DIN EN ISO/IEC 27040

ICS 35.030

Informationstechnik – IT-Sicherheitsverfahren – Speichersicherheit (ISO/IEC 27040:2015); Deutsche Fassung EN ISO/IEC 27040:2016

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

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

Gesamtumfang 137 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

© DIN Deutsches Institut für Normung e. V. · Jede Art der Vervielfältigung, auch auszugsweise, nur mit Genehmigung des DIN Deutsches Institut für Normung e. V., Berlin, gestattet.
Alleinverkauf der Normen durch Beuth Verlag GmbH, 10772 Berlin

Preisgruppe 34
www.din.de
www.beuth.de

Documents
Document Sharing Hub
2552473

Full document details: DIN EN ISO/IEC 27040:2017-03

Nationales Vorwort

Dieses Dokument (EN 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 EN 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).

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 17788:2016-04
ISO/IEC 27000	siehe	DIN ISO/IEC 27000*)
ISO/IEC 27001:2013	siehe	DIN ISO/IEC 27001:2015-03

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*

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

*) In Bearbeitung.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 27040

August 2016

ICS 35.040

Deutsche Fassung

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

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

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

Diese Europäische Norm wurde vom CEN am 19. Juni 2016 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN-CENELEC oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, der ehemaligen jugoslawischen Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

CEN-CENELEC Management-Zentrum: Avenue Marnix 17, B-1000 Brüssel

© 2016 CEN- und CENELEC Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den nationalen Mitgliedern von CEN- und CENELEC vorbehalten.

Ref. Nr. EN ISO/IEC 27040:2016 D

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

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 ... 17
5.1 Allgemeines ... 17
5.2 Speicherkonzepte ... 17
5.3 Einführung in die Speichersicherheit ... 18
5.4 Risiken der Speichersicherheit ... 20
5.4.1 Hintergrund ... 20
5.4.2 Bruch der Vertraulichkeit ... 21
5.4.3 Datenbeschädigung und Datenvernichtung ... 22
5.4.4 Vorübergehender oder dauerhafter Verlust des Zugriffs/der Verfügbarkeit ... 23
5.4.5 Versagen des Erfüllens gesetzlicher, behördlicher oder rechtlicher Anforderungen ... 23

6 Unterstützende Maßnahmen ... 24
6.1 Allgemeines ... 24
6.2 Direct Attached Storage (DAS) ... 24
6.3 Speichernetzwerk ... 25
6.3.1 Hintergrund ... 25
6.3.2 Speichernetzwerke (SAN) ... 25
6.3.3 Netzwerkspeicher (NAS) ... 30
6.4 Speichermanagement ... 32
6.4.1 Hintergrund ... 32
6.4.2 Authentifizierung und Autorisierung ... 33
6.4.3 Schutz der Managementschnittstellen ... 34
6.4.4 Sicherheitsprüfung, Kontenführung und Überwachung ... 36
6.4.5 Härten von Systemen ... 38
6.5 Blockbasierter Speicher ... 39
6.5.1 Fibre-Channel-Speicher (FC-Speicher) ... 39
6.5.2 IP-Speicher ... 40
6.6 Dateibasierte Speicherung ... 40
6.6.1 NFS-basierte NAS ... 40
6.6.2 SMB/CIFS-basierte NAS ... 41
6.6.3 Parallele NFS-basierte NAS ... 42
6.7 Objekt-basierter Speicher ... 43
6.7.1 Cloud-Computing-Speicher ... 43
6.7.2 Objektbasiertes Speichergerät (OSD) ... 45
6.7.3 Content Adressable Storage (CAS) ... 46
6.8 Dienste für die Speichersicherheit ... 47
6.8.1 Daten-Löschung ... 47
6.8.2 Vertraulichkeit von Daten ... 50
6.8.3 Daten-Reduzierung ... 53

7 Leitlinien für Design und Umsetzung der Speichersicherheit ... 54
7.1 Allgemeines ... 54

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

7.2 Designgrundsätze der Speichersicherheit ... 54
7.2.1 Konzept der gestaffelten Verteidigung ... 54
7.2.2 Sicherheits-Domains ... 55
7.2.3 Resilienz des Designs ... 56
7.2.4 Sichere Initialisierung ... 56
7.3 Verlässlichkeit, Verfügbarkeit und Resilienz von Daten ... 57
7.3.1 Verlässlichkeit ... 57
7.3.2 Verfügbarkeit ... 58
7.3.3 Backup und Vervielfältigung ... 58
7.3.4 Disaster Recovery und Business Continuity (DR/BC) ... 59
7.3.5 Resilienz ... 60
7.4 Datenaufbewahrung ... 60
7.4.1 Langfristige Datenaufbewahrung ... 60
7.4.2 Kurz- bis mittelfristige Datenaufbewahrung ... 61
7.5 Vertraulichkeit und Integrität von Daten ... 62
7.6 Virtualisierung ... 65
7.6.1 Speichervirtualisierung ... 65
7.6.2 Speicher für virtualisierte Systeme ... 66
7.7 Überlegungen zu Design und Umsetzung ... 67
7.7.1 Themen zu Verschlüsselung- und Schlüsselmanagement ... 67
7.7.2 Ausrichten von Speicher und Richtlinie ... 68
7.7.3 Compliance ... 69
7.7.4 Sichere Mandantenfähigkeit ... 70
7.7.5 Sichere autonome Datenverschiebung ... 71

Anhang A (normativ) Löschen von Datenträgern ... 73
A.1 Methoden zum Löschen von Datenträgern ... 73
A.2 Löschen von verschiedenen Datenträgertypen ... 74
A.3 Leitlinien zum kryptographischen Löschen von Geräten ... 87

Anhang B (informativ) Auswahl geeigneter Speichersicherheitsmaßnahmen ... 91
B.1 Kriterien zur Auswahl von Maßnahmen ... 91
B.1.1 Überblick ... 91
B.1.2 Datensensibilitätsklassen ... 92
B.1.3 Sicherheitsvorrangcodes ... 93
B.2 Zusammenfassung der Speichersicherheitsmaßnahmen ... 93
B.2.1 Unterstützende Maßnahmen für die Speichersicherheit ... 93
B.2.2 Leitfaden für Design und Umsetzung der Speichersicherheit ... 105

Anhang C (informativ) Wichtige Sicherheitskonzepte ... 117
C.1 Authentifizierung ... 117
C.2 Autorisierung und Zugriffskontrolle ... 118
C.3 Selbstverschlüsselnde Festplatten (SED) ... 120
C.4 Löschung ... 121
C.5 Logging ... 123
C.6 N_Port_ID Virtualization (NPIV) ... 123
C.7 Fibre-Channel-Sicherheit ... 124
C.7.1 Überblick ... 124
C.7.2 DH-CHAP-Authentifizierung ... 126
C.7.3 ESP_Header ... 127
C.7.4 CT_Authentication ... 127
C.7.5 FC-SP-Zoning ... 128
C.8 OASIS Key Management Interoperability Protocol (KMIP) ... 128

Literaturhinweise ... 132

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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 als EN ISO/IEC 27040:2016 übernommen.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Februar 2017, und etwaige entgegenstehende nationale Normen müssen bis Februar 2017 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN [und/oder CENELEC] sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die ehemalige jugoslawische Republik Mazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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 (http://www.iso.org/iso/foreword.html).

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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 Compliance. 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 vereinzelten 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. Obwohl sie die Bedeutung dieser Einflüsse betont, kann sie sie aber nicht gesondert aufführen, da sie vom jeweiligen Land, von der Geschäftsart usw. abhängig sind.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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 an deren Speicherort und auf die Sicherheit der Informationen bei der Übertragung über die Kommunikationsschnittstellen in Verbindung mit der Speicherung. 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, Datenträger 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 Sicherheitsrichtlinie 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 ist.

Diese Internationale Norm liefert einen Überblick über 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 Band*geräten* (3.14), in der Daten *gespeichert* (3.50) und abgerufen werden

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

3.2
(logisch) löschen
mithilfe logischer Techniken Daten in allen von Anwendern adressierbaren Speicherorten zum Schutz vor einfachen nicht invasiven Datenwiederherstellungstechniken, die dieselbe Schnittstelle nutzen, die auch für den Anwender zugänglich ist, *löschen* (3.38)

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 Kompression (d. h. Kompression 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 zur Löschung (3.37), bei der der Verschlüsselungscode für die verschlüsselten *Zieldaten* (3.52) *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 offengelegt).

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]

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

3.10
Deduplikation
Methode, die den *Speicher*bedarf (3.43) verringert, indem sie redundante Daten eliminiert, die durch einen Verweis auf die einzige Datenkopie ersetzt werden

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

3.11
entmagnetisieren
degaußen
Daten unlesbar machen, indem ein starkes Magnetfeld auf die Datenträger einwirkt

3.12
zerstören
mithilfe physischer Techniken *löschen* (3.38), die durch Einsatz von Labortechniken auf dem neuesten Stand der Technik eine Wiederherstellung 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: *Zerkleinern* (3.15), *Veraschen* (3.21), *Einschmelzen* (3.25), *Pulverisieren* (3.34) und *Schreddern* (3.41) sind Zerstörungsformen zur Löschung (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
zerkleinern
durch Zertrennen der Datenträger in ihre Einzelteile *zerstören* (3.12)

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 Datenträger *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 Datenträger 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 System*speicher* (3.43), Zugriff auf den Mainframe-*Speicher* (3.43) und Networking

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

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
durch vollständiges Verbrennen der Datenträger zu Asche *zerstören* (3.12)

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 zurückzuversetzen

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

3.25
einschmelzen
durch Ändern des Aggregatzustands der Datenträger von fest zu flüssig, üblicherweise durch den Einsatz von Wärme, *zerstören* (3.12)

3.26
Metadaten
Daten, die andere Daten definieren und beschreiben

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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 in der Lage ist zu tun“.

[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
durch Zermahlen der Datenträger zu Pulver oder Staub *zerstören* (3.12)

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

3.35
(physisch) löschen
mithilfe von physischen Techniken *löschen* (3.38), 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 die Verweisung wurden nicht aufgenommen.]

3.37
Löschung
Prozess oder Methode zum *Löschen* (3.38)

3.38
löschen
Zugriff auf *Zieldaten* (3.52) auf dem *Speichermedium* (3.48) bis zu einem gewissen Aufwand unmöglich machen

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) *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 System zu brechen

3.41
schreddern
durch Zerschneiden oder Zerreißen von Datenträgern in kleine Stücke *zerstören* (3.12)

3.42
einzelner Ausfallpunkt
(en: Single Point of Failure)
Element oder Komponente eines Systems, ein Pfad in einem System, oder ein System, das im Falle 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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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 (en: Management Layer), die die Verbindungen, *Speichergeräte* (3.45) und Computersysteme so verwaltet, dass der Datentransfer sicher und beständig abläuft.

3.45
Speichergerät
jedes *Speicherelement* (3.47) oder eine Gruppierung von *Speicherelementen* (3.47), die hauptsächlich zur Daten*speicherung* (3.43) und Datenbereitstellung vorgesehen und gebaut sind

3.46
Speicher-Ökosystem
komplexes System aus voneinander abhängigen Komponenten, die zusammen agieren, um die *Speicher*dienste (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 Daten*speicherung* (3.43) und Datenbereitstellung 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, detektierend, korrigierend, abwehrend, wiederherstellend oder kompensierend sein.

3.50
speichern
Daten in einem *flüchtigen Speicher* (3.53) oder in einem *nichtflüchtigen Speicher* (3.30) aufzeichnen

3.51
starke Authentifizierung
Authentifizierung mittels kryptographisch abgeleiteter Identitätsnachweise

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

3.52
Zieldaten
Informationen, die von einem bestimmten Prozess abhängen und in der Regel die meisten oder alle Informationen auf einer Einheit eines *Speichermediums* (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 bestimmen 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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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 verstand man unter Speicher am Computer angeschlossene Festplatten (HDD, en: Hard Disk Drives) und Bandlaufwerke zum Speichern von Daten. 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. Alternative Ansätze, die auf der Verwendung von Speichernetzwerktechnologien basieren, wurden mit dem Aufkommen ausgereifter Technologien verfügbar, 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. Das Networking 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);

— Backup-/Wiederherstellungssysteme, Continuous Data Protection (CDP) usw. (d. h. Datenschutzsysteme).

Der Speicher hat sich zu einer bedeutsamen und eigenständigen Schicht in der Informations- und Kommunikationstechnologie(IKT)-Infrastruktur in unternehmensweiten und mittelgroßen Computing-Umgebungen entwickelt. Die Anforderungen an diese Umgebungen überschreiten häufig die einfachen Datenspeicherfähigkeiten. Beispiele für 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) erforderlich sind;

— desastertolerante Remote-Online-Spiegelung von auftragsentscheidenden Daten;

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

— Ansammlung von fehlertoleranten Anwendungen und zugehörigen Systemen um eine einzelne Datenkopie;

— Langzeitaufbewahrung von sensiblen oder wertvollen Geschäftsinformationen;

— dezentrale Datenbanken und Dateisysteme;

— Unterstützung für behördliche und gesetzliche Compliance-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 vorantreiben wie z. B.:

— Löschung von Speichermedien;

— Sicherheit bei der Virtualisierung;

— selbstverschlüsselnde Festplatten (siehe C.3) wie HDD, Solid State Drives (SSD) und Solid State Hard Drives (SSHD);

— Schlüssel-Managementdienste;

— Dienste für die Datenauthentizität und Datenintegrität;

— Schutz von Data-in-Motion (Verschlüsselung und Datenreduktion);

— Verzeichnisdienste und andere Anwenderverwaltungssysteme.

Für ein besseres Verständnis von Sicherheitsfragen und ihren Auswirkungen für die Speicherung sollte man sich damit vertraut machen, 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 je nach Netzwerktechnologie sowie angewendeter Topologie stark variieren.

— 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 Speichermethoden. Ebenso können die Sicherheitsmaßnahmen jeder dieser Methoden grundlegende Unterschiede aufweisen, besonders im Hinblick auf die Zugriffskontrollen, Verschlüsselung und Datenintegrität.

— Für normale Speichervorgänge verfügen viele Speichergerätetypen über eine höhere interne Medienkapazität als durch die Schnittstelle freigegeben wird. SSDs und SSHDs sind häufig überdimensioniert (Over-Provisioning), wobei die Daten intern zwischen physischen Medienbereichen verschoben werden dürfen, um Verzögerungszeiten beim Schreiben zu verbessern. HDDs enthalten oftmals freie Bereiche, in denen die Daten intern zwischen physischen Medienbereichen verschoben werden dürfen, wenn ein temporäres Zugriffsproblem auftritt. Anwenderdaten können in diesen Bereichen erhalten bleiben, selbst nachdem das Gerät über seine Schnittstelle beschrieben wurde. Solche Geräte können möglicherweise nicht durch Überschreiben über die Schnittstelle logisch gelöscht werden.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

— Das Speichermanagement ist sowohl ein Element der Speicherinfrastruktur als auch eine Funktion, die auf zahlreichen Systemen ausgeführt wird. Privilegierte 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 durch Einführung von Choke-Points und zusätzlichen einzelnen Ausfallpunkten (single point-of-failure) ausgehebelt werden.

— Viele Organisationen setzen umfangreiche Strategien für die Resilienz 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 Resilienz 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 für den Server), die eigentliche Kapazität eines Gerätes verdecken, eine richtlinienbezogene 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 Datenzuwachsgeschwindigkeiten treiben 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-Vorgängen 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 angemessen gelöscht werden, wenn sie nicht mehr benötigt werden.

— 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 tiefer in den Netzwerkverkehr blicken. Ob man sich auf IPsec oder andere Schutzmaßnahmen für Data-in-Motion verlässt, 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 Compliance-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 Bedeutung der zu schützenden Daten können ebenfalls Auswirkungen auf den Schlüssel-Managementansatz haben.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

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

— Schutz des Speichermanagements (Vorgänge 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;

— ordnungsgemäßes Löschen und 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 Speichersysteme und Speicherinfrastruktur zählen, neben anderen, folgende:

— unbefugte Nutzung;

— unbefugter Zugriff;

— Haftbarkeit durch Nichteinhaltung (en: non-compliance) von behördlichen Vorschriften;

— Denial-of-Service(DoS)- und verteilte Distributed-Denial-of-Service(DDoS)-Angriffe auf den Speicher;

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

— Beschädigung/Änderung und Vernichtung von Daten;

— Datenverlust/Bruch der Vertraulichkeit;

— Datendiebstahl oder versehentlicher Datenverlust;

— Angriff durch Schadsoftware (en: Malware) oder deren Eindringen;

— unangemessene Behandlung oder unsachgemäße Löschung 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 Datenbeschädigung 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 Kosten für die Untersuchung des Bruchs der Vertraulichkeit, der erforderlichen Unterrichtung betroffener 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 vermelden 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);

— Informationen zu finanziellen Bilanzen oder 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

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 Datenbeschädigung
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
DoS-Angriffe	Unbefugte(r) Datenvernichtung, -verlust oder -änderung
Überwachung des Netzwerkverkehrs mit böser Absicht	Unrechtmäßige/unbefugte Offenlegung

5.4.3 Datenbeschädigung und Datenvernichtung

Datenbeschädigung ist die Verschlechterung bzw. die Schädigung 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 Datenbeschädigung betrifft möglichweise 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. Datenbeschädigung 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 Datenbeschädigung und die Datenvernichtung. Hintergrundstrahlung, Head-Crashes und Alterung bzw. Abnutzung der Speicherhardware sind weitere Ursachen für eher speicherbasierte Probleme. Die hardwarebasierte Datenbeschädigung kann in der Regel mithilfe von Prüfsummenfunktionen erkannt werden und oftmals auch 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).

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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 Schlüssel oder einem unbekannten Mechanismus verschlüsselt werden können. Angriffe ohne böse Absicht sind üblicherweise auf Fahrlässigkeit, Unwissenheit oder absichtliches Umgehen der Sicherheit zurückzuführen, um „einen Auftrag erledigt zu bekommen“, 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 Datenbeschädigung 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 Zugriffs[1)] 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 des Erfüllens gesetzlicher, behördlicher oder rechtlicher Anforderungen

Organisationen können erhebliche Haftungssummen und Strafen bei Nichteinhaltung (en: non-compliance) von gesetzlichen, behördlichen oder rechtlichen Anforderungen auferlegt werden. Die Anforderungen können sich von Rechtsordnung zu Rechtsordnung deutlich unterscheiden und in multinationalen Organisationen haben landesspezifische Gesetze großen Einfluss auf die Anforderungen an die Informationssicherheit.

Übliche Probleme bei der Compliance umfassen:

— Verletzung von landesspezifischen Anforderungen an den Datenschutz;

— unrechtmäßiger Datentransfer (d. h. Übermittlung geheimer Daten aus einer bestimmten Rechtsordnung heraus);

— Bruch der Vertraulichkeit;

— Nichteinhaltung von Richtlinien der Organisation (z. B. Löschen);

— unangemessene Aufbewahrung und unangemessener Schutz von Daten;

— unzureichender Sicherheitsnachweis (z. B. Auditprotokolle, Nachweis über die Verschlüsselung/über das Löschen usw.).

Diese Probleme der Nichteinhaltung (en: non-compliance) 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

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 über mehrere Schnittstellen (Ports) verfügt, die den gleichzeitigen und direkten Zugriff erlauben.

Diese Speicherelemente besitzen begrenzte Datenzugriffs- und -managementschnittstellen (letztgenannte 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 selbstverschlüsselnde Festplatten (SED, en: Self-Encrypting Drive);

  — computerbasierte oder anwendungsbasierte Verschlüsselung einschließlich Festplattenverschlüsselung (FDE, en: Full Disk Encryption).

— Das 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 Löschen;

  — Einsatz einer computerbasierten oder anwendungsbasierten Funktion zum Löschen.

— Sofern möglich, sollte eine Authentifizierung wie Fibre Channel — Security Protocol — 2[2)] (FC-SP-2) AUTH-AAuthentication (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 Datenbeschädigung 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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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. Keine der Einsatzzwecke 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, welche von einem Server für den Datenzugriff und gleichzeitig über eine TCP/IP-Verbindung zur Managementschnittstelle des Speichersystems genutzt wird.

6.3.2 Speichernetzwerke (SAN)

6.3.2.1 Allgemeines

Ein Speichernetzwerk (SAN) 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. Auslagerung von Speicherfunktionen, 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).

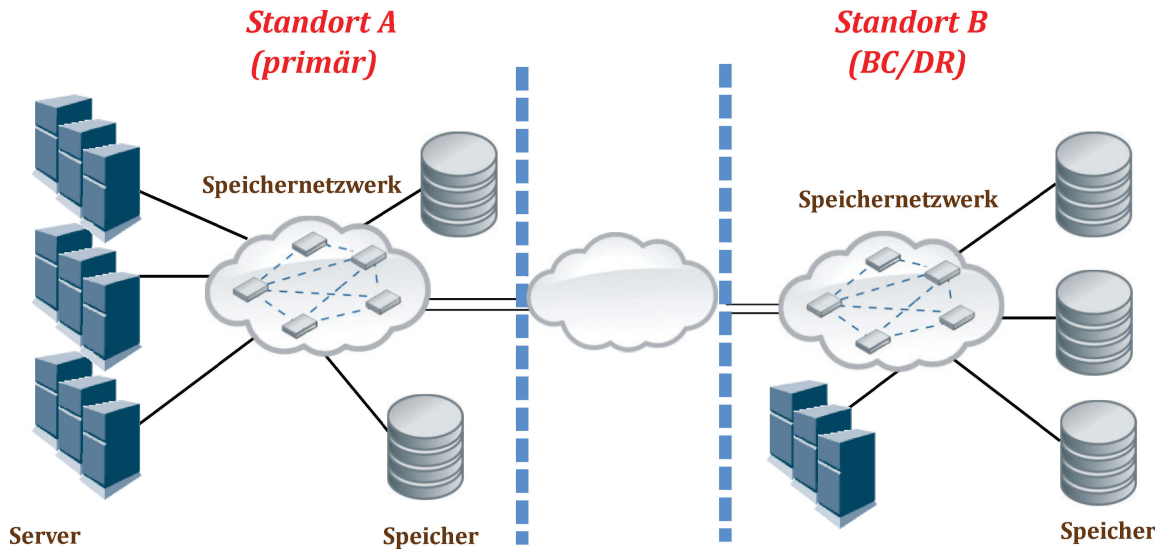

Bild 1 — Beispiel eines Speichernetzwerks (SAN)

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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(FC)-Technologie, 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 das Internet Small Computing System Interface (iSCSI), das üblicherweise in kleinen und mittleren Organisationen als eine kostengünstigere Alternative zu FC verwendet wird, 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 allmählich die Eigenschaften eines SAN an.[3)] Zusätzlich besteht die Möglichkeit, Daten zwischen verschiedenen SAN-Technologien mithilfe von Gateways zu übertragen (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 Port-Binding-Mechanismen 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 Anfragen begrenzt, insofern, dass davon ausgegangen wird, dass Server keine Speichergeräte kontaktieren, die über den Nameserver nicht erreicht werden. Beim Hard-Zoning kommen physische Port-Nummern an SAN-Switches zum Einsatz, um die Weiterleitung des Datenverkehrs einzuschränken, und es stellt eine sicherere Zoning-Methode dar, weil es nicht auf ein korrektes Serververhalten angewiesen ist und insbesondere ist es nicht anfällig für die Spoofing einer Serveridentität ist.

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

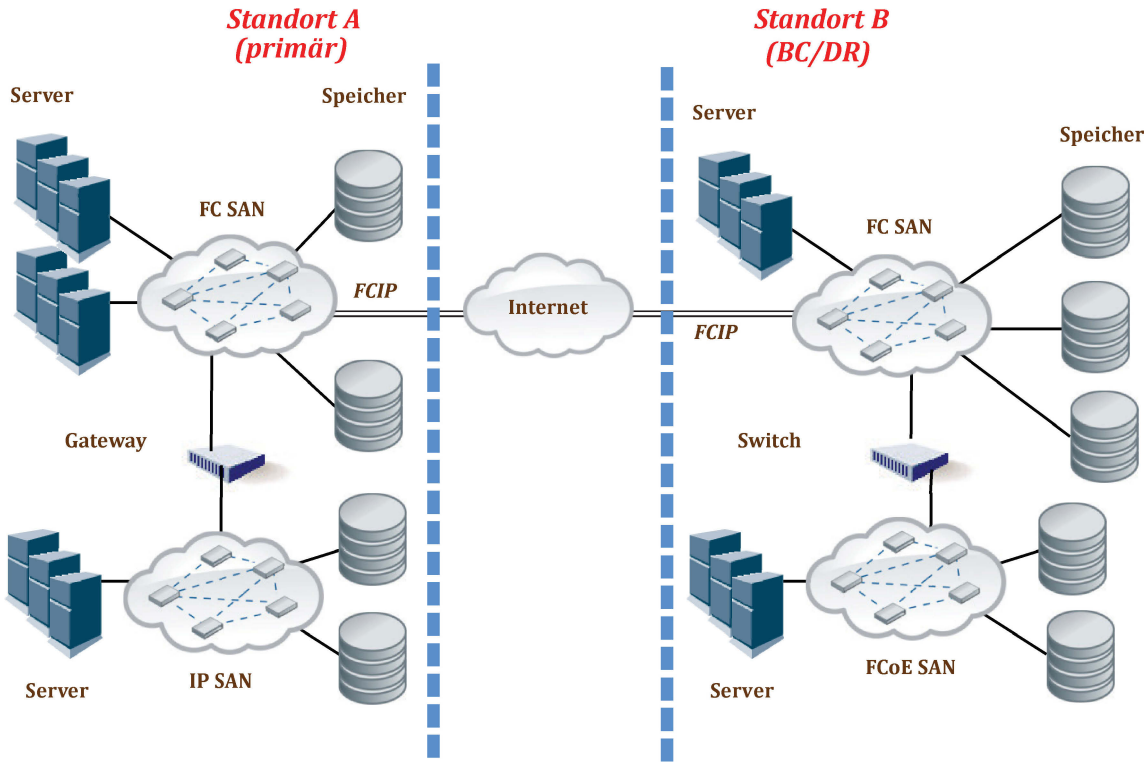

Bild 2 — Beispiel eines Speichernetzwerks (SAN)

— **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 und das Nichtsichtbarmachen für andere Server.

— **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 Rogue-Switch einem SAN beitreten und potentiell SAN-Daten 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 sein, sowohl während sie übertragen werden (en: data in motion) und wenn sie auf einem Speichergerät liegen (en: data at rest). 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 (en: Single Point of Failure) zu mindern, das die zu schützenden Daten beeinträchtigt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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

— 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 Speicherdatenverkehrs vom normalen Serverdatenverkehr 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 Speichermanagementdatenverkehrs von allen anderen Datenverkehrsarten;

  — Sicherstellung, 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 von Ports miteinander verbunden ist: Point-to-Point (zwei Geräte sind direkt miteinander verbunden), Arbitrated-Loop und Switched-Fabric. Switched-Fabric-Topologien sind zusammen mit dem Fibre-Channel-Protokoll (FCP), welches das Schnittstellenprotokoll zur Übertragung des SCSI-Verkehrs in dieser Netzwerktechnologie darstellt, aus Sicht der Sicherheit von größerem Interesse.

Fabric-Administratoren sollten Maßnahmen einleiten zur:

— Kontrolle des Zugriffs auf FCP-Knoten einschließlich:

  — einer Einschränkung des Serverzugriffs auf die Switches mithilfe von Techniken wie einer Zugriffskontrollliste (ACL), verbindlichen Listen und FC-SP-2-Fabric-Richtlinien (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-Richtlinien (siehe C.7.1);

  — Zoning sollte in FC-SAN-Fabrics eingesetzt werden, mit der Präferenz für Hard Zoning;

  — Bestimmung, ob grundlegendes Zoning eine ausreichende Sicherheitsmaßnahme für die Zielumgebung ist; falls nicht, sind strengere Techniken wie FC-SP-Zoning (siehe C.7.5) zu nutzen, soweit sie vom Anbieter unterstützt werden;

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

- Deaktivieren von ungenutzten Ports;
- sorgfältige Nutzung von Default-Zonen und Zonensätzen (unter Annahme der Least-Privilege-Haltung).

— sichere Verbindung von Speichernetzwerken durch Konfigurieren von Switches, Extendern, Routern und Gateways, die notwendig sind, um die Anforderungen zu erfüllen.

6.5.1 enthält Leitlinien für blockbasierte 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 erfolgt 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-Speichernetzwerken durch IP-basierte Netzwerke, um ein einheitliches Speichernetzwerk zu bilden.

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

— Erstellen der Peer-to-Peer-Beziehung zwischen FCIP-Einheiten, unter Anerkennung, dass die Sicherheitsrichtlinien 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 minimalen kryptographischen Authentifizierung und 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 blockbasierten IP-Speichern enthalten. Darüber hinaus enthält IETF RFC 7146, *Securing Block Storage Protocols over IP: RFC 3723 Requirements Update for IPsec v3* wichtige Sicherheitsupdates für IETF RFC 3720, 3723 und 3821.

6.3.2.4 FCoE SAN

Fibre Channel over Ethernet (FCoE) ist eine Protokollspezifikation[4)] zur Kapselung von Fibre-Channel-Frames in Ethernet-Paketen. Das Ethernet-Netzwerk, das FCoE unterstützt, muss ein verlustfreies Ethernet-Netzwerk[5)] sein, mit Switches, deren interne Architektur so ausgelegt ist, dass sie die Fähigkeit einer verlustlosen Paketübermittlung anbietet, und mit Kontrollfunktionen für den Netzwerkfluss, um eine verlustfreie Übertragung von Paketen über die Ethernet-Infrastruktur zu ermöglichen.

---

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-Datenframes einzukapseln.

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

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 einer Verschlechterung des Durchsatzes 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

Die Netzwerkspeicherung (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 dargestellt wird. 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 implementiert werden, die auf dynamische Weise Client-Verbindungen durch Slicing oder Striping von Daten oder Metadaten über die gruppierten Speicherserver verteilen (siehe Bild 3); parallele NFS-(pNFS)-Systeme sind Beispiele für gruppierte NAS-Systeme.

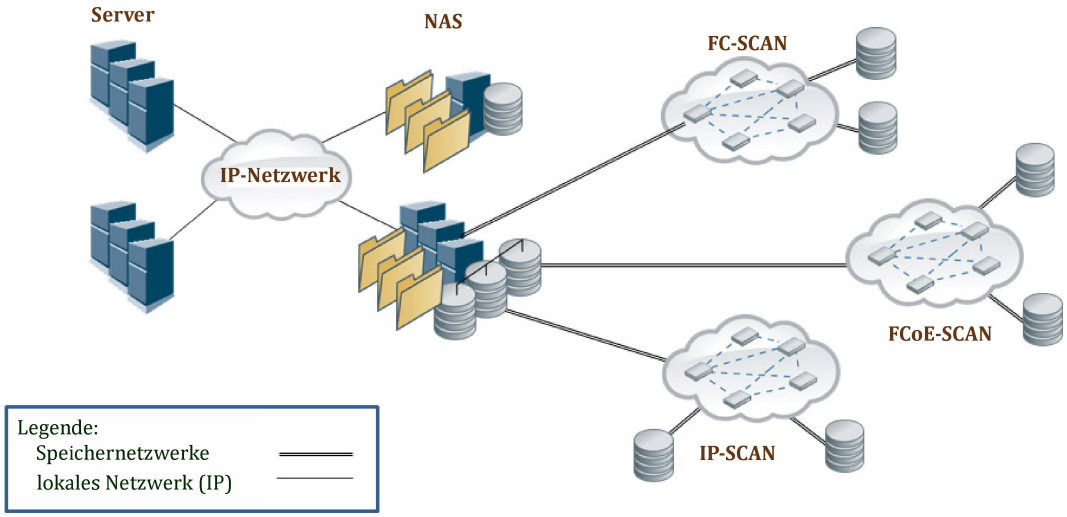

Bild 3 — Beispiel für Netzwerkspeicher (NAS)

Übliche Umsetzungen von Dateisystemen umfassen das Netzwerkdateisystem (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, sowohl von Data-in-Motion als auch von 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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

6.3.3.2 Netzwerkdateisystem (NFS, en: Network File System)

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

— die Verschlüsselung des Client-Datenzugriffs (z. B. IPsec) bei Bedarf .

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 Personalcomputern und Workstations findet und eine große Bandbreite an Betriebssystemen unterstützt.

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

— Einsatz neuerer 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

6.4 Speichermanagement

6.4.1 Hintergrund

Speichernetzwerke und Infrastrukturelemente sind komplexe Architekturen, die strenge Management-ansprüche an Administratoren stellen können. Zur Behandlung dieser Ansprüche implementieren Organisationen 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 Compliance-Anforderungen sicherzustellen (siehe Bild 4).

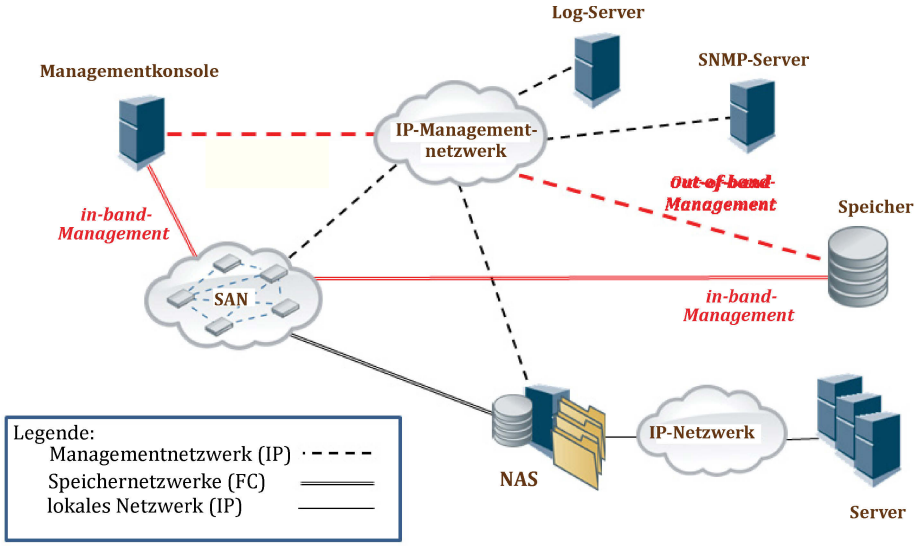

Bild 4 — Beispiel für das Speichermanagement

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

— Der 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 schnellstmöglich zu erkennen, bestenfalls bevor Anwender betroffen werden;

— Die 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;

— Die 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 Speicher-netzwerk ein neuer Switch hinzugefügt wird. Wartung umfasst ebenfalls Korrektur- und Vorbeugungs-maßnahmen, um den Betrieb des Speichers zu verbessern, wie z. B. das Einstellen von Parametern der Gerätekonfiguration;

— Die Bereitstellung behandelt die Initialisierung und Ausstattung eines Systems, um es auf die Bereitstellung von Diensten vorzubereiten;

— Das 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).

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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. Nach 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 Systemsicherheitsverstöße darstellen. Als Beitrag zur Minderung dieser Bedrohungen können möglicherweise sichere Anmeldeverfahren, wie in ISO/IEC 27002:2013, 9.4.2, beschrieben, mit zusätzlichen Authentifizierungsmaßnahmen (siehe C.1) erforderlich sein, die unter anderem einschließen:

— alle Anwender sollten eine eindeutige Kennzeichnung (Anwender-ID) ausschließlich für ihre personengebundene Nutzung besitzen;

— ein geeignetes Authentifizierungsverfahren sollte gewählt werden 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. Smartcards).

— für jeden Fernzugriff eine sichere Authentifizierung oder Multi-Faktor-Authentifizierung zusammen mit sicheren Kanälen verwenden;

— wenn möglich, eine zentralisierte Authentifizierungslösung (z. B. Remote Authentication Dial-In User Service bzw. RADIUS, Single Sign-on oder SSO usw.) für eine verbesserte Überwachung und Kontrolle verwenden;

— Verwendung einer Multi-Faktor-Authentifizierung bei der Handhabung von sensiblen Daten oder Daten von hohem Wert;

— Deaktivieren des Anmeldens mit dem Root-Account. Alle Operationen der Rechteausweitung 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 Transport-Layer-Security- (TLS) und IPsec-Verbindungen sowie innerhalb von Speicherprotokollen (z. B. Challenge-Handshake-Authentication-Protokoll mit iSCSI, Diffie-Hellman Challenge Handshake Authentication Protocol in FCP, usw.) stattfinden. Wenn möglich, sollten diese Instrumente zur Entitäts-Authentifizierung verwendet werden. Ein zusätzlicher Leitfaden ist in den Abschnitten enthalten, die diese Instrumente behandeln.

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

6.4.2.2 Autorisierung und Zugriffskontrolle

In Branchen wie der Finanzdienstleistung und dem Gesundheitswesen gibt es Entwicklungen, die Autorisierung und Zugriffskontrolle (C.2) auf ein Modell mit minimalen Rechten 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/Berechtigungen, für Auditlogging-Konfigurationen und -Inhalte (Auditlog-Ereigniseinträge 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, 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“ zugeordnet 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 serielle 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 weit verbreitet. Um diese physischen Schnittstellen zu schützen, sollte eine Organisation:

— den physischen Zugriff auf Managementschnittstellen beschränken;

— serielle Management-Ports deaktivieren und trennen, wenn sie nicht in Verwendung sind;

— LAN-Schnittstellen, die für Managementzwecke verwendet werden, von sonstigem LAN-Datenverkehr trennen, wobei darauf hingewiesen wird, dass die physische Trennung bevorzugt wird, jedoch mindestens eine logische Trennung (wie VLAN) verwendet werden sollte.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

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

— Firewalls und TCP-Wrapper verwenden, um den Zugriff auf Management-Netzwerke auf autorisierte Systeme und Protokolle zu 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 anomales Verhalten zu identifizieren und davor zu schützen;

— eine ICT-Infrastruktur (Domain Name System bzw. DNS, Service Locator Protocol bzw. SLP, Network Time Protocol bzw. NTP) mit geeigneten Sicherheitskontrollen zur Vermeidung indirekter Angriffe einsetzen;

— 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 Angriffe gehärtet sind (siehe 6.4.5).

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

— Verwendung sicherer Kanäle für jeden 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 Rechten auf das erforderliche Mindestmaß (d. h. minimale Rechte).

Die Organisation sollte organisatorische und technische Maßnahmen ausarbeiten, um die für Fernwartungssitzungen (nicht lokal) des Anbieters genutzte Management-Schnittstelle einzuschränken. Fernwartungstätigkeiten des Anbieters, 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 Anbieters erforderliche Mindestmaß einschränken. Nachdem die zugreifende Seite authentifiziert ist, sollten zusätzliche Kontrollen für den Zugriffspunkt entwickelt werden, um die Wartungssitzung des Anbieters 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 Anbieters 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 Anbieter eine Wartungssitzung beantragt und die Organisation diese Anfrage autorisiert hat.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

6.4.4 Sicherheitsprüfung, Kontenführung und Überwachung

Vorschriften zur Compliance 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 als auch als Bestandteil einer Vorfalluntersuchung angewendet werden kann. Daher müssen Speichersysteme und -infrastrukturen am Ereignis-Logging-Programm der Organisation teilhaben (für einen maßgebenden Leitfaden siehe auch ISO/IEC 27002:2013, 12.4).

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

— der Speicher ist derart in der Logging-Richtlinie aufzunehmen, dass

  — bezüglich Speichersystemen und -geräten die folgenden Richtlinienelemente behandelt werden sollten:

    — Speichersysteme und -geräte sollten am Audit-Logging teilhaben;

    — alle *signifikanten* Speichermanagementereignisse sollten gesammelt werden;

    — Logdaten werden aufbewahrt;

    — Logdaten werden entsprechend der Richtlinie zur Logdatenaufbewahrung archiviert und erhalten; und

    — die Gerätezeit ist mit einer zuverlässigen externen Quelle synchronisiert.

  — die Logging-Richtlinie (siehe auch 7.7.2) beweiserhebliche Erwartungen einschließen (Authentizität, Obhutskette usw.) sollte.

— Anwendung von externem oder zentralisiertem Ereignis-Logging an einer vertrauenswürdigen[6)] Remote-Quelle durch:

  — Umsetzung von zentralisiertem[7)] Audit-Logging, um Ereignisse aus allen Quellen in einem einzelnen Repository zu sammeln;

  — Festlegen und Verwenden 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, ein begrenzter Speicherplatz für Logs zur Verfügung steht und sie die Anwendung einer zentralisierten Analyse, Alarmgebung und Archivierung ausschließen;

  — das native Logging von Ereignissen auf einem, und vorzugsweise auf mehreren[8)], 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 seine Sicherheitsfunktionen korrekt durchführt.

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, dass Speichersysteme/-ökosysteme innerhalb einer einzelnen Sicherheitsdomain eine gemeinsame Audit-Logging-Infrastruktur verwenden.

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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

- Verwendung von Standard-Logging-Protokollen wie Syslog[9)], die den zuverlässigen Empfang und sichere Übermittlungen (z. B. TLS) unterstützen;
- Konfiguration von Geräten derart, dass Ereignisse bei ihrem Auftreten protokolliert werden (d. h. ungepuffert), wenn die Hauptbeweggründe für das Audit-Logging Compliance, Zurechenbarkeit oder Sicherheit sind;
- Umsetzung eines Analyseprotokolls zum Korrelieren von Audit-Log-Aufzeichnungen über Ereignisquellen hinweg, 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 alle Vorkommnisse dieser Ereignisse protokolliert werden (ob in-Band oder out-of-Band);
- die folgenden Ereignisarten sollten protokolliert werden (ein Mindestsatz an sicherheitsbezogenen Ereignissen):
  - fehlgeschlagene und erfolgreiche Anmeldeversuche;
  - fehlgeschlagene Zugriffsversuche auf Dateien und Objekte bei sensiblen Daten 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 oder NTP, Domain Name System oder DNS, Authentifizierung);
  - Systemabschaltung und -neustarts;
  - privilegierte Vorgänge (d. h. von Administratoren initiierte Änderungen);
  - Nutzung sensibler Dienstprogramme (z. B. Befehle zur Rechteausweitung);
  - Zugriff auf kritische Dateien;
  - Verlagern von virtuellen Servern zwischen physischen Servern.
- 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.

9) Syslog ist in IETF RFC 5424 festgelegt, 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 27040:2017-03

  - Sorgfalt beim Filtern nach Merkmalen wie dem Schweregrad, weil die Logging-Richtlinie des Unternehmens als Leitfaden bei der Bestimmung dienen sollte, welche Art der Filterung geeignet ist und welches Niveau von Informationen eine Langzeitspeicherung erfordert.

- geeignete Aufbewahrung und geeigneter Schutz ist derart umzusetzen, dass:

  - Audit-Log-Daten, die möglicherweise einen beweiserheblichen Wert besitzen, korrekt gehandhabt werden sollten (z. B. Aufrechterhalten der Obhutskette, verifizierbare Integrität und Authentizität usw.);

  - Audit-Log-Daten mit spezifischen Aufbewahrungsanforderungen (z. B. Einhaltung gesetzlicher Auflagen) sollten nach 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 Vertraulichkeitsmechanismen[10)] geschützt werden;

  - für spezifische Audit-Logging-Anforderungen (z. B. hohe Volumen, besondere Aufbewahrung, Ereignis-Signatur usw.) sollten dedizierte 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;

- ausschließlich benötigte Netzwerk-Ports öffnen;

- 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 erhalten, sollte sichergestellt sein, dass die anzuwendende Software aus vertrauenswürdiger Quelle stammt. Anderenfalls

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

können Angreifer selbst ein „Update“ programmieren, das stattdessen einen Schadcode ihrer Wahl enthält wie ein Rootkit, Botnet oder andere Schadsoftware.

Anbieter 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 (LUNs) 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; wirksames Einsetzen zentralisierter Authentifizierungsdienste wenn möglich;

  — wenn möglich, sollten Fibre-Channel-Verbindungen, die den geschützten Bereich (z. B. Grenzen eines physisch kontrollierten Datenzentrums) verlassen, unter Verwendung von ESP_Header[11)] (siehe 6.8.2.2 und C.7.3) verschlüsselt werden.

— Umsetzung von Verschlüsselungsmaßnahmen für Data-at-Rest (siehe 6.8.2.3) einschließlich:

  — Sensible Daten und Daten von hohem Wert sollten verschlüsselt sein, während sie sich auf dem Speichergerät oder -medium[12)] befinden;

  — die Verschlüsselung sollte in Speichergeräten implementiert werden, die in Kontakt mit sensiblen oder regulierten Daten kommen können, sowie, um eine schnelle Löschung (siehe A.3) zu ermöglichen.

— Umsetzung von Maßnahmen zur Datenlöschung (siehe 6.8.1 und Anhang A) einschließlich:

  — eine an die Datenträger angepasste Löschung (siehe 6.8.1.2) sollte für sensible Daten und Daten die einer Regulierung unterliegen verwendet werden;

  — logisches Löschen (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.

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

---

11) Die Integrität oder Vertraulichkeit von Fibre-Channel-Frames kann mit optionalen ESP_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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03

6.5.2 IP-Speicher

Anders als FC-Speicher verwendet der IP-Speicher eine TCP/IP-Netztechnologie (siehe 6.3.2.3), insbesondere iSCI, um Computern blockbasierte Speicherressourcen zu präsentieren.

Für IP-Speichersysteme sollte Folgendes berücksichtigt werden:

— Kontrolle des iSCI-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. nicht wiederholte) 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 Daten oder Daten von hohem Wert offengelegt 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 Data-at-Rest-Verschlüsselungsmaßnahmen (siehe 6.8.2.3);

  — Sensible Daten und Daten von hohem Wert sollten verschlüsselt sein, während sie sich auf dem Speichergerät oder -medium[13)] 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 Löschen (siehe 6.8.1.3) sollte verwendet werden, um virtualisierten Speicher zu löschen, insbesondere, wenn die tatsächlichen Speichergeräte und -medien nicht bestimmt werden können.

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

6.6 Dateibasierte Speicherung

6.6.1 NFS-basierte NAS

Diese 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.

---

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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 27040:2017-03