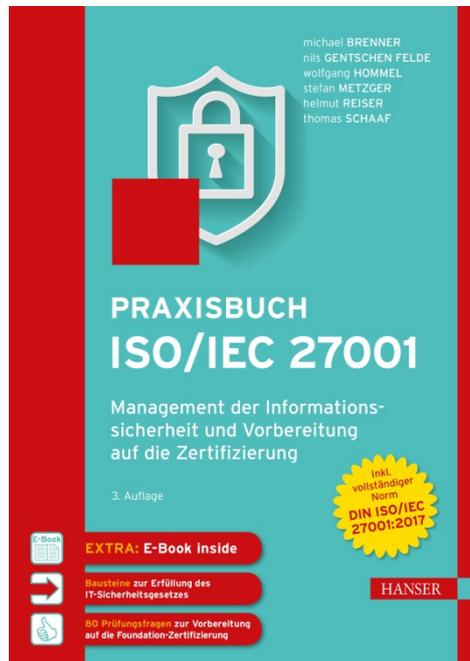


HANSER



Leseprobe

zu

„Praxisbuch ISO/IEC 27001“

von Michael Brenner et al.

Print-ISBN: 978-3-446-46170-3

E-Book-ISBN: 978-3-446-46276-2

E-Pub-ISBN: 978-3-446-46371-4

Weitere Informationen und Bestellungen unter
<http://www.hanser-fachbuch.de/978-3-446-46170-3>

sowie im Buchhandel

© Carl Hanser Verlag, München

2.4.1	ISO/IEC 27000: Grundlagen und Überblick über die Standardfamilie	16
2.4.2	Normative Anforderungen	16
2.4.2.1	ISO/IEC 27001: Anforderungen an ein ISMS	16
2.4.2.2	ISO/IEC 27006: Anforderungen an Zertifizierer	16
2.4.2.3	ISO/IEC 27009: Anforderungen an die branchenspezifische Anwendung von ISO/IEC 27001	17
2.4.3	Allgemeine Leitfäden	17
2.4.3.1	ISO/IEC 27002: Leitfaden für das Informationssicherheits- management	17
2.4.3.2	ISO/IEC 27003: Umsetzungsempfehlungen	17
2.4.3.3	ISO/IEC 27004: Messungen	18
2.4.3.4	ISO/IEC 27005: Risikomanagement	18
2.4.3.5	ISO/IEC 27007 und ISO/IEC TR 27008: Audit-Leitfäden	18
2.4.3.6	ISO/IEC 27013: Kombination mit dem IT Service Management	18
2.4.3.7	ISO/IEC 27014 und ISO/IEC 27016: Governance und Entschei- dungen auf Vorstandsebene	18
2.4.3.8	ISO/IEC 27018: Leitfaden zum Schutz personenbezogener Daten in öffentlichen Cloud-Diensten als Auftragsdatenver- arbeitung	19
2.4.3.9	ISO/IEC TR 27023: Gegenüberstellung mit früheren Fassungen	19
2.4.4	Sektor- und maßnahmenspezifische Leitfäden	19
2.4.4.1	Ausgewählte sektorspezifische Leitfäden	20
2.4.4.2	Ausgewählte maßnahmenspezifische Leitfäden	21
2.5	Zusammenfassung	21
2.6	Beispiele für Prüfungsfragen zu diesem Kapitel	22
3	Grundlagen von Informationssicherheitsmanagementsystemen	23
3.1	Das ISMS und seine Bestandteile	23
3.1.1	(Informations-)Werte	24
3.1.2	Richtlinien, Prozesse und Verfahren	24
3.1.3	Dokumente und Aufzeichnungen	25
3.1.4	Zuweisung von Verantwortlichkeiten	26
3.1.5	Maßnahmenziele und Maßnahmen	27
3.2	Was bedeutet Prozessorientierung?	28
3.3	Die PDCA-Methodik: Plan-Do-Check-Act	29
3.3.1	Planung (Plan)	30
3.3.2	Umsetzung (Do)	31
3.3.3	Überprüfung (Check)	31
3.3.3.1	Konformität	31
3.3.3.2	Effektivität	32
3.3.3.3	Effizienz	32
3.3.4	Verbesserung (Act)	32
3.4	Zusammenfassung	32
3.5	Beispiele für Prüfungsfragen zu diesem Kapitel	33

4	ISO/IEC 27001 – Spezifikationen und Mindestanforderungen	35
4.0	Einleitung	37
4.0.1	Allgemeines	37
4.0.2	Kompatibilität mit anderen Normen für Managementsysteme	38
4.1	Anwendungsbereich	38
4.2	Normative Verweisungen	39
4.3	Begriffe	39
4.4	Kontext der Organisation	40
4.4.1	Verstehen der Organisation und ihres Kontextes	40
4.4.2	Verstehen der Erfordernisse und Erwartungen interessierter Parteien....	41
4.4.3	Festlegen des Anwendungsbereichs des Informationssicherheitsmanagementsystems	42
4.4.4	Informationssicherheitsmanagementsystem	43
4.5	Führung	43
4.5.1	Führung und Verpflichtung	43
4.5.2	Politik	44
4.5.3	Rollen, Verantwortlichkeiten und Befugnisse in der Organisation	45
4.6	Planung	46
4.6.1	Maßnahmen zum Umgang mit Risiken und Chancen	46
4.6.1.1	Bestimmung allgemeiner Risiken und Chancen	47
4.6.1.2	Informationssicherheitsrisikobeurteilung	48
4.6.1.3	Informationssicherheitsrisikobehandlung	51
4.6.2	Informationssicherheitsziele und Planung zu deren Erreichung	53
4.7	Unterstützung	54
4.7.1	Ressourcen	54
4.7.2	Kompetenz	54
4.7.3	Bewusstsein	55
4.7.4	Kommunikation	55
4.7.5	Dokumentierte Information	56
4.8	Betrieb	58
4.8.1	Betriebliche Planung und Steuerung	58
4.8.2	Informationssicherheitsrisikobeurteilung	59
4.8.3	Informationssicherheitsrisikobehandlung	60
4.9	Bewertung der Leistung	60
4.9.1	Überwachung, Messung, Analyse und Bewertung	60
4.9.2	Internes Audit	63
4.9.3	Managementbewertung	65
4.10	Verbesserung	66
4.10.1	Nichtkonformität und Korrekturmaßnahmen	66
4.10.2	Fortlaufende Verbesserung	67
4.11	Zusammenfassung	67
4.12	Beispiele für Prüfungsfragen zu diesem Kapitel	69

5	Maßnahmenziele und Maßnahmen im Rahmen des ISMS	73
5.1	A.5 Informationssicherheitsrichtlinien	75
5.1.1	A.5.1 Vorgaben der Leitung für Informationssicherheit	75
5.2	A.6 Organisation der Informationssicherheit	77
5.2.1	A.6.1 Interne Organisation	77
5.2.2	A.6.2 Mobilgeräte und Telearbeit	79
5.3	A.7 Personalsicherheit	80
5.3.1	A.7.1 Vor der Beschäftigung	81
5.3.2	A.7.2 Während der Beschäftigung	82
5.3.3	A.7.3 Beendigung und Änderung der Beschäftigung	83
5.4	A.8 Verwaltung der Werte	84
5.4.1	A.8.1 Verantwortlichkeit für Werte	84
5.4.2	A.8.2 Informationsklassifizierung	86
5.4.3	A.8.3 Handhabung von Datenträgern	87
5.5	A.9 Zugangssteuerung	90
5.5.1	A.9.1 Geschäftsanforderungen an die Zugangssteuerung	90
5.5.2	A.9.2 Benutzerzugangsverwaltung	91
5.5.3	A.9.3 Benutzerverantwortlichkeiten	93
5.5.4	A.9.4 Zugangssteuerung für Systeme und Anwendungen	93
5.6	A.10 Kryptographie	96
5.6.1	A.10.1 Kryptographische Maßnahmen	96
5.7	A.11 Physische und umgebungsbezogene Sicherheit	98
5.7.1	A.11.1 Sicherheitsbereiche	98
5.7.2	A.11.2 Geräte und Betriebsmittel	101
5.8	A.12 Betriebssicherheit	105
5.8.1	A.12.1 Betriebsabläufe und -verantwortlichkeiten	105
5.8.2	A.12.2 Schutz vor Schadsoftware	107
5.8.3	A.12.3 Datensicherung	108
5.8.4	A.12.4 Protokollierung und Überwachung	109
5.8.5	A.12.5 Steuerung von Software im Betrieb	111
5.8.6	A.12.6 Handhabung technischer Schwachstellen	111
5.8.7	A.12.7 Audit von Informationssystemen	113
5.9	A.13 Kommunikationssicherheit	115
5.9.1	A.13.1 Netzwerksicherheitsmanagement	115
5.9.2	A.13.2 Informationsübertragung	116
5.10	A.14 Anschaffung, Entwicklung und Instandhalten von Systemen	119
5.10.1	A.14.1 Sicherheitsanforderungen an Informationssysteme	119
5.10.2	A.14.2 Sicherheit in Entwicklungs- und Unterstützungsprozessen	120
5.10.3	A.14.3 Testdaten	123
5.11	A.15 Lieferantenbeziehungen	125
5.11.1	A.15.1 Informationssicherheit in Lieferantenbeziehungen	125
5.11.2	A.15.2 Steuerung der Dienstleistungserbringung von Lieferanten	126

5.12	A.16 Handhabung von Informationssicherheitsvorfällen.....	128
5.12.1	A.16.1 Handhabung von Informationssicherheitsvorfällen und Verbesserungen	128
5.13	A.17 Informationssicherheitsaspekte beim Business Continuity Management ...	133
5.13.1	A.17.1 Aufrechterhalten der Informationssicherheit.....	133
5.13.2	A.17.2 Redundanzen.....	135
5.14	A.18 Compliance.....	136
5.14.1	A.18.1 Einhaltung gesetzlicher und vertraglicher Anforderungen	136
5.14.2	A.18.2 Überprüfungen der Informationssicherheit	138
5.15	Zusammenfassung	139
5.16	Beispiele für Prüfungsfragen zu diesem Kapitel.....	140
6	Verwandte Standards und Rahmenwerke	145
6.1	Standards und Rahmenwerke für IT- und Informationssicherheit	145
6.1.1	IT-Grundschutz-Kompendium	145
6.1.2	BSI-Standards	146
6.1.3	ISIS12	147
6.1.4	Cybersecurity Framework	147
6.1.5	ISO/IEC 15408	148
6.1.6	PCI-DSS	149
6.1.7	VDA ISA (TISAX)	150
6.2	Standards und Rahmenwerke für Qualitätsmanagement, Auditierung und Zertifizierung.....	151
6.2.1	ISO 9000	151
6.2.2	ISO 19011.....	152
6.2.3	ISO/IEC 17020	153
6.3	Standards und Rahmenwerke für Risikomanagement	154
6.3.1	ISO 31000.....	154
6.3.2	COSO ERM	154
6.4	Standards und Rahmenwerke für Governance und Management in der IT	155
6.4.1	ITIL.....	155
6.4.2	ISO/IEC 20000	156
6.4.3	FitSM.....	157
6.4.4	COBIT.....	158
6.4.5	EN 50600	159
6.5	Beispiele für Prüfungsfragen zu diesem Kapitel.....	159
7	Zertifizierungsmöglichkeiten nach ISO/IEC 27000	163
7.1	ISMS-Zertifizierung nach ISO/IEC 27001	163
7.1.1	Grundlagen der Zertifizierung von Managementsystemen.....	163
7.1.1.1	Zertifizierung.....	163
7.1.1.2	Akkreditierung	164
7.1.2	Typischer Ablauf einer Zertifizierung	165

7.1.3	Auditumfang.....	167
7.1.4	Akzeptanz und Gültigkeit des Zertifikats	167
7.1.5	Aufwände und Kosten für Zertifizierungen.....	167
7.2	Personenqualifizierung auf Basis von ISO/IEC 27000	168
7.2.1	Programme zur Ausbildung und Zertifizierung von Personal	168
7.2.1.1	TÜV Süd: Qualifizierungsprogramm nach ISO/IEC 27000.....	169
7.2.1.2	APMG: ISO/IEC 27001 Certification.....	170
7.2.1.3	ICO: Ausbildungsschema ISMS nach ISO/IEC 27000.....	170
7.2.2	Das Foundation-Zertifikat des TÜV Süd	171
7.2.2.1	Prüfungsspezifikation	171
7.2.2.2	Vorbereitung auf die Foundation-Prüfung	172
7.3	Zusammenfassung	173
7.4	Beispiele für Prüfungsfragen zu diesem Kapitel.....	174
A	Begriffsbildung nach ISO/IEC 27000	175
B	Abdruck der DIN ISO/IEC 27001.....	193
C	Prüfungsfragen mit Antworten zur ISO/IEC 27001 Foundation	231
C.1	Antworten auf die Prüfungsfragen zu den einzelnen Buchkapiteln	231
C.2	Ein beispielhafter Prüfungsfragebogen zur ISO/IEC 27001-Foundation-Prüfung	238
C.3	Antworten auf den Prüfungsfragebogen zur ISO/IEC 27001-Foundation-Prüfung	250
	Literaturverzeichnis	257
	Index.....	263

Vorwort

Dieses Buch ist sowohl zur gezielten Vorbereitung auf die Prüfung zur ISO/IEC 27001 Foundation-Personenzertifizierung als auch als Nachschlagewerk für die Inhalte dieses Standards konzipiert, der 2017 als DIN ISO/IEC 27001:2017 erschienen ist und die deutsche Version der englischsprachigen ISO/IEC 27001:2013 aus dem Jahr 2013 darstellt. Die DIN ISO/IEC 27001:2017 ist komplett als Faksimile in Anhang B dieses Buches enthalten.

Die ersten Kapitel führen Sie kompakt in die spannende, aber auch komplexe Welt der Informationssicherheit, Managementsysteme und Standards ein, die u. a. durch das IT-Sicherheitsgesetz und die Datenschutz-Grundverordnung kontinuierlich an Bedeutung gewinnt. Nach einem Überblick über die Reihe der ISO/IEC 27000-Standards und die Grundlagen von Informationssicherheitsmanagementsystemen finden Sie in den Kapiteln 4 und 5 alle Anforderungen und Maßnahmen aus ISO/IEC 27001. Sie werden in grau hinterlegten Boxen wörtlich wiedergegeben und zusätzlich erläutert.

Die Schwerpunkte der Erklärungen orientieren sich dabei an den Inhalten der Prüfungen zu den Foundation-Lehrgangskonzepten u. a. von APMG, ICO und TÜV Süd Akademie. Dieses Buch ist aber natürlich auch für die Vorbereitung auf die Foundation-Prüfung aus einem der anderen Qualifizierungsprogramme zum Informationssicherheitsmanagement nach ISO/IEC 27001 verwendbar.

In diesem Buch finden Sie insgesamt 80 Beispiel-Prüfungsfragen. Ihr Format und Schwierigkeitsgrad entspricht dem der ISO/IEC 27001 Foundation-Prüfung der TÜV Süd Akademie mit genau einer richtigen Antwort pro Frage. Die Hälfte der Fragen finden Sie über die Kapitel 2–7 verteilt jeweils am Ende, wo auch die wichtigsten Inhalte nochmals kompakt zusammengefasst werden. Sie können sich damit schon beim ersten Durchlesen darauf vorbereiten, wie Prüfungsfragen zu den Inhalten typischerweise aussehen. Im Anhang finden Sie dann nochmals 40 Fragen am Stück. Dies entspricht dem Umfang der „richtigen“ Prüfung. Dadurch können Sie ein Gespür für die 60 Minuten Prüfungszeit entwickeln.

Noch ein abschließender Hinweis zum flüssigen Lesen: Verweise auf *Kapitel* beziehen sich ohne weitere Angabe immer auf dieses Buch. Verweise auf *Abschnitte* beziehen sich immer auf den entsprechenden Standard.

Wir wünschen Ihnen viel Erfolg bei der Prüfung und bei der praktischen Anwendung des Gelernten!

München, im Dezember 2019

Die Autoren

1

Einführung und Basiswissen

In immer mehr Umfeldern gewinnt das Thema Informationssicherheit an Bedeutung, was nicht zuletzt mit einem steigenden öffentlichen Bewusstsein für Sicherheit und Schutz von Daten und Informationen zusammenhängt. Auch die mediale Aufmerksamkeit ist einem Unternehmen sicher, wenn sich beispielsweise herausstellt, dass es nachlässig mit seinen Kundendaten umgeht, oder wenn sicherheitsrelevante Vorfälle zu Ausfällen mit großer geschäftlicher Auswirkung führen.

Der Gesetzgeber hat mit dem IT-Sicherheitsgesetz [Bun15] und entsprechenden Verordnungen kritische Infrastrukturen definiert, für diese höhere gesetzliche Anforderungen im Hinblick auf die IT-Sicherheit erlassen und verpflichtet die Betreiber, angemessene organisatorische und technische Vorkehrungen für die IT-Sicherheit zu treffen und dabei den Stand der Technik einzuhalten.

Wenn sich eine Organisation heute vornimmt, einen strukturierten Ansatz zum wirksamen Management der Informationssicherheit einzuführen, kommt sie an der Standardreihe ISO/IEC 27000 praktisch nicht vorbei. Bei ISO/IEC 27000 handelt es sich um eine Reihe von Dokumenten, in denen verschiedene Aspekte des Informationssicherheitsmanagements betrachtet werden. Dass es sich um von der ISO (International Organization for Standardization) und der IEC (International Electrotechnical Commission) standardisierte Dokumente handelt, erhöht dabei die Verbreitung, Bedeutung und Akzeptanz dieser Dokumente ganz maßgeblich. Das zentrale und wichtigste Dokument der Reihe ist dabei ISO/IEC 27001.

■ 1.1 Worum geht es in ISO/IEC 27001?

Die Standardfamilie ISO/IEC 27000 befasst sich hauptsächlich mit drei Dingen:

1. **Begriffe:** Es werden die wichtigsten Fachbegriffe aus der Welt der Informationssicherheit definiert.
2. **Grundlegendes Managementsystem:** Es wird beschrieben, was eine Organisation tun und sicherstellen muss, um die eigenen Aktivitäten und Maßnahmen im Bereich Informationssicherheit wirksam steuern zu können.
3. **Maßnahmen:** Es werden 114 Maßnahmen beschrieben, die eine Organisation grundsätzlich umzusetzen hat, um ein hohes Maß an Informationssicherheit gewährleisten zu können.

Dieses Buch bietet einen Überblick über alle drei Aspekte. Während die beiden letzteren in späteren Kapiteln behandelt werden, beschäftigt sich dieses Kapitel zunächst mit dem ersten Aspekt, der Begriffsbildung.

■ 1.2 Begriffsbildung

Die Standardfamilie ISO/IEC 27000 dient also unter anderem dazu, die Verwendung von Fachbegriffen zu vereinheitlichen. Nur so kann erreicht werden, dass diejenigen, die sich mit Informationssicherheitsmanagement beschäftigen, nicht aneinander vorbeireden, obwohl sie eigentlich inhaltlich dasselbe meinen.

Im Folgenden werden die wichtigsten Begriffe und Grundlagen rund um das Thema Informationssicherheit vorgestellt, die zum Verständnis der ISO/IEC 27000 Standards erforderlich sind.

1.2.1 Informationen

In unserer zunehmend vernetzten Welt sind Informationen Werte, die von entscheidender Wichtigkeit für den Geschäftsbetrieb einer Organisation sind. Durch den höheren Vernetzungsgrad sind diese Informationen einer stark zunehmenden Zahl von Bedrohungen ausgesetzt (vgl. auch [OEC15]). Informationssysteme, Netze und Organisationen sind gefährdet durch Cyber-Angriffe (böswärtiger Code, Denial-of-Service-Angriffe, Schadsoftware, Hacking, Spam etc.), Sabotage, Spionage und Vandalismus, aber auch Elementarschäden durch Wasser, Feuer sowie Katastrophen und andere Gefahren. Gesetzliche Regelungen (wie z. B. das IT-Sicherheitsgesetz oder Datenschutzgesetze) fordern Schutzmaßnahmen für sensible Informationen.

Der Begriff „Informationen“ wird hierbei sehr weit gefasst. Sie können in Form verschiedener Medien vorliegen: geschrieben, gedruckt, elektronisch, als Film etc., und auf unterschiedlichen Wegen übermittelt werden, z. B. per Post, per Funk, elektronisch usw. Unabhängig vom Medium und dem Übertragungsmittel ist die Aufgabe der Informationssicherheit, diese Informationen angemessen vor der zunehmenden Zahl von Bedrohungen zu schützen. Nur so können die Risiken minimiert, der Geschäftsbetrieb gesichert und die Wettbewerbsfähigkeit, Rentabilität sowie die Chancen einer Organisation maximiert werden.

1.2.2 Informationssicherheit

Der Begriff Informationssicherheit wird in den Standards der Reihe ISO/IEC 27000 – und damit auch im Hauptdokument ISO/IEC 27001 – über die drei Aspekte Vertraulichkeit, Integrität und Verfügbarkeit von Informationen definiert. Diese drei Aspekte können als die primären Schutzziele angesehen werden, deren Aufrechterhaltung in Kombination die Informationssicherheit ausmacht. Weitere Aspekte und damit Schutzziele wie Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit können ebenfalls betrachtet

werden (vgl. Anhang A). Die Schutzziele werden nachfolgend im Einzelnen vorgestellt und genauer erläutert.

1.2.3 Sicherheitsanforderungen und Schutzziele

Die Gefährdung wichtiger Informationen lässt sich alleine mit Beispielen natürlich nur ungenau und unvollständig fassen. In der ISO/IEC 27000 und im Security-Engineering werden deshalb abstrakte Schutzziele bzw. Sicherheitsanforderungen für Informationswerte (zum Begriff der „(Informations-)Werte“ vgl. Kapitel 3.1.1) definiert. Die zentralen Schutzziele sind Vertraulichkeit, Integrität und Verfügbarkeit (engl. *Confidentiality, Integrity and Availability*, als Eselsbrücke gerne mit „CIA“ abgekürzt) von Informationen. Andere wünschenswerte Eigenschaften, deren Aufrechterhaltung nach ISO/IEC 27000 ebenfalls Gegenstand der Informationssicherheit sein können, sind Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit (engl. *Authenticity, Accountability, Non-repudiation and Reliability*). Diese Schutzziele, auf denen der Informationssicherheitsbegriff der Standardfamilie ISO/IEC 27000 basiert, werden im Folgenden erläutert.

Zur Beschreibung von Sicherheitsmechanismen, der Verletzung von Schutzzielen oder aber von Angriffen werden im Security-Engineering oft fiktive Personen verwendet. Diese Personen haben definierte Rollen und Namen. Die „Guten“ heißen immer Alice und Bob und versuchen in der Regel, miteinander zu kommunizieren. Der „Böse“ (engl. *malicious*) heißt Mallet; er versucht, Alice, Bob oder deren Interaktionen oder Kommunikation anzugreifen, abzu hören oder zu stören. Im Folgenden werden Alice, Bob und Mallet in diesem Sin

1.2

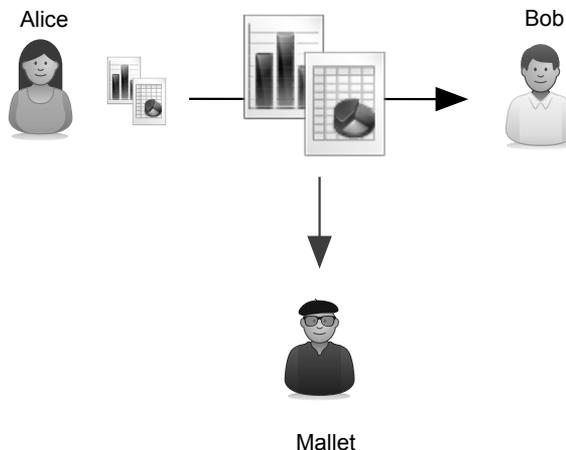


Abbildung 1.1 Verletzung der Vertraulichkeit durch Abhören

Die Vertraulichkeit bezeichnet die Eigenschaft, dass eine Information für unautorisierte Personen, Entitäten oder Prozesse nicht zugänglich ist und von diesen auch nicht offen-

gelegt werden kann. Die Vertraulichkeit ist beispielsweise verletzt, wenn ein Angreifer eine

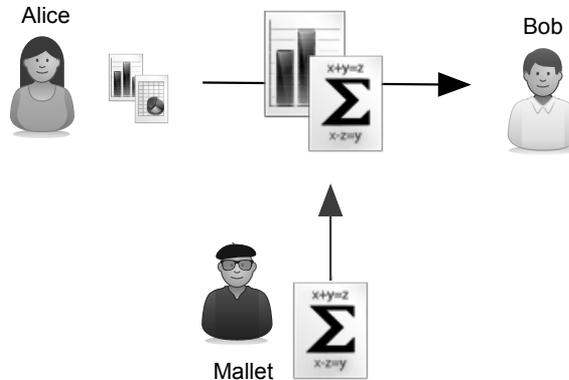


Abbildung 1.2 Verletzung der Integrität

Mit Integrität wird eine Eigenschaft bezeichnet, die Werte im Hinblick auf ihre Richtigkeit und Vollständigkeit schützt. Eine Integritätsprüfung einer digitalen Information oder Nachricht erkennt jede Veränderung an der Nachricht. Hierunter fallen alle denkbaren Manipulationen wie das Einfügen oder Löschen von Zeichen, das Wiedereinspielen einer Nachricht, das Umordnen von Daten oder Nachrichten sowie Duplikate.

Abbildung 1.2 stellt einen Angriff auf die Integrität der Kommunikation zwischen Alice und Bob dar. Mallet verändert die Nachricht, die Alice an Bob schickt.

1.2.3.3 Verfügbarkeit (Availability)

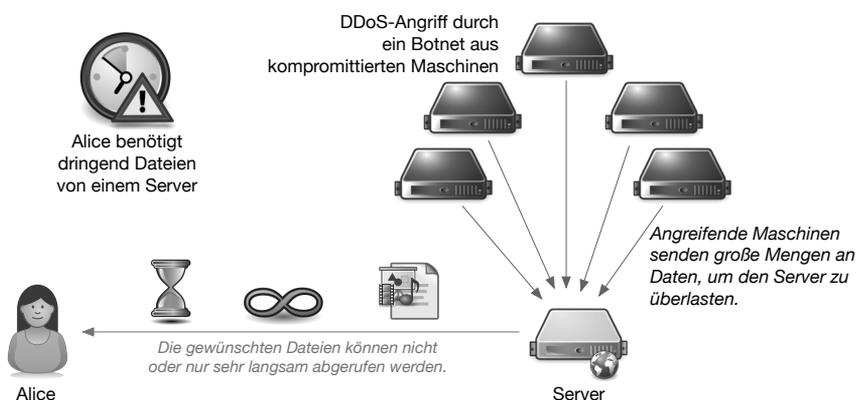


Abbildung 1.3 Verletzung der Verfügbarkeit durch DDoS-Angriff

Die Verfügbarkeit bezeichnet die Eigenschaft einer Information oder eines Wertes, für einen berechtigten Nutzer verfügbar und nutzbar zu sein, sobald der Nutzer dies ver-

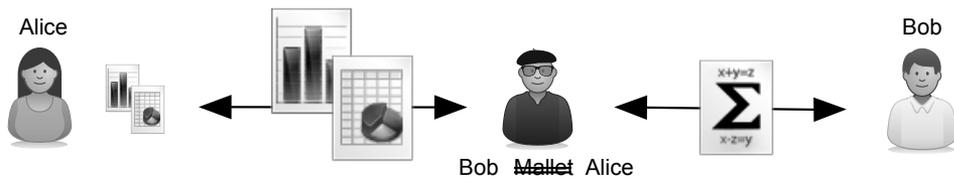


Abbildung 1.4 Verletzung der Authentizität durch einen Man-in-the-Middle-Angriff

langt. Die Verfügbarkeit wird z. B. durch Elementarschäden oder Katastrophen bedroht. Die prominentesten Angriffe auf die Verfügbarkeit von Diensten oder Ressourcen sind wie in Abbildung 1.3 dargestellt Denial-of-Service (DoS-) oder Distributed-Denial-of-Service (DDoS-) Angriffe.

1.2.3.4 Authentizität (Authenticity) und Authentisierung (Authentication)

Der Vorgang der zweifelsfreien Ermittlung und Prüfung einer Entität bzw. einer geforderten Charakteristik einer Entität wird als Authentisierung bezeichnet. Dementsprechend bezeichnet Authentizität die Eigenschaft einer Entität, das zu sein, was sie vorgibt zu sein. In der Benutzerverwaltung wird über verschiedenste Mechanismen ein Nutzer zweifelsfrei mit einer digitalen ID (z. B. einer eindeutigen Benutzerkennung) verbunden. Bei der Authentisierung wird diese Verbindung zwischen digitaler ID und Nutzer geprüft (z. B. durch Eingabe eines Passwortes, das nur der Nutzer kennt). Nach dieser Prüfung kann man davon ausgehen, dass die digitale ID authentisch ist.

In Abbildung 1.4 wird ein Man-in-the-Middle-Angriff dargestellt. Mallet unterbricht die Kommunikationsbeziehung zwischen Alice und Bob und gibt sich gegenüber Bob als Alice und gegenüber Alice als Bob aus. Er fälscht gewissermaßen seine Identität. Damit ist die Authentizität nicht mehr gewährleistet. Steht Alice und Bob nur der verwendete Kommunikationskanal zur Verfügung, so ist dieser Angriff nur sehr schwer zu erkennen.

1.2.3.5 Nichtabstreitbarkeit/Verbindlichkeit (Non-repudiation)

Mit Verbindlichkeit bezeichnet man den Vorgang, mit dem der Eintritt eines Ereignisses oder einer Aktion sowie die verursachende Entität zweifelsfrei belegt werden können. Damit können Kontroversen geklärt werden über das Eintreten oder Nichteintreten eines Events oder einer Aktion und die Beteiligung von Entitäten daran. Beispielsweise kann ein Nutzer die Auslösung einer Aktion später nicht leugnen.

1.2.3.6 Verlässlichkeit (Reliability)

Die Eigenschaft, ein konsistentes und bestimmungsgemäßes Verhalten zu zeigen und konsistente Ergebnisse zu liefern, wird als Verlässlichkeit bezeichnet. Beispielsweise würde eine Verschlüsselungssoftware für E-Mails, die jede dritte Nachricht unverschlüsselt überträgt, die Sicherheitsanforderung nach Verlässlichkeit nicht erfüllen.

1.2.3.7 Zugriffssteuerung (Access Control)

Nach ISO/IEC 27001 stellt die Zugriffssteuerung sicher, dass der Zugang zu Werten (Assets) nur autorisiert erfolgen kann und Einschränkungen auf Basis von Geschäfts- oder Sicher-

heitsanforderungen möglich sind. Die Zugriffssteuerung setzt ein Berechtigungskonzept technisch um; nur Berechtigte dürfen auf IT-Systeme und Informationen zugreifen.

1.2.3.8 Zurechenbarkeit (Accountability)

Die Zurechenbarkeit realisiert die Verantwortlichkeit einer Entität für ihre Aktionen und Entscheidungen. So müssen z. B. sicherheitsrelevante Aktionen demjenigen, der die entsprechende Aktion ausgeführt hat, zurechenbar sein. Die Zuweisung von Verantwortlichkeiten und die Übernahme von Verantwortung für Assets sind Grundsätze des Standards (vgl. Kapitel 3.1.4), die sich aber nur umsetzen lassen, wenn es Mechanismen gibt, um eine Zurechenbarkeit technisch umzusetzen.

■ 1.3 IT-Sicherheitsgesetz & KRITIS

Im Jahr 2015 wurde durch den Deutschen Bundestag das IT-Sicherheitsgesetz (IT-SiG) [Bun15] beschlossen, das in erster Linie Änderungen an bestehenden Gesetzen, darunter dem BSI-Gesetz (BSiG), umfasst. Im Kern bedeuteten diese Änderungen die Abkehr vom Prinzip der Freiwilligkeit für den Bereich sogenannter kritischer Infrastrukturen. Dabei handelt es sich gemäß der Definition aus der KRITIS-Strategie des Bundes um Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.

Betreiber solcher kritischer Infrastrukturen werden nach dem Gesetz verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen. Den Nachweis darüber haben die Betreiber durch Sicherheitsaudits, Prüfungen und/oder Zertifizierungen zu erbringen, indem sie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Aufstellung der durchgeführten Audits oder Zertifizierungen übermitteln. Darüber hinaus müssen Betreiber kritischer Infrastrukturen erhebliche IT-Sicherheitsvorfälle melden. Das BSI agiert als Zentralstelle für IT-Sicherheit und wertet Meldungen der Betreiber kritischer Infrastrukturen aus.

1.3.1 Was ist „KRITIS“?

Unter dem Schlagwort KRITIS versteht man übergreifend die Anforderungen, die sich aus dem IT-Sicherheitsgesetz und der Verordnung zur Bestimmung kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung) für Betreiber kritischer Infrastrukturen ergeben. Dabei beschränkt sich KRITIS derzeit auf die folgenden sieben Sektoren bzw. Branchen:

- Energie
- Wasser
- Ernährung

- Informationstechnik und Telekommunikation
- Gesundheit
- Finanz- und Versicherungswesen
- Transport und Verkehr

1.3.2 Wer ist in Deutschland von KRITIS betroffen?

Während die eigentlichen Gesetzestexte offenlassen, welche Organisationen oder Unternehmen tatsächlich vom IT-Sicherheitsgesetz betroffen sind und somit die KRITIS-Anforderungen erfüllen müssen, wird die BSI-Kritisverordnung konkreter. Sie definiert nämlich spezifische Anlagenkategorien, Bemessungskriterien und Schwellenwerte, aus denen jede Organisation oder Einrichtung aus einer der sieben genannten Branchen ableiten kann, ob sie als Betreiber einer kritischen Infrastruktur gilt oder nicht.

Die BSI-Kritisverordnung ist im Internet frei zugänglich unter <https://www.gesetze-im-internet.de/bsi-kritisv>. Sie ist wie folgt aufgebaut:

- §1 enthält die für diese Verordnung relevanten Begriffsbestimmungen.
- In §2 bis §8 findet man zu jedem der sieben relevanten Sektoren eine genauere Beschreibung der relevanten kritischen Dienstleistungen.
- In §8 wird festgelegt, dass die Verordnung und die enthaltenen Festlegungen (zu den kritischen Dienstleistungen, Anlagenkategorien und Schwellenwerten) alle zwei Jahre erneut evaluiert werden sollen.
- Zuletzt folgen die Anhänge 1 bis 7, die wiederum zu jedem der sieben relevanten Sektoren und den zuvor beschriebenen kritischen Dienstleistungen die Anlagenkategorien, Bemessungskriterien und Schwellenwerte tabellarisch auflisten.

Beispiel 1: Im Sektor Wasser ist eine kritische Dienstleistung die Versorgung der Allgemeinheit mit Trinkwasser. Diese umfasst gemäß §3 der BSI-Kritisverordnung die Gewinnung, Aufbereitung, Verteilung sowie Steuerung und Überwachung von Trinkwasser. Gemäß Anhang 3 sind relevante Anlagenkategorien unter anderem Gewinnungsanlagen, Aufbereitungsanlagen, Leitstellen sowie das Wasserverteilungssystem (z.B. Rohrnetz mit Druckregulierstationen). Für die Anlagenkategorie der Gewinnungsanlagen ist das relevante Bemessungskriterium die gewonnene Wassermenge in Millionen Kubikmeter pro Jahr, und der Schwellenwert wurde hierfür mit 22 festgelegt. Gewinnt ein Wasserversorger (z.B. Stadtwerk, Wasserwerk) also mehr als diese 22 Millionen Kubikmeter Trinkwasser pro Jahr in eigenen oder zumindest durch ihn verantworteten Anlagen, so gilt er als Betreiber einer kritischen Infrastruktur.

Beispiel 2: Im Sektor Transport und Verkehr ist eine kritische Dienstleistung die Versorgung der Allgemeinheit mit Leistungen zum Transport von Personen und Gütern. Diese umfasst gemäß §8 der BSI-Kritisverordnung den Luftverkehr, Schienenverkehr, die Binnen- und Seeschifffahrt, den Straßenverkehr, öffentlichen Personennahverkehr (ÖPNV) sowie die Logistik. Gemäß Anhang 7 ist eine relevante Anlagenkategorie beispielsweise ein System zur Passagierabfertigung an Flugplätzen. Das relevante Bemessungskriterium ist die Anzahl der Passagiere pro Jahr, und der Schwellenwert wurde hierfür mit 20 Millionen festgelegt. Werden also an einem Flughafen mehr als 20 Millionen Fluggäste pro Jahr abgefertigt, so gilt der Betreiber als Betreiber einer kritischen Infrastruktur.

1.3.3 KRITIS-Anforderungen – Informationssicherheit nach dem „Stand der Technik“

Nachdem nun also seit Inkrafttreten der BSI-Kritisverordnung klar sein sollte, wer genau vom IT-Sicherheitsgesetz betroffen ist und die KRITIS-Anforderungen erfüllen muss, bleibt noch die Frage: Was genau müssen Betreiber kritischer Infrastrukturen tun und worüber müssen sie Nachweise erbringen? Die wesentliche Anforderung besteht darin, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität nach dem „Stand der Technik“ aufrechterhalten werden müssen. Der Stand der Technik ist ein Rechtsbegriff, der in verschiedenen Rechtsgebieten Verwendung findet und höhere Ansprüche stellt als etwa die anerkannten Regeln der Technik. Übertroffen wird er noch vom Stand von Wissenschaft und Technik.

Unter dem Stand der Technik werden die technischen Möglichkeiten verstanden, die zum gegenwärtigen Zeitpunkt den gewünschten Effekt gewährleisten können und sich dabei auf wissenschaftliche und technische Erkenntnisse stützen. Die Erfüllung anerkannter Standards, die etwa von Standardisierungsgremien oder Branchenverbänden herausgegeben werden, kann juristisch gesehen die begründete Vermutung nahelegen, dass in dem jeweiligen Gebiet der Stand der Technik erreicht wurde. Im Zusammenhang mit der Informationssicherheit bzw. dem Management der Informationssicherheit gilt dies entsprechend auch für die Etablierung eines Informationssicherheitsmanagementsystems (ISMS) auf Basis der Standardfamilie ISO/IEC 27000.

Das BSI weist allerdings in seinen KRITIS-Orientierungshilfen darauf hin, dass eine Zertifizierung nach ISO/IEC 27001 allein noch nicht automatisch ausreichend ist, um den Anforderungen des IT-Sicherheitsgesetzes vollständig zu genügen. Das liegt beispielsweise daran, dass auch in einem nach ISO/IEC 27001 zertifizierten ISMS Akzeptanzschwellen für Informationssicherheitsrisiken vom Betreiber festgelegt werden könnten, die die Akzeptanz erheblicher Risiken für die Versorgungssicherheit erlauben würden – was der Zielsetzung von KRITIS widerspricht. Aus diesem Grund können sowohl Betreiber kritischer Infrastrukturen als auch ihre Branchenverbände eigene bzw. branchenspezifische Informationssicherheitsstandards (B3S) festlegen und ihre Eignung vom BSI feststellen lassen. Das BSI führt auf seinen Webseiten eine Übersicht über die B3S, deren Eignung festgestellt wurde und die daher zur Nachweisführung über den Stand der Technik herangezogen werden können. Praktisch alle bisher eignungsgeprüften B3S basieren in der einen oder anderen Form auf Inhalten und Anforderungen aus der Standardfamilie ISO/IEC 27000.

■ 1.4 Datenschutz-Grundverordnung

Die Europäische Union hat mit der Datenschutz-Grundverordnung (DSGVO) [DSG16] das Datenschutzrecht EU-weit vereinheitlicht. Die DSGVO, die am 25. Mai 2018 in Kraft getreten ist, bildet den gemeinsamen Datenschutzrahmen in der Europäischen Union und gilt unmittelbar für alle Mitgliedsstaaten. Nationale und föderale Gesetze, wie z.B. das Bundesdatenschutzgesetz oder Landesdatenschutzgesetze, sind weiterhin möglich, müssen aber mit der DSGVO vereinbar sein.

Die DSGVO übernimmt viele Prinzipien aus der Vorgängerrichtlinie (95/46) oder dem Bundesdatenschutzgesetz. Der zentrale Begriff der *Personenbezogenen Daten* in Art. 4 ist sehr weit gefasst: „*personenbezogene Daten*“ [sind] *alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person [...] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.*

Neu in der DSGVO sind die in Art. 5 aufgeführten Grundsätze für die Verarbeitung personenbezogener Daten:

- a) Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- b) Zweckbindung (Verarbeitung nur für definierte, eindeutige und legitime Zwecke)
- c) Datenminimierung („dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung [...] notwendige Maß beschränkt“)
- d) Richtigkeit („sachlich richtig und erforderlichenfalls auf dem neuesten Stand [...]; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung [...] unrichtig sind, unverzüglich gelöscht oder berichtigt werden“)
- e) Speicherbegrenzung („nur so lange [...], wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“)
- f) Integrität und Vertraulichkeit („in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen“)

Der letzte Grundsatz – ebenso wie Abschnitt 2 (Art. 32 bis 34) der DSGVO – fordern explizit die Sicherheit personenbezogener Daten durch technische und organisatorische Maßnahmen „unter Berücksichtigung des Stands der Technik“ sicherzustellen. Technische und organisatorische Maßnahmen zum Schutz von Daten sind ein Hauptaspekt der ISO/IEC 27001. Ein Nachweis des Stands der Technik kann z.B. durch eine Organisationszertifizierung nach ISO/IEC 27001 erfolgen.

Eine weitere Neuerung der DSGVO ist die in Art. 35 eingeführte Datenschutz-Folgenabschätzung. Falls eine Verarbeitung personenbezogener Daten „aufgrund des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat, so ist eine Datenschutz-Folgenabschätzung durchzuführen. Dabei handelt es sich um einen klassischen Risikomanagementprozess, wie er ab Abschnitt 4.6.1 erläutert wird.

Die Grundlagen, Prinzipien und Prozesse der ISO/IEC 27001 lassen sich gewinnbringend auch bei der Umsetzung der Datenschutzgrundverordnung nutzen.

■ 1.5 Überblick über die folgenden Kapitel

In Kapitel 2 wird ein grundlegender Überblick über die Standardfamilie ISO/IEC 27000 und ihre Struktur gegeben, bevor im darauffolgenden Kapitel die Grundlagen eines Informationssicherheitsmanagementsystems dargestellt werden. Der Standard ISO/IEC 27001 wird in den Kapiteln 4 und 5 ausführlich erläutert und kommentiert. Die Mindestanforderungen, d. h. die Abschnitte 1 bis 10 des Standards, finden sich in den Kapiteln 4.1 bis 4.10. Die Anhangteile A.5 bis A.18 von ISO/IEC 27001, die Maßnahmen und Maßnahmenziele enthalten, werden in Kapitel 5 ausführlich erklärt. Die folgenden Kapitel erläutern verwandte Standards und Rahmenwerke sowie die verschiedenen Zertifizierungsmöglichkeiten nach ISO/IEC 27000. Im Anhang des Buches finden Sie 40 Prüfungsfragen mit entsprechenden Musterlösungen, die vom Schwierigkeitsgrad her der ISO/IEC 27001 Foundation-Prüfung entsprechen.

■ 1.6 Beispiele für Prüfungsfragen zu diesem Kapitel

Nachfolgend finden Sie Beispiele für Prüfungsfragen, die sich thematisch mit den in diesem Kapitel erlernten Inhalten auseinandersetzen. Die richtigen Antworten inklusive Erläuterungen und Verweisen befinden sich in Anhang C.1 ab Seite 231.



Prüfungsfrage 1.1:

Was versteht ISO/IEC 27000 unter dem Begriff Vertraulichkeit (engl. *Confidentiality*)?

- A) Den Abschluss einer Vertraulichkeitsvereinbarung (Non-disclosure agreement).
- B) Die Geheimhaltungsverpflichtung aller Mitarbeiter, die Zugriff auf das ISMS haben.
- C) Die Vertraulichkeit schützt die Werte im Hinblick auf ihre Richtigkeit und Vollständigkeit.
- D) Eine Information ist für unautorisierte Personen, Entitäten oder Prozesse nicht zugänglich.



Prüfungsfrage 1.2:

Was versteht ISO/IEC 27000 unter dem Begriff Verfügbarkeit (engl. *Availability*)?

- A) Die Eigenschaft einer Information oder eines Wertes, für eine berechnigte Person oder Entität zugreifbar und nutzbar zu sein.
- B) Die Eigenschaft einer informationsverarbeitenden Einrichtung, genügend Ressourcen für eine Aufgabe zur Verfügung zu haben.
- C) Die Eigenschaft einer Information oder eines Wertes, vor Manipulation geschützt zu sein.
- D) Die Eigenschaft einer Information oder eines Wertes, vor Offenlegung geschützt zu sein.

Prüfungsfrage 1.3:

Was versteht ISO/IEC 27000 unter dem Begriff Nichtabstreitbarkeit (engl. *Non-repudiation*)?

- A) Die verbindliche Regelung interner Sicherheitsaudits.
- B) Nichtabstreitbarkeit bezeichnet die Eigenschaft eines Wertes, für einen berechtigten Nutzer verfügbar und nutzbar zu sein.
- C) Als Nichtabstreitbarkeit bezeichnet man den Vorgang, mit dem der Eintritt eines geforderten Ereignisses oder einer Aktion zweifelsfrei einem Verursacher zugerechnet werden kann. Dieser kann den Vorgang nicht leugnen.
- D) Die Eigenschaft, ein konsistentes und bestimmungsgemäßes Verhalten zu zeigen und konsistente Ergebnisse zu liefern.

Index

A

Abhören 103
Access Control 5
Accountability 6
Act-Phase 32, 35, 66
Änderungssteuerung 106
Akkreditierung 16, 164
Anforderung 186
Angriff 175
Anschaffung von Systemen 119
Anwendungsbereich 14, 38, 42, 51, 163, 167
APMG 170
Asset *siehe* Wert
Audit 18, 66, 127, 163, 165, 175
– Bericht 65
– externes 63
– Informationssysteme 113
– internes 63
– Nachweise 64
– Programm 64
– Protokoll 65
– Umfang 167, 175
Auditor 64
Aufgabe des Managements 26
Aufgabentrennung 78
Aufgeräumte Arbeitsumgebung 104
Aufzeichnung 25
ausgliedern 185
Authentication 5
Authenticity 5
Authentisierung 5, 176
Authentizität 5, 176
Availability 4
AXELOS 155

B

Bayerischer IT-Sicherheitscluster e.V. 147
Bedrohung 191
Befugnisse 45

Benutzerverantwortlichkeiten 93
Benutzerzugangsverwaltung 91
Beschäftigung 81
Best Practices 17
Betrieb 58
Betriebs- und Kommunikationsmanagement
– Netzsicherheit 115
Betriebsablauf-Verantwortung 105
Betriebsmanagement
– Überwachung 109
Betriebsmittel 101
Betriebssicherheit 105
Beweismaterial 132
Bewusstsein 55
Bildschirm Sperre 104
BSI *siehe* Bundesamt für Sicherheit in der
Informationstechnik
BSI-Standards 146
BS 7799 17
Bundesamt für Sicherheit in der
Informationstechnik 145
– IT-Grundschutz-Kompendium 145
– IT-Grundschutz-Standards 146
Business Continuity Management 133

C

CENELEC 158
CERT *siehe* Computer Emergency Response
Team
Chancen 46
Check-Phase 31, 35, 60
Chief Information Security Officer 27
CISO *siehe* Chief Information Security Officer
COBIT 158
Committee of Sponsoring Organizations of the
Treadway Commission
– ERM 154
Compliance 136
Computer Emergency Response Team 78

Computer Security Incident Response Team
128
Confidentiality *siehe* Vertraulichkeit
Control Objectives 35
Controls 35
COSO *siehe* Committee of Sponsoring
Organizations of the Treadway Commission
COSO ERM 154
CSIRT *siehe* Computer Security Incident
Response Team
Cybersecurity Framework 147

D

DAkKS *siehe* Deutsche Akkreditierungsstelle
Daten
– personenbezogene 9
– Richtigkeit 9
– Speicherbegrenzung 9
Datenminimierung 9
Datenschutz
– Folgenabschätzung 9
Datenschutz-Folgenabschätzung 9
Datenschutz-Grundverordnung 8
Datenschutzbeauftragter 26
Datensicherung 108
Datenträger 87
Definitionsebene 25
Deming-Kreislauf 30, 35
Deutsche Akkreditierungsstelle 164
Dienstleistungserbringung 126
Do-Phase 31, 35, 54, 58
Dokument 25
Dokumentation 25, 56
Dokumentenaudit 64, 165
Dokumentenlenkung 26, 57, 57
Dokumentenvorlage 58
DoS-Angriff 5
DSGVO *siehe* Datenschutz-Grundverordnung
Durchführungsebene 25

E

Effektivität 32, 65
Effizienz 32, 65
Elementarmessgröße 176
EN 50600 158, 159
Entsorgung von Datenträgern 88
Entwicklung 119
– ausgegliederte 122
Entwicklungsprozess 120
Entwicklungsumgebung 122
Ereignis 179
Ereignismeldung 130

Ereignisprotokollierung 109
Examination Institute 168
Externes Audit 63, 163
Externe Mitarbeiter 26

F

FitSM 157
Folge 177
Fortbildungsprogramme 26
Foundation-Zertifikat 169, 171
– Prüfungsspezifikation 171
– Prüfungsvorbereitung 172
Führung 43

G

Geheimhaltungsvereinbarung 118
Gesamtverantwortung 26

H

Hilfsprogramme mit privilegierten Rechten 95

I

ICO 170
IEC *siehe* International Electrotechnical
Commission
Indikator 25, 180
Information 2, 178
– Übertragung von 116
– Handhabung 87
– Kennzeichnung 86
– Klassifizierung 86
Information Security Officer 27
Information Systems Audit and Control
Association 158
Informationsaustauschende Gemeinschaft 181
Informationsbedarf 180
Informationsklassifizierung 86
Informationssicherheit 2, 180
– Aufrechterhaltung 180
– Organisation 77
– Steuerung 179
Informationssicherheitsereignis 130, 180
Informationssicherheitsmanagementsystem
23, 43
– Audit 18
– Dokumentation 25
– Kernbestandteile 23
Informationssicherheitsrichtlinie 75
Informationssicherheitsrisikobehandlung 51
Informationssicherheitsrisikobeurteilung 48
Informationssicherheitsvorfall 128, 181
– Handhabung 181

Informationssysteme 181
 – Audit 113
 – Schwachstellenmanagement 111
 – Sicherheitsanforderungen 119
 Informationsveranstaltungen 26
 informationsverarbeitende Einrichtungen 180
 Informationszugangsbeschränkung 94
 Informativer Standard 14
 Installation 111
 Instandhaltung 103, 119
 Integrität 4, 9, 181
 Integrity *siehe* Integrität
 Interessierte Partei 182
 International Electrotechnical Commission 1
 International Organization for Standardization 1
 Internes Audit 63
 Interne Organisation 77
 Inventar 84
 Inventarisierung der Werte 85
 ISACA *siehe* Information Systems Audit and Control Association
 ISIS12 147
 ISMS *siehe* Informationssystem
 Informationssystem
 ISO *siehe* International Organization for Standardization, *siehe* Information Security Officer
 ISO/IEC 15408 148
 ISO/IEC 17020 153
 ISO/IEC 17021 16, 17, 153, 164, 166
 ISO/IEC 17024 153
 ISO/IEC 17025 153
 ISO/IEC 17799 17, 73, 163
 ISO/IEC 20000 28, 156
 ISO/IEC 27000 14
 ISO/IEC 27001 16
 ISO/IEC 27002 17
 ISO/IEC 27003 17
 ISO/IEC 27004 18
 ISO/IEC 27005 18
 ISO/IEC 27006 16, 153, 166, 167
 ISO/IEC 27007 18
 ISO/IEC 27008 18
 ISO/IEC 27009 16, 17
 ISO/IEC 27010 20
 ISO/IEC 27011 20
 ISO/IEC 27013 18
 ISO/IEC 27014 18
 ISO/IEC 27016 18
 ISO/IEC 27017 20
 ISO/IEC 27018 19, 20

ISO/IEC 27019 20
 ISO/IEC 27032 21
 ISO/IEC 27034 21
 ISO/IEC TR 27023 19
 ISO 19011 152, 166
 ISO 31000 154
 ISO 9000 14, 28, 151
 ISO 9001 151
 ISO 9004 152
 IT Service Management 106
 IT-Grundschutz-Kompendium 145
 IT-Sicherheitsgesetz 6
 ITEMO e.V. 157
 ITIL *siehe* IT Infrastructure Library, 155
 ITSM *siehe* IT Service Management

K

Kapazitätssteuerung 106
 Kategorien von Werten 24
 Kennwort 94
 Kennzeichnung von Information 86
 Kernbestandteile eines ISMS 23
 Klassifizierung von Information 86
 Kommunikation 55
 Kompetenz 54, 176
 Konformität 16, 31, 65, 66, 164, 177
 Kontext 179
 – der Organisation 40
 – interner 182
 Kontinuierliche Verbesserung 29
 Korrektur 178
 Korrekturmaßnahme 178
 Kryptographie 96

L

Leistung 185
 Leitfaden 17
 Leitung 43, 191
 Lieferantenbeziehungen 125
 Lizenzmanagement 137
 Löschung 88, 104

M

Management der Netzsicherheit 115
 Management Review 65
 Managementbewertung 65
 Managementsystem 23, 183
 Maßnahme 27, 73–139, 177
 – Betriebsmanagement 111
 – Organisation der Informationssicherheit 77
 – Personalsicherheit 80

- Physische und umgebungsbezogene Sicherheit 98
- Sicherheitsrichtlinie 75
- Verwaltung der Werte 84
- Zugangssteuerung 90
- Maßnahmenziele 27, 73–139, 177
- Measurement 18
- Messfunktion 183
- Messgröße 178, 183
- Messmethode 184
- Messung 18, 60, 183
- Mobilgeräte 79

N

- NAC *siehe* Network Access Control
- Nachvollziehbarkeit 25
- National Institute of Standards and Technology
 - Cybersecurity Framework 147
- Network Access Control 115
- Network Time Protocol 111
- Netzicherheit 115
- Netzicherheitsmanagement 115
- Netztrennung 116
- Netzzugang 91
- Nichtabstreitbarkeit 5, 184
- Nichtkonformität 184
- NIM *siehe* Netzwerk für Informationssicherheit im Mittelstand
- NIST *siehe* National Institute of Standards and Technology
- Non-repudiation 5
- Norm 14
- Normative Verweisungen 39
- Normativer Standard 14
- Notfallmanagement 133
- NTP *siehe* Network Time Protocol

O

- Organisation 185
- Organisation der Informationssicherheit 77
 - Interne Organisation 77
 - Mobilgeräte 79
 - Telearbeit 79
- Organisationszertifizierung 163

P

- Passwort 94
- PCI-DSS 149
- PDCA 29, 35
- PDCA-Methodik 23, 29
- Personalsicherheit 80
 - Änderung der Beschäftigung 83

- Beendigung der Beschäftigung 83
 - vor der Beschäftigung 81
 - während der Beschäftigung 82
- Personenbezogene Daten 9
- Personenzertifizierung 163, 168
- Physische Sicherheit 98
 - Sicherheit von Betriebsmitteln 101
 - Sicherheitsbereiche 98
- PKI *siehe* Public-Key-Infrastructure
- Plan 46
- Plan-Phase 30, 35, 46
- Planung 30, 46
- Politik 44, 186
- Privilegierte Rechte 95
- Privilegierte Zugangsrechte 92
- Protokollierung 109
- Prozess 24, 28, 186
- Prozessmanagement 29
- Prozessorientierung 28
- Public-Key-Infrastructure 97

Q

- Qualifizierungsprogramm 168
- Qualitätsmanagement 29
- Quellcode 95

R

- Rahmenwerk 145
- Rechtsprechung 26
- Redundanz 135
- Registrierung und Deregistrierung von Benutzern 91
- Reliability 5
- RESILIA 156
- Ressourcen 30, 54
- Restrisiko 186
- Rezertifizierung 167
- Richtigkeit 9
- Richtlinie 24, 75
 - themenspezifisch 76
- Risiko 187
 - Absprachen 188
 - Akzeptanz 49, 188
 - Analyse 50, 188
 - Behandlung 51, 190
 - Beurteilung 49, 59, 188
 - Bewertung 50, 189
 - Eigentümer 190
 - Identifizierung 189
 - Kommunikation 188
 - Kriterien 189
 - Management 18, 85

Risikomanagement 46, 84, 154, 189
– Prozess 190
Risikoniveau 182
Rollen 26, 27
Rückgabe von organisationseigenen Werten 85
Rückverfolgbarkeit 25

S

Schadsoftware 107
Schutzniveau 27
Schutzziel 3
Schwachstellen 111, 130, 191
Schwachstellenmanagement 111
Scope *siehe* Anwendungsbereich
Scoping 14, 163
Scoping statement 163
Security Incident Coordinator 128
Security Incident Response 128
Security Information & Event Management 109
SIC *siehe* Security Incident Coordinator
Sichere Anmeldeverfahren 94
Sicherheit
– Betriebsmittel 101
– physische und umgebungsbezogene 98
– Umgebungsbezogene 98
Sicherheitsanforderung 3
Sicherheitsbereiche 98
Sicherheitsrichtlinie *siehe*
Informationssicherheitsrichtlinie
Sicherheitsvorfälle 128
Sicherheitsziele 53
Sicherung 108
SIEM *siehe* Security Information & Event
Management
SIR *siehe* Security Incident Response
Software 111
Speicherbegrenzung 9
Standard 14
– informativer 14
– normativer 14
Standardfamilie 13
Standardisierung 13
Statement of applicability 163
Steuerung 179
Steuerungsebene 25
Steuerungsgremium 179
Support 54
System zur Verwaltung von Kennwörtern 94
Systemabnahmetest 123

T

TÜV Süd 169

Telearbeit 79
Terminologie 14
Testdaten 123
Testen 122

U

Überblicksdokument 14
Überprüfung 31, 60, 127, 187
– Ziel der 187
Überprüfung von Benutzerzugangsrechten 92
Übertragung von Informationen 116
Überwachung 60, 109, 127, 184
Überwachungsaudit 167
Uhrensynchronisation 110
Umgebungsbezogene Sicherheit *siehe*
Physische Sicherheit
Umsetzung 31, 54, 58
Unterstützungsprozess 120
Urheberrecht 137

V

VDA ISA (TISAX) 150
VDE 159
Verantwortlichkeit 26, 45, 76
Verantwortung 77, 82, 84
– von Benutzern 93
Verbesserung 32, 66, 177
Verbesserungsmaßnahmen 32
Verbindlichkeit 5
Verfahren 24
Verfahrensanweisung 25
Verfügbarkeit 4, 176
Verkabelung 102
Verlässlichkeit 5, 186
Verschlüsselung 103
Versorgungseinrichtungen 102
Vertrauenswürdige Einheit 191
Vertraulichkeit 3, 9, 176
Vertraulichkeitsvereinbarung 118
Verwaltung
– geheimer Authentisierungsinformation von
Benutzern 92
– privilegierter Zugangsrechte 92
– von Kennwörtern 94
Verwaltung der Werte 84
– Datenträger 87
– Entsorgung von Datenträgern 88
– Handhabung von Werten 87
– Informationsklassifizierung 86
– Inventar 85
– Kennzeichnung von Information 86
– Klassifizierung von Information 86

- Rückgabe von Werten 85
 - Verantwortung 84
 - Wechseldatenträger 87
 - zulässiger Gebrauch 85
 - Zuständigkeit 85
 - Verwaltung geheimer
 - Authentisierungsinformation von Benutzern 92
 - Verwaltung privilegierter Zugangsrechte 92
 - Verwandte Standards 145
 - Auditierung 151
 - Governance 155
 - IT- und Informationssicherheit 145
 - Management der IT 155
 - Qualitätsmanagement 151
 - Risikomanagement 154
 - Zertifizierung 151
 - Verwertungsrecht 137
 - Vorgaben 75
 - Vorstand 26
- W**
- Wahrscheinlichkeit 183
 - Wechseldatenträger 87
 - Wert 24, 84
 - Handhabung 87
 - Inventar 85
 - Kennzeichnung 86
 - Klassifizierung 86
 - Management 84
 - Rückgabe 85
 - Verantwortung 84
 - zulässiger Gebrauch 85
 - Zuständigkeit 85
 - Wiederholungsaudit 167
 - Wirksamkeit 178
 - Wirkungsgrad 32
- Z**
- Zeitpunkte 30
 - Zertifikat 167
 - Zertifizierung 163
 - Ablauf 165
 - Akkreditierung 164
 - Organisationszertifizierung 163
 - Personenzertifizierung 163, 168
 - Rezertifizierung 167
 - Zertifizierungsaudit 16, 165
 - Zertifizierungsprüfung 231
 - Zertifizierungsstelle 16, 165
 - Ziel 184
 - Zugang 90
 - Zugang zu Netzwerken und Netzwerkdiensten 91
 - Zugangssteuerung 90, 175
 - Überprüfung von Benutzerzugangsrechten 92
 - Benutzerverantwortlichkeiten 93
 - Benutzerzugangsverwaltung 91
 - Gebrauch von Hilfsprogrammen mit privilegierten Rechten 95
 - Geschäftsanforderungen 90
 - Informationszugangsbeschränkung 94
 - Quellcode von Programmen 95
 - Registrierung und Deregistrierung von Benutzern 91
 - Sichere Anmeldeverfahren 94
 - System zur Verwaltung von Kennwörtern 94
 - Systeme und Anwendungen 93
 - Verwaltung geheimer Authentisierungsinformation von Benutzern 92
 - Verwaltung privilegierter Zugangsrechte 92
 - Zugang zu Informationen 90
 - Zugang zu Netzwerken und Netzwerkdiensten 91
 - Zugangssteuerungsrichtlinie 90
 - Zuteilung von Benutzerzugängen 92
 - Zugangssteuerungsrichtlinie 90
 - Zugriff 90
 - Zugriffskontrolle 5
 - Zugriffssteuerung 5
 - Zulässiger Gebrauch von Werten 85
 - Zurechenbarkeit 6
 - Zuständigkeit
 - organisationseigener Werte 85
 - Zuteilung von Benutzerzugängen 92
 - Zutritt 90
 - Zuweisung
 - Rollen 26
 - Zweckbindung 9