HANSER

Leseprobe

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

ISBN (Buch): 978-3-446-45139-1

ISBN (E-Book): 978-3-446-45260-2

Weitere Informationen oder Bestellungen unter

http://www.hanser-fachbuch.de/978-3-446-45139-1

sowie im Buchhandel.

Inhaltsverzeichnis

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 2015 als DIN ISO/IEC 27001:2015 erschien und die deutsche Version der englischsprachigen ISO/IEC 27001:2013 aus dem Jahr 2013 darstellt. Die DIN ISO/IEC 27001:2015 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 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 Mindestanforderungen 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 Prüfung zum *Foundation Certificate in ISMS according to ISO/IEC 27001* nach dem Lehrgangskonzept der 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 wiederum dem der ISO/IEC 27001 Foundation-Prüfung der TÜV Süd Akademie. 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 genau 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 Februar 2017 *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 Standard-Reihe 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) 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 (bösartiger 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, abzuhören oder zu stören. Im Folgenden werden Alice, Bob und Mallet in diesem Sinn verwendet, um die Verletzung von Schutzzielen zu verdeutlichen.

1.2.3.1 Vertraulichkeit (Confidentiality)

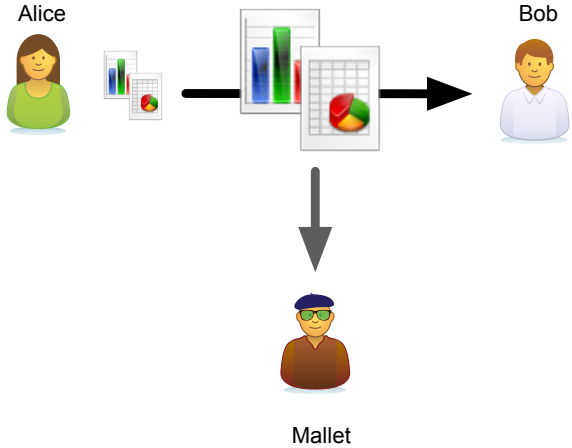

Abbildung 1.1 Verletzung der Vertraulichkeit durch Abhören

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

gelegt werden kann. Die Vertraulichkeit ist beispielsweise verletzt, wenn ein Angreifer eine Kommunikation abhören kann (vgl. Abbildung 1.1).

1.2.3.2 Integrität (Integrity)

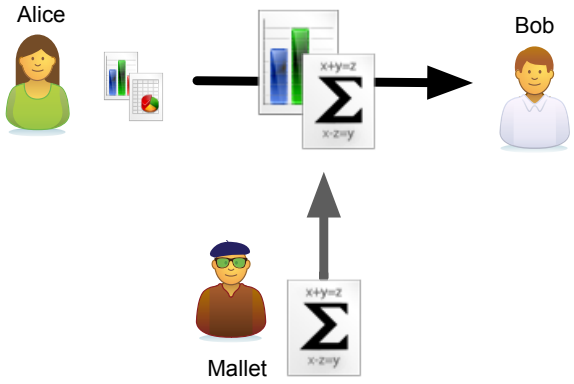

Abbildung 1.2 Verletzung der Integrität

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)

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 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 1.3 wird ein Man-in-the-Middle-Angriff dargestellt. Mallet unterbricht die Kommunikationsbeziehung zwischen Alice und Bob und gibt sich gegenüber Bob als Alice

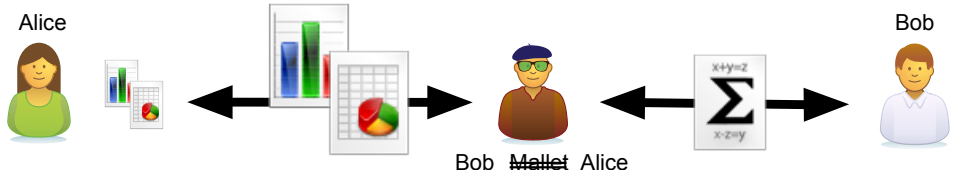

Abbildung 1.3 Verletzung der Authentizität durch einen Man-in-the-Middle-Angriff

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 Sicherheitsanforderungen 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 & Co.

Am 12. Juni 2015 wurde durch den Deutschen Bundestag das IT-Sicherheitsgesetz (IT-SiG) [Bun15] beschlossen, das in erster Linie Änderungen an bestehenden Gesetzen, darunter das BSI-Gesetz (BSIG), umfasst. Im Kern bedeuten diese Änderungen die Abkehr vom Prinzip der Freiwilligkeit für den Bereich sogenannter kritischer Infrastrukturen. Deren Betreiber 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 aus den Bereichen Energie, Informationstechnik, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen erhebliche IT-Sicherheitsvorfälle melden. Das BSI wird zur Zentralstelle für IT-Sicherheit und wertet Meldungen der Betreiber kritischer Infrastrukturen aus.

1.4 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.

1.5 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 210.

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 berechtigte 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