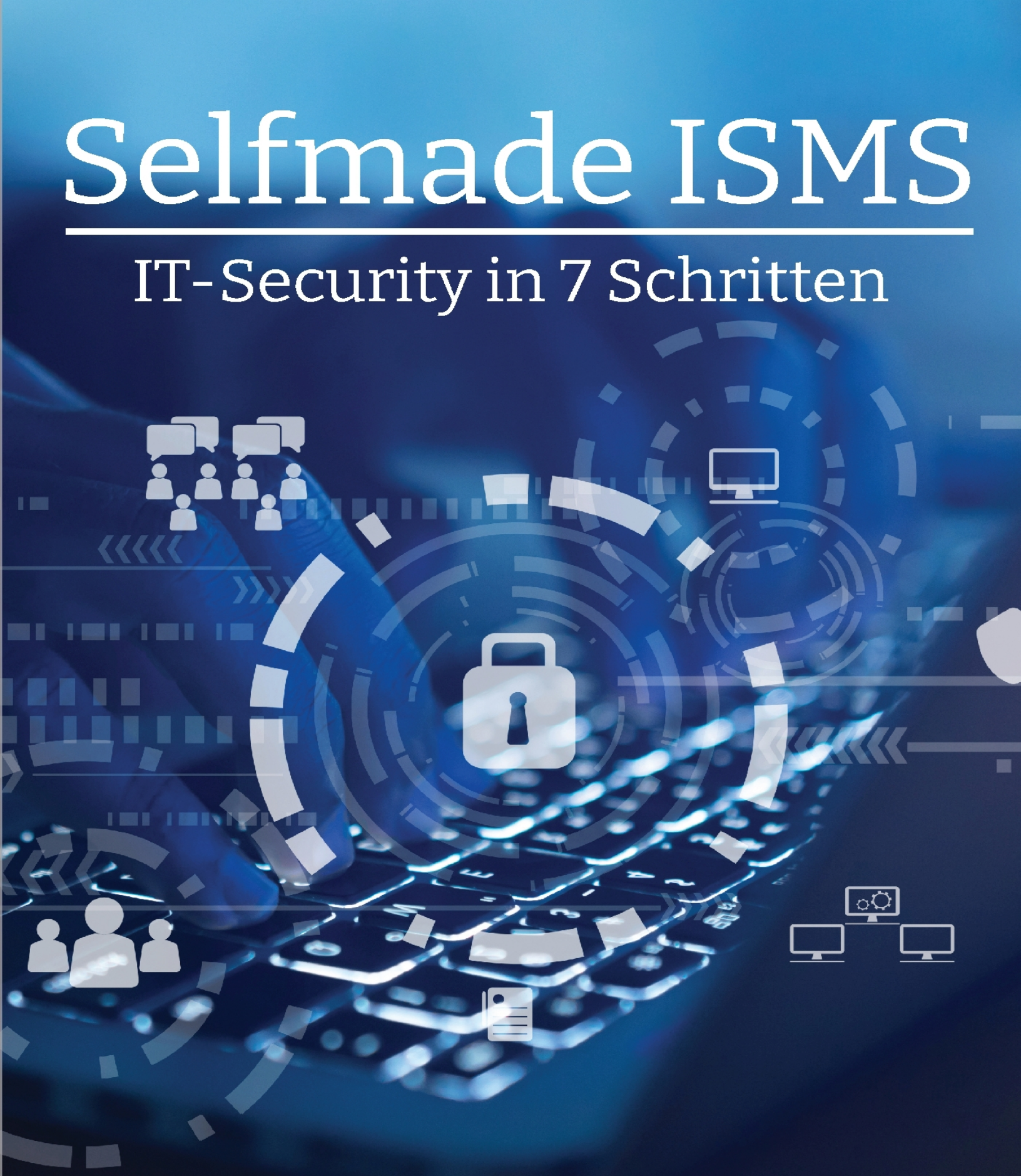
Selfmade ISMS

IT-Security in 7 Schritten



Marcel Schmidt,

Jennifer Gabriel

von

Marcel Schmidt

und

Jennifer Gabriel

1. Auflage

Umschlaggestaltung, Illustration: Adobe Stock, chinnarach

Lektorat, Korrektorat: Elisabeth Wilhelm

ISBN Softcover: 978-3-347-58651-2

ISBN E-Book: 978-3-347-58655-0

Druck und Distribution im Auftrag des Autors:

tredition GmbH, Halenreie 40-44, 22359 Hamburg, Germany

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.

Die Autoren

Marcel Schmidt

Als Marcel 2001 mit der Server- und Netzwerkadministration in die IT-Branche gestartet ist, hat er zunächst eine Ausbildung zum Fachinformatiker absolviert und sich im Laufe der Jahre immer mehr für die IT-Sicherheit interessiert. Seit 2012 ist er voll und ganz als IT-Sicherheitsberater unterwegs und kennt sich bestens mit ISMS Standards aus. Neben seinem Studium der Informatik/IT-Sicherheit an der Friedrich-Alexander-Universität Erlangen/Nürnberg hat er bereits sowohl DAX Top 30 Unternehmen und Landesverwaltungen als auch

kleine Familienunternehmen in allen Belangen der Informationssicherheit beraten. Mithilfe seiner gesammelten Erfahrungen konnte er die Zertifizierung zum PECB ISO/IEC 27001 Lead Implementer erreichen. Regelmäßig nimmt er an Sicherheitskonferenzen teil, in denen neue Erkenntnisse der Branche vorgestellt werden.

Jennifer Gabriel

Jennifer ist, nachdem sie sich viele Jahre in ihrer Freizeit damit beschäftigt hat, seit 2007 in der IT-Sicherheit als Quereinsteigerin unterwegs. Von Beginn an konnte sie viele Erfahrungen in renommierten Beratungsunternehmen, im Bereich Penetrationtesting und im Informationssicherheitsmanagement sammeln. 2020 schloss Jennifer ihr Studium Informatik/IT-Sicherheit mit dem Gesamtprädikat „sehr gut" ab. In der Beratung konnte Jennifer Erfahrung in internationalen sowie DAX Unternehmen sammeln. Ihr spezielles Fachgebiet ist in den

vergangenen Jahren der Bereich der kritischen Infrastrukturen (KRITIS) sowie die Finanzbranche geworden wo sie seit 2013 Informationssicherheitsmanagementsysteme in verschiedenen betroffenen Branchen einführt und auditiert.

Vorwort

IT-Sicherheit in kleinen und mittelständischen Unternehmen voranbringen

IT- und Informations-Sicherheit ist ein komplexes Thema und die Umsetzung nimmt oft viel Zeit und viele Ressourcen in Anspruch. Bisherige Angebote zur Umsetzung oder Beratung zu Informationssicherheit in Unternehmen sind oft schwer verständlich oder sehr teuer und daher nicht für kleine und mittelständische Unternehmen (KMU) erschwinglich. Als Resultat sind viele Unternehmen nur unzureichend gegen aktuelle Hackerangriffe geschützt, wissen nicht wie Sie die Cybersicherheit erhöhen oder Compliance zu z.B. Datenschutzvorgaben wie zur EU-DSGVO herstellen können.

Basierend auf ihrer langjährigen Erfahrung in der IT- und Informations-Sicherheit haben die Autoren dieses Buches ein spezielles Framework für KMUs entwickelt, mit dem Sie selbst mit wenig Aufwand viel in der Cybersicherheit erreichen können – Einsteigerfreundlich erklärt.

Lernen Sie mit dem „Selfmade ISMS“ die grundlegenden Best Practices der IT-Sicherheit kennen und erhalten Sie Tipps, wie Sie diese auch selbst direkt umsetzen können. Sie als Geschäftsführer kennen die Risiken Ihres Unternehmens doch am besten oder Sie als IT-Administrator wissen auch genau wo die Probleme in dem von Ihnen verwalteten Netzwerk liegen.

Kommen Sie zielgerichtet zu abgesicherten Unternehmensprozessen und lernen Sie die Gefahren und Herausforderungen der Cybersicherheit im Unternehmensalltag zu bewältigen. Sei es die Bedrohung durch einen Kryptotrojaner, die Frage, wie Sie vertrauliche Daten am besten mit Geschäftspartnern austauschen oder wie Sie Ihre Geschäftsdaten am besten vor technisch bedingtem Datenverlust schützen.

Mit unseren Quick-Wins kommen Sie in 7 Schritten zur Cybersicherheit in Ihrem Unternehmen und erreichen schnelle Ergebnisse und Verbesserung des Sicherheitsniveaus. Sie können eigenhändig Schwerpunkte setzen und so Schritt-für-Schritt zu Ihrem individuell abgesicherten KMU kommen. Hierbei wird auch auf gängige Zertifizierungen wie ISO® 27001, TISAX® oder BSI-Grundschutz eingegangen, wie sie in Deutschland und Europa verbreitet und anerkannt sind und Ihnen einen Wettbewerbsvorteil bringen können.

Das komplexe Thema IT- und Informations-Sicherheit wird hier von Grund auf ausführlich erläutert und bietet den idealen Einstieg in die Welt der Informationssicherheit.

Inhaltsverzeichnis

Level 3 - IDS/IPS

4.7. Rechtekonzept

Level 1 - Notwendigkeitsprinzip

Level 2 - Passwortanforderungen und privilegierte Zugänge

Level 3 - Notfallbenutzer oder technische Benutzerkennungen

4.8. Verschlüsselung (Kryptokonzept)

Level 1 - Grundlegende Handlungsanweisungen

Level 2 - Anpassung gemäß Empfehlungen von anerkannten Institutionen

Level 3 - Lebenszyklus von Schlüsseln

4.9. Softwareentwicklung

Level 1 - Sicherheitsanforderungen bei der Softwareentwicklung

Level 2 - Change Requests und Abnahmetests

Level 3 - Dokumentation und Versionierung

4.10. Physische Sicherheit

Level 1 - Zutrittsregelung

Level 2 - Physischer Schutz von Sicherheitsbereichen

Level 3 - Versorgungseinrichtungen

4.11. Beschaffung und externe Dienstleister

Level 1 - Management der Dienstleister

Level 2 - Auswahlkriterien und Sicherheitsanforderungen

1. Aufbau

1.1. Einordnung

Dieses Buch bildet den Einstieg in das „Selfmade ISMS“, mit dem Sie die Informationssicherheit kennenlernen und umsetzen können. ISMS steht dabei für **I**nformations**S**icherheits**M**anagement**S**ystem oder auch engl. **I**nformation **S**ecurity **M**anagement **S**ystem – ein in diesem Umfeld sehr gebräuchlicher Begriff, da die Informationssicherheit eines Unternehmens mit geltenden Regelungen und Verantwortlichkeiten ganzheitlich gesteuert werden soll. Der Begriff Informationssicherheit bezieht sich auf die Sicherheit aller Daten eines Unternehmens, also auch auf Daten in Papierform, während sich die IT-Sicherheit typischerweise auf elektronisch verarbeitete Daten sowie die dazu verwendete Soft- und Hardware bezieht. Da dieses Buch den ganzheitlichen Charakter des Aufbaus eines ISMS verfolgt, werden hier selbstverständlich auch alle Aspekte der Informationssicherheit betrachtet.

Neben diesem Buch haben die Autoren auch Dokumentenvorlagen ausgearbeitet, die Sie bei der Einführung des ISMS unterstützen können. Diese wurden auf Grundlage der jahrelangen Beratungserfahrung generalisiert erstellt und können leicht an Ihre eigenen Bedürfnisse angepasst werden. Sollten Sie weitere Unterstützung benötigen, können Sie sich auch im

persönlichen Gespräch beraten lassen, ein Review Ihrer Dokumentation oder ein Audit beauftragen.

Besuchen Sie gerne auch unsere Webseite:

https://www.selfmade-isms.de

Das Buch nennt Empfehlungen, die einen schlanken Weg zur Umsetzung von IT- und Informationssicherheit im Unternehmen aufzeigen, der bei den meisten KMUs in Deutschland grundsätzlich praktikabel ist. Natürlich kann es immer wieder vorkommen, dass einzelne hier vorgestellte Herangehensweisen nicht in jedem Unternehmen anwendbar sind, da allein schon durch das jeweilige Geschäftsfeld Individuallösungen nötig sein könnten. Jedoch sollten viele Aspekte, die in diesem Buch vorgestellt werden, praktikabel sein. Zudem ist das Buch auch dazu gedacht, Sie selbst in die Lage zu versetzen, eine für Ihre Bedürfnisse gängige Lösung zu finden.

1.2. Aufbau des Buches

In Kapitel 1 erhalten Sie alle wichtigen theoretischen Grundlagen. Fachjargon wird in einfacher Sprache erklärt und ihnen werden die wichtigen Aspekte eines ISMS aufgezeigt. Zur konkreten Definition der Themenfelder eines ISMS finden Sie alle wichtigen Informationen in Kapitel 2. Diese Kapitel bildet auch die Grundlage für die

Umsetzungsstrategien, welche in Kapitel 3 behandelt werden.

Kapitel 4 lässt sich als Hauptkapitel bezeichnen. Hier werden die konkreten Sicherheitsanforderungen und Sicherheitsmaßnahmen dargestellt. Sie gliedern sich in insgesamt 14 Bereiche:

1. ISMS - Informations-Sicherheits-Management-System
2. Assetmanagement und Gebrauch von Assets
3. Personalmanagement
4. Change-Management
5. Systemsicherheit
6. Netzwerksicherheit
7. Rechtekonzept
8. Verschlüsselung (Kryptokonzept)
9. Softwareentwicklung
10. Physische Sicherheit
11. Beschaffung und externe Dienstleister
12. Behandlung von Sicherheitsvorfällen
13. Compliance und Datenschutz
14. Business Continuity Management (BCM)

Zusätzlich werden die Bereiche in jeweils bis zu 3 Level unterteilt, die sich folgendermaßen gliedern:

- **Level 1: Grundlegende Sicherheitsmaßnahmen**, die jedes Unternehmen

umsetzen sollte und die den idealen Einstig für kleine Unternehmen bilden.

- **Level 2: Etwas komplexere Maßnahmen**, die die Sicherheit in einem Unternehmen weiter erhöhen können, jedoch oft aufwändiger in der Umsetzung sind.
- **Level 3: Weitaus aufwändigere Anforderungen**, wie sie oft von ISMS Zertifizierungen gefordert werden. Diese sind in Umgebungen mit hoch schützenswerten Daten dringend empfohlen.

Entsprechend Ihrer Möglichkeiten und Bedürfnisse bei der Absicherung von Ihren Informationen, auch in Teilbereichen, steht es Ihnen natürlich frei, bis zu welchem Level Sie Maßnahmen und Empfehlungen in welchen Bereichen umsetzen. Wenn Sie vorerst mit den grundlegenden Methoden starten wollen, können Sie auch zuerst immer nur den Level 1 eines jeden Bereiches starten. Auch kann es vorkommen, dass einzelne Bereiche wie z.B. 9. Softwareentwicklung für Ihr Unternehmen nicht relevant sind, da Sie keine betreiben. Folglich müssen Sie dieses Kapitel dann auch nicht bearbeiten.

Eine Zertifizierung des ISMS, bei der ein unabhängiger Prüfer die Erfüllung von ausgewählten Standards der Informationssicherheit in einem Unternehmen überprüft und bei Erfolg ein entsprechendes Zertifikat ausstellt, würden wir bei kleinen Unternehmen zunächst nicht generell empfehlen. Dies ist oft mit einem hohen bürokratischen Aufwand und auch Kosten für externe Prüfer verbunden. Falls jedoch ein konkreter Auftrag dahintersteht, wie ein

Großkonzern, der von einem kleineren Unternehmen eine ISMS Zertifizierung als Bedingung der Zusammenarbeit fordert, so können Aufwand und möglicher Gewinn gegeneinander abgewogen werden. Mehr zu ISMS-Standards und Zertifizierungen in Kapitel 3.

Die Texte in diesem Buch beziehen sich auf Anforderungen aus verschiedenen zertifizierungsfähigen Normen sowie allgemeinen Empfehlungen. Zusätzliche Ausführungen sind folgendermaßen gekennzeichnet:

Tipp
Praxisnahe Umsetzungstipps für KMUs zu den beschriebenen Anforderungen sind in den jeweiligen Kapiteln als Tipps hervorgehoben.

Beispiel
Um einen Sachverhalt besser veranschaulichen zu können, werden an verschiedenen Stellen Beispiele beschrieben und entsprechend hervorgehoben.

Detaillierte Ausführung und Exkurs
Hintergrundinformationen, die zeigen, welche eigentlichen Gründe hinter einer Anforderung stecken und wie die Gegebenheiten technisch funktionieren, werden im Buch anhand von Exkursen erläutert.

Zusammenfassung und Richtlinie
Um die in einem Kapitel beschriebenen Themen und Anforderungen im Unternehmen zu forcieren, bietet es sich an, zu genau diesem Themenkomplex eine Richtlinie bzw. Begleitdokumente mit Dokumentationscharakter zu

schreiben, die die Handhabung des Sachverhalts in Ihrem Unternehmen beschreiben und festlegen.
Die Kapitel in diesem Buch sind extra dafür vorbereitet und bieten am Ende jedes Kapitels eine Zusammenfassung der behandelten Themen und stellen heraus wie diese in einer entsprechenden Richtlinie beschrieben werden können.

In Kapitel 5 dieses Buches finden Sie eine speziell für KMU ausgeprägte Herangehensweise, die zeigt, wie Sie mit dem

Wie kann ein kleines oder mittelständisches Unternehmen die Informationssicherheit mit wenig Aufwand erhöhen?

umfangreichen Wissen aus Kapitel 4 nun von Null auf 100 die IT- und Informationssicherheit in Ihrem Unternehmen mit schnellem Erfolg umsetzen können. Im Mittelpunkt steht dabei immer die Frage:

Kapitel 6 des Buches ist ein Bonuskapitel. Hier erhalten Sie weitere Tipps, wie Sie die Informationssicherheit in Ihrem Unternehmen weiter verbessern können. Sie lernen teilweise sogar über die Anforderungen einiger Zertifizierungen hinausreichende Themen der Informationssicherheit praxisnah umzusetzen.

Zusätzlich finden Sie am Ende des Buches eine Checkliste, mit der Sie alle im Buch behandelten Themen, wenn sie behandelt und für Ihr Unternehmen passend umgesetzt worden sind, abhaken können.

2. Einleitung

Die IT-Sicherheit hat mit den Jahren immer mehr an Bedeutung gewonnen. Computertechnik dringt in immer weitere Bereiche der Industrie vor, die Vernetzung schreitet voran. Zusätzlich werden die Angriffsmethoden der Kriminellen immer ausgefeilter und Angriffe wie Kryptotrojaner oder ähnliche Mechanismen kommen immer häufiger vor. Diese richten oftmals immensen Schaden an und können sogar existenzbedrohend für Unternehmen sein.

2.1. Welche Unternehmen sind gefährdet?

In den letzten Jahren ist zu erkennen, dass auch immer mehr kleine Unternehmen, die ihre Dienstleistungen und Waren an Großunternehmen und Konzerne verkaufen, das Ziel von Cyberangriffen werden. Oft werden dann die aufgrund der existierenden Geschäftsbeziehungen bestehenden Zugriffe als „Sprungbrett" auf das eigentliche Angriffsziel genutzt.[1]

Dienstleister und Lieferanten von Großunternehmen, deren IT- und Informationssicherheit oft einen niedrigeren Reifegrad aufweist als die von großen Konzernen, sind oft ein leichtes Ziel. Oft sind es Familienunternehmen oder auch „hidden champions" - Unternehmen, die Weltmarktführer mit einem bestimmten Produkt sind. Es

sind zum einen Digitalunternehmen, die eine spezialisierte Anwendung - meist in Cloudumgebungen - einer ausgewählten Zahl von Kunden bereitstellen - Angreifer versuchen, direkt an die in der Cloud von Großunternehmen gespeicherten Daten zu kommen, um so Daten zu manipulieren oder auszuspionieren. Zum anderen sind es auch Unternehmen bei denen die IT nur als Mittel zum Zweck dient und die ihre Dienstleistungen und Produkte meist in einem ganz anderen Segment anbieten[2] – Interne Geschäftsprozesse werden durch die IT unterstützt, wenn diese ausfällt, lassen sich die Prozesse oft nur schwer aufrechterhalten.

2.2. Warum sollte ich IT-Sicherheit umsetzen?

Diese Frage wird wohl oft gestellt. Das Thema scheint riesig und komplex zu sein und auch sehr aufwändig in der Umsetzung. Die Vorteile liegen jedoch auf der Hand:

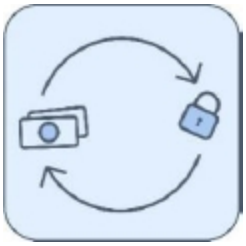
Synergieeffekte nutzen: Das Voranbringen der Informationssicherheit geht oft mit anderen Digitalisierungsschritten einher, sodass bereits bestehende Geschäftsprozesse mit der Aktualisierung von Systemen zur Erhöhung der Informationssicherheit auch gleich auf weitere Prozessoptimierungen mit neuer Software oder einer

schnelleren Verarbeitungsgeschwindigkeit hin verbessert werden können. Das hebt oft auch die Motivation der Mitarbeitenden.

Zielgerichtet anwenden und Aufwand sparen: Sie können Informationssicherheit genau dort anwenden, wo Sie sie benötigen. So können Sie zunächst Ihre Kernprozesse und zentralen Daten absichern, bevor Sie Aufwände in andere, evtl. weniger wichtige Bereiche investieren. Die vermeintlich größten Angriffsvektoren lassen sich so priorisiert angehen.

Werte schützen: Mit der Umsetzung von zentralen Sicherheitsmaßnahmen machen Sie Ihr Unternehmen stark gegen externe Einflüsse wie Hackerangriffe, die Ihre Unternehmensprozesse beeinträchtigen können. Sie schaffen zusätzlich ein Bewusstsein für IT- und Informationssicherheit, mit dem sich jeder Mitarbeitende identifizieren kann und Sie können mitunter noch vorhandene Schwachstellen oder Risiken in Ihrem Unternehmen besser einordnen. Mit der ganzheitlichen

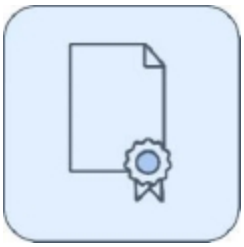
Umsetzung von Maßnahmen (technisch, organisatorisch, etc.) in allen Bereichen können Sie zusätzlich auch eine Resilienz erreichen. Sie schützen sich also auch schon vor IT-Bedrohungen, die noch gar nicht in breiter Masse ausgenutzt werden. Insgesamt schützen Sie also Ihre Werte wie Betriebs- und Geschäftsgeheimnisse, Produkte und Kundendaten.



Return of Investment: Falls es doch einmal zu einem Ernstfall kommt, so können Sie durch die vorausschauende Planung durch ein ISMS Ihre Geschäftsprozesse schneller wieder aufnehmen. Die Gesamtkosten eines Schadens oder Produktionsausfalls sinken und können die Kosten der Einführung und des Betriebs des ISMS gänzlich kompensieren.

Bessere Chancen am Markt: Mit der Botschaft nach außen, dass in Ihrem Unternehmen die Informationssicherheit zertifiziert ist, können Sie am Markt hervorstechen und eventuell einen Wettbewerbsvorteil gegenüber Konkurrenten erlangen, die diesen Nachweis

nicht erbringen können. Kunden achten auf die Sicherheit ihrer Daten und die Zuverlässigkeit der Geschäftspartner und Produkte. Mit umgesetzter Informationssicherheit können Sie hier Ihren Ruf verbessern. Vor allem Großkonzerne verlangen teilweise sogar Zertifizierungen für die Zusammenarbeit. Somit kann die flächendeckende Umsetzung und Zertifizierung des ISMS auch gewinnbringende Aufträge mit sich bringen.



Konformität zu Gesetzen: Zu guter Letzt seien auch gesetzliche Anforderungen wie z.B. die EU-DSGVO (ISMS vor allem Art. 32) genannt, die Unternehmen erfüllen müssen und deren Einhaltung mithilfe des ISMS unternehmensweit geregelt werden kann. Sie stellen also eine Konformität zu nationalen und internationalen Gesetzen her. Gesetzliche Verstöße z.B. gegen Datenschutzvorschriften können mitunter sehr teuer werden. Durch Vorbereitung und Umsetzung von best-practices können Sie diesem ebenfalls vorbeugen.

Insgesamt lässt sich sagen, dass Sie bereits mit vergleichsweise wenig Aufwand relativ viel im Bereich der Informationssicherheit erreichen können. Dieses Buch folgt daher auch dem Grundsatz:

Effektiv und effizient ans Ziel!

[1] WIK Studie: Aktuelle Lage der IT-Sicherheit in KMU, Dezember 2017

[2] https://www.spektrum.de/news/hackerangriffe-deutschlands-extrem-verwundbare-it-infrastruktur/1910719 - Aufgerufen am 12.12.2021

3. Informationssicherheitsmanagement und Standards

Zu den grundlegenden Sicherheitsmaßnahmen zählt, neben den technischen Maßnahmen, vor allem der Aufbau eines ISMS. Informationssicherheit sollte zentral verwaltet und gleichermaßen über alle Unternehmensteile aufgebaut werden. Ein ISMS bietet hier eine Leitlinie und ermöglicht die Steuerung, Überwachung und Anpassung von Prozessen. Risiken für den Geschäftsbetrieb und die bearbeiteten Daten sollten identifizierbar und verwaltbar werden. Resultierende Sicherheitsmaßnahmen orientieren sich idealerweise an anerkannten Standards und können zielgerichtet adressiert und umgesetzt werden.

Im Laufe der Jahre haben sich aus vielen Interessensgruppen oder auch staatlichen Behörden verschiedene Sicherheitsstandards bzw. ISMS Standards entwickelt, die jeweils verschiedene Ziele und Detailgrade haben. Ein ISMS Standard verfügt dabei immer über einen Prüfkatalog, der eine Vielzahl von Anforderungen oder sogar konkrete Sicherheitsmaßnahmen definiert. Die definierten Kontrollziele (Prüfpunkte) oder Anforderungen, die ein Unternehmen zu erfüllen hat, um konform zu einem der Standards zu sein, sind unterschiedlich hart formuliert. Während einige Standards harte Kontrollziele mit genauen Umsetzungsvorgaben haben, führen andere Standards Anforderungen auf, die das Unternehmen nach eigenen

Bedürfnissen erfüllen kann. Um die Formulierungen in diesem Buch nicht zu kompliziert zu gestalten, werden die Begriffe „Anforderungen“ und „Kontrollziele“ synonym verwendet. Manche der Standards bieten auch die Möglichkeit, ein Unternehmen oder Teile davon von einem unabhängigen Prüfer zertifizieren zu lassen und so die Aufrechterhaltung der Konformität zu bescheinigen.

3.1. Governance, Risk, Compliance

Ein ISMS kann auch in weiteren Unternehmensbereichen hilfreich sein. Dies drückt das im Amerikanischen geläufige Akronym „GRC“ aus. GRC steht hierbei für:

1. **Governance (Führung):** Ziele der Führungsebene für das Unternehmen - Hierzu können auch IT-Ziele wie eine Digitalisierung von etablierten, papierbasierten Prozessen gehören.
2. **Risk (Risiko):** Das Risiko für bestimmte Systeme und Prozesse des Unternehmens ermitteln und den Fortlauf der Betriebsfähigkeit sichern.
3. **Compliance (Konformität):** Einhaltung von Gesetzen, die das Unternehmen betreffen, wie z.B. Datenschutz sowie branchenspezifische Regelungen.

Durch das ISMS kann ein Unternehmen also auch aus einem gewachsenen Geschäft den Überblick über die genauen Abhängigkeiten von Geschäftsprozessen und kritischen Systemen gewinnen, die für die Erfüllung der Kundenaufträge erforderlich sind. Auch kann Informationssicherheit eine treibende Kraft bei der Digitalisierung von Unternehmen sein, indem z.B.

umständliche Verwaltungssysteme auf elektronisch gestützte Systeme entsprechend den neuesten gesetzlichen Anforderungen umgestellt werden.

Aus Sicht der Compliance kann ein ISMS somit auch ein Hilfsmittel sein, geltende Gesetze und regulatorische Anforderungen einzuhalten. Viele ISMS Standards berücksichtigen auch Gegebenheiten aus dem Datenschutz, meist auf Grundlage der DSGVO. Nach deren Artikel 32 muss die Sicherheit der Datenverarbeitung gewährleistet sein[3]. Hier können wiederum zielgerichtet definierte Sicherheitsmaßnahmen in einem ISMS die nachweisliche Einhaltung belegen. Ein Archivierungssystem kann beispielsweise die Aufbewahrungsfristen von Daten gemäß Handelsgesetzbuch (HGB) verwalten[4]. Geschäftsführer von Aktiengesellschaften und GmbHs sind sogar dazu verpflichtet, Gefahren von einem Unternehmen abzuwenden, da sie dafür gemäß § 93 Abs. 2 bzw. § 43 Abs. 2 GmbHG (Sorgfaltspflicht) privat haftbar sind. Hier hilft erneut die Risikobehandlung aus dem ISMS[5].

3.2. Schutzziele

Die Kritikalität von Systemen wird i.d.R. in Form von drei Schutzzielen definiert:

1. **Verfügbarkeit**

(Availability)
Daten müssen nutzbar, Systeme verfügbar sein.

2. **Integrität**

(Integrity)
Die Richtigkeit der Daten muss verlässlich sein.