Einleitung

Informationssicherheit stellt eine der elementaren Grundlagen für eine gesetzeskonforme und verlässliche Nutzung von Informationstechnologien und der digitalen Transformation dar.

Wer sich heute für Informationssicherheit interessiert, muss sich sowohl mit den organisatorischen als auch mit den technischen Grundlagen der Informationssicherheit befassen. Moderne Vorlesungen zur Informationssicherheit decken nicht nur den technischen Teil ab, sondern widmen sich genauso umfangreich den organisatorischen Strukturen. Leider fehlt es in der Informatikerausbildung aber häufig noch an der fachbereichsübergreifenden Darstellung und die IT-Sicherheit wird rein technisch gelehrt.

Das ist sicherlich mit ein Grund dafür, dass die Informationssicherheit noch lange nicht flächendeckend auf dem Niveau ist, auf dem sie sein sollte. Auch die regulatorischen Vorgaben durch den Gesetzgeber werden mehr. Die DS-GVO und die IT-Sicherheitsgesetzgebung fordern heute deutlich mehr IT-Sicherheit und technisch-organisatorische Maßnahmen als noch vor ein paar Jahren. Auch der IT-Planungsrat kümmert sich um einheitliche Informationssicherheitsvorgaben für Behörden. Tangiert wird das außerdem auch von den Rechnungshöfen des Bundes und der Länder, die im Rahmen ihrer Wirtschaftlichkeitsprüfungen auch die Informationssicherheit prüfen.

Das weltumspannende Internet sollten wir sicher nutzen können, deshalb benötigen wir eine einheitliche Regulierung der Informationssicherheit. Die Gültigkeit nationalen Rechts endet an der Landesgrenze. Internationale Regelungen, wie sie die EU schafft, vereinheitlichen die Vorgaben. Hier bedarf es noch weiterer internationaler Anstrengungen.

Über dieses Buch

Wir stellen im Buch die organisatorischen und die technischen Grundlagen der Informationssicherheit gemeinsam dar. Das Buch gibt eine umfassende Orientierung zur Einordnung der Informationssicherheit in das regulatorische Umfeld (Deutschland, EU), die erforderlichen organisatorischen Strukturen im Unternehmen beziehungsweise in der Behörde und die technischen Grundlagen der Informationssicherheit.

Törichte Annahmen über den Leser

Sie wollen Informationssicherheit lernen. Das ist gut und Sie sind hier richtig.

Sie haben kein Vorwissen. Kein Problem! Die Inhalte werden so präsentiert, dass sie im Wesentlichen ohne Vorwissen verständlich sind.

Sie studieren Informatik, Mathematik oder Jura. Sie denken darüber nach, eine Berufslaufbahn in der Informationssicherheit einzuschlagen. Dann sollten Sie neben den technischen Grundlagen der Informationssicherheit (eher Informatik-Themen) auch die rechtlichen und organisatorischen Grundlagen (eher juristische, Wirtschafts- und Wirtschaftsinformatik-Themen) beherrschen. Das Buch führt das erforderliche Wissen aus den Schnittstellen zu den relevanten Fachgebieten (Informatik, Rechtswissenschaften, Wirtschaftswissenschaften und Wirtschaftsinformatik) zusammen und stellt es einheitlich dar.

Was Sie nicht lesen müssen

Wenn Sie beginnen, ein Kapitel zu lesen, und Sie den Inhalt schon kennen, überspringen Sie das Kapitel. Bei einem Querschnittthema mit juristischen, technischen und betrieblichen Inhalten ist es unvermeidbar, dass Sie, je nach Ausbildung, in dem einen oder anderen dieser Themen schon Vorkenntnisse haben. Die Juristen unter Ihnen kennen sich mit den Gesetzen aus und die Mathematiker oder Informatiker unter Ihnen wissen vermutlich schon einiges über Verschlüsselung.

Beispiele und Anekdoten können Sie überspringen, wenn Sie den Sachverhalt auch so verstehen oder der Hintergrund für Sie nicht so wichtig ist.

Wie dieses Buch aufgebaut ist

Wie jedes Buch der »... für Dummies«-Reihe ist auch dieses Buch in mehrere große Teile gegliedert. Die Einführung der grundlegenden Begriffe und Anforderungen geschieht in Teil I. In Teil II lernen Sie die rechtlichen und regulatorischen Anforderungen kennen. Die Organisation im Unternehmen ist der Schwerpunkt von Teil III. Teil IV soll Ihnen die technischen Grundlagen und Bausteine vermitteln. Aus den Bausteinen bauen wir dann im Teil V das IT-Sicherheitshaus auf.

Teil I: Informationssicherheit, IT-Sicherheit und Datenschutz

IT-Sicherheit und Informationssicherheit ist das nicht dasselbe? Und was hat Datenschutz damit zu tun? Sie lernen die Definitionen und Unterschiede der Begriffe der Informationssicherheit, nämlich die klassischen Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit kennen. Wenn Sie sich mit der Umsetzung von Informationssicherheit beschäftigen wollen, müssen Sie zuerst lernen, was Informationssicherheit ist.

Erstaunlicherweise finden Sie diese Grundbegriffe nicht nur in Lehrbüchern und Standarddokumenten zur Informationssicherheit, sondern zunehmend auch in Gesetzen. Die immer weiter gehende Digitalisierung führt auch zu vermehrten Anforderungen an die Informationssicherheit. Von der Praxis Ihres Hausarztes bis zur Steuerung der Energieversorgung Ihrer Wohnung: überall werden Computer eingesetzt. Und wenn die Computer gestört sind,

fällt die Dienstleistung oder Versorgungsleistung aus. Im Juli 2021 wurde in Deutschland erstmalig der Cyberkatastrophenfall ausgelöst, und zwar im Landkreis Anhalt-Bitterfeld. Störungen der Informationssicherheit können tatsächlich katastrophale Auswirkungen haben. Deshalb muss Informationssicherheit nicht nur Schutz vor Angriffen, sondern auch Vorsorge vor Katastrophen und Unfällen sein.

Die vier Begriffe Risikomanagement, Meldepflichten, Sicherheitsstandards und Audits ziehen sich wie ein roter Faden durch alle Regelungen zur IT-Sicherheit. Sie werden lernen, was es damit auf sich hat.

Und mit den technisch-organisatorischen Maßnahmen, kurz TOM, kommt dann auch der Datenschutz ins Spiel. Um den technischen Schutz der personenbezogenen Daten zu gewährleisten, sind TOMs erforderlich. Datenschutz braucht unterstützend die IT-Sicherheit, auch wenn die Datenschutzziele nicht allein durch IT-Sicherheitsmaßnahmen erreicht werden können.

Teil II: Rechtliche Anforderungen

Da Computer und Digitalisierung immer weiter in unser Leben vordringen und deshalb die Informationssicherheit immer wichtiger wird, regelt der Gesetzgeber in immer mehr Gesetzen und Verordnungen die Anforderungen an die Informationssicherheit.

Viele Unternehmen müssen sich intensiv um Informationssicherheit kümmern. Dabei spielt es keine Rolle, ob ihnen das wichtig ist oder nicht: Es ist ihnen gesetzlich vorgeschrieben.

Sie erfahren, welche europäischen Vorschriften (Netzwerk- und Informationssicherheits-Richtlinie, Rechtsakt zur Cybersicherheit, Datenschutz-Grundverordnung) und welche deutschen Vorschriften (BSI-Gesetz, Geschäftsgeheimnisgesetz, Telekommunikationsgesetz und etliche andere) den Unternehmen Vorgaben zur IT-Sicherheit machen.

Neben den rechtlichen Vorgaben lernen Sie auch die Standards und Normen zur Informationssicherheit (ISO-Normen, BSI-Grundschutz und andere) kennen. Diese Standards sind wichtig, da sich die rechtlichen Vorgaben teilweise für die Umsetzung auf diese Standards beziehen. Gesetze haben eine deutliche längere Lebensdauer als IT-Systeme. Deshalb ist es für den Gesetzgeber schwer, IT in Gesetzen detailliert zu regeln. Der Bezug auf Standards, die sich schneller aktualisieren lassen, ist der Ausweg aus diesem Dilemma.

Und nochmal Datenschutz: Wie strukturieren Sie im Unternehmen die TOMs? Wir schauen uns gemeinsam an, was bei den TOMs wichtig ist.

Teil III: Organisation der Informationssicherheit

Ein Unternehmen muss seine Prozesse durch interne Vorgaben und Regeln gestalten. Teilweise sind das relativ banale Dinge, wie eine Nutzerordnung oder eine Passwortrichtlinie. Welche Regeln und vor allem welche Inhalte der Regeln wollen Sie als zukünftige Expertin oder zukünftiger Experte für Informationssicherheit Ihrem Unternehmen empfehlen? Sie lernen in diesem Teil, was Sie regeln sollen und wie Sie es regeln sollen.

Wer hat im Unternehmen welche Aufgaben in der Informationssicherheit? Vom Chef über den Informationssicherheitsbeauftragten und den IT-Leiter bis zur Nutzerin, jede und jeder trägt seinen Teil zur Bewältigung der Aufgabe »Informationssicherheit« bei.

Wie machen Sie eine Risikoanalyse? Was sind die Kronjuwelen im Unternehmen? Was dürfen die Nutzerinnen? Wie gehen Sie mit Sicherheitsvorfällen um? Mit all diese Fragen beschäftigen wir uns in diesem dritten Teil.

Eine der wichtigsten organisatorischen Fragen beschäftigt sich mit der alten Frage: »Wie sag ich es meinen Mitarbeitern?« Awareness und Schulung sind wichtige Maßnahmen, die Sie kennenlernen werden.

Teil IV: Bausteine der technischen IT-Sicherheit

Im vierten Teil, zugegeben ein ziemlich anspruchsvoller Abschnitt, spielen die technischen Grundlagen der IT-Sicherheit die Hauptrolle. Einen breiten Raum nehmen die Grundlagen der Verschlüsselung ein. Ganz ohne Mathematik geht es nicht, aber die Anschaulichkeit steht im Vordergrund.

Ein weiteres wichtiges Thema ist die Biometrie. Eine Anmeldung am Smartphone mit Fingerabdruck oder Gesichtserkennung haben Sie bestimmt schon gemacht. Türöffnung im Sicherheitsbereich mit Iris-Scan ist in manchen Rechenzentren Pflicht. Sie lernen die Grundlagen der Biometrie kennen und wir schauen uns auch die damit verbundenen Risiken an.

Außerdem beschäftigen wir uns noch mit Chipkarten und Sicherheitstoken. Vom neuen Personalausweis über die Girocard bis zur SIM-Karte im Smartphone haben Sie sicher schon persönliche Erfahrungen gemacht im Umgang mit den kleinen Geräten. Wir schauen uns an, wie sie funktionieren und was sie können.

Teil V: Lösungen und Umsetzungen

Aufbauend auf den Bausteinen, die Sie im vierten Teil kennengelernt haben, schauen wir uns dann die Lösungen zur IT-Sicherheit an. Backup, Verschlüsselung von Daten auf Datenträgern und bei der Übertragung, Netzwerksicherheit, Firewalls und Zugangssicherung sind Lösungen, die Sie kennenlernen werden.

Wie überwachen und messen Sie die IT-Sicherheit im Unternehmen? Was sind geeignete Metriken, um die Qualität Ihrer IT-Sicherheit zu messen? Was ist ein Patch-Management? Sie wollten sicher immer schon mal wissen, wie eine Blockchain funktioniert und was es mit Künstlicher Intelligenz auf sich hat. Auch das werden Sie in diesem Teil lernen.

Alle diese Lösungen dienen zur technischen Unterstützung der organisatorischen Prozesse im Unternehmen.

Teil VI: Der Top-Ten-Teil

Im Top-Ten-Teil geht es nochmal um die wichtigsten Begriffe und die wichtigsten organisatorischen und technischen Maßnahmen. Quasi das Take-away in aller Kürze.

Symbole, die in diesem Buch verwendet werden

Neben dem Fernglas finden Sie Beispiele, die Ihnen helfen, das Gelernte an einer konkreten Situation besser zu verstehen.

Neben der Lupe finden Sie Definitionen von Begriffen. Häufig stammen diese aus offiziellen Normen, Standards oder Gesetzen.

Wenn Sie erst in das Thema einsteigen und noch nicht so viele Erfahrungen haben, hilft der eine oder andere Tipp.

Bevor Sie einen typischen Fehler machen oder einem gängigen Irrtum unterliegen, lesen Sie die mit diesem Symbol gekennzeichneten Warnungen.

Manchmal erzählen wir Ihnen eine Anekdote. Im Gegensatz zu einem Beispiel ist es nicht das Hauptziel einer Anekdote, Sie beim Verstehen eines Sachverhalts zu unterstützen, sondern sie gibt eine Erklärung zum Hintergrund oder zur Entstehung eines Aspekts oder auch spannende Einblicke in das reale Leben der IT-Sicherheit.

Konventionen in diesem Buch

In diesem Buch verwenden wir aus Gründen der Lesbarkeit für Rollen sowohl die männliche als auch die weibliche Form. Dazu haben wir für alle Rollen jeweils ein Geschlecht definiert und verwenden dies dann durchgehend: der Informationssicherheitsbeauftragte, die Datenschutzbeauftragte, der Angreifer, die Nutzerin. Des Weiteren verwenden wir den Begriff »Unternehmen« und meinen damit jeweils sowohl Organisationen beliebiger Rechtsform wie Unternehmen jeder Art, aber auch Behörden, Universitäten, Forschungseinrichtungen, Vereine und so weiter.

Wir verwenden in diesem Buch die folgenden Begriffe und orientieren uns dabei an den Formulierungen des BSI-Grundschutz-Kompendiums:

- ✔ »MUSS« oder »DARF NUR«: Diese beiden Formulierungen werden verwendet, wenn etwas unbedingt getan werden muss, da es vorgeschrieben ist. In diesem Fall gibt es eine rechtliche Vorschrift (zum Beispiel die DS-GVO oder das BSI-Gesetz), die die Maßnahme verlangt.

- ✔ »DARF NICHT« oder »DARF KEIN«: Diese beiden Formulierungen beschreiben das Gegenteil, dass etwas auf keinen Fall getan werden darf, da es zum Beispiel gesetzlich oder regulatorisch (zum Beispiel im Strafgesetzbuch) untersagt ist.
- ✔ »SOLLTE«: Diese Formulierung besagt, dass es geboten ist, etwas zu tun. Es kann jedoch gute Gründe geben, es trotzdem nicht zu machen. Diese Abweichung muss gut überlegt und nachvollziehbar begründet werden. Außerdem ist die Ausnahme ausführlich zu dokumentieren.
- ✔ »SOLLTE NICHT« oder »SOLLTE KEIN«: Diese Formulierung besagt, dass nicht geboten ist, etwas zu tun. Es kann jedoch gute Gründe geben, es trotzdem zu machen. Diese Abweichung muss gut überlegt und nachvollziehbar begründet werden. Außerdem ist die Ausnahme ausführlich zu dokumentieren.
- ✔ »KANN«: Diese Formulierung besagt, dass etwas getan werden kann oder auch nicht. Weder für die eine noch die andere Option ist eine explizite Begründung erforderlich.

Wie es weitergeht

Wir hoffen, Sie sind jetzt richtig neugierig geworden und fangen gleich an zu lesen!

Wenn Sie Informationssicherheit dauerhaft betreiben wollen, dann dürfen Sie nach dem Durcharbeiten dieses Buches nicht aufhören. Die technischen Herausforderungen ändern sich ständig. Ständig werden neue Angriffstechniken bekannt, auf die reagiert werden muss. Die Regularien ändern sich und erfordern eine Anpassung der Organisation im Unternehmen. Standards und Normen werden an die sich weiter entwickelnde Technik angepasst. Es gibt kaum ein anderes Gebiet, wo es so wichtig ist, immer am Ball zu bleiben und sich ständig weiterzubilden.

Wer sich mit Informationssicherheit beschäftigt, muss sich auf die ständigen Änderungen einlassen. »Das haben wir schon immer so gemacht!« ist ein Argument, das Sie vergessen müssen. Aber Informationssicherheit macht auch Spaß: Es ist spannend, an vorderster Front dabei zu sein und die Entwicklung im Unternehmen mitzugestalten.

Die Sorge, dass das Thema in ein paar Jahren vom Tisch ist, müssen Sie nicht haben. Informationssicherheit ist eines der großen Themen unserer Zeit, das immer wichtiger wird. Damit wird Ihnen nie langweilig!

Dieses Buch berücksichtigt bei Darstellungen der Rechtslage in Deutschland und in der Europäischen Union den Stand der Gesetzgebung bis Herbst 2021. Gesetze (wie zum Beispiel TKG, TTDSG), die bis Mitte 2021 beschlossen wurden, aber erst am 1. Dezember 2021 in Kraft getreten sind, sind in der Fassung vom 1. Dezember 2021 berücksichtigt.

Aktualisierte Links, weitere Informationen und Errata finden Sie auf der Website `https://www.it-sfd.de`.