Michael **BRENNER**
Nils **GENTSCHEN FELDE**
Wolfgang **HOMMEL**
Stefan **METZGER**
Helmut **REISER**
Thomas **SCHAAF**

PRAXISBUCH ISO/IEC 27001

Management der Informationssicherheit und Vorbereitung auf die Zertifizierung

5. Auflage

DIN EN ISO/IEC 27001:2024

Bausteine zur Erfüllung des IT-Sicherheitsgesetzes

80 Prüfungsfragen zur Vorbereitung auf die Foundation-Zertifizierung

HANSER

Brenner/gentschen Felde/Hommel/Metzger/Reiser/Schaaf

Praxisbuch ISO/IEC 27001

Michael Brenner
Nils gentschen Felde
Wolfgang Hommel
Stefan Metzger
Helmut Reiser
Thomas Schaaf

Praxisbuch ISO/IEC 27001

Management der Informationssicherheit und Vorbereitung auf die Zertifizierung

5., aktualisierte Auflage

HANSER

Die Autoren:

Dr. Michael Brenner
Dr. Nils gentschen Felde
Prof. Dr. Wolfgang Hommel
Stefan Metzger
Prof. Dr. Helmut Reiser
Dr. Thomas Schaaf

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Lektorat: Sylvia Hasselbach
Copy editing: Sandra Gottmann, Wasserburg
Layout: die Autoren mit LaTeX
Umschlagdesign: Marc Müller-Bremer, www.rebranding.de, München
Umschlagrealisation: Thomas West
Titelmotiv: © istockphoto.com/bortonia
Druck und Bindung: CPI Books GmbH, Leck
Printed in Germany

Print-ISBN: 978-3-446-47711-7
E-Book-ISBN: 978-3-446-47845-9
E-Pub-ISBN: 978-3-446-48267-8

Inhaltsverzeichnis

Vorwort

Liebe Leserinnen und Leser,

dieses nunmehr in seiner fünften überarbeiteten Auflage vorliegende Buch verfolgt das Ziel, Sie auf Basis des Wortlauts der aktuellen deutschen Fassung der internationalen Norm ISO/IEC 27001 durch die Welt der Informationssicherheitsmanagementsysteme (ISMS) zu begleiten. Es wird Ihnen sowohl bei der Vorbereitung auf eine Personen- oder Organisationszertifizierung als auch bei der praktischen Anwendung als Nachschlagewerk nützlich sein.

Für alle, die sich mit Informationssicherheit und ISMS sowie verwandten Themen wie Datenschutz, IT-Governance, Risikomanagement und Compliance auseinandersetzen, führt branchenübergreifend faktisch kein Weg an ISO/IEC 27001 vorbei. Diese Norm ist seit rund zwei Jahrzehnten der international bewährte gemeinsame Nenner, der sich beispielsweise auch im *IT-Grundschutz* des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) und den *Branchenspezifischen Sicherheitsstandards (B3S)* für Kritische Infrastrukturen wiederfindet. Zuletzt wurde die englische ISO/IEC 27001 im Jahr 2022 deutlich überarbeitet; die 2024 erschienene deutsche Fassung, DIN EN ISO/IEC 27001:2024-01, ist in Anhang B dieses Buchs im Originallayout vollständig abgedruckt.

Die ersten drei Buchkapitel führen Sie zunächst kompakt in die spannende, aber auch komplexe Welt der ISMS und der Normenreihe ISO/IEC 27000 ein. In den Kapiteln 4 und 5 werden alle Anforderungen und Maßnahmen aus der DIN EN ISO/IEC 27001 in grau hinterlegten Kästen im Wortlaut wiedergegeben, im Sinne einer verständlichen Einführung im Einzelnen erläutert und mit Umsetzungsbeispielen sowie ergänzenden Hinweisen aus der Praxis angereichert. Anschließend zeigt Kapitel 6 Schnittstellen zu verwandten Standards und Rahmenwerken auf. Kapitel 7 erläutert die Vorgehensweisen bei der Zertifizierung von ISMS sowie bei der Personenqualifizierung. In Anhang A dieses Buchs finden Sie zudem alle in der DIN EN ISO/IEC 27000 definierten Fachbegriffe im Wortlaut.

Die Schwerpunkte unserer Erläuterungen orientieren sich an den Prüfungsinhalten zu den Foundation-Lehrgangskonzepten u. a. von APMG, ICO und der TÜV Süd Akademie. Jeweils am Ende der Kapitel 1 bis 7 finden Sie in Summe 40 exemplarische Prüfungsfragen, deren Schwierigkeitsgrad und Format der ISO/IEC 27001 Foundation-Prüfung der TÜV Süd Akademie entsprechen, aber ein auch von anderen Anbietern häufig verwendetes Prüfungsschema darstellen. In Anhang C sind 40 weitere Prüfungsfragen am Stück abgedruckt; dies entspricht dem Umfang der „richtigen“ Prüfung, sodass Sie ein Gespür für die 60 Minuten Prüfungszeit entwickeln können. Die begründeten Musterlösungen zu allen 80 Prüfungsfragen finden Sie dort ebenfalls.

Wir wünschen Ihnen viel Erfolg bei der Zertifizierung und der praktischen Anwendung!

München, im Juli 2024 *Die Autoren*

Aufgrund der besseren Lesbarkeit haben wir auf eine gendergerechte Sprache verzichtet. Selbstverständlich sprechen wir aber alle Personen jeglichen Geschlechts gleichermaßen an.

Verweise auf *Kapitel* beziehen sich ohne weitere Angabe immer auf dieses Buch. Verweise auf *Abschnitte* beziehen sich immer auf den entsprechenden Standard.

1 Einführung und Basiswissen

Kaum eine Woche vergeht mehr ohne Berichte über gravierende IT-Sicherheitsvorfälle bei bekannten Unternehmen oder Behörden in der Fach- oder Tagespresse und dringend zu installierende Updates für Betriebssysteme und Standardsoftware. Die Digitalisierung vieler Abläufe und Vernetzung nahezu aller Systeme bis hin zum Wasserkocher im Smart Home bietet viele Vorzüge, aber auch deutlich in Erscheinung tretende Risiken. Lange Zeit fand das Thema Informationssicherheit nur wenig Beachtung sowohl in der Öffentlichkeit als auch in den oberen Leitungsebenen von Organisationen. Inzwischen hat sich die Hoffnung auf eine Selbstregulierung des Markts allerdings zerschlagen – das Pendel nicht nur im deutschsprachigen und europäischen Raum schlägt um in Richtung strikter gesetzlicher und branchenspezifischer Vorgaben, wiederum mit ihren Vor- und Nachteilen.

Die Plage Ransomware als nur eines von vielen Beispielen veranschaulicht sowohl die Entwicklung als auch die Breite der Problematik recht eingängig: Auf der einen Seite war Schadsoftware, die PCs kompromittiert, Dateien verschlüsselt und nur gegen Lösegeldzahlung wieder zugänglich macht, zunächst ein Massenphänomen, das insbesondere Privatpersonen betroffen hat. Erst in den letzten rund zehn Jahren haben sich die Kriminellen zu Ransomware-Gangs organisiert, professionalisiert und sich auf die Monetarisierung über mehr oder weniger zahlungskräftige Organisationen als Opfer spezialisiert. Auf der anderen Seite laufen Ransomware-Vorfälle nicht ausschließlich technisch ab, auch der „Faktor Mensch“ spielt eine Schlüsselrolle: Häufig dienen Phishing-E-Mails oder Links auf mit Schadsoftware verseuchte Inhalte über Social-Media-Plattformen als Einfallstor für die Angreifer.

Insbesondere in Zeiten des anhaltenden Fachkräftemangels im IT-Sektor ist deshalb eklatant, dass sich Organisationen systematisch um Informationssicherheit kümmern müssen. Vorfälle bedeuten oftmals nicht nur schlechte Presse, sondern können durch längere Ausfälle oder ausgespähte Betriebsgeheimnisse sogar existenzbedrohend sein. Die „Aufräumarbeiten“ nach einem typischen Ransomware-Vorfall beschäftigen das IT-Personal oft monatelang und lähmen dadurch die Weiterentwicklung der Organisation nachhaltig. Neben den rein technischen Aspekten sind häufig auch personenbezogene Daten involviert, sodass mit einem IT-Sicherheitsvorfall oft auch ein Datenschutzvorfall einhergeht, der die Reputation und das Vertrauen von Beschäftigten, Kunden und Partnern beschädigt.

Die Gesetzgebung hat darauf zwischenzeitlich reagiert. Bereits 2015 wurde in Deutschland die erste Fassung des IT-Sicherheitsgesetzes eingeführt und 2021 überarbeitet. Damit einher gingen Verordnungen zur Festlegung sogenannter Kritischer Infrastrukturen (KRI-

TIS), für die höhere rechtliche Anforderungen in Bezug auf die IT-Sicherheit erlassen wurden. KRITIS-Betreiber wurden verpflichtet, angemessene technische und organisatorische Maßnahmen für die IT-Sicherheit umzusetzen und dabei den Stand der Technik einzuhalten. Auch die vielfältigen regulatorischen Bemühungen der Europäischen Union, von der Datenschutz-Grundverordnung (DSGVO) über die NIS-2-Richtlinie und den Cyber Resilience Act bis hin zur Richtlinie für Critical Entities Resilience (CER), drehen sich im Kern darum, dass Organisationen ihren Umgang mit – also das Management von – Informationssicherheit professionalisieren und auf ein angemessenes Niveau heben.

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 Standards maßgeblich. Das zentrale und wichtigste Dokument der Reihe ist dabei DIN EN ISO/IEC 27001.

1.1 Worum geht es in ISO/IEC 27000 und ISO/IEC 27001?

ISO/IEC 27000 ist eine Standardfamilie, also eine ganze Reihe von zusammenhängenden Standards, die sich insgesamt hauptsächlich mit drei Kernbereichen befasst:

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

DIN EN ISO/IEC 27001 ist zwar „nur“ eines der Dokumente in der Standardfamilie, ihm kommt aber eine ganz besondere Bedeutung zu: Es gibt die (Mindest-)Anforderungen an organisatorische Prozesse und umzusetzende Maßnahmen verbindlich vor und bildet somit die Grundlage für die Zertifizierung sowohl der Informationssicherheitsmanagementsysteme (ISMS) von Organisationen als auch von Einzelpersonen.

Dieses Buch behandelt ebenfalls alle drei Kernbereiche. Während die beiden letzteren in späteren Kapiteln vertieft behandelt werden, beschäftigt sich dieses Kapitel zunächst mit der grundlegenden Begriffsbildung.

1.2 Begriffsbildung

Die Standardfamilie ISO/IEC 27000 dient ganz wesentlich 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 eingeführt, die zum Verständnis von DIN EN ISO/IEC 27001 erforderlich sind. Ergänzend finden Sie alle offiziellen, kompakten Begriffsdefinitionen aus der ISO/IEC 27000 im Wortlaut in Anhang A dieses Buchs.

1.2.1 Informationen

In unserer längst hochgradig digital vernetzten Welt stellen Informationen Werte dar, die von entscheidender Wichtigkeit für den Betrieb einer Organisation sind. Dabei sind diese Informationen allerdings einer größeren Zahl von Bedrohungen ausgesetzt, die sich ihrerseits teilweise weiterentwickeln. Informationssysteme, Netze und Organisationen sind beispielsweise durch Cyber-Angriffe (Ransomware, Denial-of-Service-Angriffe, Hacking, Spam etc.), Sabotage, Spionage und Vandalismus, aber auch Elementarschäden durch Wasser, Feuer sowie Katastrophen gefährdet. Gesetzliche Regelungen (wie z. B. das IT-Sicherheitsgesetz oder die Datenschutz-Grundverordnung) fordern entsprechend Schutzmaßnahmen für sensible Informationen.

Der Begriff „Informationen“ wird hierbei sehr weit gefasst. Sie können in Form verschiedener Medien vorliegen, also geschrieben, gedruckt, elektronisch, als Film etc., und auf unterschiedlichen Wegen übermittelt werden, z. B. per Post, per Funk/WLAN, über das Internet usw. Unabhängig vom Medium und vom Übertragungsweg ist die Aufgabe der Informationssicherheit, diese Informationen angemessen vor 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

Für die Informationssicherheit existiert, anders als beispielsweise für Gewichte, Längen oder Temperaturen, keine physikalische Maßeinheit, um sie einfach in Zahlen – also *quantitativ* – auszudrücken. Deshalb wählen die Standards der Reihe ISO/IEC 27000 – und damit auch das Hauptdokument DIN EN ISO/IEC 27001 – einen seit Langem praxisbewährten *qualitativen* Ansatz über sogenannte Schutzziele. Diese 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 beschreiben. In der ISO/IEC 27000 und im Security Engineering werden deshalb abstrakte Schutzziele bzw. Sicherheitsanforderungen für Informati-

onswerte (zum Begriff der „(Informations-)Werte“ vgl. Kapitel 3.1.1) definiert. Die zentralen Schutzziele sind die 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 kann, sind Authentizität, Zurechenbarkeit, Nichtabstreitbarkeit und Verlässlichkeit (engl. *Authenticity, Accountability, Non-repudiation and Reliability*). Diese Schutzziele werden im Folgenden erläutert.

Zur Beschreibung von Angriffsszenarien und Sicherheitsmaßnahmen werden 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 bzw. gegenseitig Nachrichten auszutauschen. Der „Böse” (engl. *malicious*) heißt Mallet; er versucht, Alice, Bob oder deren Interaktionen bzw. Kommunikation anzugreifen, also z. B. abzuhören oder zu stören bzw. zu verfälschen. Im Folgenden werden Alice, Bob und Mallet in diesem Sinn verwendet, um die Verletzung von Schutzzielen zu verdeutlichen.

1.2.3.1 Vertraulichkeit (Confidentiality)

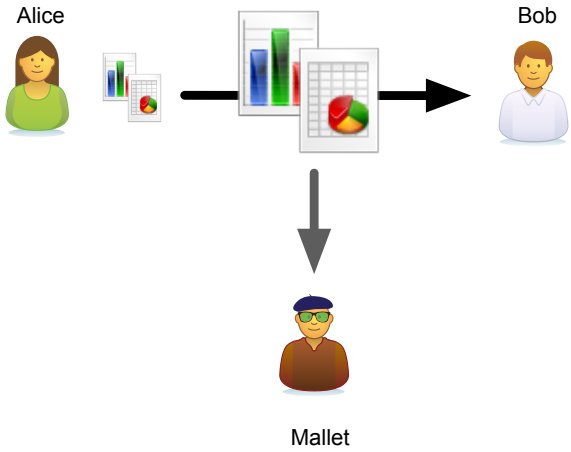

Abbildung 1.1 Verletzung der Vertraulichkeit durch Abhören

Die Vertraulichkeit bezeichnet die Eigenschaft, dass eine Information für dazu nicht berechtigte Personen, Entitäten oder Prozesse nicht zugänglich ist und von diesen auch nicht offengelegt werden kann. Die Vertraulichkeit ist beispielsweise verletzt, wenn ein Angreifer eine Kommunikation abhören kann (vgl. Abbildung 1.1). In der Praxis werden Informationen beispielsweise auf dem Übertragungsweg über das Internet häufig verschlüsselt, um die Vertraulichkeit zu gewährleisten.

1.2.3.2 Integrität (Integrity)

Mit Integrität wird die Eigenschaft bezeichnet, dass Werte im Hinblick auf ihre Richtigkeit und Vollständigkeit geschützt werden. Eine Integritätsprüfung einer digitalen Information oder Nachricht erkennt jede unautorisierte Veränderung. Hierunter fallen alle denkbaren Manipulationen wie das Einfügen oder Löschen von Zeichen, das Wiedereinspielen einer alten Nachricht, das Umordnen aufeinanderfolgender Nachrichtenteile sowie Duplikate.

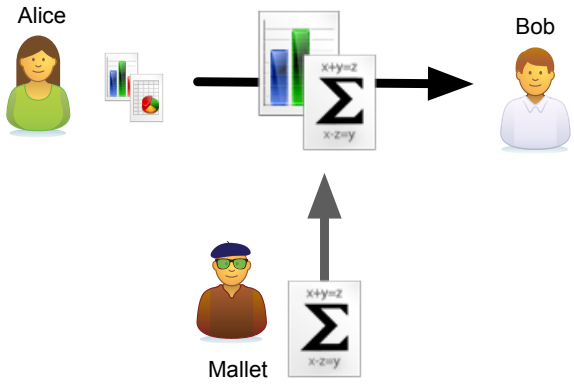

Abbildung 1.2 Verletzung der Integrität

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. In der Praxis werden zur Sicherstellung der Integrität häufig kryptographische Prüfsummen und digitale Signaturen eingesetzt.

1.2.3.3 Verfügbarkeit (Availability)

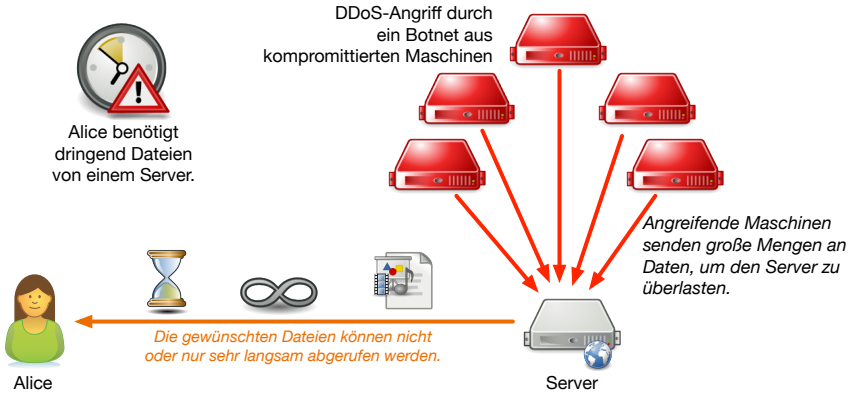

Abbildung 1.3 Verletzung der Verfügbarkeit durch DDoS-Angriff

Die Verfügbarkeit bezeichnet die Eigenschaft einer Information oder eines Wertes, für einen berechtigten Nutzer verfügbar und nutzbar zu sein, sobald der Nutzer dies verlangt. 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, bei denen beispielsweise Webserver mit Datenmüll überflutet werden, wodurch sie für legitime Nutzer nicht mehr verfügbar sind.

Anders als zur Vertraulichkeit und Integrität kann Kryptographie nur begrenzt zur Verfügbarkeit beitragen. Praktisch wird verstärkt auf Redundanz gesetzt: Beispielweise können Backups, also Kopien von Daten, verwendet werden, um auf einem System z. B. durch ein

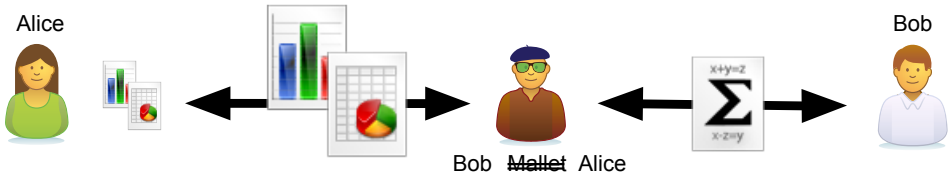

Abbildung 1.4 Verletzung der Authentizität durch einen Man-in-the-Middle-Angriff

defektes Speichermedium oder Ransomware nicht mehr verfügbare Daten wiederherstellen zu können.

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 Identität (z. B. einer eindeutigen Benutzerkennung oder Kontonummer) verbunden. Bei der Authentisierung wird diese Verbindung zwischen digitaler Identität und Nutzer geprüft (z. B. durch Eingabe eines Passworts, das nur der Nutzer kennt, oder durch ein biometrisches Merkmal, z. B. einen Fingerabdruck). Nach dieser Prüfung kann man davon ausgehen, dass die digitale Identität authentisch ist.

In Abbildung 1.4 ist ein sogenannter Man-in-the-Middle-Angriff dargestellt. Mallet unterbricht dabei die Kommunikationsverbindung zwischen Alice und Bob und gibt sich einerseits gegenüber Bob als Alice und andererseits gegenüber Alice als Bob aus. Er fälscht also gewissermaßen seine Identität. Damit ist die Authentizität nicht mehr gewährleistet. Steht Alice und Bob nur dieser verwendete Kommunikationskanal zur Verfügung, so ist der Angriff nur sehr schwer zu erkennen. In der Praxis werden z. B. X.509v3-Zertifikate in Kombination mit verschlüsselten Verbindungen eingesetzt, damit ein Client überprüfen kann, ob er mit dem richtigen Server kommuniziert. Diese Zertifikate werden von einer Certificate Authority (CA) ausgestellt, der die Clients dahingehend vertrauen müssen, dass die Identität des Zertifikatsinhabers zuverlässig überprüft worden ist.

1.2.3.5 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.

1.2.3.6 Nichtabstreitbarkeit/Verbindlichkeit (Non-Repudiation)

Unter Verbindlichkeit bzw. Nichtabstreitbarkeit versteht man, dass der Eintritt eines Ereignisses oder einer Aktion sowie die verursachende Entität zweifelsfrei belegt werden können. Beispielsweise kann ein Nutzer das Auslösen einer Aktion, z. B. eine kostenpflichtige Bestellung, bei gegebener Nichtabstreitbarkeit später nicht erfolgreich leugnen. In der Praxis wird zur Gewährleistung der Nichtabstreitbarkeit häufig darauf zurückgegriffen, gegebenenfalls kritische Aktionen authentisierter Benutzer zu protokollieren und diese Auf-

zeichnungen angemessen lange aufzubewahren. Bei Dokumenten kommen auch Unterschriften bzw. digitale Signaturen zum Einsatz.

1.2.3.7 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 Werte und Daten, sogenannte 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.

Zurechenbarkeit und Nichtabstreitbarkeit hängen somit oftmals eng zusammen. Die Abgrenzung beider Begriffe kann man sich mit einem Beispiel veranschaulichen: Fallen in einem Mobilfunktarif zusätzliche Kosten für Telefonate ins Ausland an, so fällt es in den Bereich der Zurechenbarkeit, dass einzelne Auslandstelefonate genau einem Mobilfunkvertrag zugeordnet werden können. Erst wenn der Vertragsinhaber behauptet, hohe Kosten durch Auslandstelefonate nicht selbst verursacht zu haben, kommt die Nichtabstreitbarkeit ins Spiel.

1.2.3.8 Zugangs- und Zugriffssteuerung (Access Control)

Als letzten Begriff betrachten wir noch die Zugriffssteuerung. Dabei handelt es sich zwar nicht um ein Schutzziel, aber um einen sehr grundlegenden Sicherheitsmechanismus, der in verschiedensten Maßnahmen der DIN EN ISO/IEC 27001 zum Einsatz kommt. Die Zugriffssteuerung stellt sicher, dass der Zugang zu Assets nur autorisiert erfolgen kann und Einschränkungen auf Basis von Geschäfts- oder Sicherheitsanforderungen möglich sind. Die Zugriffssteuerung setzt also ein Berechtigungskonzept technisch um; nur autorisierte Personen dürfen auf IT-Systeme und Informationen zugreifen. Bei physischem Zugang, z. B. dem Betreten gesicherter Gebäudebereiche, wird der Begriff Zutritt bzw. Zutrittskontrolle verwendet.

1.3 IT-Sicherheitsgesetz & KRITIS

2015 hatte der Deutsche Bundestag das IT-Sicherheitsgesetz (IT-SiG) beschlossen, das in erster Linie Änderungen an bestehenden Gesetzen, darunter dem BSI-Gesetz (BSIG), umfasste. 2021 ist eine überarbeitete Fassung (IT-SiG 2.0) in Kraft getreten. 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 können.

KRITIS-Betreiber (Betreiber kritischer Infrastrukturen) werden nach dem Gesetz verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informati-

onstechnischen Systeme, Komponenten und 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 KRITIS-Betreiber aus.

1.3.1 Was ist „KRITIS“?

Unter dem Schlagwort KRITIS (Kritische Infrastrukturen) versteht man übergreifend die Anforderungen, die sich aus dem IT-Sicherheitsgesetz und der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung, kurz BSI-KritisV) für KRITIS-Betreiber ergeben. Dabei beschränkt sich die BSI-Kritisverordnung in ihrer letzten Änderung vom November 2023 auf die folgenden Sektoren bzw. Branchen:

- Energie
- Wasser
- Ernährung
- Informationstechnik und Telekommunikation
- Gesundheit
- Finanz- und Versicherungswesen
- Transport und Verkehr
- Siedlungsabfallentsorgung

Darüber hinaus stellen auch einerseits Medien und Kultur und andererseits Staat und Verwaltung weitere Sektoren kritischer Infrastrukturen dar, die derzeit jedoch nicht der Regulierung durch das BSI-Gesetz unterliegen.

1.3.2 Wer ist in Deutschland von KRITIS betroffen?

Während die eigentlichen Gesetzestexte offenlassen, welche Organisationen oder Unternehmen tatsächlich 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 genannten Branchen ableiten kann, ob sie als Betreiber einer Kritischen Infrastruktur gilt oder nicht.

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

- § 1 enthält die für diese Verordnung relevanten Begriffsbestimmungen.
- In § 2 bis § 9 findet man zu jedem der betroffenen Sektoren eine genauere Beschreibung der relevanten kritischen Dienstleistungen.
- In § 10 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, die wiederum zu jedem der betroffenen 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 2 sind relevante Anlagenkategorien unter anderem Gewinnungsanlagen, Aufbereitungsanlagen, Leitzentralen 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, den 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. In Deutschland waren das im Jahr 2023 Frankfurt, München und Berlin Brandenburg.

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 KRITIS-Betreiber tun, und worüber müssen sie Nachweise erbringen?

Die wesentliche Anforderung besteht darin, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität durch angemessene organisatorische und technische Vorkehrungen nach dem „Stand der Technik“ aufrechterhalten werden müssen. Hierzu gehört seit dem 1. Mai 2023 auch die Verpflichtung zum Betrieb eines sogenannten Systems zur Angriffserkennung (SzA).

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 DIN EN 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 DIN EN 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 KRITIS-Betreiber 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. So wurde beispielsweise von der Deutschen Krankenhausgesellschaft (DKG e. V.) im Jahr 2022 die Version 1.2 des branchenspezifischen Sicherheitsstandards für die Gesundheitsversorgung im Krankenhaus herausgegeben[Deu22]; auch dieser orientiert sich in seinen empfohlenen Umsetzungsschritten eng an DIN EN ISO/IEC 27001.

1.4 Datenschutz-Grundverordnung

Die Europäische Union hat mit der Datenschutz-Grundverordnung (DSGVO) [DSG16] im Jahr 2018 das Datenschutzrecht EU-weit und für den Europäischen Wirtschaftsraum vereinheitlicht. Nationale und föderale Gesetze, wie z. B. das Bundesdatenschutzgesetz oder die Landesdatenschutzgesetze, sind weiterhin möglich, müssen aber mit der DSGVO vereinbar sein.

Die DSGVO übernimmt viele Prinzipien aus der Vorgängerrichtlinie (95/46) und dem ehemaligen deutschen 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*“)

Art. 32 der DSGVO fordert explizit die Berücksichtigung des Stands der Technik. Technische und organisatorische Maßnahmen zum Schutz von Daten sind ein Hauptaspekt der DIN EN ISO/IEC 27001. Ein Nachweis des Stands der Technik kann z. B. durch eine Organisationszertifizierung nach DIN EN 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 Kapitel 4.6.1 erläutert wird.

Die Grundlagen, Prinzipien und Prozesse der DIN EN ISO/IEC 27001 lassen sich somit gewinnbringend auch bei der Umsetzung der Datenschutz-Grundverordnung nutzen.

1.5 Weitere Richtlinien und Verordnungen der Europäischen Union

Neben der jeweiligen nationalen Gesetzgebung muss auch eine zunehmende Anzahl an Gesetzesvorhaben der EU berücksichtigt werden. Während EU-Richtlinien mit einer gewissen Frist nach Inkrafttreten in nationales Recht der Mitgliedsstaaten umgesetzt werden müssen, finden Verordnungen direkte Anwendung. Grundsätzlich zeichnet sich dabei einerseits ab, dass die Rechtsakte der EU zusätzliche Sektoren und insgesamt deutlich mehr Organisationen betreffen als die bisherigen deutschen Regelungen. Andererseits sind beispielsweise die relevanten KRITIS-Sektoren bislang nicht einheitlich bzw. konsistent definiert, sodass die Analyse der und die Entscheidung über die Relevanz der einzelnen Regulierungen mit einem erheblichen Aufwand für die potenziell betroffenen Unternehmen verbunden ist.

1.5.1 NIS-2-Richtlinie

Anfang 2023 ist die NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) [NIS22a] in Nachfolge der Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) aus dem Jahr 2016 in Kraft

getreten. Sie stellt einerseits sicher, dass die EU-Mitgliedsstaaten jeweils nationale Cybersicherheitsstrategien haben, definiert andererseits aber auch Aufgaben für Unternehmen. Zu den Kernthemen gehören beispielsweise Risikomanagement, Asset Management, die Meldung von IT-Sicherheitsvorfällen, die Betrachtung der Lieferkettensicherheit und die Umsetzung des Stands der Technik in der IT-Sicherheit. Der Schwerpunkt liegt also auf IT- und Informationssicherheit.

Die NIS-2-Richtlinie betrachtet insgesamt 18 Sektoren, von denen elf als wesentliche Sektoren mit hoher Kritikalität (engl. *essential*) und die anderen sieben als weitere wichtige kritische Sektoren (engl. *important*) bezeichnet werden. In die erste Kategorie fallen beispielsweise der Sektor digitale Infrastruktur einschließlich Anbietern von Rechenzentrumsdiensten und der Sektor Weltraum, wohingegen die zweite Kategorie unter anderem Post- und Kurierdienste, Forschungseinrichtungen sowie digitale Anbieter wie Online-Marktplätze umfasst.

Die Umsetzung in deutsches Recht erfolgt über das *NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz* (NIS2UmsuCG), das als Änderungsgesetz vor allem die KRITIS-Teile des BSI-Gesetzes betrifft.

1.5.2 Richtlinie über die Resilienz kritischer Einrichtungen (EU RCE Directive/CER-Richtlinie)

Die *Directive on the Resilience of Critical Entities* (EU RCE bzw. (EU) 2022/2557) [EU-22b] aus dem Jahr 2022, auch als CER-Richtlinie (*Critical Entities Resilience Directive*) bezeichnet, fokussiert die physische Resilienz von kritischen Infrastrukturen und hat die *European Critical Infrastructures Directive* aus dem Jahr 2008 abgelöst. Die umzusetzenden Maßnahmen betreffen neben der physischen Sicherheit beispielsweise Krisenmanagement und Wiederanlaufpläne in elf regulierten Sektoren. Zu diesen elf Sektoren gehört beispielsweise auch der Sektor Ernährung, der in der NIS-2-Richtlinie als *important*, aber nicht *essential* gilt. Hingegen betrachtet die CER-Richtlinie beispielsweise im Sektor Transport auch explizit den öffentlichen Personennahverkehr (ÖPNV), der in der NIS-2-Richtlinie fehlt.

Die EU RCE wird über das KRITIS-Dachgesetz (KRITIS-DachG) national umgesetzt. Dabei fließen z. B. von den Aufsichtsbehörden gemeldete Sicherheitsvorfälle beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) zusammen.

1.5.3 Cyber Resilience Act (CRA)

Bereits 2019 ist der Rechtsakt zur Cybersicherheit (*Cybersecurity Act*, Verordnung (EU) 2019/881) [EU-19] in Kraft getreten, der einen einheitlichen Rahmen für die IT-Sicherheitszertifizierung von Produkten, Dienstleistungen und Prozessen geschaffen hat.

Mit dem initial 2022 vorgeschlagenen Cyber Resilience Act (CRA) sollen sowohl Verbraucher als auch Unternehmenskunden, die Software oder Produkte mit digitalen Komponenten kaufen, besser vor IT-Sicherheitslücken geschützt werden. Für Hersteller und Händler sowie deren Zulieferketten ergeben sich dadurch neue Pflichten, die IT-Sicherheit ihrer Produkte über deren gesamten Lebenszyklus abzusichern und beispielsweise kostenlose Security-Updates bereitzustellen. Neben Meldepflichten für bekannt werdende Schwach-

stellen werden Hersteller auch zu regelmäßigen Tests auf Schwachstellen verpflichtet. Der CRA legt unter anderem eine Reihe von *kritischen* Produkten wie Passwortmanager und Antivirenprogramme in zwei Klassen fest, für die eine Vertrauenswürdigkeitsprüfung notwendig ist.

1.5.4 DORA-Verordnung

Der *Digital Operational Resilience Act*, Verordnung (EU) 2022/2554 (DORA, zu Deutsch *Verordnung über die digitale operationale Resilienz im Finanzsektor*) [EU-22a] gilt als Verordnung ohne weitere Gesetzgebung unmittelbar in den EU-Mitgliedsstaaten. DORA zielt auf die Resilienz der Finanz- und Versicherungsbranche sowie deren IT- und Telekommunikationsdienstleister (IKT) ab, wobei es Ausnahmen für kleinere Unternehmen gibt.

In seinen neun Kapiteln behandelt DORA unter anderem das Risikomanagement, die Behandlung und Meldung von Sicherheitsvorfällen und das Testen der digitalen operationalen Resilienz. Ein zertifizierungsfähiges Informationssicherheitsmanagementsystem stellt damit eine postulierte Grundlage dar. Durch die recht breite Definition von IKT-Drittdienstleistern gilt die DORA-Verordnung zudem für Betreiber von Cloud-Diensten, Rechenzentren und Datenanalysen, soweit diese von den Finanzunternehmen genutzt werden.

1.6 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 DIN EN 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. Der Anhang A von DIN EN ISO/IEC 27001, der umzusetzende Maßnahmen auflistet, wird in Kapitel 5 ausführlich erklärt. Die danach folgenden Kapitel erläutern verwandte Standards und Rahmenwerke sowie die verschiedenen Zertifizierungsmöglichkeiten nach DIN EN ISO/IEC 27001. Im Anhang des Buches finden Sie 40 Prüfungsfragen mit entsprechenden Musterlösungen, die vom Schwierigkeitsgrad her der DIN EN ISO/IEC 27001 Foundation-Prüfung entsprechen.

1.7 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 235.