die eingesetzten Replikationsmechanismen entsprechen den Verfügbarkeitsanforderungen der <Institution> an die Speicherlösung. Die Konfiguration der Speicherlösung wird den Verfügbarkeitsanforderungen gerecht. Außerdem ist ein Test- und Konsolidierungssystem vorhanden.

### Einsatz von Verschlüsselung für Speicherlösungen (SYS.1.8.A23 - CI)

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

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

Um die Integrität der SAN-Fabric sicherzustellen, werden Protokolle mit zusätzlichen Sicherheitsmerkmalen eingesetzt. Es werden die Sicherheitseigenschaften folgender Protokolle berücksichtigt und entsprechende Konfigurationen verwendet:

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

### Mehrfaches Überschreiben der Daten einer LUN (SYS.1.8.A25 - CI)

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

### Absicherung eines SANs durch Hard-Zoning (SYS.1.8.A25 - CI)

Um SANs zu segmentieren, wird Hard-Zoning eingesetzt.