

DIN EN ISO/IEC 27040

ICS 35.040

Einsprüche bis 2016-05-04

Entwurf

**Informationstechnik –
IT-Sicherheitsverfahren –
Speichersicherheit (ISO/IEC 27040:2015);
Deutsche und Englische Fassung FprEN ISO/IEC 27040:2016**

Information technology –
Security techniques –
Storage security (ISO/IEC 27040:2015);
German and English version FprEN ISO/IEC 27040:2016

Technologie de l'information –
Techniques de sécurité –
Sécurité de stockage (ISO/IEC 27040:2015);
Version allemande et anglaise FprEN ISO/IEC 27040:2016

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2016-03-04 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal des DIN unter www.entwuerfe.din.de bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/stellungnahme oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin (Hausanschrift: Burggrafenstr. 6, 10787 Berlin).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 257 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Dieses Dokument (FprEN ISO/IEC 27040:2016) wurde vom Technischen Komitee ISO/IEC JTC 1/SC 27 „IT Security techniques“ erarbeitet, dessen Sekretariat vom DIN (Deutschland) gehalten wird. Auf Grundlage eines CEN/BT Beschlusses wurde ISO/IEC 27040:2015 im einstufigen Annahmeverfahren (UAP) als FprEN ISO/IEC 27040:2016 ohne Abänderung übernommen.

Das zuständige deutsche Spiegelgremium ist der Arbeitskreis NA 043-01-27-04 AK „IT-Sicherheitsmaßnahmen und Dienste“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung der FprEN ISO/IEC 27040 beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Für die in diesem Dokument zitierten Internationalen Normen wird im Folgenden auf die entsprechenden Deutschen Normen hingewiesen:

ISO/IEC 17788:2014	siehe	DIN ISO/IEC 17788
ISO/IEC 27000	siehe	DIN ISO/IEC 27000 ¹
ISO/IEC 27001:2013	siehe	DIN ISO/IEC 27001

Nationaler Anhang NA (informativ)

Literaturhinweise

DIN ISO/IEC 17788, *Informationstechnik — Cloud Computing — Übersicht und Vokabular (ISO/IEC 17788:2014)*

E DIN ISO/IEC 27000, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Überblick und Terminologie (ISO/IEC DIS 27000:2015)*

DIN ISO/IEC 27001, *Informationstechnik — IT-Sicherheitsverfahren — Informationssicherheits-Managementsysteme — Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014)*

¹ In Bearbeitung.

**Informationstechnik — IT-Sicherheitsverfahren — Speichersicherheit
(ISO/IEC 27040:2015)**

Technologie de l'information — Techniques de sécurité — Sécurité de stockage (ISO/IEC 27040:2015)

Information technology — Security — Storage security (ISO/IEC 27040:2015)

ICS:

Deskriptoren

Dokument-Typ: Europäische Norm
Dokument-Untertyp:
Dokument-Stage: Einstufiges Annahmeverfahren
Dokument-Sprache: D

STD Version 2.7g

Inhalt

	Seite
Europäisches Vorwort	4
Vorwort	5
Einleitung	6
1 Anwendungsbereich	7
2 Normative Verweisungen	7
3 Begriffe	7
4 Symbole und Abkürzungen	14
5 Überblick und Konzepte	18
5.1 Allgemeines	18
5.2 Speicherkonzepte	18
5.3 Einführung in die Speichersicherheit	19
5.4 Risiken der Speichersicherheit	21
5.4.1 Hintergrund	21
5.4.2 Bruch der Vertraulichkeit	22
5.4.3 Datenkorruption und Datenvernichtung	23
5.4.4 Vorübergehender oder dauerhafter Verlust des Zugriffs/der Verfügbarkeit	24
5.4.5 Versagen beim Erfüllen gesetzlicher, behördlicher oder rechtlicher Anforderungen	24
6 Unterstützende Maßnahmen	25
6.1 Allgemeines	25
6.2 Direct Attached Storage (DAS)	25
6.3 Speichernetzwerk	26
6.3.1 Hintergrund	26
6.3.2 Speichernetzwerke (SAN)	26
6.3.3 Netzwerkspeicher (NAS)	31
6.4 Speichermanagement	33
6.4.1 Hintergrund	33
6.4.2 Authentifizierung und Autorisierung	34
6.4.3 Schutz der Managementschnittstellen	35
6.4.4 Sicherheitsprüfung, Kontenführung und Überwachung	37
6.4.5 Härten von Systemen	39
6.5 Blockbasierter Speicher	40
6.5.1 Fibre-Channel-Speicher (FC-Speicher)	40
6.5.2 IP-Speicher	41
6.6 Dateibasierte Speicherung	42
6.6.1 NFS-basierte Netzwerkspeicher (NAS)	42
6.6.2 SMB/CIFS-basierte NAS	43
6.6.3 Parallele NFS-basierte NAS	43
6.7 Objekt-basierter Speicher	44
6.7.1 Cloud-Computing-Speicher	44
6.7.2 Objektbasiertes Speichergerät (OSD)	46
6.7.3 Content-Adressable-Storage (CAS)	47
6.8 Dienste für die Speichersicherheit	48
6.8.1 Sicheres Löschen von Daten	48
6.8.2 Vertraulichkeit von Daten	51
6.8.3 Daten-Reduzierung	54
7 Leitlinien für Design und Umsetzung der Speichersicherheit	55
7.1 Allgemeines	55

7.2	Designgrundsätze der Speichersicherheit	55
7.2.1	Konzept der gestaffelten Verteidigung	55
7.2.2	Sicherheits-Domains	56
7.2.3	Belastbarkeit des Designs	57
7.2.4	Sichere Initialisierung	57
7.3	Verlässlichkeit, Verfügbarkeit und Belastbarkeit von Daten	58
7.3.1	Verlässlichkeit	58
7.3.2	Verfügbarkeit	59
7.3.3	Backup und Vervielfältigung	59
7.3.4	Disaster-Recovery und Business Continuity (DR/BC)	60
7.3.5	Belastbarkeit	61
7.4	Datenhaltung	61
7.4.1	Langfristige Datenhaltung	61
7.4.2	Kurz- bis mittelfristige Datenhaltung	62
7.5	Vertraulichkeit und Integrität von Daten	63
7.6	Virtualisierung	66
7.6.1	Speichervirtualisierung	66
7.6.2	Speicher für virtualisierte Systeme	67
7.7	Überlegungen zu Design und Umsetzung	68
7.7.1	Themen zu Verschlüsselung und Schlüsselmanagement	68
7.7.2	Abgleichen von Speicher und Politik	69
7.7.3	Übereinstimmung	70
7.7.4	Sichere Mandantenfähigkeit	71
7.7.5	Sicherer autonomer Datenverkehr	72
Anhang A (normativ)	Sicheres Löschen von Datenträgern	74
A.1	Methoden zum sicheren Löschen von Datenträgern	74
A.2	Sicheres Löschen von verschiedenen Datenträgertypen	75
A.3	Leitlinien für Geräte zum kryptographischen Löschen	89
Anhang B (informativ)	Auswahl geeigneter Speichersicherheitsmaßnahmen	93
B.1	Kriterien zur Auswahl von Maßnahmen	93
B.1.1	Überblick	93
B.1.2	Datensensibilitätsklassen	94
B.1.3	Sicherheitsvorrangcodes	95
B.2	Zusammenfassung der Speichersicherheitsmaßnahmen	95
B.2.1	Unterstützende Maßnahmen für die Speichersicherheit	95
B.2.2	Leitfaden für Design und Umsetzung der Speichersicherheit	109
Anhang C (informativ)	Wichtige Sicherheitskonzepte	122
C.1	Authentifizierung	122
C.2	Autorisierung und Zugriffskontrolle	123
C.3	Selbstverschlüsselnde Festplatten (SED, en: Self-Encrypting Drives)	125
C.4	Sicheres Löschen	126
C.5	Protokollieren	128
C.6	N_Port_ID Virtualization (NPV)	128
C.7	Fibre-Channel-Sicherheit	129
C.7.1	Überblick	129
C.7.2	DH-CHAP-Authentifizierung	131
C.7.3	ESP_Header	132
C.7.4	CT_Authentication	132
C.7.5	FC-SP-Zoning	133
C.8	OASIS Key Management Interoperability Protocol (KMIP)	133
Literaturhinweise		137

Europäisches Vorwort

Der Text von ISO/IEC 27040:2015 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und auf Grundlage eines CEN/BT Beschlusses als FprEN ISO/IEC 27040:2016 übernommen.

Dieses Dokument ist derzeit zum einstufigen Annahmeverfahren vorgelegt.

Anerkennungsnotiz

Der Text von ISO/IEC 27040:2015 wurde vom CEN als FprEN ISO/IEC 27040:2016 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Internationale Organisationen, staatlich und nicht-staatlich, in Liaison mit ISO und IEC, nehmen ebenfalls an der Arbeit teil. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames technisches Komitee (JTC, en: joint technical committee), ISO/IEC JTC 1, eingerichtet.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Direktiven, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Direktiven, Teil 2 erarbeitet (siehe www.iso.org/directives).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der empfangenen Patenterklärungen (siehe www.iso.org/patents).

Jeder in diesem Dokument verwendete Handelsname wird als Information zum Nutzen der Anwender angegeben und stellt keine Anerkennung dar.

Eine Erläuterung der Bedeutung ISO-spezifischer Benennungen und Ausdrücke, die sich auf Konformitätsbewertung beziehen, sowie Informationen über die Beachtung der WTO-Grundsätze zu technischen Handelshemmnissen (TBT, en: Technical Barriers to Trade) durch ISO enthält der folgende Link: [Foreword - Supplementary information](#).

Das für dieses Dokument verantwortliche Komitee ist ISO/IEC JTC 1, *Information technology, SC 27, Security techniques*.

Einleitung

Viele Organisationen stehen vor der Herausforderung, Maßnahmen für den Datenschutz und die Datensicherheit umzusetzen, um eine Vielzahl an Anforderungen einzuhalten, einschließlich gesetzlicher und behördlicher Anforderungen. Zu häufig wird die Sicherheit von Speichersystemen und der Infrastruktur aufgrund von falschen Vorstellungen und unzureichenden Kenntnissen der Speichertechnologie oder, im Fall von Speichermanagern und Administratoren, aufgrund eines mangelnden Verständnisses der inhärenten Risiken oder der grundlegenden Sicherheitskonzepte außer Acht gelassen. Die Bilanz aus dieser Situation ist, dass digitale Ressourcen durch Bruch der Vertraulichkeit, vorsätzliche Datenbeschädigung, Datenerpressung oder andere böswillige Ereignisse unnötigerweise einem Risiko ausgesetzt werden.

Die Datenspeicherung wurde in einem Umfeld entwickelt, in dem die Sicherheit ein sekundäres Anliegen gewesen ist, da sie damals auf einer vereinzelter Konnektivität, speziellen Technologien und der physischen Sicherheit von Rechenzentren beruhte. Selbst als die Speicherkonnektivität sich weiterentwickelte und Technologien wie Speicherprotokolle mithilfe des Transmission Control Protocol/Internet Protocol (TCP/IP) zum Einsatz kamen, haben nur wenige Anwender von den inhärenten Sicherheitsfunktionen oder den empfohlenen Sicherheitsmaßnahmen Gebrauch gemacht.

Diese Internationale Norm liefert Leitlinien für die Speichersicherheit in einer Organisation, indem sie insbesondere die Anforderungen eines Informationssicherheits-Managementsystems (ISMS) nach ISO/IEC 27001 stützt. Diese Internationale Norm empfiehlt den Ansatz des Informationssicherheits-Risikomanagements nach ISO/IEC 27005. Es liegt im Ermessen der Organisation, ihren Ansatz für das Risikomanagement festzulegen, der beispielsweise vom Anwendungsbereich des ISMS, dem Kontext des Risikomanagements oder der Branche abhängt. In dem in dieser Internationalen Norm beschriebenen Rahmen können zahlreiche Vorgehensweisen angewendet werden, um die Anforderungen eines ISMS umzusetzen.

Diese Internationale Norm ist für Manager und Angestellte relevant, die sich mit dem Informationssicherheits-Risikomanagement innerhalb einer Organisation beschäftigen und, soweit zutreffend, für externe Parteien, die solche Aktivitäten unterstützen.

Die Ziele dieser Internationalen Norm sind folgende:

- sie soll auf die Risiken aufmerksam machen;
- sie soll Organisationen dabei helfen, ihre gespeicherten Daten besser zu sichern;
- sie soll eine Grundlage für das Auditieren, Gestalten und Überprüfen von Speichersicherheitsmaßnahmen liefern.

Es wird ausdrücklich betont, dass ISO/IEC 27040 weitere ausführliche Umsetzungsregeln der Speichersicherheitsmaßnahmen liefert, die in ISO/IEC 27002 auf grundlegend vereinheitlichter Ebene beschrieben werden.

Es sollte angemerkt werden, dass diese Internationale Norm kein Referenzdokument oder normatives Dokument für gesetzliche und behördliche Sicherheitsanforderungen ist. Nichtsdestotrotz betont sie die Bedeutung dieser Einflüsse, kann sie aber nicht gesondert auflisten, da sie vom jeweiligen Land, von der Geschäftsart usw. abhängig sind.

1 Anwendungsbereich

Diese Internationale Norm liefert ausführliche technische Leitlinien darüber, wie Organisationen eine angemessene Risikominderung umsetzen können, indem sie einen bewährten und gleichbleibenden Ansatz bei der Planung, Gestaltung, Dokumentation und Umsetzung der Datenspeichersicherheit anwenden. Die Speichersicherheit bezieht sich zum einen auf den Schutz (die Sicherheit) von Information bei ihrer Speicherung und zum anderen auf die Sicherheit der Informationen bei ihrer Übertragung über die speicherbezogenen Kommunikationsverknüpfungen. Die Speichersicherheit betrifft die Sicherheit von Geräten und Datenträgern, die Sicherheit von Managementaktivitäten im Zusammenhang mit diesen Geräten und Datenträgern, die Sicherheit von Anwendungen und Diensten und die Sicherheit für den Endanwender während der Lebensdauer dieser Geräte und Datenträger und nach dem Ende von deren Nutzungsdauer.

Die Speichersicherheit ist für jede Person von Bedeutung, die Datenspeichergeräte, Speichermedien und Speichernetzwerke besitzt, betreibt oder nutzt. Neben den Führungskräften und Administratoren, die eine besondere Verantwortungen für die Informationssicherheit, die Speichersicherheit oder den Speicherbetrieb tragen, oder die für die Entwicklung des gesamten Sicherheitsprogramms und der Sicherheitspolitik einer Organisation verantwortlich sind, zählen auch hochrangige Führungskräfte, Käufer von Speicherprodukten und -diensten und andere nicht technische Führungskräfte oder Anwender dazu. Sie ist außerdem für jede Person von Bedeutung, die an der Planung, Gestaltung und Umsetzung von architekturbezogenen Aspekten der Speichernetzwerksicherheit beteiligt sind.

Diese Internationale Norm liefert einen Überblick über die Speichersicherheitskonzepte und die damit zusammenhängenden Definitionen. Sie enthält Leitlinien zu den Aspekten der Bedrohung, Gestaltung und Kontrolle, die mit typischen Speicherszenarien und Bereichen der Speichertechnologien in Zusammenhang stehen. Außerdem verweist sie auf andere Internationale Normen und Technische Berichte, die sich mit vorhandenen Praktiken und Techniken beschäftigen, die im Sinne der Speichersicherheit angewendet werden können.

2 Normative Verweisungen

Die folgenden Dokumente, die in diesem Dokument teilweise oder als Ganzes zitiert werden, sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

ITU-T Y.3500 | ISO/IEC 17788:2014, *Information technology — Cloud computing — Overview and vocabulary*

ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 27000, ISO/IEC 27005 und die folgenden Begriffe.

3.1

Block

Einheit auf Festplatten und Bandgeräten (3.14), in der Daten *gespeichert* (3.50) und abgerufen werden

3.2

(logisches) Löschen

sicheres Löschen (3.38) mithilfe logischer Techniken von Daten an allen von Anwendern adressierbaren Speicherorten zum Schutz vor einfachen, nicht invasiven Datenwiederherstellungstechniken, die dieselbe Schnittstelle nutzen, die auch für den Anwender zugänglich ist

3.3

Kompression

Komprimierung

Prozess, bei dem redundante Elemente in digitalen Daten entfernt werden, um das zu *speichernde* (3.50) oder zu übertragende Datenvolumen zu verringern

[QUELLE: ISO/TR 12033:2009, 3.1]

Anmerkung 1 zum Begriff: Zur *Speicherung* (3.43) ist eine verlustfreie Komprimierung (d. h. Komprimierung mithilfe einer Technik, die den gesamten Inhalt der Originaldaten beibehält und bei der die Originaldaten exakt rekonstruiert werden können) erforderlich.

3.4

kryptographisches Löschen

Methode zum *sicheren Löschen* (3.37), bei der der Verschlüsselungscode für die verschlüsselten *Zieldaten* (3.52) *sicher gelöscht* (3.38) wird, wodurch das Wiederherstellen von entschlüsselten *Zieldaten* (3.52) unmöglich ist

3.5

Kryptoperiode

Verschlüsselungszeitraum

festgelegter Zeitraum, in dem ein bestimmter kryptographischer Schlüssel zum Einsatz freigegeben ist, oder in dem der kryptographische Schlüssel im jeweiligen System aktiv bleiben kann

[QUELLE: ISO 16609:2004, 3.9]

3.6

Data-at-Rest

Daten, die in einem stabilen, *nichtflüchtigen Speicher* (3.30) *gespeichert* (3.50) sind

3.7

Bruch der Vertraulichkeit

Beeinträchtigung der Sicherheit, die zur zufälligen oder unrechtmäßigen *Zerstörung* (3.13), zum Verlust, zur Änderung, zur unberechtigten Offenlegung von oder den Zugang zu geschützten Daten führt, die übertragen, *gespeichert* (3.50) oder anderweitig verarbeitet werden

3.8

Data-in-Motion

Daten, die von einem Ort an einen anderen übertragen werden

Anmerkung 1 zum Begriff: Diese Transfers beziehen üblicherweise zugängliche Schnittstellen ein und sie umfassen keine internen Übertragungen (d. h. niemals außerhalb einer Schnittstelle, eines Chips oder Geräts exponierte).

3.9

Datenintegrität

Eigenschaft, die angibt, dass die Daten nicht auf unbefugte Weise geändert oder vernichtet wurden

[QUELLE: ISO 7498-2:1989, 3.3.21]

3.10

Deduplikation

Methode, die den *Speicherbedarf* (3.43) verringert, indem sie redundante Daten eliminiert, die durch einen Hinweis auf die spezifische Datenkopie ersetzt werden

Anmerkung 1 zum Begriff: Die Deduplikation wird mitunter als eine Form der *Kompression* (3.3) angesehen.

3.11

Entmagnetisieren

Degaußen

Vorgang, bei dem Daten unlesbar gemacht werden, indem ein starkes Magnetfeld auf die Datenträger einwirkt

3.12

Zerstören

sicheres Löschen (3.38) mithilfe physischer Techniken, die eine Wiederherstellung mit Labortechniken nach dem neuesten Stand der Technik unmöglich machen und dazu führen, dass die Datenträger im Anschluss daran nicht mehr zur *Speicherung* (3.43) von Daten genutzt werden können

Anmerkung 1 zum Begriff: *Zerteilen* (3.15), *Veraschen* (3.21), *Einschmelzen* (3.25), *Pulverisieren* (3.34) und *Schreddern* (3.41) sind Zerstörungsformen zum *sicheren Löschen* (3.37).

3.13

Zerstörung

Ergebnis der durchgeführten Maßnahmen, mit denen sichergestellt wird, dass Datenträger nicht mit ihrem ursprünglichen Verwendungszweck wiederverwendet werden können und dass eine Wiederherstellung von Informationen praktisch unmöglich oder unerschwinglich ist

3.14

Gerät

mechanische, elektrische oder elektronische Vorrichtung mit einem bestimmten Zweck

[QUELLE: ISO/IEC 14776-372:2011, 3.1.10]

3.15

Zerteilen

Zerstören (3.12) durch Zerlegen der Datenträger in ihre Einzelteile

3.16

elektronisch gespeicherte Informationen

Daten oder Informationen beliebiger Art und aus einer beliebigen Quelle, deren temporäre Existenz dokumentiert wird, indem sie in oder auf einem elektronischen Medium *gespeichert* (3.50) werden

Anmerkung 1 zum Begriff: Zu den elektronisch gespeicherten Informationen (ESI, en: Electronically Stored Information) zählen herkömmliche E-Mails, Notizen, Briefe, Tabellen, Datenbanken, Textverarbeitungsdokumente, Präsentationen und andere elektronische Formate, die üblicherweise auf einem Computer zu finden sind. Zu den ESI zählen außerdem die system-, anwendungs- und dateibezogenen *Metadaten* (3.26), wie Zeitstempel, Änderungsverlauf, Dateityp usw.

Anmerkung 2 zum Begriff: Elektronische Medien können unter anderem in Form von *Speichergeräten* (3.45) und *Speicherelementen* (3.47) vorliegen.

3.17

Fibre Channel

serielle I/O-Schnittstelle, die mehrere Protokolle unterstützen kann, einschließlich des Zugriffs auf den offenen *Systemspeicher* (3.43), Zugriff auf den *Mainframe-Speicher* (3.43) und Netzwerkverbindungen

Anmerkung 1 zum Begriff: Fibre Channel unterstützt Point-to-Point-, Arbitrated-Loop- und Switched-Fabric-Topologien mit einer Mischung aus Kupfer- und LWL-Übertragungsleitungen bei einer Geschwindigkeit von 1 Gigabit je Sekunde bis über 10 Gigabits je Sekunde.

3.18

Fibre-Channel-Protokoll

serielles SCSI-Transportprotokoll (en: Small Computer System Interface), das an *Fibre-Channel*-Schnittstellen (3.17) zum Einsatz kommt

3.19

Gateway

Gerät (3.14), das ein Protokoll in ein anderes Protokoll umwandelt

3.20

in-band

Kommunikation oder Übertragung, die mit einer vorher festgelegten Kommunikationsmethode oder innerhalb eines vorher festgelegten Kommunikationskanals stattfindet

Anmerkung 1 zum Begriff: Die Kommunikationen oder Übertragungen nehmen oftmals die Form eines separaten Protokolls an, z. B. ein Managementprotokoll auf demselben Datenträger wie das primäre Datenprotokoll.

3.21

Veraschen

Zerstören (3.12) durch vollständiges Verbrennen der Datenträger zu Asche

3.22

Schadsoftware

(en: Malware)

schädliche Software, die speziell dafür ausgelegt ist, ein System zu beschädigen oder zu stören und die Vertraulichkeit, Integrität oder Verfügbarkeit anzugreifen

Anmerkung 1 zum Begriff: Computerviren und Trojaner sind Beispiele für Schadsoftware.

[QUELLE: ISO/IEC 27033-1:2009, 3.22]

3.23

durchschnittlicher Ausfallabstand

erwartete Zeit zwischen zwei aufeinanderfolgenden Ausfällen in einem System oder Bauteil

[QUELLE: ISO/IEC/IEEE 24765:2010, 3.1713, modifiziert — im Englischen wurde die Benennung großgeschrieben]

3.24

durchschnittliche Reparaturdauer

erwartete oder beobachtete Zeit, um ein fehlerhaftes System oder ein fehlerhaftes Bauteil in seinen Normalzustand zurückzusetzen

[QUELLE: ISO/IEC/IEEE 24765:2010, 3.1714, modifiziert — im Englischen wurde die Benennung großgeschrieben]

3.25

Einschmelzen

Zerstören (3.12) durch Ändern des Aggregatzustands der Datenträger von fest zu flüssig, üblicherweise durch den Einsatz von Wärme

3.26

Metadaten

Daten, die andere Daten definieren und beschreiben

[QUELLE: ISO/IEC 11179-1:2004, 3.2.16]

3.27

Multifaktor-Authentifizierung

Authentifizierung mit mindestens zwei der folgenden Faktoren:

- Wissensfaktor, „etwas, das eine Person weiß“;
- Besitzfaktor, „etwas, das eine Person hat“;
- Biometriefaktor, „etwas, das eine Person ist oder ausmacht“

[QUELLE: ISO 19092:2008, 4.42]

3.28

Mandantenfähigkeit

derartige Zuordnung von physischen oder virtuellen Ressourcen, dass verschiedene Mandanten und deren Berechnungen und Daten voneinander getrennt sind und kein gegenseitiger Zugriff möglich ist

[QUELLE: Empfehlung ITU-T Y.3500 | ISO/IEC 17788:2014, 3.2.27]

3.29

Netzwerkspeicher

(en: Network Attached Storage)

Speichergerät (3.45) oder -system, das mit einem Netzwerk verbunden ist und Computersystemen den Zugriff auf Dateien ermöglicht

3.30

nichtflüchtiger Speicher

Speicher (3.43), dessen Inhalte auch nach dem Trennen der Stromzufuhr erhalten bleiben

3.31

out-of-band

Kommunikation oder Übertragung, die außerhalb einer vorher festgelegten Kommunikationsmethode oder eines vorher festgelegten Kommunikationskanals stattfindet

3.32

Over-Provisioning

Technik, die von *Speicherelementen* (3.47) und *Speichergeräten* (3.45) genutzt wird und bei der ein Teil der verfügbaren Datenträger über die Schnittstelle freigegeben wird

Anmerkung 1 zum Begriff: *Speichermedien* (3.48) werden intern und unabhängig vom *Speicherelement* (3.47) genutzt, um die Leistung, Beständigkeit oder Verlässlichkeit zu verbessern.

3.33

Verschlüsselungspunkt

Stelle in der Informations- und Kommunikationstechnologie-Infrastruktur (IKT), an der Daten auf ihrem Weg in den *Speicher* (3.43) verschlüsselt werden und, im umgekehrten Fall, Daten entschlüsselt werden, wenn auf sie im *Speicher* (3.43) zugegriffen wird

Anmerkung 1 zum Begriff: Der Verschlüsselungspunkt gilt nur für *Data-at-rest* (3.6).

3.34

Pulverisieren

Zerstören (3.12) durch Zermahlen der Datenträger zu Pulver oder Staub

3.35

(physisches) Löschen

sicheres Löschen (3.38) mithilfe von physischen Techniken, die durch Einsatz von Labortechniken auf dem neuesten Stand der Technik eine Wiederherstellung unmöglich machen, aber das *Speichermedium* (3.48) in einem potentiell wiederverwendbaren Zustand erhalten

3.36

Verlässlichkeit

Fähigkeit eines Systems oder einer Systemkomponente, seine bzw. ihre geforderten Funktionen unter den angegebenen Bedingungen über einen festgelegten Zeitraum auszuführen

[QUELLE: ISO/IEC/IEEE 24765:2010, 3.2467, modifiziert — Die zweite Definition von ISO/IEC 9126-1:2001 und der Verweis wurden nicht aufgenommen.]

3.37

sicheres Löschen

Prozess oder Methode zum *sicheren Löschen* (3.38)

3.38

sicher löschen

unmöglich machen des Zugriffs auf *Zieldaten* (3.52) auf dem *Speichermedium* (3.48) bis zu einem gewissen Aufwand

Anmerkung 1 zum Begriff: *Logisches Löschen* (3.2), *physisches Löschen* (3.35) und *Zerstören* (3.12) sind Maßnahmen, die umgesetzt werden können, um ein *Speichermedium* (3.48) *sicher zu löschen* (3.38).

3.39

sichere Mandantenfähigkeit

Art der *Mandantenfähigkeit* (3.28), die Sicherheitsmaßnahmen einsetzt, um ausdrücklich vor dem *Bruch der Vertraulichkeit* (3.7) zu schützen, und die eine Validierung dieser Maßnahmen für eine ordnungsgemäße Governance vornimmt

Anmerkung 1 zum Begriff: Eine sichere Mandantenfähigkeit liegt vor, wenn das Risikoprofil eines einzelnen Mandanten nicht höher ist als es in einer zugehörigen Einzelmandantenumgebung wäre.

Anmerkung 2 zum Begriff: In sehr sicheren Umgebungen wird sogar die Identität der Mandanten geheim gehalten.

3.40

Sicherheitsstufe

Nummer in Verbindung mit dem Aufwand, der erforderlich ist, um einen kryptographischen Algorithmus oder ein System auszuschalten

3.41

Schreddern

Zerstören (3.12) durch Zerschneiden oder Zerreißen von Datenträgern in kleine Stücke

3.42

einzelner Ausfallpunkt

Element oder Komponente eines Systems, ein Pfad in einem System, oder ein System, das im Fall eines Ausfalls dazu führt, dass das gesamte System oder eine Reihe von Systemen nicht mehr in der Lage ist, die primären Funktionen auszuführen

Anmerkung 1 zum Begriff: Ein einzelner Ausfallpunkt wird oftmals als Designfehler kritischer Elemente angesehen.

3.43

Speicher

Speicherung

Gerät (3.14), Funktion oder Dienst, das/die/der die Dateneingabe und den Datenabruf unterstützt

3.44

Speichernetzwerk

Storage Area Network

Netzwerk, dessen wesentlicher Zweck darin besteht, Daten zwischen Computersystemen und *Speichergeräten* (3.45) und zwischen verschiedenen *Speichergeräten* (3.45) zu übertragen

Anmerkung 1 zum Begriff: Ein Speichernetzwerk (SAN, en: Storage Area Network) besteht aus einer Kommunikationsinfrastruktur, die physische Verbindungen bereitstellt, und einer Managementschicht (Management Layer), die die Verbindungen, *Speichergeräten* (3.45) und Computersystemen so organisiert, dass der Datentransfer sicher und beständig abläuft.

3.45

Speichergerät

jedes *Speicherelement* (3.47) oder eine Gruppierung von *Speicherelementen* (3.47), die hauptsächlich zur *Datenspeicherung* (3.43) und Datenlieferung vorgesehen und gebaut sind

3.46

Speicher-Ökosystem

komplexes System aus eigenständigen Komponenten, die zusammen agieren, um die *Speicherdienste* (3.43) und Speicherfähigkeiten bereitzustellen

Anmerkung 1 zum Begriff: Zu den Komponenten zählen häufig *Speichergeräte* (3.45), *Speicherelemente* (3.47), Speichernetzwerke, Speichermanagement- und andere Informations- und Kommunikationstechnologie-Infrastrukturen (IKT).

3.47

Speicherelement

Bauteil zur Gestaltung von *Speichergeräten* (3.45), das an der *Datenspeicherung* (3.43) und Datenlieferung beteiligt ist.

Anmerkung 1 zum Begriff: Übliche Beispiele für ein Speicherelement sind Festplatten oder Bandgeräte.

3.48

Speichermedium

Speichermedien

Material, auf dem *elektronisch gespeicherte Informationen* (3.16) oder digitale Daten aufgezeichnet sind bzw. aufgezeichnet werden können

3.49

Speichersicherheit

Umsetzung von physischen, technischen und administrativen Maßnahmen zum Schutz von Speichersystemen und der Infrastruktur sowie der darauf *gespeicherten* (3.50) Daten

Anmerkung 1 zum Begriff: Die Speichersicherheit konzentriert sich auf den Schutz von Daten (und deren Speicherinfrastruktur) vor unbefugter Offenlegung, Modifikation oder Vernichtung bei gleichzeitiger Sicherstellung ihrer Verfügbarkeit für befugte Anwender.

Anmerkung 2 zum Begriff: Diese Maßnahmen dürfen präventiv, detektivisch, korrigierend, abwehrend, wiederherstellend oder kompensierend sein.

3.50

Speichern

Aufzeichnen von Daten in einem *flüchtigen Speicher* (3.53) oder in einem *nichtflüchtigen Speicher* (3.30)

3.51

starke Authentisierung

Authentisierung mittels kryptographisch abgeleiteter Identitätsnachweise

[QUELLE: ISO/TS 22600-1:2006, 2.23]

3.52

Zieldaten

Informationen, die von einem bestimmten Prozess abhängen und in der Regel die meisten oder alle Informationen auf einem *Speichermedium* (3.48) enthalten

3.53

flüchtiger Speicher

Speicher (3.43), dessen Inhalte nach dem Trennen der Stromzufuhr nicht erhalten bleiben

3.54

schwacher Schlüssel

Schlüssel, der mit einigen Aspekten eines bestimmten Verschlüsselungsverfahrens so interagiert, dass dadurch die *Sicherheitsstufe* (3.40) des Verschlüsselungsverfahrens geschwächt wird

4 Symbole und Abkürzungen

ACE	Access Control Entry
ACL	Access Control List
AD	Active Directory
AES	Advanced Encryption Standard
ATA	Advanced Technology Attachment
BC	Business Continuity
BCM	Business Continuity Management
CAS	Content Addressable Storage
CBC	Cipher Block Chaining
CCM	Counter with Cipher block chaining Message authentication code
CDMI	Cloud Data Management Interface
CDP	Continuous Data Protection
CHAP	Challenge Handshake Authentication Protocol
CIFS	Common Internet File System
CLI	Command Line Interface
CNA	Converged Network Adaptor
DAC	Discretionary Access Control
DAS	Direct Attached Storage
DDoS	Distributed Denial of Service
DH-CHAP	Diffie-Hellman Challenge Handshake Authentication Protocol
DES	Data Encryption Standard
DLM	Data Lifecycle Management
DMZ	De-Militarized Zone
DNS	Domain Name System
DoS	Denial of Service
DR	Disaster Recovery

DRP	Disaster Recovery Planning
EHR	Electronic Healthcare Record
ESI	Electronically Stored Information
ESP	Encapsulating Security Payload
FC	Fibre Channel
FC-SP	Fibre Channel – Security Protocol
FCAP	Fibre Channel Certificate Authentication Protocol
FCEAP	Fibre Channel Extensible Authentication Protocol
FCIP	Fibre Channel over TCP/IP
FCoE	Fibre Channel over Ethernet
FCP	Fibre Channel Protocol
FCPAP	Fibre Channel Password Authentication Protocol
FCS	Fixed Content Storage
FDE	Full Disk Encryption
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HAMR	Heat Assisted Magnetic Recording
HBA	Host Bus Adapter
HDD	Hard Disk Drive
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communications Technology
ID	IDentifier
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
ILM	Information Lifecycle Management
I/O	Input/Output
IP	Internet Protocol
IPS	Intrusion Prevention System
IPOCM	Incident Preparedness and Operational Continuity Management
IPsec	Internet Protocol Security
IRBC	ICT Readiness for Business Continuity
iSCSI	Internet Small Computer Systems Interface
ISL	Inter-Switch Link
ISMS	Information Security Management System
iSNS	Internet Storage Name Service

KEK	Key Encryption Key
KMIP	Key Management Interoperability Protocol
LAN	Local Area Network
LBA	Logical Block Address
LDAP	Lightweight Directory Access Protocol
LUN	Logical UNit
MAC	Mandatory Access Control
MD5	Message-Digest algorithm 5
MEK	Media Encryption Key
MTBF	Mean Time Between Failure
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
NAS	Network Attached Storage
NAT	Network Address Translation
NFS	Network File System
NIC	Network Interface Card
NIS	Network Information Service
NPIV	N_Port_ID Virtualization
NTLM	NT LAN Manager
NTP	Network Time Protocol
NVM	Non-Volatile Memory
OASIS	Organization for the Advancement of Structured Information Standards
OID	Object Identifier
OSD	Object-based Storage Device
PCIe	Peripheral Component Interconnect express
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
pNFS	parallel Network File System
PRNG	Pseudo-Random Number Generator
RADIUS	Remote Authentication Dial In User Service
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RBAC	Role-Based Access Control
REST	REpresentational State Transfer
RNG	Random Number Generator
ROM	Read-Only Memory
RPC	Remote Procedure Call

SAN	Storage Area Network
SAS	Serial Attached SCSI
SCSI	Small Computer System Interface
SED	Self-Encrypting Drive
SHA	Secure Hash Algorithm
SIEM	Security Information and Event Management
SLP	Service Locator Protocol
SMB	Server Message Block
SMI-S	Storage Management Initiative – Specification
SNIA	Storage Networking Industry Association
SNMP	Simple Network Management Protocol
SOHO	Small Office/Home Office
SSC	Security Subsystem Class
SSD	Solid State Drive
SSH	Secure SHell
SSHD	Solid State Hard Drive
SSO	Single Sign-On
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VM	Virtual Machine
VSAN	Virtual Storage Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WORM	Write Once Read Many
WWN	World Wide Name
WWPN	World Wide Port Name
XEX	Xor-Encrypt-Xor
XTS	XEX-based Tweaked-codebook mode with ciphertext Stealing

5 Überblick und Konzepte

5.1 Allgemeines

Die Datenspeicherung oder Informationsspeicherung auf Computern, häufig nur als Speicherung bezeichnet, bezieht sich auf Computerkomponenten, Speicherelemente, Speichergeräte und Speichermedien, die elektronisch gespeicherte Informationen (ESI) oder digitale Daten enthalten. Obwohl flüchtige und auch nichtflüchtige Speicherformen existieren, beschäftigt sich diese Internationale Norm hauptsächlich mit den nichtflüchtigen Speichern. Der Speicher ist eine Hauptfunktion und ein wesentlicher Bestandteil von Computern.

Um die Speicherinfrastruktur abzusichern, ist eine klare Vorstellung der Speichertechnologien und -konzepte notwendig. Außerdem sind die Arten der Sicherheitsmaßnahmen und das Verständnis darüber, wie sie die Speichertechnologie beeinflussen und mit ihnen interagieren, ebenfalls von Bedeutung. Letztendlich werden die Bedrohungen für diese Infrastruktur und die erheblichen Risiken, die durch diese Bedrohungen entstehen, bei den Bemühungen, die Speicherinfrastruktur oder einzelne Speichersysteme zu sichern, berücksichtigt.

5.2 Speicherkonzepte

In der Vergangenheit wurde der Speicher lediglich in Form von Festplatten (HDD, en: Hard Disk Drives) und Bandlaufwerken angesehen, die zum Speichern von Daten mit einem Computer verbunden sind. Dieser Ansatz, der in der Regel als Direct Attached Storage (DAS) bezeichnet wird, kommt heute noch in den Rechenzentren von Unternehmen und in Kleinbüros/Heimbüros (SOHO, en: Small Office/Home Office) zum Einsatz. Es stehen alternative Ansätze zur Verfügung, die auf der Verwendung von Speichernetzwerktechnologien basieren und die sich als ausgereifte Technologien herauskristallisiert haben, um Lösungen im Hinblick auf das Verwalten, Verbinden, Schützen, Sichern, Teilen und Optimieren der Datenspeicherung anzubieten. Diese Lösungen werden immer besser umsetzbar und kostengünstiger, da sich die Speichertechnologie von nicht intelligenten internen und externen DAS zu intelligenten Netzwerkspeichern weiterentwickelt hat. Die Vernetzung führt bei diesen Lösungen jedoch zu einer größeren Angriffsfläche und erfordert zusätzliche Aufmerksamkeit im Hinblick auf die Sicherheit.

Heutige Speicherlösungen umfassen einige oder alle der folgenden Elemente:

- Speicher-Arrays mit Speichernetzwerk-Schnittstellen;
- Netzwerkspeicher (NAS);
- Content Addressable Storage (CAS);
- objektbasierte Speichergeräte (OSD; Object-based Storage Devices);
- Backup-/Wiederherstellungssysteme, Continuous Data Protection (CDP) usw. (d. h. Datenschutzsysteme).

Der Speicher hat sich zu einer herausragenden und eigenständigen Schicht in der Informations- und Kommunikationstechnologie-Infrastruktur (IKT) in unternehmensweiten und mittelgroßen Computing-Umgebungen entwickelt. Die Anforderungen an diese Umgebungen überschreiten häufig die einfachen Datenspeicherfähigkeiten. Beispiele der Anwendungen und Funktionen, die die Entwicklung neuer Speichertechnologien vorantreiben, sind:

- Teilen von umfangreichen Speicherressourcen (gemessen in Petabytes und Exabytes) zwischen mehreren Systemen über Netzwerke;
- Backups, für die keine lokalen Netzwerke (LAN, en: Local Area Network) erforderlich sind;

- rechnerferne, desastertolerante On-line-Spiegelung von auftragsentscheidenden Daten;
- Ansammlung von fehlertoleranten Anwendungen und zugehörigen Systemen um eine einzelne Datenkopie;
- Langzeitaufbewahrung von sensiblen oder wertvollen Geschäftsinformationen;
- dezentrale Datenbanken und Dateisysteme;
- Unterstützung bei der Übereinstimmung mit behördlichen und gesetzlichen Anforderungen;
- Unterstützung für zentrale Datenbestände für die schnelle Wiederherstellung (z. B. Backups) und Archivierung.

5.3 Einführung in die Speichersicherheit

Die Speichersicherheit beschäftigt sich mit den physischen, technischen und administrativen Maßnahmen sowie mit den präventiven, detektivischen und korrigierenden Maßnahmen im Zusammenhang mit den Speichersystemen und der Infrastruktur, wie in 5.2 beschrieben. Die Speichersicherheit kann auch die Einführung von speziellen Technologien erzwingen, wie z. B.:

- sicheres Löschen von Speichermedien;
- Sicherheit bei der Virtualisierung;
- selbstverschlüsselnde Festplatten (siehe C.3), wie HDD, Solid State Drives (SSD) und Solid State Hard Drives (SSHD);
- grundlegende Managementdienste;
- Dienste für die Datenauthentizität und Datenintegrität;
- Schutz von Data-in-Motion (Verschlüsselung und Datenreduktion);
- Verzeichnisdienste und andere Anwendermanagementsysteme.

Für ein besseres Verständnis von Sicherheitsfragen und Sicherheitsimplikationen bei der Speicherung sollte bekannt sein, wie und warum die jeweiligen Speichertechnologien eingesetzt werden. Als Ausgangspunkt ist Folgendes zu betrachten:

- Die Speichersysteme können als Knoten in Speichernetzwerken agieren, die unter anderem auf Technologien wie Transmission Control Protocol/Internet Protocol (TCP/IP), Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) und InfiniBand basieren können. Die potentiellen Bedrohungen können deutlich variieren, was auf die jeweilige Netzwerktechnologie sowie die angewendeten Topologien zurückzuführen ist.
- Im Speicher erfolgt die Repräsentation von und der Zugriff auf Daten in der Regel entweder in Form von Blockdaten oder als Dateien/Objekte; es gibt deutliche Unterschiede zwischen diesen beiden Speicher- methoden. Ebenso können die Sicherheitsmaßnahmen jeder dieser Methoden grundlegende Unterschiede aufweisen, besonders im Hinblick auf die Zugriffskontrollen, Verschlüsselung und Daten- integrität.
- Bei normalen Speichervorgängen verfügen viele Speichergerätetypen über eine höhere interne Medien- leistung als durch die Schnittstelle freigegeben wird. SSDs und SSHDs sind häufig überdimensioniert (Over-Provisioning), wobei die Daten intern zwischen physischen Medienbereichen verschoben werden können, um Verzögerungszeiten beim Schreiben zu verbessern. HDDs enthalten oftmals freie Bereiche, in denen die Daten intern zwischen physischen Medienbereichen verschoben werden können, wenn ein temporäres Zugriffsproblem auftritt. Anwenderdaten können in diesen Bereichen erhalten bleiben, selbst nachdem das Gerät über seine Schnittstelle beschrieben wurde. Solche Geräte dürfen nicht durch Überschreiben über die Schnittstelle logisch gelöscht werden.

- Das Speichermanagement ist sowohl ein Element der Speicherinfrastruktur als auch eine Funktion, die auf zahlreichen Systemen ausgeführt wird. Erfahrene Anwender nehmen üblicherweise Änderungen an den Konfigurationen vor, dimensionieren den Speicher und nehmen eine Abstimmung und Überwachung usw. der Infrastruktur vor. Ein Teil der Managementfunktionen kann aus der Ferne durchgeführt werden und eine Drittpartei beteiligen, wie z. B. die Herstellerunterstützung.
- Die Datenverfügbarkeit und Datenintegrität sind grundlegende Faktoren der Speicherarchitektur einer Organisation, weshalb es im Hinblick auf die Sicherheit wichtig ist, dass sie eher eine Ergänzung anstatt eines Kompromisses darstellen, und dass Hochverfügbarkeitsmaßnahmen nicht negiert werden, indem Choke-Points und zusätzliche einzelne Ausfallpunkte eingesetzt werden.
- Viele Organisationen setzen umfangreiche Strategien für die Ausfallsicherheit ihrer Daten ein, die fester Bestandteil ihrer Pläne für die Disaster Recovery (DR) und Business Continuity (BC) sind. Sicherheitsmechanismen, wie die Verschlüsselung von Data-at-Rest, müssen mit großer Sorgfalt umgesetzt werden, um sicherzustellen, dass die Strategien für die Ausfallsicherheit nicht beeinträchtigt werden.
- Die Speichervirtualisierung kann auf verschiedene Weisen erfolgen und an verschiedenen Punkten der Speicherinfrastruktur umgesetzt werden. Diese Virtualisierung kann die physischen Details im Zusammenhang mit der Präsentation des Speichers verdecken (z. B. eine Logical Unit oder ein Dateisystem zum Server), die eigentliche Kapazität eines Gerätes verdecken, eine konzeptbezogene autonome Datenverschiebung vornehmen (wie mehrschichtige Speicher), oder die Speicherinfrastruktur vollkommen abstrahieren (z. B. Cloud-Computing-Speicher). Das Gleichgewicht zwischen Sicherheit und Virtualisierung, damit sie nebeneinander bestehen können, erfordert eine sorgfältige Planung und Auswahl der richtigen Technologien.
- Die Datenzuwachsgeschwindigkeit treibt in einigen Organisationen den vermehrten Einsatz von Datenspeichertechnologien voran. Alternativ zum Erwerb von zusätzlichen Speichern wenden Organisationen Technologien zur Datenreduzierung an, wie Komprimierung und Deduplikation. Diese Technologien zur Datenreduzierung können jedoch durch Verschlüsselungsmechanismen der Data-at-Rest beeinflusst werden, die wiederum Probleme im Hinblick auf die Datenintegrität während DR- und BC-Operationen hervorrufen können.
- Im Rahmen der normalen Datenschutzstrategie werden letztendlich viele Datenkopien erstellt (z. B. Replikationen zwischen Systemen und Seiten, Backups, Speicherauszüge usw.). Diese Kopien müssen angemessen geschützt werden, während sie in Benutzung sind, und anschließend sicher gelöscht werden, wenn deren Nutzen endet.
- Sensible Daten und Daten von hohem Wert müssen häufig mithilfe von Mechanismen, wie der Internet Protocol Security (IPsec), geschützt werden, wenn sie zwischen Systemen übertragen werden. IPsec kann negative Auswirkungen auf die Anwendung bestimmter Technologien haben, wie Network Address Translation (NAT), Intrusion Detection System (IDS) und Intrusion Prevention System (IPS), oder auf andere Systeme, die einen tieferen Einblick in die Netzwerkauslastung besitzen. Ob IPsec oder andere Schutzmaßnahmen für Data-in-Motion zum Einsatz kommen, kann von den Abwägungen abhängen, die möglicherweise den Wert anderer Technologien aufheben oder davon, wo sie im Netzwerk angewendet werden.
- Viele Organisationen verwenden eine Verschlüsselung von Data-at-Rest, um sensible Daten und Daten von hohem Wert zu schützen. Die spezifischen Verschlüsselungsmechanismen und der Verschlüsselungspunkt sind wichtige Faktoren für den tatsächlichen Datenschutz sowie für das Erfüllen von Anforderungen.
- Der erfolgreiche Einsatz der Verschlüsselung hängt häufig vom ordnungsgemäßen Lifecycle-Management des Schlüsselmaterials ab. Dazu zählt die korrekte Generierung von Schlüsseln, die sichere Speicherung und Übertragung des Schlüsselmaterials, das Kopieren von Schlüsseln als Teil der üblichen Strategie zur Sicherstellung der Datenverfügbarkeit, und die ordnungsgemäße Entsorgung des Schlüsselmaterials, wenn es nicht mehr gebraucht wird. Die Sensibilität und die Wichtigkeit der zu schützenden Daten dürfen ebenfalls in den Schlüssel-Management-Ansatz einbezogen werden.

Eine angemessene Vertraulichkeit, Integrität und Verfügbarkeit von Daten sicherzustellen, die auf derzeitigen und künftigen Speichertechnologien gespeichert sind und von denen aus auf sie zugegriffen wird, erfordert aufeinander abgestimmte Aktionen auf dieser IKT-Schicht. Viele dieser Sicherheitsaktionen konzentrieren sich auf Folgendes:

- Schutz des Speichermanagements (Operationen und Schnittstellen);
- Sicherstellen eines angemessenen Managements von Zugangsdaten und Vertrauenswürdigkeiten;
- Schutz von Datenbackup- und Wiederherstellungsressourcen;
- Schutz von Data-in-Motion;
- Schutz von Data-at-Rest;
- Schutz der Datenverfügbarkeit;
- Unterstützung der Disaster Recovery und der Business Continuity;
- sicheres Löschen und ordnungsgemäßes Entsorgen;
- sichere autonome Datenbewegung;
- sichere Mandantenfähigkeit.

5.4 Risiken der Speichersicherheit

5.4.1 Hintergrund

Die Risiken der Speichersicherheit werden durch den Einsatz von spezifischen Speichersystemen oder -infrastrukturen durch die Organisation hervorgerufen. Risiken der Speichersicherheit sind zurückzuführen auf:

- a) Bedrohungen der in den Speichersystemen und der Speicherinfrastruktur behandelten Informationen;
- b) Schwachstellen (technische und nicht technische); und
- c) Auswirkungen der erfolgreichen Ausnutzung von Schwachstellen durch die Bedrohungen.

Das Risikomanagement ist ein Grundkonzept in der Informationssicherheit. ISO/IEC 27005 besagt, dass „der Prozess des Informationssicherheits-Risikomanagements auf die gesamte Organisation, auf einen beliebigen Teil der Organisation (z. B. eine Abteilung, ein physischer Standort, eine Dienstleistung), auf jedes Informationssystem, auf bestehende oder geplante oder bestimmte Aspekte der Lenkung (z. B. Business-Continuity-Planung) angewendet werden kann“. Der in ISO/IEC 27005 dargestellte Prozess des Informationssicherheits-Risikomanagements besteht aus der Kontextbestimmung, der Risikobeurteilung, der Risikobehandlung, der Risikoakzeptanz, der Risikokommunikation und der Risikoüberwachung und -überprüfung.

Zu den Bedrohungen für die Speichersysteme und die Speicherinfrastruktur zählen, neben anderen, folgende:

- unbefugte Nutzung;
- unbefugter Zugriff;
- Haftbarkeit durch Nichteinhaltung von behördlichen Vorschriften;

- Dienstverweigerungs- (DoS, en: Denial of Service) und verteilte Dienstblockaden-Angriffe (DDoS, en: Distributed Denial of Service) auf den Speicher;
- Verfälschung/Änderung und Vernichtung von Daten;
- Datenverlust/Bruch der Vertraulichkeit;
- Datendiebstahl oder versehentlicher Datenverlust;
- Angriff durch Malware oder deren Eindringen;
- unangemessene Behandlung oder nicht sicheres Löschen nach dem Lebensdauerende.

Diese Bedrohungen können Anlass für zahlreiche Risiken geben. Für Speichersysteme und Speicherinfrastrukturen sind jedoch die Risiken in Verbindung mit dem Bruch der Vertraulichkeit, der Datenkorruption oder -vernichtung, dem vorübergehenden oder dauerhaften Verlust des Zugriffs/der Verfügbarkeit und der Nichterfüllung von gesetzlichen, behördlichen oder rechtlichen Anforderungen die größten Anliegen.

5.4.2 Bruch der Vertraulichkeit

Der Bruch der Vertraulichkeit kann das Ergebnis einer Sicherheitsgefährdung sein und in unterschiedlichen Formen auftreten. Unbefugter Zugriff und die Offenlegung von geschützten Informationen sind zwei allgemein bekannte Formen für den Bruch der Vertraulichkeit, wobei es jedoch darauf ankommt, zu verstehen, dass zu den weniger bekannten Formen auch versehentliche oder unrechtmäßige Vernichtung, Verlust oder Änderung von Daten zählen können.

Abhängig von Umfang und Art der jeweiligen Informationen (z. B. personenbezogene Daten, geschützte Gesundheitsinformationen usw.) sowie von geltenden Gesetzen und Verordnungen kann ein Bruch der Vertraulichkeit für die Organisationen ein bedeutendes Risiko darstellen, das aus den Ermittlungskosten für den Bruch der Vertraulichkeit, dem Stellen von notwendigen Anzeigen gegen die betroffenen Personen, den Kosten für Gerichtsverfahren, behördlichen Bußgeldern und anderen gesetzlichen Strafen entsteht, sowie dem Markenschaden aufgrund der Bekanntgabe des Bruchs der Vertraulichkeit gegenüber der Öffentlichkeit.

Es gibt wirtschaftliche und sicherheitsbezogene Risiken für die Organisation, die einen Verlust ihrer eigenen oder organisationsfremden Informationen zu vermeiden hat, insofern als dass der Verlust der Informationen beispielsweise Folgendes umfassen könnte:

- geheime oder vertrauliche Informationen (z. B. Passwörter, Verschlüsselungscodes usw.);
- geistiges Eigentum oder andere sensible Geschäftsinformationen;
- personenbezogene Informationen (PII, en: Personally Identifiable Information);
- Informationen oder Bilanzen von Finanzkonten;
- personenbezogene Gesundheitsinformationen.

Nicht vertrauenswürdige oder unbefugte Organisationen, die Interesse an diesen durchgesickerten oder bekanntgewordenen Informationen zeigen, können unterschiedlichster Art sein, kapitalkräftig sein und unterschiedliche Beweggründe haben.

In Tabelle 1 werden die speicherbasierten Sicherheitsbedrohungen zusammengefasst, die mit größerer Wahrscheinlichkeit auftreten, und es werden die Formen des Bruchs der Vertraulichkeit aufgelistet, die aus diesen Beeinträchtigungen hervorgehen können.

Tabelle 1 — Speicherbasierte Brüche der Vertraulichkeit

Sicherheitsbedrohungen	Potentielle Formen des Bruchs der Vertraulichkeit
Diebstahl von Speicherelementen oder Speichermedien	Unrechtmäßiger Zugriff, unrechtmäßige Offenlegung, unrechtmäßiger Datenverlust, unrechtmäßige Datenvernichtung
Verlust von Speicherelementen oder Speichermedien	Unbefugter Zugriff, unbefugte Offenlegung, versehentlicher Datenverlust, versehentliche Datenvernichtung
Datenverlust	Unrechtmäßige, unbefugte oder versehentliche Datenvernichtung oder Datenkorruption
Versehentliche Änderungen der Konfiguration (z. B. Speichermanagement, Speicher-/Netzwerkressourcen, inkorrektes Patch-Management usw.) durch befugtes Personal	Versehentlicher Zugriff, versehentliche Offenlegung, versehentliche Datenvernichtung, versehentliche Änderung von Daten
Änderungen der Konfiguration (Speichermanagement, Speicher-/Netzwerkressourcen, Anwendungsmanipulation usw.) durch externe oder interne Widersacher mit böser Absicht	Unrechtmäßiger Zugriff, unrechtmäßige Offenlegung, unrechtmäßige Datenvernichtung, unrechtmäßige Änderung von Daten
Anwendermissbrauch durch befugte Anwender (z. B. unangemessenes Mitlesen von Daten)	Unrechtmäßige(r)/unbefugte(r) Zugriff oder Offenlegung
Datenmanipulation durch externe oder interne Widersacher mit böser Absicht	Unrechtmäßige Datenvernichtung oder -änderung
Verweigerung von Dienstangriffen	Unbefugte Datenvernichtung, -verlust oder -änderung
Überwachung des Netzwerkverkehrs mit böser Absicht	Unrechtmäßige/unbefugte Offenlegung

5.4.3 Datenkorruption und Datenvernichtung

Datenkorruption ist die Verschlechterung bzw. die Beschädigung von Computerdaten (d. h. unbeabsichtigte Änderungen der Originaldaten) durch Personen, durch Hardware-Fehler und durch Software-Fehler. Sie kann beim Schreiben, Lesen, Speichern, Übertragen oder Verarbeiten von Daten auftreten. Die Datenkorruption betrifft möglicherweise nur einen kleinen aber bedeutenden Teil der Daten oder Metadaten, die unter den richtigen Bedingungen wiederhergestellt werden können; sie könnte aber auch zum dauerhaften Datenverlust führen, falls die Grundursache bestehen bleiben kann. Datenvernichtung führt wiederum zum Datenverlust, der dauerhaft sein kann, falls die Datenschutzmechanismen, wie Backups, nicht umgesetzt worden sind. Datenkorruption und auch Datenvernichtung können das Ergebnis von sowohl unbeabsichtigten als auch von beabsichtigten Ereignissen sein, wobei sie im letztgenannten Fall weiter unterteilt werden können in Ereignisse mit böser Absicht oder Ereignisse ohne böse Absicht.

Ereignisse wie Brände, Überschwemmungen, Stromausfälle, Programmierfehler und Anwenderfehler sind Beispiele für allgemeine, unbeabsichtigte Ursachen für die Datenkorruption und die Datenvernichtung. Hintergrundstrahlung, Head-Crashes und Alterung bzw. Abnutzung der Speicherhardware sind weitere Ursachen für eher speicherbasierte Probleme. Die hardwarebasierte Datenkorruption kann in der Regel vom Anwender mithilfe von Prüfsummenfunktionen erkannt werden und oftmals auch vom Anwender mithilfe von Fehlerkorrekturcodes behoben werden, wobei jedoch diese „stillen Korrekturen“ andere Probleme aufwerfen können, falls der Speicher nicht ordnungsgemäß verwaltet wird (d. h. vorübergehende korrigierbare Fehler können zu dauerhaften Fehlern werden, wenn das Speichergerät bzw. das Speichermedium sich verschlechtert).

Absichtliche Angriffe/Ereignisse mit böser Absicht können durch externe Parteien oder durch Mitglieder der Organisation begangen werden, deren Absicht es ist, einige oder alle betroffenen Daten unbrauchbar zu machen oder sie zu vernichten. In diesem Zusammenhang könnte unbrauchbar bedeuten, dass unbefugte Änderungen durchgeführt wurden, Änderungen vermutet werden oder die Daten mit einem unbekannten Code oder einer unbekannten Funktion verschlüsselt worden sind. Angriffe ohne böse Absicht sind üblicherweise auf Fahrlässigkeit, Unwissenheit oder absichtliches Umgehen der Sicherheit zurückzuführen, um „einen Auftrag zu erledigen“, wobei jedoch die Auswirkungen auf die Daten genauso verheerend sein können wie bei Angriffen mit böser Absicht.

Die Umsetzung geeigneter Mechanismen zum Erkennen und Vermeiden der Datenkorruption ist eine wichtige Maßnahme zur Aufrechterhaltung der Datenintegrität. Ebenso kann das Erkennen von Datenverlust und die Wiederherstellung dieser Daten mit Datenschutzmechanismen Schutz vor totalem Datenverlust bieten.

5.4.4 Vorübergehender oder dauerhafter Verlust des Zugriffs/der Verfügbarkeit

Die Verfügbarkeit beschäftigt sich mit der Zusicherung, dass keine oder nur eine eingeschränkte Verweigerung des befugten Zugriffs¹⁾ auf Speicherelemente, Speichernetzwerkelemente, gespeicherte Informationen, Informationsflüsse, Dienste und Anwendungen vorliegt. In der Regel wird die Datenverfügbarkeit durch Redundanz des Speicherorts von Daten und deren Zugriffsart erreicht.

Der Verlust der Verfügbarkeit kann häufig einem Problem mit mindestens einem der folgenden Punkte zugeordnet werden:

- Verlässlichkeit;
- Zugänglichkeit;
- Rechtzeitigkeit.

5.4.5 Versagen beim Erfüllen gesetzlicher, behördlicher oder rechtlicher Anforderungen

Organisationen können hohe Haftungen und Strafen bei Nichterfüllung von gesetzlichen, behördlichen oder rechtlichen Anforderungen auferlegt werden. Die Anforderungen können sich von Rechtsordnungen zur Rechtsordnung deutlich unterscheiden und in multinationalen Organisationen haben landestypische Gesetze großen Einfluss auf die Anforderungen an die Informationssicherheit.

Übliche Probleme bei der Erfüllung umfassen:

- Verletzung von landestypischen Anforderungen an die Privatsphäre;
- unrechtmäßiger Datentransfer (d. h. Herausgabe geheimer Daten aus einer bestimmten Rechtsordnung);
- Bruch der Vertraulichkeit;
- Nichteinhaltung von Politiken der Organisation (z. B. sicheres Löschen);
- unangemessene Aufbewahrung und unangemessener Schutz von Daten;
- unzureichender Sicherheitsnachweis (z. B. Auditprotokolle, Nachweis über die Verschlüsselung/über das sichere Löschen usw.).

Diese Probleme der Nichterfüllung können zu kostspieligen Sanktionen und Wiedergutmachungen führen (z. B. Meldepflicht bei Verstößen).

1) In diesem Zusammenhang bedeutet „eingeschränkte Verweigerung des befugten Zugriffs“, dass die Daten weiterhin auf dem erforderlichen Leistungsniveau innerhalb eines bestimmten Zeitfensters verfügbar sind.

6 Unterstützende Maßnahmen

6.1 Allgemeines

Abschnitt 6 enthält die Maßnahmen, die die technischen Architekturen der Speichersicherheit unterstützen, sowie deren zugehörige technische Maßnahmen, und sonstige Maßnahmen (technische und nicht-technische), die nicht nur für den Speicher gelten. Informationen über viele dieser Maßnahmen können ISO/IEC 27002 entnommen werden. Die Maßnahmen, die für die Nutzung des Speichers besonders wichtig sind, werden nachstehend in 6.2 bis 6.8 erläutert. Sie richten sich an die Sicherung des Direct Attached Storage, von Speichernetzwerken, des Managements der Speichernetzwerksicherheit, der technischen Maßnahmen für unterschiedliche Speichertypen (block-, datei- und objektbasierte Speicher) und der Speichersicherheitsdienste. Die Sensibilität, Kritikalität und der Nutzen der Daten können ebenfalls wichtige Aspekte bei der Auswahl und Nutzung der Maßnahmen darstellen, weshalb Anhang B und insbesondere B.1.2 ebenfalls berücksichtigt werden sollten.

6.2 Direct Attached Storage (DAS)

Ein DAS-Gerät ist ein Speicherelement (z. B. HDD, Bandlaufwerk usw.), das direkt an einen Computer angeschlossen wird, ohne dass ein Speichernetzwerk zwischengeschaltet ist (d. h. kein zwischengeschaltetes Netzwerkgerät wie ein Hub, Router oder Switch). DAS-Geräte können interne Speicher (d. h. fester Bestandteil des Computersystems) oder externe Speicher (d. h. Hilfsspeicher) sein. Außerdem sind sie üblicherweise dem System zugehörig, mit dem sie verbunden sind; ein DAS-Gerät kann von mehreren Computern gemeinsam genutzt werden, solange es mehrere Schnittstellen (Ports) gibt, die den gleichzeitigen und direkten Zugriff erlauben.

Diese Speicherelemente besitzen begrenzte Datenzugriffs- und -managementschnittstellen (letztenannte sind in der Regel in-band). Daher sind die Möglichkeiten zur Sicherung des DAS eher begrenzt und umfassen Folgendes:

- Der DAS ist von eher geringer Größe und kann sich in Büroräumen befinden, in denen er Angriffen mit böser Absicht ausgesetzt sein kann (z. B. Diebstahl, Zerstörung, unbefugter Zugriff usw.), so dass der DAS physisch gesichert werden sollte.
- Um den unbefugten Zugriff auf sensible Daten und auf Daten von hohem Wert im DAS zu verhindern, sollte eine Art von Verschlüsselung eingesetzt werden, um die Data-at-Rest zu schützen, einschließlich:
 - Speicherelemente mit integrierter Verschlüsselung und Zugriffskontrolle, auch bekannt als selbst-verschlüsselnde Festplatten (SED, en: Self-Encrypting Drive);
 - computerbasierte oder anwendungsbasierte Verschlüsselung, einschließlich Festplattenverschlüsselung (FDE, en: Full Disk Encryption);
- Das sichere Löschen von Datenträgern (siehe 6.8.1.2 und Anhang A für weitere Informationen) sollte auf allen DAS, die sensible Daten oder Daten von hohem Wert enthalten, mit einem der folgenden Verfahren erfolgen:
 - Einsatz der integrierten Funktion in den Speicherelementen zum sicheren Löschen;
 - Einsatz einer computerbasierten oder anwendungsbasierten Funktion zum sicheren Löschen.
- Sofern möglich, sollte eine Authentifizierung, wie Fibre Channel — Security Protocol — 2²⁾ (FC-SP-2) AUTH-AAAuthentication (siehe C.7.2), erfolgen, um unbefugten Zugriff auf sensible Daten und auf Daten von hohem Wert zu verhindern.
- Zum Schutz vor versehentlichem oder absichtlichem Datenverlust oder versehentlicher oder absichtlicher Datenkorruption sollten regelmäßige Backups der DAS-Inhalte erstellt werden.

2) FC-SP-2 wird in ANSI INCITS 496-2012, *Information Technology — Fibre Channel — Security Protocols — 2 (FC-SP-2)* näher bestimmt.

6.3 Speichernetzwerk

6.3.1 Hintergrund

Mit der eventuellen Ausnahme von DAS, spielen Netzwerke eine wichtige Rolle in der Speicherinfrastruktur; diese Netzwerke können übliche Netzwerktechnologien (z. B. LAN und WAN), speicherspezifische Netzwerkprotokolle, die diese Technologien anwenden, und speicherspezifische Technologien (z. B. Fibre Channel) umfassen. Im ersten Fall sind die Sicherheitsleitlinien nach ISO/IEC 27033 für den Schutz von Speicherressourcen, die diese Technologien nutzen, behilflich. Die speicherspezifischen Netzwerkprotokolle und -technologien werden in der vorliegenden Internationalen Norm behandelt.

Speichersysteme nutzen Netzwerke aus drei wesentlichen Gründen: 1) Speichern und Abrufen von Daten, 2) Schutz von Daten, und 3) Management von Speichersystemen. Keiner der Gründe erfordert eine bestimmte Netzwerktechnologie oder ein bestimmtes Netzwerkkonzept. Ein Teil des Speichermanagements kann beispielsweise mithilfe der gleichen Fibre-Channel-Schnittstelle (d. h. in-band) durchgeführt werden, wie die von einem Server für den Datenzugriff genutzte, und gleichzeitig mit einer TCP/IP-Verbindung zur Managementschnittstelle des Speichersystems.

6.3.2 Speichernetzwerke (SAN)

6.3.2.1 Allgemeines

Ein Speichernetzwerk (SAN, en: Storage Area Network) ist ein spezielles Hochgeschwindigkeitsnetz, das den Zugriff auf den Speicher über das Netzwerk auf Blockebene ermöglicht. SANs bestehen üblicherweise aus Servern, Switches, Speicherelementen und Speichergeräten, die mithilfe unterschiedlicher Technologien, Topologien und Protokolle miteinander verbunden sind. SANs können sich auch über mehrere Standorte erstrecken.

SANs werden häufig verwendet, um die Verfügbarkeit von Anwendungen zu verbessern (z. B. mehrere Datenpfade), die Leistung von Anwendungen zu verbessern (z. B. Leeren des Speicher, Einsatz separater Netzwerke usw.), die Speichernutzung und Speichereffektivität zu steigern (z. B. Zusammenlegen von Speicherressourcen, mehrschichtige Speicher usw.) und den Datenschutz und die Datensicherheit zu verbessern. Zusätzlich spielen SANs üblicherweise eine wichtige Rolle für die DR- und BC-Aktivitäten einer Organisation (siehe Bild 1).

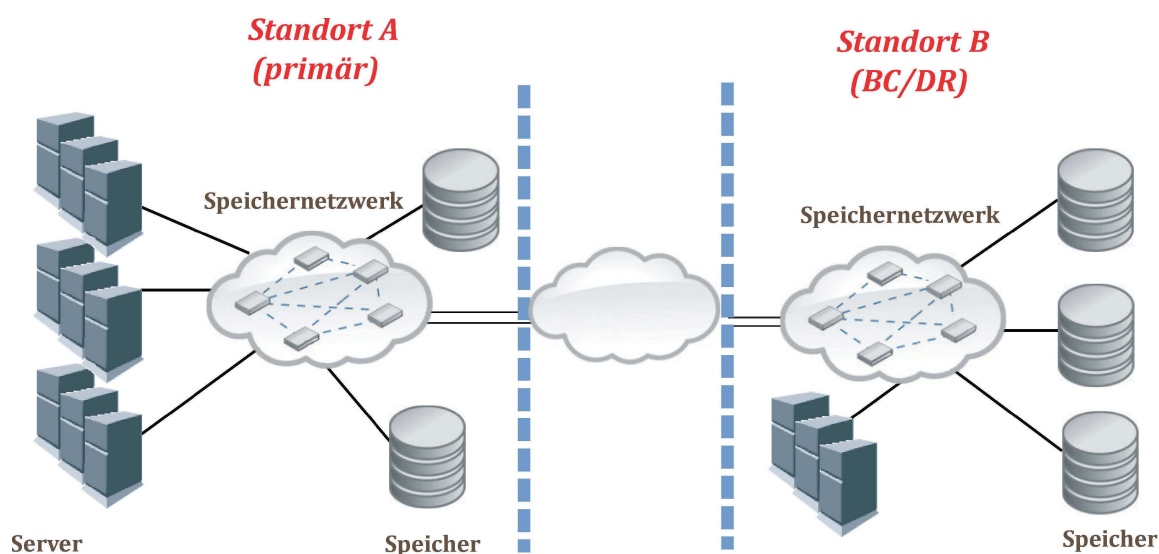


Bild 1 — Beispiel eines Speichernetzwerks (SAN)

Ein SAN präsentiert die Speichergeräte (wie Disk-Arrays und Bandbibliotheken) einem Serverbetriebssystem, so dass es dem Server erscheint, als wäre der Speicher lokal angeschlossen. Diese vereinfachte Präsentation eines Speichers gegenüber einem Server wird durch den Einsatz unterschiedlicher Arten der Virtualisierung erreicht.

SANs basieren üblicherweise auf einer Fibre-Channel-Technologie (FC), die das Fibre-Channel-Protokoll (FCP) für offene Systeme und proprietäre Varianten für die Mainframes nutzt. Zusätzlich ermöglicht Fibre Channel over Ethernet (FCoE) es, den FC-Verkehr über die bestehende Hochgeschwindigkeits-Ethernet-Infrastruktur zu leiten und führt Speicher und IP-Protokolle auf einem einzigen Kabeltransportweg und an einer Schnittstelle zusammen. Andere Technologien, wie Internet Small Computing System Interface (iSCSI), die üblicherweise in kleinen und mittleren Organisationen als eine kostengünstigere Alternative zu FC verwendet werden, sowie InfiniBand, das üblicherweise in Hochleistungs-Computerumgebungen verwendet wird, können ebenfalls verwendet werden. Verbindungen wie Serial Attached SCSI (SAS) und Peripheral Component Interconnect express (PCIe), die Erweiterungen und Switches wirksam einsetzen, nehmen ebenfalls die Eigenschaften eines SAN an.³⁾ Zusätzlich besteht die Möglichkeit, Daten zwischen verschiedenen SAN-Technologien mithilfe von Gateways zu verschieben (siehe Bild 2).

Sicherheitsmaßnahmen, die für ein SAN relevant sind, sind in folgende Kategorien unterteilt:

- **Zugriffskontrolle:** Die Zugriffskontrolle eines SAN wird mithilfe von Zoning (Zoneneinteilung), LUN-Masking und Mechanismen zur Port-Binding umgesetzt.
- **Port-Binding:** Weltweit eindeutige Kennzeichner, bekannt als World Wide Names (WWN), werden zur Identifikation in einem SAN verwendet. Port-Binding ist ein SAN-Sicherheitsmechanismus, der eine physische Port-ID und die WWN des angeschlossenen Geräts miteinander in Beziehung setzt. Diese Beziehung kann Versuche der Datenspionage durch einen potentiellen Widersacher mindern und sollte nach Möglichkeit eingesetzt werden.
- **Zoning:** Eine SAN-Fabric kann in separate Zonen eingeteilt werden, um die Sichtbarkeit von Teilen eines SAN für bestimmte Server und Speichergeräte einzuschränken. Beim Soft-Zoning sind die Nameserver-Antworten der SAN-Fabric auf die Anfragen begrenzt, die auf der Annahme basieren, dass die Server nicht die Speichergeräte kontaktieren, die über den Nameserver nicht erreicht werden. Beim Hard-Zoning kommen physische Port-Nummer an SAN-Switches zum Einsatz, um die Verkehrsweiterleitung zu einschränken, und es stellt eine sicherere Zoning-Methode dar, weil es nicht auf einem korrekten Serververhalten basiert und insbesondere weil es nicht anfällig für die Vortäuschung einer Serveridentität ist.

3) Diese Internationale Norm enthält keine Leitlinien speziell für InfiniBand, SAS oder PCIe, sondern es gelten die allgemeinen Leitlinien.

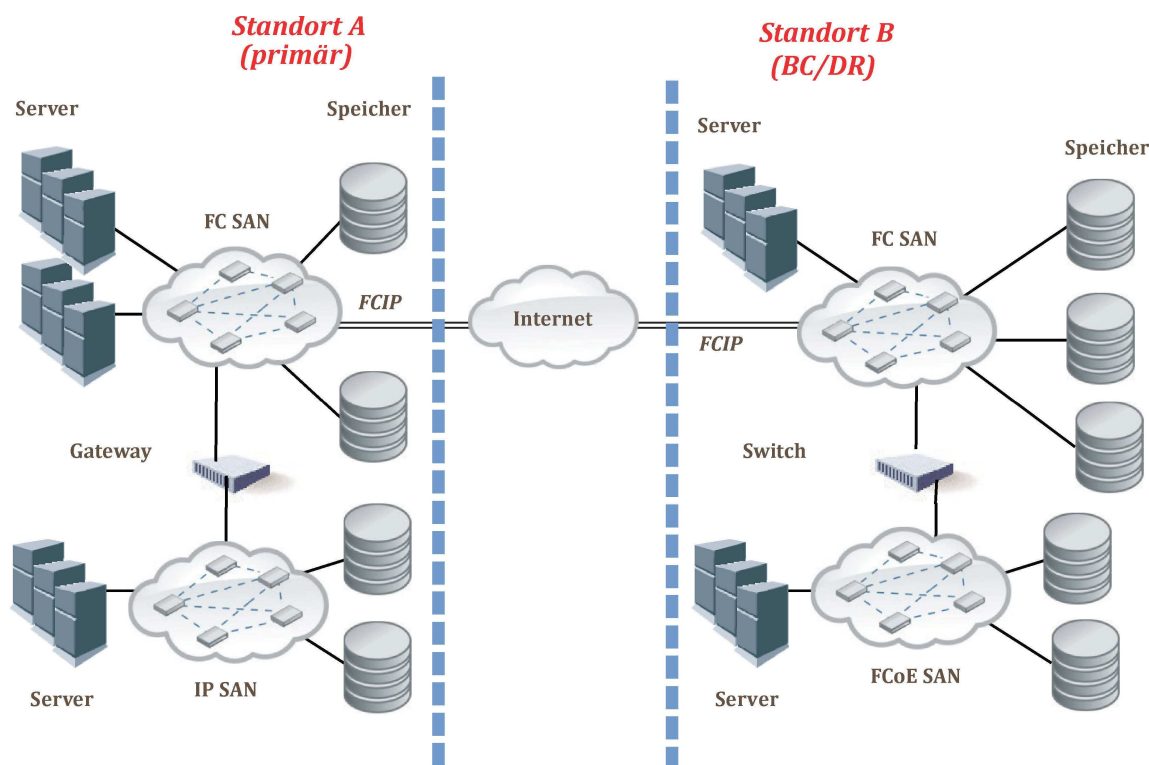


Bild 2 — Beispiel eines Speichernetzwerks (SAN)

- **LUN-Masking und LUN-Mapping:** Ein Speichergerät kann in verschiedene Logical Units (LUN) unterteilt werden, die durch Logical-Unit-Nummern gekennzeichnet sind. LUN-Mapping bezieht sich auf die Zuordnung einer Nummer zu einem LUN und findet in der Regel in einem Speicher-Array statt, kann aber auch als Teil einer Umleitung (Anfangsadresse zu einer neuen Adresse) im Switch, Host-Bus-Adapter (HBA) oder Converged-Network-Adapter (CNA) und der Virtualisierungsschicht stattfinden. LUN-Masking bezieht sich auf das Sichtbarmachen einer LUN für einige Server, aber nicht für andere.
- **Authentifizierung:** Bei SANs ist es für einen Switch wichtig, die Identität anderer Switches im SAN, mit denen er kommuniziert, zu verifizieren. Falls die Switch-Authentifizierung nicht umgesetzt wird, könnte ein fehlerhafter Switch einem SAN beitreten und SAN-Daten potentiell beeinträchtigen. Demzufolge müssen die Knoten in einem SAN (z. B. Speichergeräte und Server) eine Authentifizierung vornehmen, um Schutz vor dem Bruch der Vertraulichkeit zu bieten.
- **Verschlüsselung:** Es gibt zwei wesentliche Komponenten der Datenvertraulichkeit in einem SAN: 1) Data-in-Motion und 2) Data-at-Rest. Sensible Daten und Daten von hohem Wert müssen durch Verschlüsselung in SANs geschützt werden, sowohl in Bewegung (in Motion) als auch in Ruhe (at Rest) in einem Speichergerät. Dies kann den Einsatz von spezieller Hardware erfordern, die Daten verschlüsseln kann, die an ein Speichergerät gesendet werden. Siehe 6.8.2.2 für weitere Leitlinien zum Schutz von Data-in-Motion und 6.8.2.3 für Leitlinien zum Schutz von Data-at-Rest.

Ein Konzept der gestaffelten Verteidigung (siehe 7.2.1) hilft dabei, das Risiko durch Versagen einer Sicherheitsmaßnahme (möglicher einzelner Ausfallpunkt) zu mindern, das die zu schützenden Daten beeinträchtigt.

Eine physische und logische Trennung von Speicherelementen in einem SAN kann ebenfalls eine wichtige Rolle spielen und kann folgendermaßen stattfinden:

- Physische Trennung umfasst:
 - Trennen der Produktion von den anderen Systemklassen (z. B. Qualitätssicherung, Entwicklung);
 - nach Möglichkeit, Vermeiden von Netzwerkverbindungen zwischen Klassen (z. B. ein Produktionsserver, der sowohl an das Produktionsnetzwerk als auch an das Entwicklungsnetzwerk angeschlossen ist);
 - Trennen von Netzwerken und Speicher anhand der Klasse, soweit angemessen;
 - physische Trennung von Systemen in jeder Klasse.
 - Trennen der Speichergeräte von anderen Geräten in Rechenzentren, soweit praktisch durchführbar.
- Logische Trennung umfasst:
 - Trennung des Speicherverkehrs vom normalen Serververkehr mithilfe von:
 - verfügbaren Netzwerkkontrollen zur Erstellung eigenständiger logischer Domains in einer üblichen physischen Infrastruktur;
 - Kontrolle der Vertrauenswürdigkeit und des Zugang für die Verwaltung von Mitgliedschaften in den logischen Domains;
 - Trennung des Speichermanagementverkehrs von allen anderen Verkehrsarten;
 - Sicherstellen, dass Konfigurationen der Netzwerk-Gateways eine angemessene Netzwerktrennung aufrechterhalten.

6.3.2.2 Fibre-Channel-SAN

Fibre Channel ist eine Netzwerktechnologie mit Multi-Gigabit-Geschwindigkeit, die für die blockbasierte Speicherung verwendet wird. Es gibt drei wesentliche Fibre-Channel-Topologien, die beschreiben, wie eine Anzahl an Ports miteinander verbunden ist: Point-to-Point- (zwei Geräte sind direkt miteinander verbunden), Arbitrated-Loop- und Switched-Fabric-Topologien. Switched-Fabric-Topologien sind zusammen mit dem Fibre-Channel-Protokoll (FCP), das das Schnittstellenprotokoll zur Übertragung des SCSI-Verkehrs in dieser Netzwerktechnologie darstellt, aus Sicht der Sicherheit von größerem Interesse.

Fabric-Administratoren sollten Maßnahmen einleiten, um:

- den Zugriff auf FCP-Knoten zu kontrollieren, einschließlich:
 - einer Einschränkung des Serverzugriffs auf die Switches mithilfe von Techniken wie einer Zugriffskontrollliste (ACL, en: Access Control List), verbindlichen Listen und FC-SP-2-Fabric-Policys (siehe C.7.1);
 - Nutzung von NPIV-aktivierten (N_Port_ID-Virtualisierung) HBAs für die Zuordnung einzelner N_Port_IDs zu virtuellen Servern;
- Umsetzung Switch-basierter Kontrollen, einschließlich:
 - Einschränken der Switch-Verbindungen mithilfe von Techniken wie ACLs, verbindlichen Listen und FC-SP-2-Fabric-Policys (siehe C.7.1);

- Zoning sollte in FC-SAN-Fabrics eingesetzt werden, mit der Präferenz für Hard Zoning;
- es wird bestimmt, ob grundlegendes Zoning eine ausreichende Sicherheitsmaßnahme für die Zielumgebung ist und, falls nicht, sind strengere Techniken wie FC-SP-Zoning (siehe C.7.5) zu nutzen, soweit sie vom Vertreiber unterstützt werden;
- Deaktivieren von ungenutzten Ports;
- sorgfältige Nutzung von Default-Zonen und Zonensätzen (unter Annahme der Least-Privilege-Haltung);
- sicheres Verbinden von Speichernetzwerken durch Konfigurieren von Switches, Extendern, Routern und Gateways, die notwendig sind, um die Anforderungen zu erfüllen.

6.5.1 enthält Leitlinien für Block-basierte Fibre-Channel-Speicher.

6.3.2.3 IP SAN

Internet SCSI (iSCSI), das in IETF RFC 3720 beschrieben ist, ist ein verbindungsorientiertes Befehls-/Antwort-Protokoll, das über TCP läuft und für den Zugriff auf Festplatten, Bandlaufwerke und andere Geräte genutzt wird.

iSCSI-Netzwerkzugriffe und -protokolle werden wie folgt kontrolliert:

- es wird vermieden, iSCSI-Schnittstellen mit Allzweck-LANs zu verbinden; Trennung aus Gründen der Sicherheit und der Leistung;
- es werden Virtual Local Area Networks (VLANs) verwendet, wenn der Einsatz von physisch getrennten LANs keine Option darstellt.

Fibre Channel over TCP/IP (FCIP), festgelegt in IETF RFC 3821, ist ein reines Fibre-Channel-Encapsulation-Protokoll. Es erlaubt die Verbindung von Inseln aus Fibre Channel Storage Area Networks durch IP-basierte Netzwerke, um ein einheitliches Storage Area Network zu bilden.

FCIP-Netzwerkzugriff und -protokollmaßnahmen sollte wie folgt kontrolliert werden:

- Erstellen der Peer-to-peer-Beziehung zwischen FCIP-Einheiten, unter Anerkennung, dass die Sicherheitsleitlinien einheitlich umgesetzt werden;
- Nutzung eines privaten IP-Netzwerks ausschließlich durch die FCIP-Einheiten, wann immer dies möglich ist.

Umsetzung von IPsec-Sicherheitsmaßnahmen in Verbindung mit FCIP durch:

- Durchführung einer kryptographischen Authentifizierung und minimale Datenintegrität;
- Schutz von sensiblen Daten durch geeignete Vertraulichkeitsmaßnahmen.

IETF RFC 3723, *Securing Block Storage Protocols over IP*, enthält weitere nützliche Informationen zu sowohl iSCSI als auch FCIP. In 6.5.2 sind Leitlinien zu Block-basierten IP-Speichern enthalten. Außerdem enthält IETF RFC 7146, *Securing Block Storage Protocols over IP: RFC 3723 Requirements Update for IPsec v3* wichtige Sicherheitsupdates für IETF RFCs 3720, 3723 und 3821.

6.3.2.4 FCoE SAN

Fibre Channel over Ethernet (FCoE) ist eine Protokollspezifikation⁴⁾ zur Kapselung von Fibre-Channel-Rahmen in Ethernet-Paketen. Das Ethernet-Netz, das das FCoE unterstützt, muss ein verlustfreies Ethernet-Netz⁵⁾ sein, mit Schaltgeräten, deren interne Architektur so ausgelegt ist, dass sie eine nicht abfallende Paketleistung erzielen und mit Kontrollfunktionen für den Netzwerkfluss, um eine verlustfreie Übertragung von Paketen über die Ethernet-Infrastruktur zu ermöglichen.

FCoE SANs sollten durch folgende Maßnahmen geschützt werden:

- wirksames Einsetzen von Fibre-Channel-Sicherheitsmechanismen (siehe C.7);
- Schutz vor Ethernet-Broadcast-Überlastungen (z. B. Zuweisung von angemessenen Eingabepuffern), die zu Durchsatz und Zeitüberschreitungen führen können;
- Einsatz von ACLs zur Kontrolle des Netzwerkzugriffs (z. B. Verweigerung des unnötigen oder ungewollten Datenverkehrs bestimmter Computer);
- Einsatz von FCoE VLANs, wenn der Einsatz von physisch getrennten LANs keine Option darstellt.

6.3.3 Netzwerkspeicher (NAS)

6.3.3.1 Allgemeines

Netzwerkspeicher (NAS) ist eine Datenspeichertechnologie, die für heterogene Clients einen Zugriff auf Dateiebene über ein Netzwerk bietet. Ein NAS ermöglicht einem Dateisystem, das sich physisch auf einem Server oder einem Gerät befindet, dass durch Remote-Client-Computer darauf zugegriffen wird und es den Anwendern als lokales Dateisystem erscheint. NAS-Systeme sind in der Regel speziell für NAS-Zwecke ausgelegt und gebaut, wobei jedoch Servercomputer für allgemeine Zwecke ebenfalls zum Einsatz kommen können.

NAS-Systeme können als individuelle Speicherserver oder als gruppierte Zusammenstellung von Speicherservern, die auf dynamische Weise Client-Verbindungen verteilen, durch Slicing oder Auswerten von Daten oder Metadaten über die gruppierten Speicherserver (siehe Bild 3); parallele NFS-(pNFS)-Systeme sind Beispiele für gruppierte NAS-Systeme.

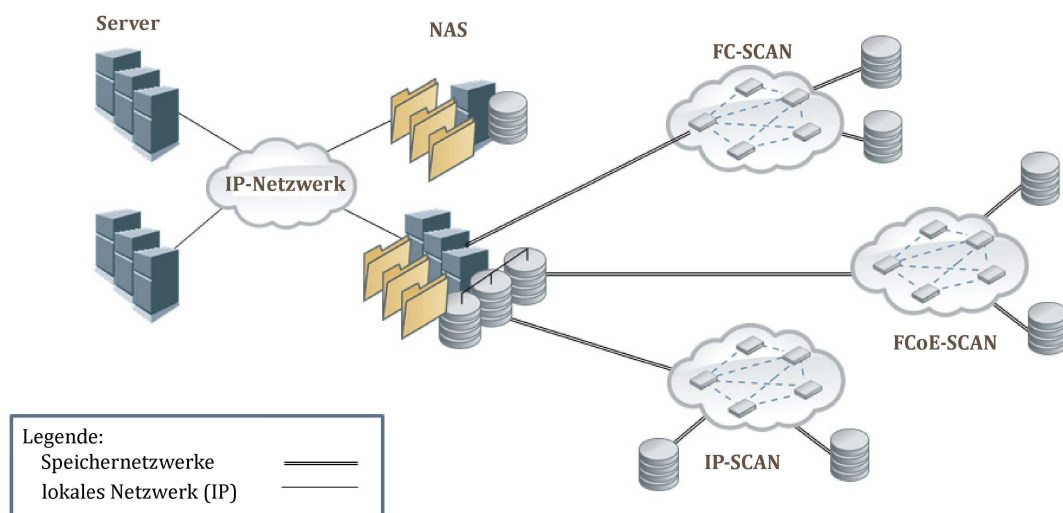


Bild 3 — Beispiel für Network Attached Storage (NAS)

4) FCoE ist in ANSI INCITS 462-2010, *Information Technology — Fibre Channel — Backbone — 5 (FC-BB-5)* festgelegt.

5) Diese Netzwerke sind Vollduplex-Netzwerke nach IEEE 802.3, die 802.3x PAUSE und Jumbo Frames dabei unterstützen, die 2-Kilobyte-FC-Datenrahmen einzukapseln.

Übliche Umsetzungen von Dateisystemen umfassen das Netzwerk-Dateisystem (NFS) und Server Message Block (SMB)/Common Internet File System (CIFS), aber es gibt ebenso andere Technologien wie Object-based Storage Device (OSD) (de: objektbasierter Speicher) und Cloud-Computing-Speicher.

Sicherheitsmaßnahmen, die für NAS relevant sind, werden in folgende Kategorien eingeteilt:

- Autorisierungsmaßnahmen, wie ACLs, die den Zugriff von Anwendern auf Datei- und Ordnerressourcen beschränken, die durch das NAS-Gerät bereitgestellt werden;
- Verschlüsselung von Daten, von sowohl Data-in-Motion als auch Data-at-Rest; und
- Authentifizierungsmaßnahmen, wie Kerberos, zur Verifizierung der Identität von Anwendern, die versuchen, auf NAS-Daten zuzugreifen.

Für einen weiterführenden Leitfaden zur Umsetzung von NAS und dateibasiertem Speicher siehe 6.6.

6.3.3.2 Netzwerk-Dateisystem (NFS, en: Network File System)

Das NFS ist eine Client/Server-Anwendung, die mit einem RPC-basierten Protokoll (en: Remote Procedure Call) kommuniziert. Mehrere NFS-Versionen sind festgelegt und werden eingesetzt, einschließlich NFS-Version 3 (festgelegt nach IETF RFC 1813), NFS-Version 4 (festgelegt nach IETF RFC 3530) und NFS-Version 4.1 (festgelegt nach IETF RFC 5661). Aus dem Blickwinkel der Sicherheit wird die NFS-Version 3 (NFSv3) als weniger sicher eingeschätzt, und bei ihrer Verwendung mit sensiblen oder Daten von hohem Wert von hohem Wert sollte eine besondere Sorgfalt aufgewendet werden.

Der folgende netzwerktechnische Leitfaden ist auf NFS-basierte NAS anwendbar und sollte angewendet werden für:

- die Steuerung von NFS-Netzwerkzugriff und Protokollen indem:
 - das NFS ausschließlich bei Bedarf aktiviert wird. Das wird es als möglichen Angriffsvektor für einen Angreifer ausschließen;
 - nach Möglichkeit NFSv4 (oder spätere Versionen) angewendet und die Nutzung von NFSv3 eingeschränkt wird;
 - für die zusätzliche Sicherheit, der Zugriff von Client und Management nach IP-Adresse gefiltert wird.
- der Client-Datenzugriff bei Bedarf verschlüsselt wird (z. B. IPsec).

6.3.3.3 SMB/CIFS

Server Message Block (SMB) 3.0 – der Nachfolger von CIFS (Common Internet File System), das wiederum der Nachfolger von SMB 1.0 ist – ist ein Protokoll, das dafür vorgesehen ist, ein offenes plattformübergreifendes Instrument für Client-Systeme bereitzustellen, um Datei-Dienste von Server-Systemen über ein Netzwerk abzufragen. Es basiert auf dem Standard-SMB-Protokoll, das breite Anwendung bei Personal Computern und Workstations findet, das eine große Vielfalt von Betriebssystemen unterstützt.

Der folgende netzwerktechnische Leitfaden ist auf SMB/CIFS-basierte NAS anwendbar und sollte angewendet werden:

- Einsatz späterer Versionen des SMB-Protokolls;
- Abschaltung von Session-Negotiation-Protokollen mit geringer Sicherheit, wie NT LAN Manager (NTLM) v1, LanMan und Klartext und stattdessen Einsatz von NTLM v2 oder Kerberos;
- Patch-Levels werden auf neuestem Stand gehalten;

- Verwendung der SMB-Signatur;
- Aufrechterhaltung sicherer Active-Directory-Dienste (AD);
- Verwendung von One-Way-Trusts, von Leaf-Domains zu Parent-Domains, sofern möglich;
- die Steuerung von SMB/CIFS-Netzwerkzugriff und -Protokollen, durch:
 - die Aktivierung von SMB/CIFS ausschließlich bei Bedarf. Das wird es als möglichen Angriffsvektor für einen Angreifer ausschließen;
 - die Verschlüsselung des Client-Datenzugriffs bei Bedarf.

6.4 Speichermanagement

6.4.1 Hintergrund

Speichernetzwerke und Infrastrukturelemente sind komplexe Architekturen, die strenge Managementansprüche an Administratoren stellen können. Zur Behandlung dieser Ansprüche verwirklichen die Organisation Instrumente und Prozesse für das Speicherinfrastruktur-Management, um die Verfügbarkeit und Leistung aller Speicherelemente, einen erweiterten Datenschutz und Datensicherheit, eine zentralisierte Auditierung und die Erfüllung der Einhaltung von Anforderungen sicherzustellen (siehe Bild 4).

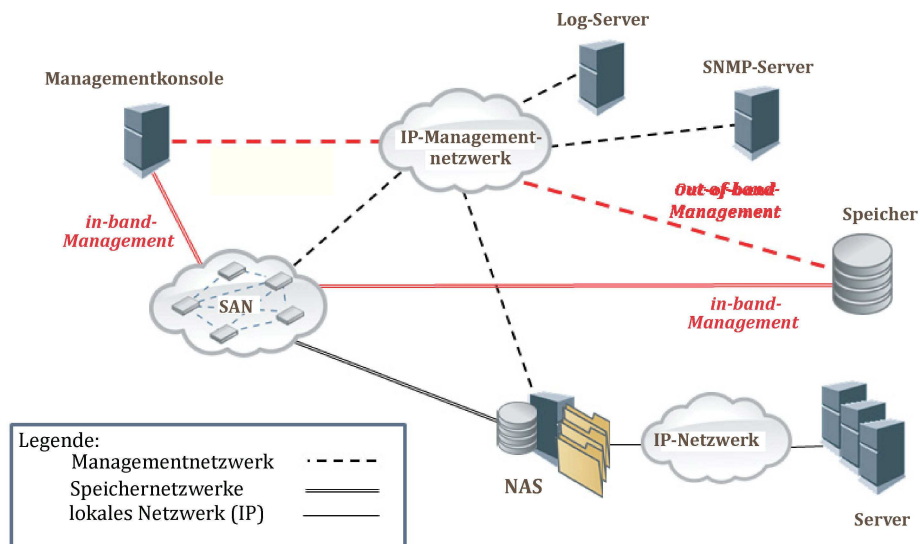


Bild 4 — Beispiel für das Speichermanagement

Wie die Beschreibung des Netzwerkmanagements nach ISO/IEC 27033-2, bezieht sich auch das Speichermanagement auf einschlägige Aktivitäten, Methoden, Verfahren, und Tools in Hinsicht auf den Betrieb, die Verwaltung, Bereitstellung und Datenlöschung von Speichersystemen.

- Betrieb umfasst, den Speicher (und die Dienste, die die Speicherinfrastruktur bereitstellt) betriebsbereit und störungsfrei am Laufen zu halten. Das umfasst die Überwachung des Speichers, um Probleme schnellst möglich zu erkennen, bestenfalls, bevor Anwender beeinträchtigt werden;
- Verwaltung befasst sich damit, Ressourcen in der Speicherinfrastruktur und die Art ihrer Zuweisung nachzuverfolgen. Es umfasst die gesamte „interne Systemorganisation“ (en: housekeeping), die erforderlich ist, um das System zu steuern;
- Wartung betrifft die Durchführung von Reparaturen und Upgrades – z. B., wenn Geräte ausgetauscht werden müssen, wenn ein Speicher-Array ein Mikrocode-Update benötigt oder wenn einem Speichernetzwerk ein neuer Switch hinzugefügt wird. Wartung umfasst ebenfalls Korrektur- und Vorbeugungsmaßnahmen, um die Ausführung des Speichers zu verbessern, wie z. B. das Einstellen von Parametern der Gerätekonfiguration;

- Bereitstellung behandelt die Initialisierung und Ausstattung eines Systems, um es auf die Bereitstellung von Diensten vorzubereiten;
- das sichere Löschen behandelt den Schutz der Vertraulichkeit von Informationen, die bei Außerbetriebnahme oder Wiederverwendung von Datenträgern auf diesen verbleiben, indem die Daten unlesbar gemacht werden (z. B. durch Überschreiben mit zufälligen Daten, Zerstörung der Verschlüsselungscodes für verschlüsselte Daten oder durch physische Zerstörung des Geräts).

Die sichere Durchführung dieser Speichermanagementtätigkeiten erfordert Maßnahmen im Zusammenhang mit Authentifizierung und Autorisierung (6.4.2), dem Schutz der Speichermanagement-Schnittstellen (6.4.3), der Aufrechterhaltung der Zurechenbarkeit und Rückverfolgbarkeit von Systemen und Anwendern (6.4.4) sowie der Sicherstellung, dass die dem Speichermanagement zugrundeliegenden Systeme angemessen gehärtet sind (6.4.5). Ein Leitfaden für jedes dieser Themen ist in den entsprechenden Unterabschnitten von 6.4 enthalten.

6.4.2 Authentifizierung und Autorisierung

6.4.2.1 Authentifizierung

Die Personen, die mit dem Management von Speichersystemen und -infrastrukturen betraut sind, sind üblicherweise privilegierte Anwender. In Übereinstimmung mit ISO/IEC 27002:2013, 9.2.3, sollte die Erteilung und Anwendung von privilegierten Zugriffsrechten beschränkt und gesteuert werden. Missbräuchliche Nutzung von Systemadministrationsrechten (jede Funktion oder Einrichtung eines Informationssystems, die dem Anwender ermöglicht, System- oder Anwendungskontrollen zu übergehen) können eine Hauptursache für Systemversagen oder Systemgefährdungen darstellen. Als Beitrag zur Minderung dieser Bedrohungen, können möglicherweise sichere Anmeldeverfahren wie nach ISO/IEC 27002:2013, 9.4.2, mit zusätzlichen Authentifizierungsmaßnahmen (siehe C.1) erforderlich sein, die unter anderem einschließen:

- dass sämtliche Anwender eine eindeutige Kennzeichnung (Anwender-ID) besitzen sollten, ausschließlich für ihre personengebundene Nutzung;
- dass ein geeignetes Authentifizierungsverfahren gewählt werden sollte, zum Nachweis der vorgegebenen Identität eines Anwenders, durch Verwendung von:
 - sicheren Passwörtern (erhöhte Mindestzeichenzahl, erhöhte Komplexität usw.) mit einem kürzeren Geltungszeitraum;
 - sicherer Authentifizierung (z. B. Challenge-Response-Protokoll); oder
 - Multi-Faktor-Authentifizierung, wie biometrische Daten (z. B. Verifizierung durch Fingerabdruck, Unterschriftenprüfung) und Verwendung von Hardware-Token (z. B. Smartkarten).
- dass für jeden Fernzugriff eine sichere Authentifizierung oder Multi-Faktor-Authentifizierung, zusammen mit sicheren Kanälen verwendet wird;
- dass wenn möglich, eine zentralisierte Authentifizierungslösung (z. B. Remote Authentication Dial-In User Service bzw. RADIUS, Single Sign-on bzw. SSO usw.) für eine verbesserte Überwachung und Kontrolle verwendet wird;
- dass bei der Handhabung von sensiblen oder Daten von hohem Wert eine Multi-Faktor-Authentifizierung verwendet wird;
- das Blockieren des Einloggens in den Root-Account. Sämtliche Operationen der Privileg-Eskalation werden fernprotokolliert.

Zusätzlich zur Anwenderauthentifizierung setzen Speichersysteme mitunter Entität-Authentifizierung ein, die der Prozess ist, durch den ein Agent in einem verteilten System Vertrauen in die Identität eines Kommunikationspartners erlangt. Diese Entität-Authentifizierung kann in der Transport Layer Security (TLS) und IPsec-Verbindungen, sowie innerhalb von Speicherprotokollen (z. B. Challenge-Handshake-Authentication-Protocol mit iSCSI, Diffie-Hellman Challenge Handshake Authentication Protocol in FCP, usw.) Wenn möglich, sollten diese Instrumente zur Entitäts-Authentifizierung verwendet werden. Ein zusätzlicher Leitfaden ist in den Abschnitten enthalten, die diese Instrumente behandeln.

6.4.2.2 Autorisierung und Zugriffskontrolle

In Marktsegmenten, wie Finanzdienstleistungen und im Gesundheitswesen gibt es Entwicklungen, die Autorisierung und Zugriffskontrolle (C.2) auf ein Modell des minimalen Privilegs auszurichten, das spezielle Rollen wirksam einsetzt. Die folgenden Rollen sollten in Speichertechnologien umgesetzt und verwendet werden:

- *Sicherheitsadministrator* – Diese Rolle besitzt Lese- und Änderungsrechte, für die Einrichtung und das Management von Benutzerkonten sowie für die Erzeugung und Zuweisung von Rollen/Genehmigungen, für Auditlogging-Konfigurationen und -Inhalte (Auditlog-Ereignisse können niemals geändert werden), um vertrauenswürdige Verbindungen mit der IT-Infrastruktur aufzubauen (z. B. gemeinsame Geheimnisse für RADIUS), um Zertifikat- und Schlüsselspeicher zu verwalten, um das Verschlüsselungs- und Schlüsselmanagement zu verwalten, und um Zugriffskontrollen festzulegen.
- *Speicheradministrator* – Diese Rolle besitzt Lese- und Änderungsrechte für alle Aspekte des Speichersystems. Zu sicherheitsbezogenen Elementen oder Daten wird kein Zugriff gewährt.
- *Sicherheitsauditor* – Diese Rolle besitzt Leserechte, die Berechtigungsüberprüfungen, die Verifizierung von Sicherheitsparametern und -konfigurationen, und Inspektionen von Audit-Logs zulassen. Auf Speicher, Konfiguration oder Daten wird kein Zugriff gewährt.
- *Speicherauditor* – Diese bedienerähnliche Rolle besitzt Leserechte, die die Verifizierung von Speicherparametern und Konfigurationen sowie Prüfungen von Health-/Fault-Logs zulassen. Auf sicherheitsbezogene Elemente oder Daten wird kein Zugriff gewährt.

Jede Speichermanagementtransaktion sollte einer „Sicherheits-“ oder „Speicher-“Rolle zugehörig sein. Diese Rollen können wichtige Maßnahmen sein, um die Funktionstrennung in Hinsicht auf die Managementfähigkeiten sicherzustellen.

6.4.3 Schutz der Managementschnittstellen

Das Schützen der Managementschnittstellen vor unberechtigtem Zugriff und Ausspähung ist von höchster Wichtigkeit. Unberechtigter Zugriff auf Managementschnittstellen, aufgrund von Nichtumsetzung geeigneter Kontrollen könnte zur Datenzerstörung, -beschädigung oder zur Verweigerung des Zugriffs führen.

Managementschnittstellen für Speichersysteme können mehrere physische Formen annehmen, einschließlich seriellen Schnittstellen (z. B. RS-232, DB9, DB25 usw.), lokale Netzwerke, Modems und sogar die für den Datenpfad verwendete Technologie (z. B. Fibre-Channel). Hybrid-Schnittstellen (z. B. serielle Schnittstellen, die in einen Console Concentrator eingesteckt sind, der eine Schnittstelle mit einem LAN bereitstellt) sind ebenfalls relativ verbreitet. Um diese physischen Schnittstellen zu schützen, sollte eine Organisation:

- den physischen Zugriff auf Managementschnittstellen beschränken;
- serielle Managementschnittstellen sperren und trennen, wenn sie nicht in Verwendung sind;
- LAN-Schnittstellen, die für Managementzwecke verwendet werden von sonstigem LAN-Verkehr absondern, wobei darauf hingewiesen wird, dass die physische Trennung bevorzugt wird, jedoch mindestens eine logische Trennung (wie VLAN) verwendet werden sollte.

Zusätzlich zu den physischen Schnittstellen, nutzen Speichersysteme eine Vielzahl von Software und Firmware um die Verwaltung von Speichersystemen zu ermöglichen. Die Software-Schnittstellen können einfache Command-Line-Interfaces (CLI), webbasierte Graphical-User-Interfaces (GUI) umfassen, Simple-Network-Management-Protocols (SNMP) unterstützen und serverbasierte Proxies, für die Handhabung des In-band-Managements (d. h. über den Datenpfad). Zum Schutz dieser Software-/Firmware-Schnittstellen sollten Organisationen:

- Firewalls und TCP-Wrapper verwenden, um den Zugriff auf Management-Netzwerke, auf autorisierte Systeme und Protokolle beschränken;
- Entitäts-Authentifizierung verwenden, um vertrauenswürdige Verbindungen zwischen Speichersystemen und den Managementsystemen (z. B. unter Verwendung von FC-SP-2 AUTH-A für die Authentifizierung der Entitäten, die das In-band-Management nach C.7.1 durchführen) aufzubauen;
- IDS- und IPS-Instrumente wirksam einsetzen, um anomale Verhalten zu identifizieren und davor zu schützen;
- ICT-Infrastruktur einsetzen (Domain-Name-System bzw. DNS, Service-Locator-Protocol bzw. SLP, Network Time Protocol bzw. NTP), mit geeigneten Sicherheitskontrollen zur Vermeidung indirekter Angriffe;
- geeignete Kontrollen privilegierter Anwender nutzen, einschließlich Authentifizierung (siehe 6.4.2.1), Autorisierung (siehe 6.4.2.2) und sicherer Auditierung/Überwachung (siehe 6.4.4);
- sicherstellen, dass Betriebssysteme und Anwendungen auf dem neuesten Stand und ausreichend gegen Angriffen gehärtet sind (siehe 6.4.5).

Wenn Speichersysteme fernverwaltet werden, sollten die folgenden zusätzlichen Sicherheitsmaßnahmen angewendet werden:

- Verwendung sicherer Kanäle für jeglichen Fernzugriff (Virtual Private Network bzw. VPN, TLS, Secure Shell bzw. SSH, Hypertext Transfer Protocol Secure bzw. HTTPS);
- Nutzung von sicherer Authentifizierung oder Multi-Faktor-Authentifizierung;
- Beschränkung von Privilegien auf das erforderliche Mindestmaß (d. h. minimales Recht).

Die Organisation sollte organisatorische und technische Maßnahmen ausarbeiten, um die Nutzung der Management-Schnittstelle für Fernwartungssitzungen (nicht lokal) des Verkäufers zu einzuschränken. Fernwartungstätigkeiten des Verkäufers, die von Personen durchgeführt werden, die über ein externes Netzwerk, wie das Internet, kommunizieren, schaffen signifikante Risiken, nicht nur bezüglich der Verfügbarkeit, sondern auch der Integrität und Vertraulichkeit.

Technische Maßnahmen sollten den Kommunikationsverkehr (d. h. Systeme, Anschlüsse und Protokolle) auf das für Fernwartungstätigkeiten des Verkäufers erforderliche Mindestmaß einschränken. Nachdem die zugreifende Seite authentifiziert ist, sollten zusätzliche Kontrollen für den Zugriffspunkt entwickelt worden sein, um die Wartungssitzung des Verkäufers zu autorisieren. Diese umfassen das Akzeptieren, die Genehmigungsanfrage oder die Ablehnung der beantragten Sitzung. Es sollten geeignete Logs erzeugt werden, die Auditaufzeichnungen der Aktionen des Verkäufers enthalten.

Die Organisation sollte Einwahl-Zugriffsleitungen auf autorisierte zugreifende Seiten beschränken. Das schließt ein, dass ein Modem-Rückruf-Protokoll und die Sperrung des Verbindungsaufbaus in Kraft gesetzt werden, bis der Verkäufer eine Wartungssitzung beantragt und die Organisation diese Anfrage autorisiert hat.

6.4.4 Sicherheitsprüfung, Kontenführung und Überwachung

Vorschriften zur Übereinstimmung und Vertragsklauseln enthalten häufig Anforderungen an die Überwachung und Berichterstattung. Ereignis-Logging und System-Kontenführung sind Schlüsselfähigkeiten (siehe C.5), um den Umgang mit diesen Anforderungen zu unterstützen. Aus Sicht der Speichersicherheit, ist das Ereignis-Logging möglicherweise die nützlichere dieser beiden Fähigkeiten, weil sie sowohl in Echtzeit angewendet werden kann als auch als Bestandteil einer Vorfallsuntersuchung. Daher müssen Speichersysteme und -infrastrukturen Teil des Ereignis-Logging-Programms der Organisation sein (für einen maßgebenden Leitfaden siehe auch ISO/IEC 27002:2013, 12.4).

Der folgende Logging-Leitfaden ist auf Speichersysteme anwendbar und sollte verwendet werden:

- zur Aufnahme des Speichers in die Logging-Politik, derart, dass:
 - bezüglich Speichersystemen und -geräten, die folgenden Elemente der Politik behandelt werden sollten:
 - Speichersysteme und-geräte sollten Teil des Audit-Loggings sein;
 - alle *signifikanten* Speichermanagementereignisse sollten gesammelt werden;
 - Logdaten aufbewahrt werden;
 - Logdaten entsprechend der Politik zur Logdatenaufbewahrung archiviert und erhalten werden; und
 - die Gerätezeit mit einer zuverlässigen externen Quelle synchronisiert ist.
 - die Logging-Politik (siehe auch 7.7.2) sollte beweisrelevante Erwartungen einschließen (Authentizität, Beweismittelkette usw.)
- Anwendung von externem oder zentralisiertem Ereignis-Logging an einer vertrauenswürdigen⁶⁾ Remote-Quelle, durch:
 - Umsetzung von zentralisiertem⁷⁾ Audit-Logging, um Ereignisse aus allen Quellen in einem einzelnen Repository zu sammeln;
 - Festlegen und Verwendung einer gemeinsamen, genauen Zeitquelle in der gesamten Umgebung, um sicherzustellen, dass Ereignisaufzeichnungen aus verschiedenen Quellen korreliert werden können;
 - Vermeidung der Verwendung von geräteresidenten Logs für etwas anderes als die Überwachung der Systemgesundheit (en: system health) und das Debugging, weil sie einfacher von Manipulation oder Zerstörung betroffen sein können, steht für Logs begrenzter Speicherplatz zur Verfügung, und sie schließen die Anwendung einer zentralisierten Analyse, Alarmgebung und Archivierung aus;
 - das native Logging von Ereignissen auf einem, und vorzugsweise auf mehreren⁸⁾, externen Log-Servern;

6) Eine vertrauenswürdige externe Ereignis-Logging-Quelle ist ein IT-Sicherheitsmanagementprodukt, das in einem ausgewiesenen Sicherheitsbereich bzw. -domain lokalisiert ist und von dem angenommen wird, dass es die Sicherheitsfunktionen korrekt verstärkt.

7) Zentralisierung sollte in diesem Kontext nicht so verstanden werden, dass das gesamte Audit-Logging in einer Organisation eine gemeinsame Infrastruktur nutzen muss. Es ist wichtiger, Speichersysteme/-ökosysteme innerhalb einer einzelnen Sicherheitsdomain zu besitzen, die eine gemeinsame Audit-Logging-Infrastruktur verwenden.

- Verwendung von Standard-Logging-Protokollen, wie Syslog⁹⁾, die den zuverlässigen Empfang und sichere Übermittlungen (z. B. TLS) unterstützen;
- Vorhalten von Geräten, die konfiguriert sind, Ereignisse bei ihrem Auftreten zu protokollieren (d. h. ungepuffert), wenn die Hauptbeweggründe für das Audit-Logging Übereinstimmung, Zurechenbarkeit oder Sicherheit sind;
- Umsetzung eines Analyseprotokolls, um Audit-Log-Aufzeichnungen über die Ereignisquellen korrelieren, um signifikante sicherheitsbezogene Ereignisse zu identifizieren, die Hinweise auf sicherheitsbezogene Vorfälle liefern;
- Sicherstellen, dass das Speicher-Logging in den Security-Information-and-Event-Management-Lösungen (SIEM) berücksichtigt wird, wenn derartige Technologie eingesetzt wird.
- Sicherstellen von vollständigem Ereignis-Logging;
 - sobald die zu protokollierenden Ereignisarten bestimmt wurden, sollten sämtliche Vorkommnisse dieser Ereignisse protokolliert werden (ob in-Band oder out-of-Band);
 - die folgenden Ereignisarten sollten protokolliert werden (ein Mindestsatz von sicherheitsbezogenen Ereignissen):
 - fehlgeschlagene und erfolgreiche Anmeldeversuche;
 - fehlgeschlagene Zugriffsversuche auf Dateien und Objekte bei sensiblen und Daten von hohem Wert;
 - Hinzufügungen, Änderungen und Löschungen von Benutzerkonten- und Gruppenprofilen;
 - Änderungen der Konfigurationen der Systemsicherheit (z. B. Audit-Logging, Netzwerkfilterung, Zoning-Änderungen);
 - Änderungen der Nutzung von Sicherheitsservern (z. B. syslog, Network Time Protocol bzw. NTP, Domain Name System bzw. DNS, Authentifizierung);
 - Systemabschaltungen und -neustarts;
 - privilegierte Operationen (d. h. von Administratoren initiierte Änderungen);
 - Nutzung sensibler Dienstprogramme (z. B. Privileg-Eskalationsbefehle);
 - Zugriff auf kritische Dateien;
 - Verlagern von virtuellen Servern zwischen physischen Servern;

8) Einige Logging-Protokolle verwenden unzuverlässige Netzwerk-Protokolle, wie User-Datagramm-Protocol (UDP) und dadurch können Log-Nachrichten aufgrund der Server- oder Netzwerkleistung verloren gehen. Das Senden von Nachrichten an mehrere Log-Destinationen verringert das Risiko von unbeabsichtigten Verlusten.

9) Syslog ist festgelegt in IETF RFC 5424, mit zusätzlichen Einzelheiten, die in IETF RFC 3195, IETF RFC 5425, IETF RFC 5426, IETF RFC 5427, IETF RFC 5848, IETF RFC 6012, und IETF RFC 6587 enthalten sind.

- jeder Log-Eintrag sollte enthalten:
 - einen Zeitstempel (Datum und Uhrzeit);
 - ein Schweregrad (en: Severity-Level);
 - die Quelle des Log-Eintrags (Kennname, IP-Adresse usw.);
 - eine Ereignis-ID sowie eine Textbeschreibung (notwendig, um die Lokalisierung/Internationalisierung von Ereignissen zu ermöglichen – bei denen die Ereignis-ID unverändert bleibt, aber die Textbeschreibung in andere Sprachen übersetzt werden könnte); und
 - eine Beschreibung des Ereignisses.
- Sorgfalt beim Filtern von Feldern wie „Severity“, weil die Logging-Politik des Unternehmens als Leitfaden bei der Bestimmung dienen sollte, welche Art der Filterung geeignet ist und welches Niveau von Informationen eine Langzeitspeicherung erfordert.
- das Umsetzen von geeigneter Aufbewahrung und geeignetem Schutz, derart dass:
 - Audit-Log-Daten, die möglicherweise einen beweiserheblichen Wert besitzen, korrekt gehandhabt werden sollten (z. B. Aufrechterhalten der Beweismittelkette, verifizierbare Integrität und Authentizität usw.);
 - Audit-Log-Daten mit spezifischen Aufbewahrungsanforderungen (z. B. Erfüllung gesetzlicher Auflagen) sollten mit der Datenaufbewahrungslösung der Organisation (siehe 7.4) aufbewahrt werden;
 - geeignete Maßnahmen zur Bewahrung der Log-Integrität und zur Verhinderung ihrer Änderung oder Zerstörung (entweder böswillig oder unbeabsichtigt) umgesetzt werden;
 - wenn Audit-Log-Einträge sensible Informationen enthalten, sollten die Audit-Log-Daten mit geeigneten Vertraulichkeitsinstrumenten¹⁰⁾ geschützt werden;
 - für eindeutige Audit-Logging-Anforderungen (z. B. hohe Volumen, besondere Aufbewahrung, Ereignis-Signatur usw.) sollten zugehörige und besonders gehärtete und konfigurierte Systeme verwendet werden;
 - Log-Relays und Log-Filterung wirksam eingesetzt werden, um die Auswirkung von speziellen Speicheranforderungen (z. B. Write-Once-Read-Only bzw. WORM) auf ein Mindestmaß zu beschränken.

6.4.5 Härten von Systemen

Sämtliche Betriebssysteme, Hypervisoren und Anwendungen sollten im Verhältnis zur Nutzung des Speichersystems gehärtet werden. Zusätzlich zum Leitfaden für den Umgang mit technischen Schwachstellen nach ISO/IEC 27002:2013, 12.6, gibt es zahlreiche bestehende bewährte Praktiken für verschiedene Betriebssysteme, die auf Grundlage des verwendeten Betriebssystems, in Bezug genommen werden sollten. Einige der bewährten Praktiken, die für jedes Betriebssystem verwendet werden sollten, umfassen:

- das Entfernen nicht benötigter/ungenutzter Software;
- das Entfernen von unnötigen Benutzerkonten;
- Änderungen (z. B. Umbenennung, Sperrung, Änderung aller voreingestellten Passwörter usw.) an jeglichen voreingestellten oder Standard-Benutzerkonten;

10) Einige Log-Einträge können Dinge wie Passwörter preisgeben (z. B. wenn ein Anwender anstatt der User-ID ein Passwort eingibt), es können aber auch subtilere Probleme bestehen (z. B. Suchbefehle, die spezielle Namen und Gesundheitsprobleme preisgeben).

- ausschließlich benötigte Netzwerk-Ports werden geöffnet;
- Installation der neuesten Patches, die aus einer vertrauenswürdigen Quelle stammen;
- Einspielen von Firmware-Updates aus einer vertrauenswürdigen Quelle;
- Installation und Instandhaltung des Schutzes vor Schadsoftware (siehe auch ISO/IEC 27002:2013, 12.2).

Wenn Elemente der Speicherinfrastruktur ein Update (z. B. Mikrocode) oder Patches empfangen, sollte sichergestellt sein, dass die anzuwendende Software aus vertrauenswürdiger Quelle stammt. Anderenfalls können Angreifer selbst ein „Update“ programmieren, das stattdessen einen Schadcode ihrer Wahl enthält, wie ein Rootkit, Botnet oder andere Schadsoftware.

Verkäufer sollten für Elemente in ihrer Zuständigkeit die in 6.4.5 beschriebenen Maßnahmen durchführen.

6.5 Blockbasierter Speicher

6.5.1 Fibre-Channel-Speicher (FC-Speicher)

Fibre-Channel-Speichersysteme verwenden spezialisierte Netztechnologie (siehe 6.3.2.2), um Computern blockbasierte Speicherressourcen darzustellen. Diese Ressourcen tragen üblicherweise die Form von logischen Einheiten (LUN) und Bandgeräten (einschließlich virtuellem Band).

Bei Fibre-Channel-Systemen sollte folgendes berücksichtigt werden:

- LUN-Masking und -Mapping (WWN-Filterung) und andere Zugriffskontrollinstrumente sollten für die Einschränkung des Speicherzugriffs verwendet werden;
- Umsetzung von FCP-Sicherheitsmaßnahmen, einschließlich:
 - gegenseitige Authentifizierung unter Verwendung von FC-SP-2 AUTH-A (siehe C.7) sollte mit allen Servern und Switches verwendet werden; wenn möglich, werden zentralisierte Authentifizierungsdienste wirksam eingesetzt;
 - wenn möglich, sollten Fibre-Channel-Verbindungen, die den geschützten Bereich (z. B. Grenzen eines physisch kontrollierten Datenzentrums) verlassen, unter Verwendung von ESP_Header¹¹⁾ (siehe 6.8.2.2 und C.7.3) verschlüsselt werden.
- Umsetzung von Verschlüsselungsmaßnahmen für ruhende Daten (siehe 6.8.2.3), einschließlich:
 - sensibler und Daten von hohem Wert, die verschlüsselt sein sollten, während sie sich auf dem Speichergerät oder-medium¹²⁾ befinden;
 - die Verschlüsselung sollte in Speichergeräten implementiert werden, die in Kontakt mit sensiblen oder regulierten Daten kommen können, sowie, um die schnelle Löschung (siehe A.3) zu ermöglichen.

11) Die Integrität oder Vertraulichkeit Fibre-Channel-Rahmens kann mit ESP_Header optionalen Headern bereitgestellt werden, die in ANSI INCITS 470–2011, *Fibre Channel – Framing and Signaling-3 (FC-FS-3)* festgelegt sind.

12) Die Verschlüsselung in FC-Speicher-Ökosystemen bietet einen Schutz auf Datenträgerebene und kann ein „Sicherheitsnetz“ für Daten sein, die üblicherweise von einem Server, einer Anwendung usw. als hauptsächliche Form des Schutzes verschlüsselt werden.

- Umsetzung von Maßnahmen zur Datenlöschung (siehe 6.8.1 und Anhang A), einschließlich:
 - an die Datenträger angepasste Löschung (siehe 6.8.1.2) sollte für sensible und regulierte Daten verwendet werden;
 - logische Löschung (siehe 6.8.1.3); sollte verwendet werden, um virtualisierten Speicher (siehe 7.6.1) zu löschen, insbesondere, wenn die tatsächlichen Speichergeräte und -medien nicht bestimmt werden können.

Verkäufer sollten die Funktionalität für die Zugriffskontrolle, Authentifizierung, Löschung und Verschlüsselung nach 6.5.1 in ihren Produkten umsetzen.

6.5.2 IP-Speicher

Anders als FC-Speicher, verwendet IP-Speicher TCP/IP-Netztechnologie (siehe 6.3.2.3), speziell iSCSI, um Computern blockbasierte Speicherressourcen zu präsentieren.

Für IP-Speichersysteme sollte folgendes berücksichtigt werden:

- Kontrolle des iSCSI-Initiator-Zugriffs, durch Filterung auf Grundlage von Quell-IP-Adressen und -Protokollen;
- Umsetzung von iSCSI-Sicherheitsmaßnahmen einschließlich:
 - bidirektionale CHAP-Authentifizierung, die zufällige Challenges (d. h. unbeantwortete) verwendet, sollte sowohl für Initiatoren als auch Ziele in allen iSCSI-Implementierungen verwendet werden;
 - IPsec sollte verwendet werden, um den Kommunikationskanal zu sichern, wenn sensible oder Daten von hohem Wert exponiert sein könnten (siehe 6.8.2.2);
 - Internet-Storage-Name-Service- (iSNS), SLP-, DNS-Infrastruktur sollten mit geeigneten Sicherheitsmaßnahmen verwendet werden, um indirekte Angriffe zu verhindern.
- Umsetzung von Verschlüsselungsmaßnahmen für ruhende Daten (siehe 6.8.2.3);
 - sensible und Daten von hohem Wert sollten verschlüsselt sein, während sie sich auf dem Speichergerät oder-medium¹³⁾ befinden;
 - die Verschlüsselung sollte in Speichergeräten implementiert werden, die in Kontakt mit sensiblen oder regulierten Daten kommen können, sowie, um die schnelle Löschung (siehe A.3) zu ermöglichen.
- Umsetzung von Maßnahmen zur Datenlöschung (siehe 6.8.1 und Anhang A);
 - an die Datenträger angepasste Löschung (siehe 6.8.1.2) sollte für sensible und regulierte Daten verwendet werden;
 - logisches sicheres Löschen (siehe 6.8.1.3) sollte verwendet werden, um virtualisierten Speicher logisch zu löschen, insbesondere, wenn die tatsächlichen Speichergeräte und -medien nicht bestimmt werden können.

Verkäufer sollten die Funktionalität für die Zugriffskontrolle, Authentifizierung, Löschung und Verschlüsselung nach 6.5.2 in ihren Produkten umsetzen.

13) Die Verschlüsselung in IP-Speicher-Ökosystemen bietet einen Schutz auf Datenträgerebene und kann ein „Sicherheitsnetz“ für Daten sein, die üblicherweise von einem Server, einer Anwendung usw. als hauptsächliche Form des Schutzes verschlüsselt werden.

6.6 Dateibasierte Speicherung

6.6.1 NFS-basierte Netzwerkspeicher (NAS)

Die Art von Speicher ist ein LAN-gebundener Dateiserver, der Dateien unter Verwendung des Netzwerkprotokolls, NFS (siehe 6.3.3.2) darstellt. Er besteht aus einer Engine, die die Dateidienste und ein oder mehrere Speichergeräte, auf dem/denen die Daten gespeichert sind, implementiert. Ein NAS-System kann auch SAN-angebunden sein; in diesem Fall wird das NAS-System wie jeder andere Server im SAN behandelt (z. B. bereitgestellter Speicherzugriff, LAN-freie Backups usw.). NFS-basierte NAS-Systeme können zahlreiche verschiedene Formen aufweisen, (z. B. von einfachen NAS-Servern bis zu hochskalierbaren Clustern) und sind zumeist hochgradig optimiert für den Umgang mit großen Mengen von gleichzeitig erfolgenden Dateizugriffen.

Für NFS-basierte NAS-Systeme sollte folgendes berücksichtigt werden:

- Anwendung von Zugriffskontrollen auf NFS-exportierte Dateisysteme, einschließlich:
 - wann immer möglich, Nutzung von Authentifizierung auf Anwenderebene, (z. B. NFSv4 mit Kerberos V5);
 - Konfigurieren des NFS-Servers zum Export von Dateisystemen explizit für die autorisierten Anwender;
 - Konfigurieren des NFS-Servers zum Export von Dateisystemen mit den minimal erforderlichen Privilegien;
 - Verhinderung, dass „Root-“ oder „Administrator-“Zugriff auf Dateien in Netzwerk-Dateisystemen gewährt wird;
 - Sicherstellung, dass NFSv4 ACLs (Access Control Lists) korrekt zugewiesen werden;
 - Verwendung der Kerberos-Authentifizierung für NFSv3;
 - Berücksichtigung, dass die sicheren und privaten Modi von Kerberos verwendet werden, um NFS-Verkehr zu signieren und zu verschlüsseln.
- Einschränken des Verhaltens der NFS-Clients;
 - Clientzugriff auf NFS-Freigaben wann immer möglich filtern;
 - NFS-Clients wird nicht gestattet, *suid*- und *sgid*-Programme auf exportierten Dateisystemen zu betreiben.
- Sichern der Daten auf NFS-Server
 - exportierte Dateisysteme sollten in ihren eigenen Partitionen laufen, um Funktionsbeeinträchtigungen des Systems durch einen Angreifer zu vermeiden, der ein exportiertes Dateisystem beschreibt, bis es voll ist;
 - ruhende Daten werden bei Bedarf verschlüsselt;
 - NFS-Exporte von administrativen Dateisystemen (z. B. */etc*) werden nicht zulassen;
 - Schutz vor Schadsoftware (z. B. Viren, Würmer, Rootkits usw.);
 - fortlaufende Überwachung von Inhalten, die in NFS-Freigaben platziert sind sowie entsprechende Zugriffskontrollen.

Verkäufer sollten die Funktionalität für die Zugriffskontrolle, Authentifizierung und Verschlüsselung nach 6.6.1 in ihren Produkten umsetzen.

6.6.2 SMB/CIFS-basierte NAS

Wie NFS-basierte NAS (siehe 6.6.1), ist SMB/CIFS-basierte NAS ein LAN-angebundener Dateiserver, der Dateien bedient, sich jedoch in seiner Verwendung von Netzwerk-Protokollen, SMB/CIFS (siehe 6.3.3.3), unterscheidet.

Bei SMB/CIFS-basierten NAS-Systemen sollte folgendes berücksichtigt werden:

- Anwendung von Zugriffskontrollen auf SMB/CIFS-exportierte Dateisysteme;
 - Sperrung unauthentifizierten Zugriffs auf CIFS-Freigaben und NAS-Geräte (d. h. Einschränken von *Anonymous*);
 - Sperrung von „Gast“- und „Everyone“-Zugriff auf sämtliche CIFS-Freigaben;
 - Umsetzung der Authentifizierung und Zugriffskontrolle über ein zentralisiertes Instrument (RADIUS, Lightweight-Directory-Access-Protocol bzw. LDAP).
- Einschränkung des SMB/CIFS-Clientverhaltens durch Ermöglichen einer SMB-Signatur für Clients und das NAS-Gerät;
- Sichern der Daten auf SMB/CIFS-Servern:
 - Ermöglichen von CIFS-Prüfungen, wann immer möglich;
 - fortlaufende Überprüfung von Inhalten, die in CIFS-Freigaben platziert werden sowie von relevanten Zugriffskontrollen;
 - Verschlüsseln von ruhenden Daten bei Bedarf;
 - Schutz vor Schadsoftware (z. B. Viren, Würmer, Rootkits usw.);
- Umsetzung von CIFS mit sicherer Authentifizierung (NTLMv2, Kerberos).

Verkäufer sollten die Funktionalität für die Zugriffskontrolle, Authentifizierung und Verschlüsselung nach 6.6.2 in ihren Produkten umsetzen.

6.6.3 Parallele NFS-basierte NAS

Wie in 6.3.3.1 angeführt, können NAS-Geräte als einzelne Speicherserver oder als gruppierte Zusammenstellung von Speicherservern implementiert werden. Diese Cluster treten in zwei Formen auf, symmetrisch und asymmetrisch, und die beiden können kombiniert werden. Symmetrische Cluster ermöglichen allen Dateiservern, vollständige Dateiserver zu sein, mit Umleitung oder ähnlichen Techniken, die für die Auswahl geeigneter Server verwendet werden, auf Grundlage des Clients und der Art der Dateien, auf die der Client zugreifen möchte. Ein übliches Verfahren ist das Partitionieren des Namensraums des Dateisystems mit verschiedenen Servern, die für die verschiedenen Abschnitte dieses Namensraums zuständig sind – in einer derartigen Struktur kann eine Auflösung des Dateinamens dazu führen, dass ein Client den Pfad eines Namensraums durchläuft, der eine Vielzahl von Dateiservern umfasst. Asymmetrische Cluster teilen die Funktionalität serverübergreifend auf – ein paralleles NFS verwendet mindestens einen primären Dateiserver und viele sekundäre Speicherserver, die dem Primärserver untergeordnet (en: *slaved*) sind (Client muss den primären Dateiserver kontaktieren, um nachzuvollziehen, welche Daten auf dem sekundären Speicherservern gespeichert sind und wie darauf zugegriffen werden kann).

Bei einem symmetrischen Cluster, einschließlich der Clusterbildung von primären Dateiservern für ein pNFS, ist der wichtigste Leitfaden für die einheitliche Anwendung von Kontrollen und Kontrollinstrumenten (z. B. Authentifizierung und Autorisierung) übergreifend über die gruppierten Server, so dass die Eigenschaften zur Wahrung der Sicherheit nicht davon abhängig sind, auf welche Dateiserver der Client tatsächlich zugreift.

Bei asymmetrischen Clustern ist die einheitliche Anwendung von Kontrollen und Kontrollinstrumenten wichtig, die verschiedenen Rollen der Server können jedoch Verantwortungen auf den Client übertragen, die es in einem symmetrischen Cluster nicht gibt. Eine spezifische Komplikation bei pNFS ist, dass sekundäre Speicherserver möglicherweise nicht dasselbe Protokoll (NFS) wie der/die primäre(n) Dateiserver verwenden, wodurch die Implementierung von Kontrollen auf einheitliche Weise, über beide Protokolle übergreifend, erforderlich wird. Ein anderes wichtiges Beispiel ist, dass das pNFS-Block-/pNFS-Volume-Layout erfordert, dass dem Client dahingehend vertraut wird, dass er die vom Primärserver erhaltenen Layout-Informationen respektiert und nicht auf den Blockspeicher zugreift, für den er kein Layout besitzt – das sollte irgendwie in einer Maßnahme festgehalten werden, die die Empfehlung durchsetzt, kein pNFS-Block-/pNFS-Volume-Layout zu verwenden, wenn Clients nicht dahingehend vertraut werden kann – siehe Sicherheitsüberlegungen (Abschnitt 4) in IETF RFC 5663.

In beiden Fällen sollten Kontrollen nicht vom Durchqueren des Pfads des serverübergreifenden Dateisystem-Namensraums abhängig sein – der direkte Zugriff vom Client auf Server, die nicht dafür vorgesehen sind, dass der Client „von ihnen startet“ ist eine wichtige Überlegung bei der wirksamen Umsetzung von Kontrollen, da manche Server einen partiellen Dateisystem-Namensraum (kein „Root“, von dem zu starten, vom Client erwartet wird) oder gar keinen Dateisystem-Namensraum exportieren können. Ein spezifisches Beispiel des letzteren ist, dass begrenzte oder keine Kontrolle in Abhängigkeit von der Tatsache bestehen sollten, dass einige Server keinen Dateisystem-Namensraum exportieren können (z. B. wie bei pNFS-Speicherservern der Fall). Ein anderes Beispiel ist, dass eine Verzeichnis-ACL, die einen Namensraum-Pfad-Durchquerung blockiert, eine unzureichende Kontrolle bei einem Namensraum-Pfad sein kann, der auf einen anderen Dateiserver übergreift – eine wirksame Kontrolle muss den direkten Clientzugriff zu dem letztgenannten Dateiserver behandeln, weil ein derartiger Zugriff die Verzeichnis-ACL umgehen würde.

Bei pNFS-Systemen sollte folgendes berücksichtigt werden:

- Kontrollen und Kontrollinstrumente sollten konsistent clusterübergreifend (sowohl symmetrische als auch asymmetrische) angewendet werden;
- Eigenschaften zur Wahrung der Sicherheit sollten nicht davon abhängig sein, dass ein Client auf einen spezifischen Dateiserver zugreift;
- bei asymmetrischen Clustern sollten Kontrollen umgesetzt werden, so dass sie über verschiedene Protokolle übergreifend konsistent sind;
- Sicherheitsmaßnahmen sollten nicht von der serverübergreifenden Pfad-Traversal des Dateisystem-Namensraums abhängig sein.

6.7 Objekt-basierter Speicher

6.7.1 Cloud-Computing-Speicher

6.7.1.1 Sicherung von Cloud-Computing-Speicher

Es sind sowohl proprietäre als auch standardbasierte Cloud-Computing-Speicher-Angebote gebräuchlich und sie stellen üblicherweise Kopierfähigkeiten (z. B. Spiegeln eines Teils oder des gesamten Speichers in einem System), Backup- und Wiederherstellungsfähigkeiten, Langzeitaufbewahrungsfähigkeiten (z. B. Archive) und Multisystem-Synchronisierungsfähigkeiten (z. B. ermöglicht einem Anwender die Datensynchronisierung zwischen mehreren, potentiell unterschiedlichen Arten von Geräten) bereit. Personen und Organisationen zögern jedoch, ihre Daten einem Cloud-Computing-Speicher anzuvertrauen, sofern sie nicht die Gewissheit haben, dass die relevanten sicherheitsbezogenen Bedrohungen und Herausforderungen behoben wurden¹⁴⁾.

14) Die Empfehlung ITU-T X.1601, *Security framework for cloud computing*, enthält eine nützliche Zusammenfassung von sicherheitsbezogenen Bedrohungen und Herausforderungen beim Cloud-Computing.

Einige dieser Cloud-Computing-Implementierungen sind objektbasiert und sind häufig HTTPS-abhängig (HTTP über TLS), zum Schutz der zugrundeliegenden Kommunikation. Zusätzliche Sicherheitsmerkmale dürfen festgelegt werden, es kann jedoch ein signifikanter Unterschied bestehen, in Bezug auf das, was implementiert wird, gegenüber dem, was letztendlich Verwendung findet.

Die sichere Verwendung von Cloud-Computing-Speicher sollte das Folgende teilweise oder vollständig einbeziehen:

- sicherstellen, dass die Übertragungssicherheit, wie IPsec oder Transport-Layer-Security (TLS) bei allen Transaktionen verwendet wird (siehe 6.8.2.2);
- wenn sensible Daten in der Cloud-Umgebung einer dritten Seite gespeichert werden, sollte eine Verschlüsselung der ruhenden Daten (und geeignete Schlüssel-Managementprozesse) angewendet werden, um den Zugriff durch unautorisierte Dritte zu verhindern (z. B. Personal des Cloud-Diensteanbieters, andere Mandanten, Widersacher usw.);
- Sichern der Anwenderregistrierung und Verwendung sicherer Passwort-Authentifizierung, um den Datenzugriff zu schützen;
- Nutzung von Zugriffskontrollen, die vor unautorisiertem Zugriff durch andere Mandanten schützen, während Anwendern, denen der Datenzugriff gestattet ist, geeignete Zugriffsprivilegien zur Verfügung gestellt werden;
- Verwendung geeigneter Fähigkeiten zum sicheren Löschen, um sensible Daten aus dem Cloud-Computing-Speicher logisch zu löschen.

ANMERKUNG In einigen Rechtssystemen können Anforderungen an die Privatsphäre, wie das „Recht auf Löschung“ oder das „Recht auf Vergessenwerden“, zusätzliche Sicherheitskontrollen notwendig machen.

Cloud-Computing-Implementierungen setzen häufig verschiedene Formen der Virtualisierung ein, so dass der Leitfaden in 7.6 ebenfalls relevant sein kann.

Verkäufer sollten die geeignete Funktionalität des Cloud-Computing-Speichers für die Zugriffskontrolle, Authentifizierung, Verschlüsselung, Logging, Löschung usw. nach 6.7.1.1 in ihren Produkten umsetzen.

6.7.1.2 CDMI-Sicherheit

Cloud-Computing-Speicher, auf Grundlage der Festlegung nach ISO/IEC 17826:2012, *Cloud data management interface (CDMI)*, ist eine objektbasierte Speichertechnologie, die eine RESTful-HTTP-Schnittstelle verwendet. Sie besitzt ausreichend beschriebene Sicherheitselemente, sodass ein spezifischer Leitfaden bereitgestellt werden kann. Sicherheitsmaßnahmen im CDMI können zusammengefasst werden als Übertragungssicherheit, Anwender- und Entität-Authentifizierung, Autorisierung und Zugriffskontrollen, Datenintegrität, sicheres Löschen von Daten und Datenträgern, Datenaufbewahrung, Schutz vor Schadsoftware, Data-at-Rest-Verschlüsselung und Abfragen der Sicherheitsfähigkeit. Mit Ausnahme sowohl der Übertragungssicherheit und der Abfragen der Sicherheitsfähigkeit (Instrument zum Bestimmen, was unterstützt wird), deren Umsetzung obligatorisch ist (die Anwendung ist immer optional), können die Sicherheitsmaßnahmen von Umsetzung zu Umsetzung erheblich von einander abweichen.

CDMI-Clients sollten:

- sicherstellen, dass die Transport-Layer-Security (TLS) für alle Transaktionen verwendet wird (siehe 6.8.2.2);
- die Sicherheitsfähigkeiten der CDMI-Umsetzung des Cloud-Diensteanbieters abfragen und eine risikobasierte Entscheidung treffen, ob die angebotene Sicherheit angemessen ist;

- CDMI-Entitäten authentifizieren (Zertifikate für Server und HTTP-Basic-Authentication für Clients);
- CDMI-Domains verwenden, um einen Platz für Authentifizierungsmappings für externe Authentifizierungsanbieter bereitzustellen;
- CDMI-Sicherheits-Logging ermöglichen und die Sicherheitsereignisdaten aus der entsprechenden Logging-Warteschlange regelmäßig und rechtzeitig wiederherstellen;
- die automatische Löschungsfähigkeit (CDMI-Löschung) an die Politik der Organisation zur Datenaufbewahrung anpassen;
- vor der Verwendung von CDMI-Holds, den Prozess und das Instrument für die Anhebung des CDMI-Holds nachvollziehen;
- Maßnahmen zur Verschlüsselung ruhender Daten anwenden, um sensible und Daten von hohem Wert zu schützen;
- für die kryptografische Funktionalität, stets verifizieren, dass bei der Umsetzung ausschließlich eine geforderte CDMI-Capability (unterstützte Operation) verwendet wurde;
- die bereitgestellten Einrichtungen zum sicheren Löschen verwenden, um sensible Daten aus dem Speicher des Cloud-Diensteanbieters logisch zu löschen.

Verkäufer sollten die geeignete CDMI-Funktionalität für die Zugriffskontrolle, Authentifizierung und Verschlüsselung, Logging, sichere Löschung usw. nach 6.7.1.2 in ihren Produkten umsetzen.

6.7.2 Objektbasiertes Speichergerät (OSD)

Ein objektbasiertes Speichergerät (OSD) ist ein Computerspeichergerät, das dem Platten-Speicher ähnelt, aber auf einer höheren Ebene arbeitet (d. h. die physischen Speicherorte sind unter der Objektschnittstelle verborgen und werden durch den Speicher selbst verwaltet). Anstatt eine blockorientierte Schnittstelle bereitzustellen, die Datenblöcke von fester Größe liest und schreibt, organisiert ein OSD Daten in Datencontainern flexibler Größe, die „Objekt“ genannt werden. Jedes Objekt hat sowohl Daten (eine lineare Abfolge von Bytes) als auch Metadaten (ein erweiterbarer Satz von Attributen, die das Objekt beschreiben), auf die durch die Festlegung von Object-IDentifiern (OID) und einem (Offset, Länge) Tupel zugegriffen wird. Die OSD-Schnittstelle umfasst Befehle¹⁵⁾ zum Erzeugen und Löschen von Objekten, Schreiben von Bytes und Lesen von Bytes von einzelnen Objekten, und um Attribute von Objekten festzulegen und abzurufen. Das OSD ist zuständig für die Verwaltung der Speicherung von Objekten und ihrer Metadaten. Das OSD implementiert ein Sicherheitsinstrument, das eine Zugriffskontrolle je Objekt und je Befehl bietet.

Zur Sicherstellung des sicheren Zugriffs auf den Speicher, ist jeder Befehl mit einer kryptografisch sicheren Fähigkeit verbunden, die ein spezifisches Objekt und die Liste der an einem spezifischen Objekt durchführbaren Operationen identifiziert. Fähigkeiten stellen nicht nur die geräteeigene Sicherheit bereit, die bei üblichen blockbasierten Speichern fehlt, sondern sie erleichtern ebenfalls den feinkörnigen Zugriff auf Einzelobjekte. Das ermöglicht die Speichergerätefreigabe zwischen unterschiedlichen Anwendungen mit eindeutigen Sicherheitsanforderungen.

OSD verwendet ein auf Anmeldeinformationen basierendes Zugriffskontrollsystem, das sich aus drei aktiven Entitäten zusammensetzt: dem Objektspeicher (das OSD), einem Sicherheitsmanager und einem Client. Als ein fähigkeitenbasiertes Zugriffskontrollsystem werden alle Anfragen an den Objektspeicher mit einer Fähigkeit verbunden, die einen Satz von Rechten, den der Halter an einem Objekt hat, verschlüsselt und die kryptografisch geschützt ist.

15) Die ursprüngliche OSD-Norm ANSI INCITS 400-2004, *Information technology — SCSI Object-based Storage Device Commands (OSD)*, wurde 2004 angenommen, eine neuere Version der OSD-Norm ist ANSI INCITS 458-2011, *Information technology — SCSI Object-Based Storage Device Commands – 2 (OSD-2)*.

Für die sichere Verwendung von OSD:

- sollte IPsec für alle Transaktionen verwendet werden, die sensible Daten in unsicheren Netzwerken betreffen;
- sollte der Objektspeicher die Authentizität der Fähigkeit vor Durchführung einer Operation verifizieren;
- sollte die Uhrensynchronisierung zwischen dem OSD und dem Sicherheitsmanager unter Verwendung eines sicheren Protokolls umgesetzt werden;
- sollten die Gültigkeitsdauern von Fähigkeiten begrenzt sein, um die Dauer zu minimieren, für die eine kompromittierte Fähigkeit verwendet werden kann;
- Arbeitsschlüssel (für die Erzeugung von Fähigkeitsschlüsseln) sollten häufig erneuert werden.

Verkäufer sollten die geeignete OSD-Funktionalität für die Zugriffskontrolle, Authentifizierung und Verschlüsselung usw. nach 6.7.2 in ihren Produkten umsetzen.

6.7.3 Content-Adressable-Storage (CAS)

Die Technologie des Content-Adressable-Storage (CAS), mitunter als Fixed-Content-Storage (FCS) bezeichnet, ist dazu vorgesehen, Daten zu speichern, die sich nicht zeitabhängig ändern (d.h. zeitlich unveränderbar). CAS exponiert üblicherweise einen Hashwert, der durch eine kryptografische Hash-Funktion (wie MD5 oder SHA-1) aus dem Dokument erzeugt wurde, auf das er sich bezieht. Die Hauptvorteile der CAS-Technologie sind, dass der Anwender nicht den Ort der tatsächlichen Daten und die Anzahl der gespeicherten Kopien zu kennen braucht.

CAS unterstützt die Wiederherstellung von Dokumenten, die Hashwerte ihres Contents (de: Inhalt) vorausgesetzt, und stellt sicher, dass das wiederhergestellte Dokument mit dem ursprünglich gespeicherten identisch ist. (Falls die Dokumente verschieden waren, würden ihre Content-Adressen abweichen.) Ferner gibt es, weil Daten ihrem Inhalt entsprechend in einem CAS-System gespeichert werden, keine Situation, in der mehr als eine Kopie eines identischen Dokuments im Speicher existiert. Der Definition nach, besitzen zwei identische Dokumente dieselbe Content-Adresse.

Falls die vom CAS-System verwendete Hash-Funktion schwach ist, könnte dieses Verfahren in einer ungünstigen Umgebung (verschiedene Dokumente erzeugen denselben Hash) Gegenstand von Kollisionen sein. Daher ist es für das CAS-System wichtig, ein robustes Hashing-Instrument zu verwenden.

Anwender und Anwendungen sollten authentifiziert und autorisiert werden, bevor der Zugriff auf das CAS-System gewährt wird. Dadurch wird verhindert, dass unautorisierte Anwender Daten speichern oder wiederherstellen. Zusätzlich sollte das CAS-System sicherstellen, dass Inhalte über ihren gesamten Lebenszyklus lesbar und zugreifbar bleiben. Schließlich sollte das CAS-System ein robustes Hashing-Instrument verwenden.

CAS ist eine besonders nützliche Technologie beim Umgang mit Erfordernissen aus Anforderungen an die kurz- und langfristige Aufbewahrung (siehe 7.4.2).

Verkäufer sollten die geeignete CAS-Funktionalität für die Authentifizierung, Autorisierung, Verfügbarkeit, Hashing usw. nach 6.7.3 in ihren Produkten umsetzen.

6.8 Dienste für die Speichersicherheit

6.8.1 Sicheres Löschen von Daten

6.8.1.1 Allgemeines

Ein wichtiges Element des Leitfadens für den Umgang mit Datenträgern, wie in ISO/IEC 27002:2013, 8.3, beschrieben, ist die Sicherstellung, dass Daten nicht wiederhergestellt werden können, wenn Datenträger nicht länger benötigt werden. Sicheres Löschen bezieht sich auf den allgemeinen Prozess, zuvor in einem Speichermedium geschriebene Daten, nicht wiederherstellbar zu machen, so dass eine begründete Gewissheit besteht, dass die Daten nicht ohne weiteres wiederhergestellt oder rekonstruiert werden können (siehe C.4).

Für die wirksame Anwendung dieser Norm auf alle Arten von Datenträgern, sollten Organisationen und Einzelpersonen ihre Information kategorisieren, die Beschaffenheit des Datenträgers, auf dem sie aufgezeichnet sind, bewerten, das Risiko für die Vertraulichkeit bewerten und die zukünftigen Pläne für den Datenträger (z. B. Wiederverwendung) bestimmen. Dann wird über die geeignete Art der sicheren Löschung entschieden. Die gewählte Art sollte in Hinsicht auf Kosten, Umweltauswirkungen usw. bewertet werden, und es sollte eine Entscheidung gefällt werden, durch die das Risiko für die Vertraulichkeit am besten gemindert und die den anderen, dem Prozess auferlegten Einschränkungen am besten gerecht wird.

Die Entsorgung von Speichergeräten oder Speicherelementen ohne sicheres Löschen sollte ausschließlich in Fällen erwogen werden, in denen eine Offenlegung der Informationen keine Auswirkung auf die Mission der Organisation haben würde, nicht zu Schäden an organisationseigenen Assets führen würde und nicht zu finanziellem Verlust oder Schaden von Personen führen würde.

Logisches Löschen, physisches Löschen und Zerstörung (Vernichten) sind Maßnahmen, die zum sicheren Löschen von Speicher ergriffen werden können. In A.1 wird jedes Verfahren beschrieben und, sofern zutreffend, zusätzliche Optionen bereitgestellt. Diese Information wird durch A.2 ergänzt, indem ein spezifischer Leitfaden zum sicheren Löschen von sowohl Hardcopy- als auch elektronischen (Soft-)Copy-Medien bereitgestellt wird.

Sichere Löschvorgänge können kostenintensiv und zeitaufwändig sein, sie sind jedoch aus Sicherheitsgründen notwendig. Das Niveau der sicheren Löschvorgänge sollte anhand der Risiken abgewogen werden. Besondere Sorgfalt sollte bei personenbezogenen Daten (PII) und elektronischen Patientenakten (EHR, en: electronic healthcare record) angewendet werden, sowie bei geschäfts- oder auftragsentscheidenden Daten (z. B. Geschäftsgeheimnisse, geistiges Eigentum usw.).

Wenn das sichere Löschen ein Element der Übereinstimmung ist, sollten die spezifischen Anforderungen und zugehörigen Spezifikationen überprüft werden, um zu bestimmen, ob sie bestimmte Verfahren des Überschreibens, dokumentierte Nachweise des sicheren Löschens usw. vorschreiben. Diese Anforderungen können die Form von spezifischen Verfahren des Überschreibens, Nachweis der sicheren Löschung usw. tragen.

Um geeignete Fähigkeiten zum sicheren Löschen zur Verfügung zu stellen, sollten Verkäufer die Funktionalität nach 6.8.1.2, 6.8.1.3, 6.8.1.4, 6.8.1.5 und Anhang A in ihren Produkten umsetzen.

6.8.1.2 Datenträgerbasierte Löschung

Wenn Speichermedien weitergegeben werden, veralten, nicht mehr nutzbar sind oder nicht von einem Informationssystem benötigt werden, sollten die verbleibenden magnetischen, optischen, elektrischen oder sonstigen Darstellungen von Daten sicher gelöscht werden.

Anhang A sollte angewendet werden, um die empfohlene sichere Löschung von spezifischen Datenträgern zu bestimmen. Obwohl die Anwendung von Anhang A nachdrücklich empfohlen wird, bestehen andere Verfahren, die den Zweck des logischen Löschens, physischen Löschens (in einigen Fällen noch relevant) und Zerstörens erfüllen; nicht in Anhang A festgelegte Verfahren können geeignet sein, sofern sie durch die Organisation überprüft und als zufriedenstellend befunden wurden. Diese Internationale Norm legt nicht