1 EINLEITUNG

„Natürlich gibt es sie [Budgetplanung], aber sie ist nach meiner beruflichen Erfahrung eine glorreiche Ausnahme! In den meisten Unternehmen läuft es nach dem Motto: "Wenn wir es brauchen, machen wir es".”

- GESCHÄFTSFÜHRER EINES KLEINEN UNTERNEHMENS (s. HEIDT ET AL. 2019, S. 1295)

1.1 Ausgangssituation und Problemstellung

Die zunehmende Digitalisierung und Vernetzung in Unternehmen ermöglichen neue digitale Produkte, Geschäftsmodelle und Prozesse (s. SCHUH ET AL. 2022, S. 3). Eine Großzahl von Unternehmen befindet sich heute in einem fundamentalen Wandel hin zu digital vernetzen Unternehmen der Zukunft, für die die Bedürfnisse ihrer Kunden den Dreh- und Angelpunkt aller Aktivitäten darstellen (s. HOFMANN ET AL. 2020, S. 43) und einen entscheidenden Wettbewerbsvorteil garantieren (s. HICKING ET AL. 2020, S. 5). In der Vergangenheit wurde nur bedingt über Unternehmensgrenzen hinweg gedacht. Heute jedoch sind Unternehmen, die Anwendungsfälle von Industrie 4.0 umsetzen, durch eine stärkere interne und externe Vernetzung geprägt (s. KIESEL ET AL. 2021, S. 442).

Eine nicht beabsichtigte Nebenwirkung dieser Entwicklung stellen die an Anzahl und Intensität zunehmenden Risiken von Cyberkriminalität gegen Unternehmen dar (s. DREIßIGACKER ET AL. 2020, S. 13; s. KLAIBER ET AL. 2017, S. 100; s. LOMEN 2017, S. 113; s. SCHUH ET AL. 2020b, S. 587; BMI 2020, S. 1). In Studien gegen zwar nur rund zwei Drittel (65,0 %) der Unternehmen in Deutschland an, mindestens einmal Opfer eines Cyber-Angriffs gewesen zu sein (s. DREIßIGACKER ET AL. 2020, S. 101f.), allerdings ist hier von einer deutlich höheren Dunkelziffer (sog. Dunkelfeld) auszugehen (s. BUNDESKRIMINALAMT 2022, S. 4). Trotz dieser zahlreichen Vorfälle im industriellen Umfeld treiben diese Unternehmen ihre Digitalisierung und Vernetzung voran. Insbesondere durch die Umsetzung von Industrie 4.0 und dem Voranschreiten der IT/OT-Konvergenz, also der Verschmelzung klassischer *Information Technology* (ERP, CRM, …) mit der produktionsnahen *Operational Technology* (SPS, SCADA, …), entstehen neue Sicherheitsrisiken. (s. MANTRAVADI ET AL. 2020, S. 200305f.; HÄNISCH U. ROGGE 2017, S. 93ff.)

Allein durch die COVID-19-Pandemie konnte im Zeitraum von März bis Mai 2020 eine Steigerung von Scam- und Malware-Angriffen um 600 % registriert werden. Angreifer nutzten dazu die Unsicherheit der betroffenen Personen aus. (s. GALLAGHER U. BRANDT 2020)

Google bestätigte, im April 2020 täglich schätzungsweise rund 18 Millionen schadhafte E-Mails an Unternehmen mit Bezug zu COVID-19 geblockt zu haben (s. KUMARAN U. LUGANI 2020). Dies bekräftigt die Wichtigkeit, die Kontrolle über Informationen und die Absicherung wichtiger Infrastruktur sicherzustellen (s. LALLIE ET AL. 2020b, S. 13).

Die steigende Anzahl der Cyber-Angriffe spiegelt allerdings nur die externe Betrachtung wider. Eine interne Betrachtung in den Unternehmen offenbart große Missstände im Umgang mit dem Management der Informationssicherheit, um den Cyber-Angriffen zu begegnen (s. ALI ET AL. 2021, S. 2f.; HEIDT ET AL. 2019, S. 1289). Produzierenden und insbesondere kleinen und mittleren Unternehmen (KMU) fehlt es häufig zum einen an dem Bewusstsein, dass Informationssicherheit entscheidend für das Bestehen des Unternehmens sein kann (s. OZKAN U. SPRUIT 2019, S. 61). Zum anderen mangelt es häufig schlicht an Know-how und Budget, um die relevanten technischen, organisatorischen und kulturellen bzw. personellen Maßnahmen

auszuwählen, priorisieren und umzusetzen sowie ihre Wirkungszusammenhänge zu kennen und zu verstehen (s. MÜLLER 2018, S. 204ff.). Zwar ist erkennbar, dass dem Thema managementseitig immer mehr Aufmerksamkeit geschenkt wird, es mangelt aber häufig an ganzheitlichen Herangehensweisen (s. DONG ET AL. 2021, S. 6; HASAN ET AL. 2021, S. 11; OZKAN U. SPRUIT 2019, S. 61; vgl. MÜLLER 2018, S. 17; GERCKE 2017, S. 31f.).

> *„Wenn Sie mit Ihrer Cybersicherheit langsam vorankommen, bewegen Sie sich relativ gesehen rückwärts“.* (s. KANNUS U. MELLIN 2018, S. 8)

Sofern diese offenkundigen Missstände in Unternehmen nicht behoben werden, ist davon auszugehen, dass jene Unternehmen erhöhten Risiken ausgesetzt sein werden. Denn unbekannte Sicherheitslücken machen es einfach, Systeme zu kompromittieren. (s. GOELZ 2021)

Eine steigende IT-Komplexität, die zunehmende Anbindung von Maschinen und Anlagen, deren stärkere Vernetzung, neue Verbindungen und Schnittstellen und der Einsatz von Datenplattformen eröffnen zusätzliche Problemfelder (s. HOFFMANN 2018, S. 1ff.). Insbesondere prototypische Umsetzungen in Industrie-4.0-Umgebungen, sogenannte Piloten, erweisen sich häufig als unsicher, werden allerdings erst dann abgesichert, wenn Schwachstellen bereits zu Problemen geführt haben (s. TIEDEMANN 2021, S. 86). Schwachstellen in solchen Umgebungen ermitteln und kontinuierlich evaluieren zu können, ist für viele KMU eine große Herausforderung, die sie häufig nicht allein bewältigen können (s. HEUTMANN ET AL. 2021, S. 180). Ebenso kritisch zu betrachten ist der Umgang mit Informationssicherheitsmaßnahmen, die die identifizierten Schwachstellen adressieren sollen. Da Wirkungszusammenhänge zwischen Schwachstellen und Maßnahmen ohne tiefgreifendes Know-how nicht erklärt werden können (s. ABOLHASSAN 2017a, S. 130), werden Maßnahmen nur unzureichend umgesetzt oder sind gar überdimensioniert (s. BSI 2021a, S. 48).

KMU stehen vor der zusätzlichen Herausforderung, dass ihre Nachfrage nicht durch die marktseitigen Angebote gedeckt wird (s. JOHANNSEN U. KANT 2020, S. 1061). Es existieren zwar zahlreiche Standards, wie etwa der BSI-IT-Grundschutz oder die ISO/IEC 27001, diese verfehlen allerdings die realen Herausforderungen, die sich bspw. durch limitierte Ressourcen ergeben, und zeigen darüber hinaus keinen konkreten Handlungspfad zur Absicherung des Unternehmens auf (s. HEIDT ET AL. 2019, S. 1299; WIESNER 2019, S. 1). Der erforderliche Aufwand zur Umsetzung eines solches Standards ist für KMU nicht zu rechtfertigen (s. Abbildung 1-1). Zusätzlich sollen Informationssicherheitsmanagementsysteme (ISMS) bei der unternehmensspezifischen Bestimmung und Realisierung der Ziel-Informationssicherheit unterstützen, fokussieren aber nur selten ihre Praxistauglichkeit (s. ANTUNES ET AL. 2021, S. 222f.; MÜLLER 2018, S. 17). Konkret bedeutet dies, dass KMU heute nicht dabei unterstützt werden, spezifisch und ohne Vorwissen kritische Schwachstellen auf Basis ihrer Gegebenheiten abzuleiten und dafür geeignete Gegenmaßnahmen effizient zu bestimmen (s. ENGLÄNDER U. HEIMES 2020, S. 49). Laut GAYCKEN U. HUGHES wird sich diese Situation in absehbarer Zeit nicht verbessern (s. GAYCKEN ET AL. 2015, S. 2). Darüber hinaus lassen sich viele bestehende Ansätze durch übermäßige Technologiefokussierung, unzureichende Standardisierung und fehlende Lebenszyklusorientierung charakterisieren (s. MÜLLER 2018, S. 17ff.). Auf der anderen Seite schaffen Ansätze wie die Umsetzung von Top-10-Maßnahmen basierend auf Umfragen oder die Ad-hoc-Umsetzung von Maßnahmen ohne strategische und systematische

Verankerung kein ausreichendes Sicherheitslevel. Das in dieser Arbeit entwickelte Vorgehensmodell zur Umsetzung eines Informationssicherheitsmanagementsystems positioniert sich daher zwischen diesen beiden Extremen aus Aufwand und erreichbarem Sicherheitslevel[1].

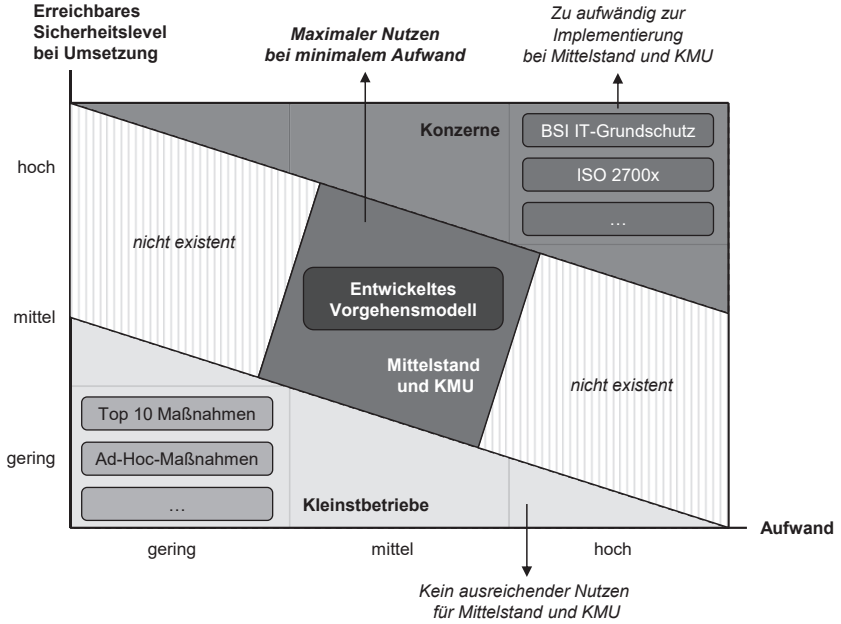


Abbildung 1-1: Positionierung des entwickelten Vorgehensmodells in Bezug auf Aufwand und erreichbares Sicherheitslevel (eigene Darstellung)

Es bleibt festzuhalten, dass KMU und der Mittelstand beim Management ihrer Informationssicherheit unterstützt werden müssen. Es mangelt an anwendbaren Vorgehensmodellen zur Bestimmung der unternehmensspezifischen Informationssicherheit, der Bestimmung von Schwachstellen und dem Ableiten notwendiger Gegenmaßnahmen. Für die Erhöhung der Informationssicherheit bedarf es daher einer effizienten und pragmatischen Herangehensweise hinsichtlich des Umgangs mit Informationssicherheit.

1.2 Zielsetzung und Forschungsfrage

Die vorlegende Untersuchung adressiert die Lösungsfindung der zuvor geschilderten Problemstellung. Sie dient dem Ziel, den Umgang mit Informationssicherheit in KMU auch ohne tiefgreifendes fachliches Know-how und mit beschränkten Ressourcen zu verbessern. Der Nutzen ergibt sich aus der Unterstützung bei der Erkennung von Implikationen relevanter Informationssicherheitsaspekte durch die Einführung von Industrie-4.0-Umgebungen und der

[1] Eine detaillierte Betrachtung der zugrundeliegenden Anforderungen an eine effiziente und pragmatische Herangehensweise findet sich in Kapitel 3.5.2

Schaffung einer besseren Argumentationsgrundlage zur Einführung notwendiger Maßnahmen gegenüber der Geschäftsführung. Das Ergebnis der Dissertationsschrift stellt ein (1) Gestaltungs- bzw. Vorgehensmodell dar, welches es KMU ermöglicht, (2) eine effiziente Bestimmung relevanter Bedrohungen und Schwachstellen auf Basis ihrer Industrie-4.0-Umgebung durchzuführen und (3) passende Maßnahmen abzuleiten. Dazu dient (4) die Erklärung von Wirkungszusammenhängen, die zusätzlich dem Aufbau von Wissen in den anwendenden KMU zugutekommt. Der Adressatenkreis umfasst IT-Leiter bzw. Verantwortliche für Informationssicherheit, die IT-Abteilung im Unternehmen sowie die Leitung der Produktion und der Digitalisierung. Der Neuheitsgrad besteht in der Entwicklung eines Vorgehensmodells zum effizienten und pragmatischen Aufbau eines Informationssicherheitsmanagementsystems und der Befähigung zur eigenständigen Identifikation von Schwachstellen und Maßnahmen durch KMU.

Aus den geschilderten Problemstellungen sowie der Zielsetzung des Dissertationsvorhabens ergibt sich folgende Forschungsfrage:

> *„Wie kann ein Gestaltungsmodell zur effizienten Absicherung der Informationssicherheit für Industrie-4.0-Umgebungen in produzierenden Unternehmen ermittelt werden?“*

Zur Beantwortung werden die folgenden Forschungsunterfragen beantwortet:

- *Wie können Industrie-4.0-Umgebungen produzierender Unternehmen vor dem Hintergrund ihrer Informationssicherheitsschwachstellen beschrieben werden?*
- *Wie lassen sich die relevantesten Maßnahmen zur Informationssicherheit im Kontext produzierender Unternehmen ermitteln und beschreiben?*
- *Welche Wirkungszusammenhänge lassen sich für die identifizierten Schwachstellen und ermittelten Maßnahmen erklären?*
- *Wie lässt sich auf Basis der identifizierten Wirkungszusammenhänge ein Gestaltungsmodell für ein ISMS zur effizienten Ermittlung der notwendigen Informationssicherheit in produzierenden Unternehmen ermitteln?*

1.3 Wissenschaftlicher Bezugsrahmen

Der wissenschaftliche Bezugsrahmen der vorliegenden Untersuchung lässt sich auf Basis der zuvor beschriebenen Zielsetzung herleiten. Dazu erfolgt die wissenschaftstheoretische Einordnung in Anlehnung an die von ULLRICH U. HILL aufgezeigte Unterscheidung, da sich diese durchgesetzt hat, obwohl eine einheitliche und allgemeingültige Erklärung der Zusammenhänge nicht existiert (s. ZELEWSKI 2008, S. 3) und erst diese Einordnung eine spezifische Bearbeitung des Themas erlaubt (s. ULRICH U. HILL 1976a, S. 304).

Grundsätzlich lässt sich die Wissenschaftstheorie in die metaphysischen Wissenschaften (Theologie und Teile der Philosophie) sowie die nicht-metaphysischen Wissenschaften unterteilen (s. WEBER ET AL. 2018, S. 24). Ferner lässt sich die nicht-metaphysische Wissenschaft in Formal-, Struktur- und Realwissenschaften unterteilen. Wo die Formalwissenschaften die Konstruktion wissenschaftlicher Sprachsysteme sowie der Sprache und Zeichen als solche behandelt, um so logische Vorgehensweisen zu beschreiben (s. ULRICH U. HILL 1976a, S. 305), ohne Anspruch auf Realitätsbezug zu besitzen und nur auf ihre „*logische Wahrheit [hin] überprüfbar [zu] sein*“ (s. ZELEWSKI 2008, S. 3), befassen sich die Strukturwissenschaften mit Strukturen realer und formaler Objekte, wie beispielsweise die System- und Problemtheorie. Letztlich haben Realwissenschaften die „*Beschaffenheit der realen Welt zum Gegenstand*“ (s. HELFRICH 2016, S. 5). Das bedeutet, dass die Aussagen faktisch prüfbar sind, wofür häufig

Formalwissenschaften, insbesondere die Mathematik, herangezogen werden (s. WEBER ET AL. 2018, S. 24). Im allgemeinen Sprachgebrauch werden Formalwissenschaften als „analytische Wissenschaften“ und Realwissenschaften als „Erfahrungswissenschaften“ bezeichnet (s. HELFRICH 2016, S. 4f.).

Die Realwissenschaften lassen sich weiterhin hinsichtlich ihres Wissenschaftsziels unterscheiden. Die Grundlagenwissenschaften verfolgen ein theoretisches, die angewandten Handlungswissenschaften ein pragmatisches Wissenschaftsziel. Ferner unterscheiden sich also die Aufgaben der Wissenschaften durch die Erforschung empirischer Wirklichkeitsausschnitte, wie in den Naturwissenschaften, sowie durch die Analyse menschlicher Handlungsalternativen, wie in den Kultur-, Geistes- und Sozialwissenschaften. (s. ULRICH U. HILL 1976a, S. 305; WEBER ET AL. 2018, S. 24f.; HELFRICH 2016, S. 4f.)

Die Realwissenschaften umfassen die Bildung von Beschreibungs-, Erklärungs- und Gestaltungsmodellen, die im vorliegenden Dissertationsvorhaben Anwendung finden werden. Des Weiteren dient die Untersuchung der Bearbeitung interdisziplinärer Fragestellungen und berührt daher die Ingenieurwissenschaften, die Betriebswirtschaftslehre und die Wirtschaftsinformatik. Durch ihr pragmatisches Wissenschaftsziel lassen sich sowohl die Ingenieurwissenschaften, die technisch orientierte Objekte untersuchen, als auch die Betriebswirtschaftslehre, die die Modellbildung anwendungsorientierter Handlungsempfehlungen verfolgt, in die angewandten Handlungswissenschaften einordnen (s. ULRICH U. HILL 1976a, S. 305; HELFRICH 2016, S. 6f.). Auch, wenn allgemein die Auffassung vertreten wird, dass die Wirtschaftsinformatik eine eigenständige und interdisziplinäre Wissenschaft darstellt (s. WEBER ET AL. 2018, S. 489), lässt sie sich aufgrund der Kombination aus Betriebswirtschaftslehre und Informatik sowie ihres pragmatischen Wissenschaftsziels ebenfalls den angewandten Handlungswissenschaften zuordnen (s. LEHNER ET AL. 2008, S. 17ff.; DEINDL 2013a, S. 5).

Die beschriebene Systematik sowie die Einordnung der vorliegenden Untersuchung werden zusammenfassend in Abbildung 1-2 illustriert. Da die Zielsetzung dieses Dissertationsvorhabens die Entwicklung eines Gestaltungsmodells und somit von Handlungsempfehlungen umfasst, ist sie den angewandten Handlungswissenschaften zuzuordnen. Genauer werden durch die Beschreibung von Industrie-4.0-Umgebungen mitsamt ihrer Komponenten und Informationssystemen, die Ermittlung ihrer relevanten Schwachstellen und die Ableitung relevanter Informationssicherheitsmaßnahmen unter Berücksichtigung betriebswirtschaftlicher Aspekte alle drei genannten Disziplinen behandelt.

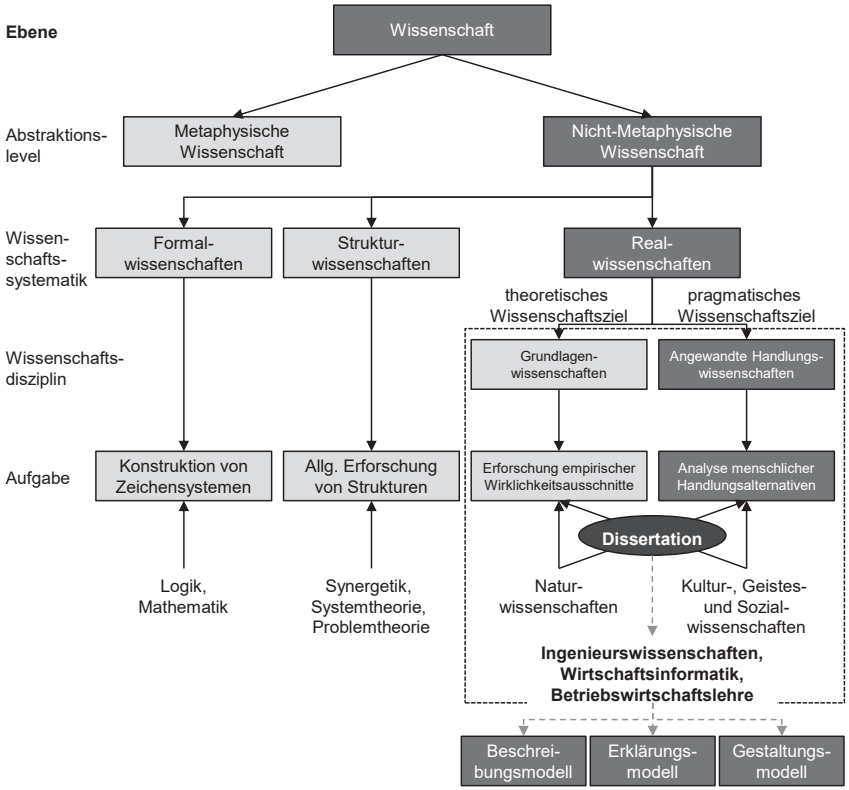


Abbildung 1-2: Wissenschaftssystematik (eigene Darstellung i. A. a. ULRICH U. HILL 1976a, S. 305; WILDE U. HESS 2007, S. 280; DEINDL 2013a, S. 6; WEBER ET AL. 2018, S. 24; ZELLER 2018, S. 9)

1.4 Forschungskonzeption

Zur Lösung der in Kapitel 1.1 und 1.2 skizzierten Problemstellung wird die Forschungskonzeption vor dem Hintergrund des pragmatischen Wissenschaftsziels ausgewählt. Die Forschungslogik ergibt sich dabei aus der Zuordnung zu diesem Wissenschaftsziel. Das pragmatische Wissenschaftsziel entspricht einer *operationsanalytischen Forschungslogik*, im Vergleich zum theoretischen Wissenschaftsziel mit *realanalytischer Wissenschaftskonzeption*. Während bei der operationsanalytischen Forschungslogik Begründungszusammenhänge auf Basis von Ziel-Mittel-Beziehungen gesucht werden, die ihrerseits auf den Ergebnissen der realanalytischen Forschungslogik aufgebaut werden können, wird in jener Grundlagenwissen entwickelt, um bestimmte Beobachtungen und Ereignisse erklären zu können. Deswegen sind beide Konstrukte als ergänzend und nicht als subsituierend zu verstehen. (s. HILL ET AL. 1994, S. 34f.; OEDEKOVEN 2011, S. 6)

Neben der Einordnung der Forschungslogik existieren verschiedene Ansätze, welche die Zielerreichung und den Erkenntnisprozess unterstützen bzw. sicherstellen sollen. Grundsätzlich

kann hier zwischen einem *induktiv-empirischen* und einem *deduktiv-theoriekritischen Erkenntnisweg* unterschieden werden (s. BORCHERT ET AL. 2004, S. 2). Die Induktion[2] beschreibt den Ansatz, bei dem spezielle Beobachtungen verallgemeinert werden und so eine allgemeingültige Theorie ergeben. Diese Aussage wird meist auf die Aussage von ARISTOTELES zurückgeführt, für den die Induktion „das Schließen vom Besonderen auf das Allgemeine zum Zweck des Erkenntnisgewinns" bedeutet (s. ESSLER 1973, S. 10).

Aufgrund des allgemein bekannten Problems der Induktion, dass eine grundsätzliche Anspruchsgrundlage fehlt, um spezielle Gegebenheiten, seien es noch so große empirische Studien, zu einem allgemeingültigen Umstand abstrahieren zu können, gilt dieser nur, solange sie falsifiziert worden ist. Somit handelt es sich in den Realwissenschaften um eine beschränkte Induktion mit Falsifikation (s. OEDEKOVEN 2011, S. 6; BORCHERT ET AL. 2004, S. 10f.).

Die Deduktion[3] hingegen leitet aus allgemeingültigen Theorien spezielles Wissen ab. Im Gegensatz zur Induktion steht der Beobachter einer Theorie kritisch gegenüber (s. POPPER 1935, S. 5) und nutzt seine Erfahrungen nicht als Baustein, sondern als Prüfstein (s. BORCHERT ET AL. 2004, S. 12). Als Nachteil der Deduktion ergibt sich die Tatsache, dass sich Experimente zur Verifikation aufgestellter Hypothesen gegebenenfalls als ungeeignet herausstellen und somit zu falschen Schlussfolgerungen führen können (s. BORCHERT ET AL. 2004, S. 12).

Da das vorliegende Dissertationsvorhaben sowohl auf empirisch-induktive (Aufbau der Beschreibungsmodelle) als auch auf analytisch-deduktive (Herleitung des Erklärungsmodells und Konstruktion des Gestaltungsmodells) Forschungsaktivitäten zurückgreift, wird der systemtheoretische Ansatz nach ULRICH gewählt (s. ULRICH U. HILL 1976a, S. 308f.). Dieser widmet sich sowohl der Theorie als auch der Praxis, ist durch seinen interdisziplinären Ansatz sowie seine Offenheit charakterisiert und wird um terminologisch-deskriptive Forschungsaktivitäten ergänzt, um ein einheitliches Begriffsverständnis der zu beschreibenden Objekte zu schaffen (s. ULRICH U. HILL 1976b, S. 347f.). Die Vorteile des systemtheoretischen Ansatzes nach ULRICH lassen sich wie folgt durch drei Funktionen zusammenfassen (s. ULRICH U. HILL 1976a, S. 308):

- Terminologische Funktion: Zurverfügungstellung eines abstrakten und interdisziplinären Begriffssystems, welches nicht durch Vorurteile oder A-priori-Annahmen über die Wirklichkeit geprägt ist.
- Heuristische Funktion: Zurverfügungstellung von Strukturelementen, die eine Entdeckung neuer Aspekte und Zusammenhänge ermöglicht.
- Integrationsfunktion: Integration verschiedenster Einflussfaktoren und Variablen aus verschiedenen Disziplinen.

Der Forschungsprozess wird im Rahmen dieses Dissertationsvorhabens als iterativer Lernprozess (s. KUBICEK 1976, S. 14) ausgelegt (s. Abbildung 1-3). Hinter diesem liegt das Prinzip des wachsenden Verständnisses der Realität von KUBICEK. Den Ausgangspunkt stellt die Bildung eines Begriffssystems dar. Dazu dienen persönliche Erfahrungen des Autors sowie sein theoretisches Vorwissen, erworben durch die Mitarbeit und Leitung einer Vielzahl von Forschungs- und Beratungsprojekten im Bereich Informationsmanagement des FIR an der RWTH Aachen. Ergänzt werden diese beiden Aspekte um die strukturierte Literaturanalyse (auch

---

[2] Wortzusammensetzung aus den lateinischen Begriffen *inductivus* = „zur Annahme geeignet, zur Voraussetzung geeignet" und *inducere* = „hinführen" (s. BORCHERT ET AL. 2004, S. 10).
[3] Vom lateinischen *deductio* = „Hinführung, Weiterführung" (s. BORCHERT ET AL. 2004, S. 12).

Desk-Research genannt, s. Kapitel 5.2.1) zu vorhandenen Quellen des Themengebiets (s. DÜNNEBACKE 2016, S. 13). Der Erkenntnisgewinn speist sich dabei aus der Sammlung von Daten, dem ein Realisierungsversuch und eine Realitätsanalyse vorausgeht. Die Durchführung von Interviews, Gesprächen, Diskussionen und Workshops mit Experten und die Anwendung in Forschungs- und Beratungsprojekten dient der ständigen Entwicklung und Überprüfung des Vorgehens.

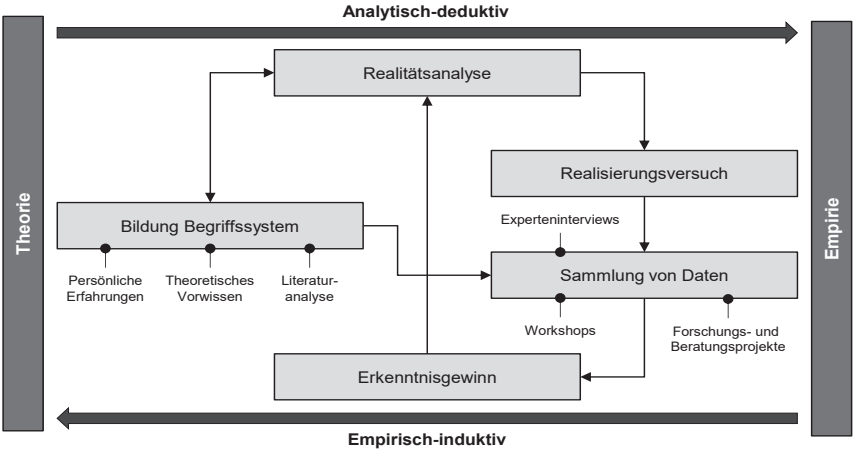
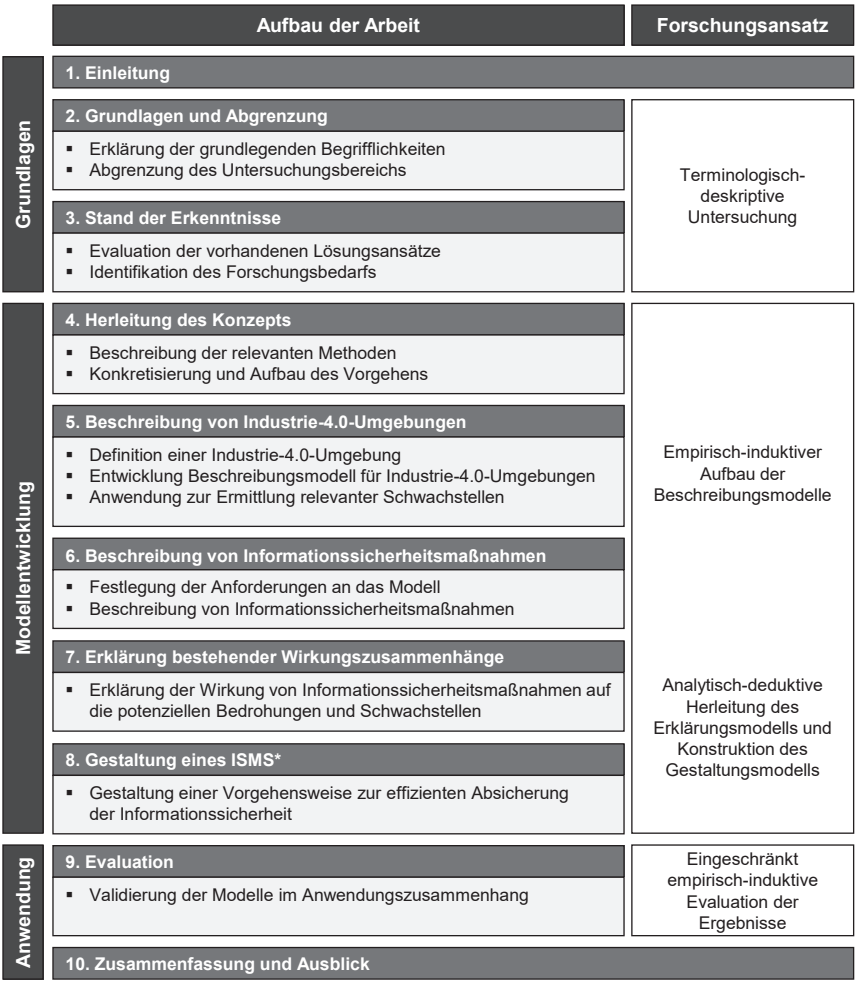


Abbildung 1-3: Forschungsprozess (eigene Darstellung i. A. a. ULRICH U. HILL 1976b, S. 348; KUBICEK 1976, S. 14ff.; NIENKE 2018, S. 11)

Die vorliegende Dissertationsschrift bildet den durchgeführten und zu einem gewissen Punkt festgehaltenen Forschungsprozess ab. Sie stellt durch die enge Verknüpfung von Theorie und Empirie einen Ansatz zur partizipativen Aktionsforschung dar (s. WILDE U. HESS 2007, S. 282).

1.5 Aufbau der Untersuchung

Es lässt sich festhalten, dass die vorliegende Dissertationsschrift das Ziel verfolgt, ein Vorgehensmodell zum effizienten Umgang mit Informationssicherheit zu entwickeln. Sie ist den angewandten Handlungswissenschaften zuzuordnen und baut insbesondere auf den Erkenntnissen von ULLRICH U. HILL auf. Der Aufbau (s. Abbildung 1-4) orientiert sich an dem verbreiteten Vorgehen bei angewandten Wissenschaften nach LEHNER ET AL. und ULRICH (s. LEHNER ET AL. 2008, S. 23; ULRICH 1981, S. 20).



*ISMS: Informationssicherheitsmanagementsystem

Abbildung 1-4: Aufbau der Untersuchung und angewendete Forschungsaktivitäten (eigene Darstellung)

Abbildung 1-4 kann entnommen werden, dass sich die Untersuchung in 10 Kapitel unterteilt, die im Folgenden kurz dargestellt und hinsichtlich ihrer angewendeten Forschungsansätze eingeordnet werden.

Kapitel 1 leitet in die Untersuchung ein. Die Ausgangssituation stellt als praktische Problemstellung den Rahmen einer angewandten Wissenschaft dar. Die beschriebene Zielsetzung mit ihren Forschungsfragen dient in der vorliegenden Untersuchung als Lösungsansatz. Diese wurden zunächst auf Basis von Projekterfahrungen identifiziert und im späteren Verlauf als

Vorbereitung auf das Dissertationsvorhaben mit Experten und durch Nutzung bestehender Literaturquellen reflektiert sowie auf eine für den Untersuchungsbereich allgemeingültige Problemstellung abstrahiert.

Kapitel 2 dient der Schaffung eines einheitlichen Verständnisses der verwendeten Begrifflichkeiten und stellt demgemäß eine terminologisch-deskriptive Tätigkeit dar. Gerade in den Bereichen der Industrie 4.0 und der Informationssicherheit ist ein einheitliches Verständnis nicht immer gegeben, da für beide Begrifflichkeiten die unterschiedlichsten Definitionen existieren. Diese Tatsache wird noch verstärkt, wenn deutsche und angelsächsische Definitionen voneinander abgegrenzt werden müssen. Schließlich wird der Untersuchungsbereich in Kapitel 2 abgegrenzt. Ferner behandelt Kapitel 3 den Stand der Technik in Form der Beschreibung von Industrie-4.0-Umgebungen, der Identifikation von sicherheitskritischen Schwachstellen und der Beschreibung von Informationssicherheitsmaßnahmen. Das Kapitel dient der Evaluation bestehender Lösungsansätze in Bezug auf die aufgezeigte Problem- und Zielstellung. Daraus leiten sich die Forschungslücke, der spezifische Forschungsbedarf sowie konkrete Anforderungen ab, die einen Einfluss auf die Entwicklung des Gestaltungsmodells hat. Hier wird ebenfalls ein terminologisch-deskriptiver Ansatz gewählt.

In Kapitel 4 werden relevante Methoden vorgestellt, die im Rahmen der Untersuchung zur Problemlösung verwendet werden. Weiterhin werden der konkretisierte Aufbau der Untersuchung und die Vorgehensweise erläutert. Die Anwendung der Methoden führt in Kapitel 5 zur Beschreibung von Industrie-4.0-Umgebungen und zeigt relevante Bedrohungen und Schwachstellen auf, die sich durch deren Umsetzung ergeben. Die Modellentwicklung erfolgt empirisch-induktiv. Kapitel 6 wiederum widmet sich der Festlegung von Anforderungen an das und die Entwicklung des Beschreibungsmodells für Informationssicherheitsmaßnahmen und folgt ebenfalls einem empirisch-induktiven Ansatz.

Die Herleitung zur Erklärung von Wirkungszusammenhängen zwischen Informationssicherheitsmaßnahmen und potenziellen Schwachstellen in Industrie-4.0-Umgebungen erfolgt analytisch-deduktiv in Kapitel 7. In Kapitel 8 wird das Gestaltungsmodell zur effizienten Absicherung der Informationssicherheit ebenfalls analytisch-deduktiv konstruiert. Die Evaluation der entwickelten Modelle im Anwendungszusammenhang in Kapitel 9 erfolgt, wie im Vorfeld beschrieben, eingeschränkt empirisch-deduktiv durch Expertengespräche.

In Kapitel 10 werden die Ergebnisse der Untersuchung kritisch reflektiert und zusammengefasst. Abschließend wird ein Ausblick auf den weiteren Forschungsbedarf gegeben.