

**Pascal Wenger**

**Sicherheit als Teil des  
Informationsmanagements  
verstärkt in die Unternehmensführung  
einbinden**

**Investitionen in die Sicherheit von  
Informationstechnologien als kritischer  
Erfolgsfaktor der Zukunft**

**Wenger, Pascal: Sicherheit als Teil des Informationsmanagements verstärkt in die Unternehmensführung einbinden: Investitionen in die Sicherheit von Informationstechnologien als kritischer Erfolgsfaktor der Zukunft. Hamburg, Diplomica Verlag GmbH 2014**

Buch-ISBN: 978-3-8428-9399-3

PDF-eBook-ISBN: 978-3-8428-4399-8

Druck/Herstellung: Diplomica® Verlag GmbH, Hamburg, 2014

**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.

---

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Dies gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Bearbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden und die Diplomica Verlag GmbH, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

Alle Rechte vorbehalten

© Diplomica Verlag GmbH  
Hermannstal 119k, 22119 Hamburg  
<http://www.diplomica-verlag.de>, Hamburg 2014  
Printed in Germany

# I Inhalt

<b>1. Einleitung</b> .....	<b>1</b>
1.1. Ausgangslage .....	1
1.2. Schwachstellen in der Interaktion zwischen Management und Sicherheit in der Informationstechnologie .....	3
1.3. Ziele und Abgrenzung .....	5
1.4. Vorgehen und Aufbau.....	6
<b>2. Sicherheit der Informationstechnologie und das Einbinden in die Managementperspektive</b> .....	<b>8</b>
2.1. Unternehmensführung .....	9
2.2. Managementkonzepte .....	10
2.2.1. Corporate Governance/COSO .....	12
2.2.2. IT-Governance/COBIT .....	14
2.2.3. Informationssicherheit / ISO/IEC 2700x .....	15
2.2.4. IT-Service Management / ITIL .....	17
2.2.5. IT-Risikomanagement / ISO/IEC 31000 .....	18
2.3. Technische und organisatorische Aspekte der Sicherheit .....	19
2.3.1. Abgrenzung der Sicherheit .....	19
2.3.2. Abhängigkeiten zwischen Risiken und der Sicherheit.....	23
2.3.3. Sicherheit - eingebunden in die Organisation der Unternehmung .....	27
2.4. Eine integrale Perspektive auf das Unternehmen zeigt ein vernetztes System.....	29
2.4.1. System.....	31
2.4.2. Systemisches Denken .....	35
2.5. Fazit.....	40
<b>3. Theoretische Untersuchung zur Überprüfung der Forschungsfrage</b> .....	<b>42</b>
3.1. Überlegung bei der Vorbereitung zur Durchführung der Untersuchung.....	42
3.1.1. Methodik der Untersuchung .....	42
3.1.2. Qualität der Untersuchung.....	44
3.1.3. Vorgehen bei der Untersuchung.....	45
3.2. Entwicklung des Wirkungsdiagramms – Informationssicherheit und Unternehmensführung ..	50
3.3. Untersuchung der Feedbackschleifen als Teil des Wirkungsdiagramms.....	53
3.3.1. Feedbackschleife - Unternehmenswachstum .....	53
3.3.2. Feedbackschleife IT-Service Funktionalität.....	60
3.3.3. Feedbackschleife-Risiko.....	64
3.4. Untersuchung der Kommunikation im Wirkungsdiagramm .....	68
3.5. Fazit.....	70
<b>4. Wirkungszusammenhänge und Empfehlungen</b> .....	<b>71</b>
4.1. Erkenntnisse zu den Wirkungszusammenhängen .....	71
4.2. Erkenntnisse im Kontext der Forschungsfrage .....	74
4.3. Empfehlungen zur verstärkten Einbindung der Sicherheit in die Unternehmensführung .....	76
4.3.1. Empfehlung zu den Dimensionen: Organisation, Managementkonzept und Prozess .....	76
4.3.2. Empfehlung zu den Dimensionen: Kommunikation.....	78
4.4. Praxis.....	79

<b>5.</b>	<b>Kritische Würdigung</b> .....	<b>84</b>
<b>6.</b>	<b>Schlussbetrachtung und Ausblick</b> .....	<b>86</b>
6.1.	Schlussbetrachtung.....	86
6.2.	Ausblick.....	87
<b>7.</b>	<b>Verzeichnisse</b> .....	<b>89</b>
7.1.	Abkürzungsverzeichnis .....	89
7.2.	Abbildungsverzeichnis .....	90
7.3.	Literaturverzeichnis .....	91

## 1. Einleitung

Im ersten Kapitel soll in diesem Buch die Ausgangslage (Kapitel 1.1), die Schwachstellen in der Interaktion zwischen der Unternehmensführung und der Sicherheit der Informationstechnologie (Kapitel 1.2) und die Nutzung der Managementkonzepte untersucht und erläutert werden. Ausgehend von der Forschungsfrage und den aufgestellten Thesen werden folgend die Zielsetzungen, erwartete Ergebnisse aufgezeigt und eine Abgrenzung des Themenbereichs vorgenommen (Kapitel 1.3). Die Beschreibung zum Vorgehen und Aufbau der Untersuchung (Kapitel 1.4). schliesst dieses erste Kapitel ab.

### 1.1. Ausgangslage

Die Informations- und Kommunikationstechnologie hat sich in der Vergangenheit stark entwickelt; mit einer Weiterentwicklung ist auch zukünftig zu rechnen. Bereits im Jahr 1993 wurde dazu erklärt, dass die Systeme der Informationstechnologie zunehmend für die Unternehmungen relevant werden und dies als ernst zu nehmendes Thema einzustufen ist.<sup>1</sup> Diese Wichtigkeit der Informationen, welche in den Geschäftsprozessen der Unternehmen genutzt werden, wurde im Jahre 2004 im Lexikon der Wirtschaftsinformatik ausser Frage gestellt. Dabei äussern sich die Herren Heinzl und Roithmayer dahin gehend, dass Informationen alle anderen Produktionsfaktoren durchdringen werden.<sup>2</sup> Äusserungen, die sich nach heutiger Betrachtung bewahrheitet haben. So macht die Konferenz für Berufsbildung *Information and Communication* folgende Angaben zur Entwicklung der Informationstechnologie. Es zeichnet sich für die Zukunft ab, dass bis 2017 rund 212'300 Schweizerinnen und Schweizer im Sektor der Informations- und Kommunikationstechnologie arbeiten werden. Das entspricht einem dreifachen Wert der erwerbstätigen Personen, welche im historisch verankerten Landwirtschaftssektor (62'000) tätig sind und einem fast doppelt so hohen Wert der im Bankensektor (110'000) Beschäftigten.<sup>3</sup> Eine Entwicklung, welche unter anderem auch an der steigenden Anzahl mobiler Geräte erkennbar ist, wie die rasant zunehmende Vielfalt an Funktionalitäten bei Geräten und Anwendungen im Gebiet der Informations- und Kommunikationstechnologie zeigt. Der *Mobile-Report* der Firma Net-Matrix liefert quantitative Auswertungen und Informationen zur Entwicklung der mobilen Internetnutzung über sogenannte Small Screen Devices. Die aktuelle Ausgabe des Reports zeigt, dass der mobile Besuch im Internet immer beliebter wird. Nutzte das Internet im Jahr 2010 mehr als jeder vierte Anwender über mobile Geräte wie z. B. das Smartphone, ist es gemäss Mitteilung von Net-Matrix aktuell fast jeder zweite Internetanwender.<sup>4</sup>

Diese immer neueren und weiter ausgereiften Informations- und Kommunikationstechnologien können nicht nur für den privaten Bereich genutzt werden. Auch Unternehmen wird ermöglicht, diese in fast allen betriebswirtschaftlichen Abläufen einzusetzen.

---

<sup>1</sup> (Baskerville, 1993)

<sup>2</sup> (Lutz, Arminl, & Friedrich, 2004), S.935

<sup>3</sup> (Bildungsdirektion Kanton Zürich, 2011)

<sup>4</sup> (NET-Matrix AG, 2012)

Bei einem Einsatz kann somit die Informationstechnologie die entscheidenden Geschäftsprozesse eines Unternehmens unterstützen, bei der Bearbeitung von Aufträgen bis hin zum Rechnungswesen. „[...] In vielen Industriebereichen hat die Informationstechnologie dabei zu wesentlichen Transformationen und Innovationen geführt. Im Finanzdienstleistungssektor hat sich die ICT zu einer wesentlichen Kernkompetenz entwickelt, in anderen Branchen hat die Informationstechnologie durch digitale Multimedia neue Produktwelten rund um Video und Audio geschaffen.“<sup>5</sup> In der heutigen Art der Nutzung der Informationstechnologie spielen somit die Informationen und deren Daten eine immer grössere Rolle. Untersuchungen von IBM zu den Datenmengen gehen davon aus, dass 90 % aller weltweit verfügbaren Daten in den vergangenen zwei Jahren entstanden sind.<sup>6</sup> Dabei müssen die Unternehmen nicht nur mit dieser Menge an Daten umzugehen wissen. So wirkt sich dies auch auf die Anzahl von Informations- und Kommunikationsbeziehungen aus und stellt erhöhte Anforderungen an die Fachbereiche der Informationstechnologie, aber auch an die Sicherheit.<sup>7</sup> Unter Betrachtung dieser Entwicklung und deren Einflüsse auf das Unternehmen stellt die Information heute einen Wert dar. Durch den Wert der eingesetzten Daten und Informationen innerhalb der Unternehmen hat sich die Technologie für die Informations- und Datenverarbeitung, in den vergangenen Jahren zu einem Faktor entwickelt, welcher heute wie auch in der Zukunft nicht unwesentlich für die Unternehmensführung ist. Der Umgang mit Daten innerhalb vieler Unternehmen wird jedoch als problematisch beschrieben.<sup>8</sup> Eine Tatsache, welche es nachvollziehen lässt, dass die Bewertung der Informationstechnologie heute in Unternehmen strategisch höher ist als noch vor einigen Jahren. Wie durch den Autor in der Literaturrecherche festgestellt wurde, wird jedoch der Beitrag der Fachbereiche Informationstechnologie wie die Nutzen von neueren Funktionalitäten zum Unternehmenserfolg in der Theorie und Praxis zurzeit noch unterschiedlich und widersprüchlich diskutiert, obwohl verschiedene empirische Studien eine Beziehung zwischen der Informationstechnologie und dem Erfolg von Unternehmen nachweisen.<sup>9</sup>

Aufgrund dieser stetigen Entwicklung von Daten und Informationen sowie der damit verbundenen Anforderungen an die Qualität wird die Frage der Sicherheit immer stärker zu einem entscheidenden Faktor für die Gestaltung der Infrastruktur der Informationstechnologie und deren Betrieb. So wirken sich zum Beispiel die mobilen Geräte, Cloud Services oder die sozialen Medien nachhaltig auf die Risiken der Informationstechnologie und die dadurch benötigten Sicherheitsmassnahmen einer Unternehmung aus. Ausfallzeit, Geld-, Zeit- und Imageverlust sollen tunlichst vermieden werden. Ein Bestreben der Unternehmen, welches verständlich wird, wenn man diesbezüglich Zahlen aus der Marktforschung betrachtet. Das Marktforschungsunternehmen Coleman Parkes liefert z. B. in seiner Studie *Avoidable Cost of Downtime 2010* Zahlen, welche die Ausfälle in der Informationstechnologie beziffern. Dabei geben die an der Studie teilgenommenen europäischen Unternehmen Kosten von durchschnitt-

---

<sup>5</sup> Lothar Dietrich 2006, S.21

<sup>6</sup> (VDI Verlag GmbH, 2011)

<sup>7</sup> (Böhm, 2008)

<sup>8</sup> ( Bundesamt für Sicherheit ind der Informationstechnik (BSI), 2011)

<sup>9</sup> (Beimborn, Franke, Gomber, & Wagner, 2006)

tlich 263'347 Euro/jährlich an.<sup>10</sup> Es ist daher nachvollziehbar, dass Unternehmen von einer weiter steigenden Bedeutung der Informationstechnologie und deren Sicherheit ausgehen und dabei der Sicherheit einen hohen bis sehr hohen Stellenwert einräumen. So jedenfalls äussert sich die Mehrheit der befragten Unternehmen in einer durchgeführten Studie des ibi Research über den Status quo und Entwicklungstendenzen hinsichtlich Sicherheitsstandards und Compliance.<sup>11</sup>

Nicht nur die Fachbereiche Informationstechnologie, auch die Unternehmensführung wird durch die oben beschriebenen Entwicklungstendenzen beeinflusst. Erkennbar wird dies dadurch, dass die Unternehmensführung sich vermehrt mit Informationen zu bestehenden und benötigten Ressourcen in der Informationstechnologie befasst. Dabei wird von der Unternehmensleitung erwartet, dass sie mögliche Sicherheitsrisiken erkennt und nachhaltige Massnahmen zur Behandlung einleitet. Die Transformation von bestehenden Informationen und vorhandenem Wissen in nutzbare Steuerungsgrössen der Unternehmensführung spielt dabei ein wichtiger Aspekt, vor allem vor dem Hintergrund der steigenden Komplexität. Dabei wird die Komplexität durch die Veränderung bei der innerbetrieblichen Arbeitsteilung, wie durch die hoch technologischen Fertigungsprozesse, weiter genährt.<sup>12</sup> Die Unternehmensleitung sieht sich heute wie auch zukünftig in ihrer Führungsaufgabe vor der Herausforderung, dass immer mehr Entscheidungen gefragt sind, die sinnvolle Kompromisse darstellen. Kompromisse, bei welchen alle Perspektiven, somit auch die der Informationstechnologie und die damit verbundene Sicherheit, berücksichtigt werden müssen.

## **1.2. Schwachstellen in der Interaktion zwischen Management und Sicherheit in der Informationstechnologie**

Persönliche Beobachtungen in unterschiedlichen Unternehmungen zeigen dem Autor, dass in der Praxis Managementkonzepte im Rahmen der Unternehmensführung, der Informationstechnologie und der Sicherheit eingesetzt werden. Mit diesen werden Informationen bereitgestellt, welche jedoch bei einer ungenügenden Abstimmung Insel-Lösungen darstellen. Eine ungenügende integrale Betrachtung beim Aufbau und der Nutzung der Konzepte kann zu Fehlinterpretationen und nicht zuletzt zu Fehlentscheidungen führen. Um die Beobachtungen und die damit erkannte Problematik der Sicherheit und deren Informationen aufzeigen zu können, soll der Zusammenhang anhand einer Darstellung in Abbildung 1 und einer Situationsbeschreibung vereinfacht dargestellt werden, die Darstellung beruht auf Erfahrungswerten des Autors.

---

<sup>10</sup> (Coleman Parkes Research: CA Technologies, 2011)

<sup>11</sup> (Kronsnab, Weber, Dirnberger, Török, & Münch, 2010)

<sup>12</sup> (Malik, Management: Das A und O des Handwerks, 2007), S.33

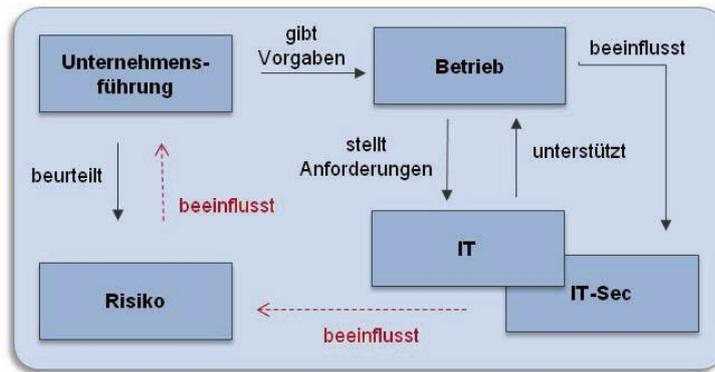


Abbildung 1: Situationsdarstellung  
Quelle: Eigene Darstellung

### Situationsbeschreibung

Gemäss der allgemeinen Wirtschaftslehre strebt die Unternehmensführung auf Basis der strategischen und taktischen Vorgaben eine operative Umsetzung an. Wird die Sicherheit der Informationstechnologie dabei als rein technisches Problem bewertet und folglich nach *unten* in den Fachbereich Sicherheit der Informationstechnologie delegiert, zeigen sich negative Auswirkungen in den Folgeaktivitäten. David Birchall befasst sich in seinem Buch: *Information assurance - Strategic alignment and competitive advantage*<sup>13</sup> mit solchen Auswirkungen. Die Erfahrungswerte des Autors zeigen ein ähnliches Bild, welches folgend mit einer Beschreibung der Verkettung der Aktivitäten sowie möglichen negativen Auswirkungen zusammenfassend aufgezeigt wird.

Die durch die delegierte Stelle ermittelten Sicherheitsrisiken bzw. mögliche Schäden für den Betrieb werden mit entsprechenden Instrumenten/Methoden transparent gemacht und in Bezug zu den Kosten möglicher Handlungsoptionen gestellt. Dabei werden die Methoden und spezifischen Instrumente der Fachbereiche laufend verbessert, immer mit dem Ziel der Unternehmensführung Daten und Informationen liefern zu können, womit diese effizient und nachhaltig ihre Arbeit erbringen kann. Gegenüber der Unternehmensleitung wird folglich aus der Sicht der Sicherheit und der Technik argumentiert. Argumente, mit denen sich die Unternehmensführung wiederum schwer tut, zumal dabei auch unterschiedliche Terminologien benutzt werden. Die benötigte Transparenz fehlt. Die Wichtigkeit einer Investition in die Sicherheit im Bereich der Informationstechnologie kann durch die Unternehmensführung in dieser Situation nicht oder nur ungenügend betrachtet werden. Eine Situation, welche die Unternehmensleitung in eine ungünstige Lage bringt, in der sie mit den nicht abgestimmten und integral funktionierenden Managementkonzepten in eine Zeit blickt, in welcher die Informationstechnologien rasante Entwicklungen durchlaufen. Die Unternehmensführung hat dabei oftmals keine Vorstellung über den aktuellen, integralen Stand der Sicherheit im Bereich der Informationstechnologie.

<sup>13</sup> (Birchall, Ezingear, McFadzean, Howlin, & Yoxall, 2004), S.17-35

## **Ausgestaltung und Einbindung der Sicherheit in die Methoden der Unternehmensführung**

Die Situationsbeschreibung lässt erkennen, dass es sich bei der Ausgestaltung und Einbindung der Sicherheit der Informationstechnologie in die Konzepte der Unternehmensführung somit nicht nur um die Führung der Technologie handelt. Es geht auch um eine Ausrichtung auf gemeinsame Ziele, um den Transfer von Informationsinhalten und das persönliche Verhalten. Informationen müssen so festgelegt werden, dass sie dabei als Steuerungsgrößen genutzt werden können und die Instrumente und Konzepte durch die betroffenen Akteure nicht nur als rein zu befolgende Regelungen verstanden werden.

Schlagzeilen in der öffentlichen Presse und den Medien während der vergangenen Wochen und Monate, wie zum Beispiel über den Diebstahl von Daten, haben aufgezeigt, dass die Situation in Bezug auf die Sicherheit der Informationstechnologie durch die Unternehmensführung falsch verstanden oder eingeschätzt wurde. Auswirkungen haben sich für die jeweiligen Unternehmungen in unterschiedlichster Form gezeigt. Eine Situation, die zu einem Umdenken veranlassen sollte.

Eine Anpassung und Abstimmung der eingesetzten Managementkonzepte tut not; benötigte Handlungen, mit welchen sich jedoch die Unternehmensführung seit Längerem schwertut. So wurde zu diesem Verhalten der Unternehmensführung bereits im Jahr 2005 in einer Studie von Kaplan und Norton festgestellt, dass z. B. 67 % der Unternehmen mit ihren Führungskräften ihre operativen Strategien nicht mit der Unternehmensstrategie in Einklang bringen.<sup>14</sup> Auch heute ist das Thema der Verbindung der Unternehmensprozesse mit der Informationstechnologie immer noch aktuell und wird in der Fachliteratur unter den Begriffen wie z. B. IT-Business Alignment oder Strategic-Alignment besprochen.

Aus Sicht der Unternehmensführung scheint es also Argumente und Motive zu geben, warum Informationen, welche nach dem aktuellen Wissen und den eingesetzten Managementkonzepten zur Sicherheit der Informationstechnologie nicht genutzt werden können. Der Autor nimmt an, dass ein persönliches Vorgehen der Führungskraft und die Verschiedenheit der praktischen Ausgestaltung der Führungsinstrumente die Informationen wesentlich beeinflussen und so auch deren Nutzen bestimmen.

### **1.3. Ziele und Abgrenzung**

Die geschilderten Sachverhalte wie auch die Problembeschreibung bilden das inhaltliche und zentrale Thema dieses Buchs und sind in der allgemeinen Forschungsfrage wie folgt zusammenfasst.

Können die Informationen zur Sicherheit der Informationstechnologie, welche durch Instrumente und Methoden bereitgestellt werden, durch die Unternehmensleitung in die Führungsstrukturen- und -prozesse eingebunden und genutzt werden?

---

<sup>14</sup> (Norten & Kaplan, 2006)

Anhand der gestellten Forschungsfrage lassen sich folgende Thesen aufstellen:

- a) Wenn Managementkonzepte der Unternehmensleitung keine integrale Perspektive in Bezug auf die Sicherheit in der Informationstechnologie aufweisen, dann reduziert sich der Nutzen für die Unternehmensführung.
- b) Die integrale Perspektive der Unternehmensführung in ihrer Aufgabe bestimmt die Effektivität der Sicherheit in der Informationstechnologie.
- c) Die Risikobetrachtung wirkt als ein verbindendes Element für die effektive Nutzung der Managementkonzepte.

Das erste Ziel der in diesem Buch vorgestellten Untersuchung ist anhand bestehender Literatur die theoretischen Managementkonzepte, Instrumente und Methoden bezüglich der Informationstechnologie und deren Sicherheit als auch deren Einbindung in die Führungsstrukturen- und -prozesse zu untersuchen. Dabei sollen die Zusammenhänge erfasst und analysiert werden. Mit diesen Aktivitäten wird geklärt, was die Literatur zu ausgewählten Themen besagt und wie diese für das Management nutzbar sind.

Weiter soll dieses Buch mittels Analyse der Transformation von Informationen zur Sicherheit mögliche Ursachen und Auswirkungen aufzeigen, mit welchen die Unternehmensführung wie auch die Sicherheitsverantwortlichen in den Fachbereichen während ihrer Aufgaben konfrontiert sind. Es soll, auf einer konzeptionellen Ebene eine strukturierte Sichtweise auf die Abhängigkeit und Interaktion zwischen den wesentlichen Elementen (Risiko, Betrieb, Sicherheit, Governance) darzustellen.

Abgeleitet von den gewonnenen Erkenntnissen sollen Empfehlungen für ein grundsätzliches Konzept beschrieben werden. Bei einer Umsetzung soll dies der Unternehmensleitung ermöglichen, die wesentlichen Bestandteile von Sicherheit im Bereich der Informationstechnologie zu kennen und entsprechende Massnahmen einordnen und beurteilen zu können.

Die Grenzen der Untersuchung beziehen sich auf die oben erwähnten Ziele und die Ausarbeitung von Empfehlungen. Explizit nicht behandelt werden in diesem Buch folgende Punkte:

- Monetäres Bewertungsinstrument für Investitionen im Bereich der Sicherheit
- Bewertung der Methoden und Instrumente
- Gestaltung eines unternehmensübergreifenden Informationssystems

#### **1.4. Vorgehen und Aufbau**

Im ersten Kapitel wird die Forschungsfrage erarbeitet. Dabei werden die Ausgangslage erfasst und die Problematik im Bereich der Informationstechnologie und der Sicherheit wie deren Interaktion mit der Unternehmensführung beschrieben; anschließend wird die Forschungsfrage formuliert.

Im Kapitel zwei werden die theoretischen Grundlagen über Konzepte des Service-, Risiko- und der Sicherheit im Fachbereich der Informationstechnologie (IT), inhaltlich erarbeitet. Dabei werden nach der Definition wichtiger Begriffe auch deren Bedeutungen in der Unternehmung erklärt. Dies bildet die aktuelle Grundlage für die vorliegende Untersuchung. Auf Basis dieser Ausführungen ist es möglich die weiteren Ausführungen, in diesem Buch, nachvollziehen zu können.

Im Kapitel drei werden das Vorgehen und die Durchführung der Untersuchung beschrieben. Dabei werden auch die Unternehmensleitung und deren Verhaltensweise im Umgang mit der IT-Sicherheit und den Risiken beleuchtet. Insbesondere werden die in Kapitel 1.2 dargestellten Praxisprobleme verdeutlicht.

Das vierte Kapitel enthält eine Zusammenfassung der wesentlichen Erkenntnisse, welche das bestehende Wissen ergänzt und leitet daraus Empfehlungen ab und dient als fundierter Ausgangspunkt für weitere Untersuchungen.

Das fünfte Kapitel enthält eine kritische Würdigung der Untersuchung. Der sechste und abschliessende Teil fasst die Untersuchung zusammen und dient dem Ausblick auf weitere Themenbereiche welche es zu klären und zu untersuchen gilt.

Abbildung 2 verdeutlicht die Struktur mit den Schwerpunkten der jeweiligen Kapitel und die Vorgehensweise. Die Gliederung der Unterkapitel wird jeweils zu Beginn der Kapitel erläutert.

Kapitel	Schwerpunkte	Vorgehensweise
1 Einleitung	<ul style="list-style-type: none"> <li>• Ausgangslage</li> <li>• Forschungsfrage</li> <li>• Zielsetzungen und erwartete Ergebnisse</li> </ul>	Erarbeitung der Forschungsfrage
2 Sicherheit der Informationstechnologie und das Einbinden in die Managementperspektive	<ul style="list-style-type: none"> <li>• Unternehmensführung</li> <li>• Managementkonzepte</li> <li>• Technische und organisatorische Aspekte der Sicherheit</li> <li>• Integrale Perspektive</li> </ul>	Erarbeitung der inhaltlichen Grundlagen
3 Theoretische Untersuchung zur Überprüfung der Forschungsfrage	<ul style="list-style-type: none"> <li>• Überlegung bei der Vorbereitung zur Durchführung der Untersuchung</li> <li>• Entwicklung des Wirkungsdiagramm – Sicherheit und Unternehmensführung</li> <li>• Untersuchung der Feedbackschleifen als einen Teil des Wirkungsdiagramm</li> <li>• Reflexion</li> </ul>	<ul style="list-style-type: none"> <li>• Vorbereitung und Durchführung der Untersuchung</li> <li>• Grafische und Deskriptive Beschreibung</li> </ul>
4 Zusammenhänge und Empfehlungen	<ul style="list-style-type: none"> <li>• Verdichtung der Wirkungszusammenhänge</li> <li>• Ableitung von Empfehlungen</li> <li>• Beantwortung der Forschungsfrage</li> </ul>	Erarbeitung von Empfehlung
5 Kritische Würdigung	<ul style="list-style-type: none"> <li>• Hinterfragen der Vorgehensweise und der getroffenen Annahmen.</li> </ul>	Reflexion
6 Schlussbetrachtung und Ausblick	<ul style="list-style-type: none"> <li>• Überblick und Zusammenfassung der Arbeit.</li> </ul>	Zusammenfassung

Abbildung 2: Aufbau und Struktur der vorliegenden Untersuchung  
Quelle: Eigene Darstellung