FH CAMPUS WIEN
UNIVERSITY OF APPLIED SCIENCES

> RISIKO- UND SICHERHEITSMANAGEMENT

Wirtschaftsschutz

Durchführung eines systematischen Reviews im Bereich Wirtschaftsschutz

MASTERARBEIT

zur Erlangung des akademischen Grades

Master of Arts (MA)

der Fachhochschule Campus Wien

im Rahmen des Studiums

Risk Management and Corporate Security

eingereicht von

Philipp Reschl, MSc

1410645019

betreut durch:

FH-Prof. Dipl.-Inform. Timo Kob

Justina Kaiser, MA

Wien, am 20.12.2016

Erklärung zur Verfassung der Arbeit

Hiermit erkläre ich, dass ich diese Arbeit selbstständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Ort, Datum	Philipp Reschl, MSc

Danksagung

Nach intensiven Jahren des Studiums bildet die Masterarbeit den gebührenden Abschluss. Deshalb möchte ich mich an dieser Stelle bei allen Menschen, die mich auf diesem Weg begleitet und unterstützt haben, bedanken.

An erster Stelle möchte ich meinem Betreuerteam, Justina Kaiser (MA) und FH-Prof. Dipl.-Inform. Timo Kob, für die wertvolle Unterstützung bei der Anfertigung der Masterarbeit danken. Vor allem die Hinweise auf Aspekte und Blickwinkel, die ich in dieser Form zuvor noch nicht kannte, haben mir geholfen.

Mein besonderer Dank gilt meiner Familie, vor allem meiner Mutter und ihrem Partner, die mich stets unterstützt und motiviert haben. Meiner Freundin danke ich besonders für den starken emotionalen Rückhalt über die Dauer meines gesamten Studiums. Ohne eure Unterstützung wären für mich das Studium und die Masterarbeit nicht möglich gewesen.

Kurzfassung

Kontext und Fragestellung

Aufgrund der steigenden medialen Beachtung des Themas Sicherheit im Allgemeinen, vor allem auch im digitalen Zeitalter, wächst auch im gleichen Ausmaß die Frage nach den zugrundeliegenden Angriffen, die auf Unternehmen abzielen. Diese Situation befördert jährlich neue Studien rund um den Themenkomplex Wirtschafts- und Industriespionage in die Öffentlichkeit. Dabei wird des Öfteren der finanzielle Schaden für die Wirtschaft medienwirksam diskutiert, welcher demnach alleine im deutschsprachigen Raum mehrere Milliarden Euro übersteigen soll.

Ziele der Arbeit

Das Ziel der vorliegenden Arbeit ist festzustellen, inwiefern die einzelnen Erkenntnisse aus diesen Studien überhaupt den Informationsbedarf der potenziell betroffenen Unternehmen decken.

Theorie

Um die relevanten Studien auswählen und auswerten zu können, wird ein systematisches Review herangezogen. Dabei werden die Auswahlkriterien für die Studien erarbeitet und transparent dargestellt. Außerdem werden die Schwerpunkte, Gemeinsamkeiten und Unterschiede der Studien identifiziert und genauer betrachtet. Zusätzlich wird der Aspekt der Hell- und Dunkelfeldforschung beleuchtet, um die in den Medien berichtete Schadenssummen und Auswirkungen angemessen bewerten zu können.

Wissenschaftliche Methoden

Im Rahmen eines systematischen Reviews werden anhand zuvor definierter Kriterien Studien ausgewählt und analysiert. Die anschließende Aufarbeitung der Themenschwerpunkte dieser Studien, vor allem der Gemeinsamkeiten und Unterschiede, schafft einen Überblick zum aktuellen Forschungsstand. Dabei werden jene Schwerpunkte identifiziert und analysiert, welche bisher in den Studien näher betrachtet wurden.

Basierend darauf werden Leitfadeninterviews mit Expertinnen und Experten aus der Praxis durchgeführt, welche beruflich mit den Herausforderungen der Wirtschafts- und Industriespionage laufend konfrontiert sind. Damit wird die Relevanz der Erkenntnisse aus den Studien in der Praxis überprüft.

Ergebnisse

Die identifizierten Gemeinsamkeiten und Unterschiede der Studien haben in der Praxis eine hohe Relevanz. Die Informationen zu Maßnahmen der technischen und physischen Sicherheit von Organisationen sind ausreichend abgedeckt. Gleichermaßen werden auch einzelne Aspekte von Expertinnen und Experten genannt, die in den Studien nur rudimentär abgehandelt werden.

Abstract

Context of the Thesis

Owing to the fact, that security is receiving more media attention since the past years, the question arises about the rationale behind those attacks. Every year new studies about industrial and economic espionage are published, whereby most of them take into account the immediate financial loss from an incident of espionage. The financial damage in German-speaking countries alone is about several billion Euros. But there is no evidence so far, that the published information in those studies meets the needs of the concerned companies.

Goal of the Thesis

The goal of the thesis at hand is to point out, which information in the studies of industrial and economic espionage is helpful for companies.

Theory

Based on a systematic review, studies about industrial and economic espionage of companies in German-speaking countries will be analyzed. Especially the similarities and differences will be discussed. Additionally, the aspects of the dark field research will be highlighted.

Based on these findings, a guided interview will be done with experts from companies, to check if the results are helpful for the daily business.

Methodology

The criteria for choosing those studies will be made, to select the relevant ones and analyze those using a systematic review. Afterwards, the identified emphases, especially focusing on the commonalities and distinctions of the studies, will provide a structured overview about the state of research.

Based on these findings, experts in the field of industrial and economic espionage and the proper counter measures will be consulted, using a guide interview of security experts. The interviews will include the key findings of the

analyzed studies. By following this course of action, the pertinence of the information will be checked for the needs of the relevant companies.

Results

The identified emphases of the studies are quite helpful in practice for companies. Especially the aspects of the technical and physical security of companies are mostly covered. A few other security aspects have been discussed isolated with security experts, whereby just a few studies cover these aspects.

Inhaltsverzeichnis

1 EINLEITUNG 15

1.1 HINTERGRUND UND PROBLEMSTELLUNG 15
1.2 INNOVATIONSGEHALT 17
1.3 STAND DER FORSCHUNG 18
1.3.1 Phänomenologie Wirtschafts- und Industriespionage 19
1.3.2 Betrachtete Studien 20
1.4 FORSCHUNGSFRAGE UND HYPOTHESE 29
1.5 ZIELSETZUNG UND ABGRENZUNG 30
1.6 AUFBAU DER ARBEIT 31
1.7 GENDER-ASPEKT 31
1.8 GESELLSCHAFTS- UND UMWELTASPEKTE 32

2 THEORETISCHER TEIL 35

2.1 BEGRIFFSDEFINITIONEN 35
2.2 THEORIE 38
2.2.1 Systematische Übersichtsarbeit 38
2.2.2 Grenzen der systematischen Übersichtsarbeit und Kritik 40
2.2.3 Hell- und Dunkelfeldforschung 42

3 ANWENDUNG DER THEORIE AUF DIE FORSCHUNGSFRAGE 45

3.1 ALLGEMEINES UND RAHMENBEDINGUNGEN ZU DER ANWENDBARKEIT DER THEORIE AUF DIE FORSCHUNGSFRAGE 45
3.2 AUSWAHLKRITERIEN FÜR DIE BETRACHTETEN STUDIEN 45
3.3 GEMEINSAMKEITEN UND UNTERSCHIEDE DER BETRACHTETEN STUDIEN 47

4 EMPIRISCHER TEIL 55

4.1 FORSCHUNGSFRAGE UND HYPOTHESE 55
4.2 FORSCHUNGSDESIGN 56
4.2.1 Grundlegende Entscheidungen für eine qualitative Forschung 57
4.2.2 Verfahren und Messmethode 58
4.3 OPERATIONALISIERUNG 64
4.4 GESTALTUNG UND ANPASSUNG DES INTERVIEWLEITFADENS 66
4.5 DURCHFÜHRUNG DER ERHEBUNG 67
4.5.1 Auswahlkriterien und Rahmenbedingungen für die Experteninterviews 67
4.6 ERGEBNISSE 69
4.6.1 Anwendung der qualitativen Inhaltsanalyse 69
4.6.2 Ergebnisse der Experteninterviews 70
4.6.3 Beurteilung der Hypothese 74
4.7 ZUSAMMENFASSUNG UND INTERPRETATION 75

5 CONCLUSIO 79

5.1 FAZIT 79

5.2 KRITISCHE REFLEXION DES FORSCHUNGSVORHABENS 81
5.2.1 Einhaltung qualitativer Gütekriterien 81
5.3 AUSBLICK UND KÜNFTIGER FORSCHUNGSBEDARF 83

BIBLIOGRAPHIE 87

ABBILDUNGSVERZEICHNIS 91

TABELLENVERZEICHNIS 93

ANHANG A: AUSWERTETABELLE DER SYSTEMATISCHEN ÜBERSICHTSARBEIT DER BETRACHTETEN STUDIEN 95

ANHANG B: EMPIRISCHE DATENERHEBUNG UND INTERVIEWLEITFADEN FÜR DIE EXPERTENINTERVIEWS 97

ANHANG C: AUSWERTETABELLE DER QUALITATIVEN INHALTSANALYSE DER INTERVIEWS 103

Abkürzungsverzeichnis

AT	Österreich
BCM	Business Continuity Management
BDI	Bundesverband der Deutschen Industrie
Bitkom	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
CH	Schweiz
DACH	Deutschland, Österreich und Schweiz
DE	Deutschland
DIHK	Deutscher Industrie- und Handelskammertag
e.V.	eingetragener Verein
GI	Gesellschaft für Informatik e.V.
GmbH	Gesellschaft mit beschränkter Haftung
IEC	International Electrotechnical Commission
ISMS	Informationssicherheitsmanagementsystem
ISO	International Organization for Standardization
IT	Informationstechnologie
MA	Mitarbeiterinnen und Mitarbeiter
VDMA	Verband Deutscher Maschinen- und Anlagenbau
VOICE	Verband der IT-Anwender e.V.
WIS	Wirtschafts- und Industriespionage
ZVEI	Zentralverband Elektrotechnik- und Elektronikindustrie

1 Einleitung

Inhalt

1.1	Hintergrund und Problemstellung	15
1.2	Innovationsgehalt	17
1.3	Stand der Forschung	18
1.3.1	Phänomenologie Wirtschafts- und Industriespionage	19
1.3.2	Betrachtete Studien	20
1.4	Forschungsfrage und Hypothese	29
1.5	Zielsetzung und Abgrenzung	30
1.6	Aufbau der Arbeit	31
1.7	Gender-Aspekt	31
1.8	Gesellschafts- und Umweltaspekte	32

1.1 Hintergrund und Problemstellung

Industrie- und Wirtschaftsspionage werden oft mit komplexen Angriffsmustern in Verbindung gebracht und können sich für nahezu alle Organisationen existenzbedrohend auswirken. Die Folgen können sich einerseits durch finanzielle Schäden und andererseits meist auch durch qualitative Einbußen, wie Image- oder Reputationsverlust, äußern. Aktuelle Studien zeigen auf, dass in Österreich pro Jahr mit Schäden im Milliardenbereich gerechnet werden muss, wobei sich in den letzten Jahren eine stetig steigende Tendenz der Vorfälle abzeichnet (Corporate Trust, 2014, S. 8).

Diese Summen sind mit großer Wahrscheinlichkeit nur die Spitze des Eisbergs. Viele Organisationen sind sich oft gar nicht bewusst, dass sie Opfer von Wirtschafts- oder Industriespionage wurden. Deshalb ist davon auszugehen, dass die veröffentlichten Studien über bekannte Fälle, die wahre Dunkelziffer nur erahnen und abschätzen können. Laut Expertinnen und Experten liegt die Schadenssumme für Österreich zwischen zwei und drei

Milliarden Euro. Nahezu jedes dritte österreichische Unternehmen in Österreich (31%) war bisher bereits von Wirtschafts- oder Industriespionage betroffen (Langer, Jabinger & Grasser, 2011, S. 8). In etwa drei Viertel aller Spionagevorfälle in Österreich werden die Behörden durch die Unternehmen nicht kontaktiert. Die Gründe dafür liegen hauptsächlich an der mangelnden Beweislage und der geringen Erwartungshaltung gegenüber einer Verurteilung (Körmer & Langer, 2015, S. 23).

Im Durchschnitt beläuft sich der direkte finanzielle Schaden, für die eine Hälfte der österreichischen Unternehmen, auf maximal 50.000 Euro. Für mehr als 17% beträgt der Schaden mehr als eine Million Euro. Neben den direkten finanziellen Schäden beklagen über 70% der betroffenen, österreichischen Organisationen vor allem den Verlust von Kundinnen und Kunden, den Rückgang von Aufträgen, als auch die Schädigung des Rufes. Dieser Schaden lässt sich nur bedingt messen und stellt die Unternehmen vor zusätzliche Herausforderungen (Körmer & Langer, 2015, S. 19).

Dabei lässt sich bereits zu einem gewissen Grad erahnen, dass die unterschiedlichen Ebenen der Folgen von Wirtschafts- und Industriespionage für Unternehmen kaum abschätzbar sind. Die aktuellen Studien und Erkenntnisse betrachten das Thema aus unterschiedlichen Blickwinkeln und setzen unterschiedliche Schwerpunkte.

Dadurch stehen Organisationen vor der Entscheidung, wie mit den Maßnahmen zur Abwehr von Wirtschafts- und Industriespionage umzugehen ist. Dabei stellt sich im Sinne der Effektivität die Frage nach den adäquaten Maßnahmen, um den Risiken in wirtschaftlich sinnvoller Weise begegnen zu können. Erst eine Betrachtung aller relevanten Faktoren ermöglicht eine glaubhafte Einschätzung der möglichen Risiken und eine entsprechende Beurteilung (Talbot & Jakeman, 2009, S. 56).

Durch eine umfassende Beurteilung der Risiken wird es möglich, Gegenmaßnahmen zu erarbeiten. Jede Gegenmaßnahme hat zum Ziel das Risiko zu minimieren bzw. mitigieren und ist mit Aufwand und Kosten verbunden. Durch diese Informationen wird eine Abschätzung des Kosten-Nutzen-Verhältnisses, sowie möglicher Folgewirkungen ermöglicht. Damit erhalten Entscheidungsträgerinnen und –träger das notwendige Werkzeug, um im Sinne der Organisation effizientes Risikomanagement zu betreiben (Talbot & Jakeman, 2009, S. 172).

Somit gibt es zu diesem Thema unterschiedlichste Berichte von verschiedenen Interessensgruppen, welche diverse Ziele verfolgen. Deshalb gibt es derzeit zwar eine Fülle an veröffentlichten Zahlen und Fakten zu diesem Thema, jedoch stellt sich die Frage, ob ein Unternehmen für die Herstellung von Antiviren-Lösungen den Fokus auf die gleichen Schwerpunkte legt wie das Bundesamt für Sicherheit in der Informationstechnologie in Deutschland. Aufgrund der steigenden Digitalisierung der Gesellschaft legen viele dieser Studien den Schwerpunkt auf Angriffe mittels neuer Technologien. So könnte der Eindruck entstehen, dass die Angriffs- und Verteidigungsmöglichkeiten auf rein technische Vorgänge reduziert werden.

In den vergangenen Jahren stiegen die gesetzlichen und regulatorischen Vorgaben, welche eine Meldung und zum Teil auch Veröffentlichung von Vorfällen betreffend den Missbrauch von Informationen und Daten fordern. Damit steigt der öffentliche Druck auf Organisationen, da größere Vorfälle somit publik werden und damit die Reputation des Unternehmens einem großen Risiko ausgesetzt wird (Europäische Kommission, 2016).

Die Studien unterscheiden sich neben anderen Faktoren vor allem hinsichtlich der Angriffsvektoren, Stichprobengröße, geografische Zuordnung der Angreifer und der Betroffenen, sowie der Fragestellungen. Um einen Überblick zu den veröffentlichten Daten zu erhalten, scheint es sinnvoll eine Analyse dieser Studien durchzuführen und damit ein möglichst umfassendes und aktuelles Verständnis der Bedrohungslage für den deutschsprachigen Raum zu erhalten.

1.2 Innovationsgehalt

Aufgrund der steigenden medialen Beachtung des Themas Sicherheit im Allgemeinen, vor allem auch im digitalen Zeitalter, wächst auch im gleichen Ausmaß die Frage nach den zugrundeliegenden Angriffen, die auf Unternehmen abzielen. Diese Situation befördert jährlich neue Studien, rund um den Themenkomplex Wirtschafts- und Industriespionage, in die Öffentlichkeit. Dabei wird des Öfteren der finanzielle Schaden für die Wirtschaft medienwirksam diskutiert, welcher demnach alleine im deutschsprachigen Raum mehrere Milliarden Euro übersteigen soll (Bachmann, Shahd & Grimm, 2015, S. 17). Deshalb gilt es festzustellen,

inwiefern die einzelnen Erkenntnisse aus diesen Studien überhaupt den Informationsbedarf der potenziell betroffenen Unternehmen decken.

Einen weiteren großen Unsicherheitsfaktor spielt die ungewisse Datenlage zu realen Fällen der Wirtschafts- und Industriespionage im deutschsprachigen Raum, da nur rund jedes fünfte Unternehmen derartige Delikte an staatliche Behörden meldet (Bachmann et al., 2015, S. 35). Damit ist es derzeit kaum möglich eine realistische, faktenbasierte Diskussion zu diesem Themenkomplex zu führen, wobei die Dunkelziffer nicht realistisch einzuschätzen ist (Corporate Trust, 2014, S. 86).

Wie die dargestellten Gemeinsamkeiten und Unterschiede der ausgewählten Studien im Kapitel 3.3 zeigen, werden bestimmte Themenschwerpunkte rund um die bekannten Schäden von einigen Studien abgedeckt. Andere Schwerpunkte, wie die Identifizierung der relevanten Assets, die Analyse von Aktivitäten auf IT-Systemen, oder genauere Details zu den bekannten Vorfällen werden nur von einzelnen Studien in unterschiedlichen Ausprägungen behandelt.

Der Innovationsgehalt der vorliegenden Arbeit liegt in der strukturierten Aufarbeitung bestehender Studien zu Wirtschafts- und Industriespionage im deutschsprachigen Raum. Dabei wird der Fokus vor allem auf die behandelten Schwerpunkte in den Studien gelegt, um mögliche Überlappungen oder auch Lücken identifizieren zu können.

Das Ergebnis trägt somit zu einem umfassenderen und einheitlicheren Verständnis der Schwerpunkte von Wirtschafts- und Industriespionage bei. Außerdem werden damit auch mögliche blinde Flecken dieser Studien aufgedeckt, welche bisher kaum erhoben wurden, jedoch für Unternehmen von hoher Relevanz sein könnten.

1.3 Stand der Forschung

Im folgenden Kapitel wird der aktuelle Stand der Forschung hinsichtlich der Phänomenologie Wirtschafts- und Industriespionage erläutert und systematische Übersichtsarbeiten beleuchtet, um unterschiedliche Studien miteinander vergleichen zu können. Anschließend werden die Auswahlkriterien für die betrachteten Studien, als auch die Studien und deren wichtigsten Eckdaten, behandelt.

1.3.1 Phänomenologie Wirtschafts- und Industriespionage

In der Literatur werden die Begriffe der Wirtschaftsspionage und der Industriespionage oft vermischt, oder gar synonym verwendet. Das folgende Kapitel beschreibt diese beiden Phänomene und deren gemeinsamen Nenner, als auch die Unterschiede.

Bei beiden Ausprägungen handelt es sich um Spionage, wobei im deutschen Sprachgebrauch für diesen Begriff unterschiedliche Interpretationen vorherrschen. Nach dem lateinischen Wort „spicari“ bedeutet Spionage grundsätzlich Erspähen oder Ausspähen. Im Allgemeinen kann daraus abgeleitet werden, jedes Mittel ist recht, um an wichtige Informationen zu gelangen, was der Gegner hat und wie seine nächsten Schritte aussehen werden. Nahezu alle Spionagefälle der heutigen Zeit haben gemein, dass ein ungewollter Informationsabfluss zum Nachteil für ein Wirtschaftsunternehmen stattfindet (Schaaf, 2009, S. 7). In der heutigen Industriewelt sind zumeist Nachrichtendienste anderer Länder, konkurrierende Unternehmen, eigene Mitarbeiterinnen oder Mitarbeiter, organisierte Kriminalität oder Hacker am Werk (Schaaf, 2009, S. 22). Für die meisten Unternehmen und Organisationen ist der Unterschied zwischen Wirtschafts- und Industriespionage irrelevant, da sie in beiden Fällen einen Datenverlust erlitten haben, unabhängig davon, wer die Täter sind. Aus diesem Grund werden die Begriffe der Wirtschaftsspionage und der Industriespionage in den Medien, als auch der Literatur oft unterschiedlich verwendet und interpretiert. Um diese Phänomene differenzierter zu betrachten, wird in der Literatur aufgrund der Motivation der Täterinnen und Täter unterschieden (Schaaf, 2009, S. 22; Schreiner, 2008, S. 27-28). Dabei können die Angriffe gegen dieselben Opfer gerichtet sein, doch ist ausschließlich die Unterscheidung der Angreifenden maßgeblich.

Unter Wirtschaftsspionage ist die staatlich gelenkte, von Nachrichtendiensten anderer Länder durchgeführte Spionage von Unternehmen oder Organisationen zu verstehen. Die Täterin oder der Täter ist in diesem Fall ein Staat, welcher auch mit den notwendigen finanziellen Mitteln solch einen Angriff durchführt oder entsprechende Kräfte dafür mobilisiert (Schaaf, 2009, S. 23) (Schreiner, 2008, S. 27-28).

Industriespionage, oder auch Konkurrenzausspähung genannt, beschreibt das Phänomen der Spionage von einem Wirtschaftsunternehmen durch ein anderes, meist konkurrierendes Unternehmen (Schaaf, 2009, S. 23). In den

meisten Fällen geht es den angreifenden Unternehmen darum, kurzfristig Informationen zu Produkten, Entwicklungen oder Projekten zu erhalten (Schreiner, 2008, S. 28).

Eine wichtige Rolle für Wirtschafts- und Industriespionage spielt die technische Entwicklung der privaten und beruflichen Kommunikationsmittel. Ab den 90er Jahren erfuhr das Internet seine große Verbreitung. Bis heute hat dies eine große Veränderung erfahren und ist für viele Menschen aus dem täglichen Leben kaum wegzudenken (Köhler, 2014, S. 15). Außerdem sind mittlerweile viele Daten nicht mehr ausschließlich auf Papier gespeichert, sondern viel häufiger auf digitale Art und Weise. Somit ist der Zugang zu Informationen nicht mehr an den physischen Zutritt in einem Archiv eines Unternehmens gebunden. Es ist in Zeiten der Verbreitung von Cloud-Diensten viel häufiger möglich auf schützenswerte Daten über das Internet zuzugreifen. Dabei stellt sich jedoch die grundlegende Auslegung von solchen Internetprotokollen als Problem heraus. Diese Protokolle sind grundsätzlich nicht für eine sichere Kommunikation ausgelegt. Einige Spezialprotokolle verfügen bereits über eingebaute Sicherheitsmechanismen, doch diese sind nur auf wenige beschränkt. Oft ist es nur schwer möglich die Identität des Absenders einer digitalen Nachricht feststellen und auch nachweisen zu können. Auch im World Wide Web gibt es per se keine Sicherheitsmechanismen. Diese wurden durch Ergänzungen und Erweiterungen erst nachträglich hinzugefügt. Dabei werden immer wieder neue Sicherheitslücken bekannt, welche die Sicherheitsmechanismen wiederum schwächen (Köhler, 2014, S. 18).

1.3.2 Betrachtete Studien

Das folgende Kapitel gibt einen Überblick zu den Studien, welche im Rahmen dieser Arbeit näher betrachtet wurden. Außerdem werden die wichtigsten Eckdaten der einzelnen Studien dargestellt, um die wichtigsten Faktoren direkt gegenüberstellen zu können.

Im Rahmen der Recherche wurden über 20 Studien identifiziert, welche dem Themenkomplex Wirtschafts- und Industriespionage zugeordnet werden könnten. Es wurden Auswahlkriterien definiert, nach denen die identifizierten Studien gefiltert wurden. Dabei wurde vor allem auf die Angaben zu dem Forschungsdesign in den Studien geachtet, um eine möglichst hohe Transparenz ermöglichen zu können. So soll eine Vergleichbarkeit der

Erkenntnisse nach der Analyse möglich werden. Durch diesen Schritt konnte die Anzahl der Studien auf sieben reduziert werden. Damit wurden jene Studien ausgeschlossen, welche die notwendige Detailtiefe nicht aufweisen konnten.

Die letzte Spalte der Tabelle 1 mit der Beschriftung „Abhängigkeit“ beschreibt die Einschätzung der jeweiligen Studie hinsichtlich der Abhängigkeit zu der Motivation der Auftraggeberinnen oder Auftraggeber. Es ist davon auszugehen, dass Dienstleisterinnen und Dienstleister im Bereich IT-Security oder Wirtschaftsschutz ein hohes Maß an Interesse aufweisen, sodass die Ergebnisse die Notwendigkeit von Gegenmaßnahmen unterstreichen. Die Einstufung erfolgt in drei Kategorien, nämlich gering, mittel und hoch.

Die drei Studien „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter“, „Cyber-Sicherheits-Umfrage 2015“ und „Wirtschafts- und Industriespionage in österreichischen Unternehmen 2015“ wurden von Organisationen beauftragt und durchgeführt, welchen eine geringe Motivation zugeschrieben werden kann, die Ergebnisse möglichst dramatisch darzustellen. Somit wurden diese Arbeiten hinsichtlich der Abhängigkeit als gering eingestuft und damit wird gleichzeitig die Glaubwürdigkeit der Ergebnisse entsprechend gut bewertet.

Die Studie „IT-Security in heimischen Unternehmen“ wurde zwar von SORA Institute for Social Research and Consulting durchgeführt, jedoch von A1 Telekom Austria AG beauftragt. Die beauftragende Organisation ist seit mehreren Jahren an der Börse notiert und damit ist auch ein Interesse an der Darstellung der Risiken durch Wirtschafts- und Industriespionage zu erwarten (Telekom Austria Group, 2016, S. 24-26).

Die anderen drei Studien wurden von Unternehmen beauftragt, welche direkt in der Beratung von anderen Unternehmen tätig sind. Somit ist davon auszugehen, dass die Studienergebnisse dieser beauftragenden Organisationen direkte Auswirkungen auf die Geschäftstätigkeiten haben werden. Deshalb wurde die Abhängigkeit mit „hoch“ bewertet, weshalb die Ergebnisse unter diesem Aspekt auch weiter in der vorliegenden Arbeit berücksichtigt werden.

Tabelle 1: Übersicht der untersuchten Studien

Name	Auftrag-geber	Beauftrag-tes Institut	Länder	Branchen	Unterneh-mensgröße	Jahr der Veröffent-lichung	Anzahl befragter Unterneh-men	Rücklauf-quote	Abhängig-keit
IT-Security in heimischen Unternehmen	A1 Telekom Austria AG	SORA Institute for Social Research and Consulting	AT	Alle Branchen und IT-Dienstleis-tungen genauer	Keine Einschrän-kung	2015	Keine Angabe	500	Mittel
Spionage, Sabotage und Datendieb-stahl – Wirtschafts-schutz im digitalen Zeitalter	Bitkom - Bundesverband Informations-wirtschaft, Telekommunika tion und neue Medien e.V.	Bitkom Research GmbH	DE	Keine Einschrän-kung	Mehr als 10 MA	2015	Keine Angabe	1.074	Gering
Cyber-Sicherheits-Umfrage 2015	Bundesamt für Sicherheit in der Informations-technik	SecuMedia Verlags GmbH	AT, CH, DE	Alle Branchen, vor allem IT-Dienstleister und Öffentlicher Dienst	Keine Einschrän-kung	2015	632	424	Gering
Industrie-spionage 2014: Cybergeddon der deutschen Wirtschaft durch NSA & Co.?	Corporate Trust Business Risk & Crisis Management GmbH	Corporate Trust Business Risk & Crisis Management GmbH; AON Risk Solutions; Securiton GmbH; Zurich Gruppe Deutschland	AT, DE	Keine Einschrän-kung	Mehr als 10 MA und Bilanz-summe größer als 1 Mio. Euro	2014	8.163	530	Hoch
Kriminelle Risiken im Mittelstand: Gefahren, Schäden und Prävention – eine Studie	Result Group GmbH	forsa Gesellschaft für Sozialfor-schung und statistische Analysen mbH; F.A.Z. - Institut für Management -, Markt- und Medien-information GmbH	DE	Keine Einschrän-kung	Zwischen 50 und 500 MA	2014	Keine Angabe	100	Hoch
Cyber Security in Österreich Studie IT-Advisory	KPMG Austria GmbH	KPMG Austria GmbH	AT	Keine Einschrän-kung	Keine Einschrän-kung	2016	Keine Angabe	94	Hoch

Wirtschafts- und Industrie-spionage in öster-reichischen Unternehmen 2015	Bundes-ministerium für Inneres/ Bundesamt für Verfassungs-schutz und Terrorismus-bekämpfung	FH Campus Wien Forschungs- und Entwicklungs GmbH (Fachbereich Risiko- und Sicherheits-manage-ment); Wirtschafts-kammer Österreich; Industriellen-vereinigung	AT	Keine Einschrän-kung	Keine Einschrän-kung	2015	15.000	1.149	Gering

Quelle: Eigene Darstellung

IT-Security in heimischen Unternehmen

Diese Studie wurde im Jänner 2015 veröffentlicht und von der A1 Telekom Austria beauftragt und von der SORA Institute for Social Research and Consulting durchgeführt. Die Arbeit wurde von Daniel Schönherr, Corinna Mayerl und Horst Traunmüller erstellt. Zu dem Themenkomplex „IT-Security in heimischen Unternehmen“ wurden mittels Telefoninterviews 500 österreichische Organisationen befragt.

Knapp 80% der österreichischen Organisationen hatte bereits Störfälle in der IKT-Umgebung, wobei die Gründe dafür von Schadsoftware aus dem Internet bis hin zu Netzwerkausfällen reichen. Etwa 30% der Unternehmen mussten bereits einen Datenverlust verkraften. Vor allem für KMUs sind die Folgen möglicherweise existenzbedrohend, wenn durch Imageschäden die Kundenbeziehungen belastet werden, oder auch bei personellen Folgen.

In nahezu allen österreichischen Unternehmen ist ein Security-Basisschutz vorhanden, wie Antivirus-Software, Firewalls oder auch die Absicherung der Zugriffe durch Passwörter. In drei von vier Unternehmen werden auch laufende Wartungen und Backups von bestehenden Systemen durchgeführt.

In dieser Studie wurden Schwachpunkte bei österreichischen Organisationen hinsichtlich mangelhafter Risikobewertung, fehlendem Krisenmanagement und nicht ausreichender Datensicherheitsstrategien festgestellt (Schönherr, Mayerl & Traunmüller, 2015).

Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter

Die Studie „Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter“ legt den Fokus vor allem auf Betreiber kritischer Infrastrukturen, welche für die Versorgung der Gesellschaft von besonderer Bedeutung sind. Zu diesem Zweck wurden 1.074 ausgewählte Unternehmen mit mindestens zehn Mitarbeiterinnen oder Mitarbeitern befragt. Dabei wurden Führungskräfte von Organisationen aus Deutschland im Jänner 2015 interviewt, welche für die Themen IT-Sicherheit, Risikomanagement oder Finanzen verantwortlich sind. Die Bitkom Research GmbH wurde von dem Bitkom - Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. zur Durchführung dieser Studie beauftragt. Der Fragebogen wurde in Kooperation beider Unternehmen erstellt.

In den letzten zwei Jahren waren mehr als die Hälfte aller befragten Unternehmen in Deutschland von Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen. Der resultierende Schaden beläuft sich auf 51 Mrd. € pro Jahr. Genauso viele Unternehmen verfügen nicht über ein funktionierendes Notfallmanagement, welches ermöglichen würde, die Schäden eingrenzen zu können. Außerdem werden Angriffe auf die Daten stetig komplexer, wofür auch die Gegenmaßnahmen angepasst werden müssen: Dazu ist ein Umdenken in den Unternehmen notwendig. Alle der befragten Organisationen setzen rudimentäre, technische Sicherheitsmaßnahmen, wie Firewalls und Antivirenlösungen, ein und etwa 90% regeln den Zugriff auf ihre Daten.

Abgesehen von den technischen Angriffen sind bei der Hälfte der betroffenen Organisationen direkt die eigenen Mitarbeiterinnen oder Mitarbeiter involviert. In 19% der Fälle wurde gezielt Social Engineering eingesetzt, um an schutzwürdige Unternehmensdaten zu gelangen, wobei nur die Hälfte der Unternehmen auf entsprechende Security Awareness Schulungen setzen (Bachmann et al., 2015).

Cyber-Sicherheits-Umfrage 2015

Diese Studie wurde im Oktober 2015 veröffentlicht, vom Bundesamt für Sicherheit in der Informationstechnik beauftragt und in einer Kooperation folgender Organisationen erstellt.

- Bundesverband der Deutschen Industrie (BDI)

- Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM)
- Deutscher Industrie- und Handelskammertag (DIHK)
- Gesellschaft für Informatik e.V. (GI)
- Verband Deutscher Maschinen- und Anlagenbau (VDMA)
- Verband der IT-Anwender e.V. (VOICE)
- Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI)

Die Befragung und die Interviews wurden von SecuMedia Verlags GmbH und OTARIS Interactive Services GmbH durchgeführt. Die Datenbasis stellen Online-Umfragen dar, welche die ausgewählten Organisationen im Zeitraum von Juni bis September 2015 beantworteten. Die Antworten wurden anonymisiert, wobei insgesamt 632 Datensätze erfasst und nach Durchsicht nunmehr 424 übrig blieben. Die befragten Unternehmen sind laut eigenen Angaben vor allen IT-Dienstleister, oder für den öffentlichen Dienst tätig.

Knapp 60% der befragten Organisationen waren in den letzten beiden Jahren das Ziel von Cyber-Angriffen. 11% konnten nicht feststellen, ob sie von solchen Angriffen betroffen waren. Vor allem große Unternehmen, mit mehr als 10.000 Mitarbeiterinnen und Mitarbeitern konnten die Angriffe feststellen und waren damit in der Lage darauf zu reagieren. Etwa jede vierte Organisation geht davon aus, dass ein Cyber-Angriff bereits erfolgreich war. Das stellt eine Steigerung von 13,4% der erfolgreichen Cyber-Angriffe von 2015 gegenüber 2014 dar.

Die häufigsten Ursachen für erfolgreiche Cyber-Angriffe stellen bei den befragten Unternehmen vor allem unbeabsichtigtes Fehlverhalten von Mitarbeiterinnen und Mitarbeitern, Angriffe über Malware und fehlende Patches dar. Die Auswirkungen waren weitreichend, wobei vor allem Betriebsausfälle und Kosten für die Wiederherstellung als große Folgeschäden angegeben wurden (Bundesamt für Sicherheit in der Informationstechnik, 2015).

Industriespionage 2014: Cybergeddon der deutschen Wirtschaft durch NSA & Co.?

Die Studie „Industriespionage 2014 – Cybergeddon der deutschen Wirtschaft durch NSA & Co.?“ wurde von Corporate Trust Business Risk & Crisis Management GmbH beauftragt und in Zusammenarbeit mit AON Risk Solutions, der Securiton GmbH und der Zürich Gruppe Deutschland erstellt. Es wurden dabei 6.767 Organisationen aus Deutschland und 1.396 aus Österreich berücksichtigt, wobei den Themen Risikomanagement und den entsprechenden Vorfällen besonderes Augenmerk gewidmet wurde. Es wurde ein möglichst umfassender Querschnitt von unterschiedlichen Branchen und Unternehmensgrößen gefasst, um ein umfassendes Lagebild für Deutschland und Österreich bilden zu können. Außerdem wurden ausschließlich Unternehmen berücksichtigt, welche mehr als zehn Mitarbeiterinnen oder Mitarbeiter zählen und zusätzlich eine Bilanzsumme über einer Million Euro aufweisen können. Die Befragung wurde im April 2014 durchgeführt, wofür insgesamt 530 Vorstände, Geschäftsführerinnen oder Geschäftsführer, bzw. Leiterinnen oder Leiter für die Bereiche Risikomanagement, Unternehmenssicherheit, Informationsschutz, Recht, Finanzen, Controlling, IT, Interne Revision, Compliance oder Personal postalisch oder per Mail einen Fragebogen beantworteten. Zusätzlich war auch die Beantwortung eines Online-Fragebogens möglich, wobei auch telefonische Interviews durchgeführt wurden.

Die Hälfte aller Unternehmen war in den vergangenen zwei Jahren von Spionage oder konkreten Verdachtsfällen betroffen. Der potenzielle Schaden dadurch beläuft sich in Deutschland auf 11,8 Mrd. Euro und in Österreich auf 1,6 Mrd. Euro. Bei dem Großteil der Einzelfälle lag die Schadenssumme zwischen 10.000 und 100.000 Euro. Außerdem verzeichneten 4,5% der deutschen und 3,1% der österreichischen Organisationen zumindest einen Schaden mit mehr als 1 Mrd. Euro. Am meisten hatten die Unternehmen mit dem Ausfall von IT, sowie Diebstahl oder Schädigung der IT zu kämpfen. Die betroffenen Unternehmen erlitten auch immaterielle Schäden, wie Patentrechtsverletzungen, als auch Imageschäden bei Kundinnen und Kunden, sowie Lieferantinnen und Lieferanten.

In Anbetracht der Größe der Organisationen wird mit 67,7% bzw. 62,7% der Mittelstand am häufigsten angegriffen. Die Spionageangriffe stammen zumeist aus Asien, Osteuropa und den GUS-Staaten, wobei eine Zuordnung vor allem durch die Digitalisierung immer schwieriger wird. Am häufigsten wurden

Hacker-Angriffe verzeichnet, dicht gefolgt vom Abhören von elektronischer Kommunikation und damit der Exfiltration von schützenswerten Daten. Die Mehrheit der Unternehmen ist sich sicher, dass Industriespionage noch deutlich zunehmen wird, wobei in Deutschland 52,6% dieser Meinung sind und in Österreich 41,7% (Corporate Trust, 2014).

Kriminelle Risiken im Mittelstand: Gefahren, Schäden und Prävention – eine Studie

Im Jänner 2014 wurden von der Marktforschungsgesellschaft forsa 100 Verantwortliche für die Themen Risikomanagement oder Compliance in deutschen Unternehmen befragt. Die Organisationen setzen sich aus Industrie, Dienstleistungen, sowie Agrar-, Garten- und Landschaftsbau zusammen. Diese haben zwischen 50 und 500 Mitarbeiterinnen und Mitarbeiter. Die Interviews wurden mithilfe eines strukturierten Fragebogens durchgeführt.

Der Fokus dieser Studie liegt auf dem deutschen Mittelstand, da aufgrund der wachsenden Konjunktur und Innovationskraft diese Unternehmen von einem erhöhten Risiko der Spionage ausgehen müssen.

Mehr als die Hälfte aller mittelständischen Unternehmen in Deutschland wurden seit den letzten fünf Jahren Opfer von Wirtschafts- oder Industriespionage. Die meisten Anlagen- und Maschinenbauer beklagen Schäden in Folge von kriminellen Handlungen. Die höchsten Einzelverluste sind im Dienstleistungssektor zu verzeichnen, wobei in den letzten fünf Jahren Einzelschäden in der Höhe zwischen 500.000 Euro und 5 Mio. Euro entstanden. Nach Angriffen werden nur vereinzelt staatliche Behörden, Forensik-Unternehmen hinzugezogen. Als größte Bedrohungen sehen die befragten Unternehmen derzeit Diebstahl, Betrug, sowie Angriffe von außen und innen.

Der deutsche Mittelstand sieht die eigenen Mitarbeiterinnen und Mitarbeiter, die IT, als auch die oberste Managementebene als besonders gefährdet an. Dabei werden erhebliche Risiken für die Menschen und auch die Datenverarbeitung verortet. Die Gegenmaßnahmen, welche von den Unternehmen getroffen wurden, stellen die Mitarbeiterinnen und Mitarbeiter in den Mittelpunkt der Angriffe, sowohl als mögliche Opfer, als auch potenzielle Angreifer. Das Risiko eines Angriffs von Businesspartnern steigt rasant an (F.A.Z. Institut, forsa & Result Group, 2014).

Cyber Security in Österreich Studie IT-Advisory

Diese Studie wurde im April 2016 veröffentlicht und beleuchtet die Frage, wie österreichische Unternehmen mit Cyberkriminalität umgehen und welche Maßnahmen dazu getroffen werden. Dafür wurde im November 2015 von 94 österreichischen Unternehmen unterschiedlicher Größe und Branche ein Onlinefragebogen beantwortet. Mit sieben Vertretern von Unternehmen wurden persönliche Interviews durchgeführt.

Insgesamt sind 92% der im Rahmen dieser Studie befragten Unternehmen der Ansicht, dass Cyber Security zu den alltäglichen Herausforderungen gehört und es sich dabei nicht um einen kurzfristigen Hype handelt. Knapp die Hälfte aller Organisationen waren bereits Opfer eines Cyberangriffes, wobei knapp ein Drittel aller Unternehmen bereits einen Schaden durch diese Angriffe erlitten hat. 40% schätzen sich selbst als attraktives Ziel ein, wobei nur 23% in der Lage sind Angriffe zumindest zu erkennen und nur noch 18% können angemessen reagieren. Im Gegensatz dazu sind 71% der Ansicht, dass Cyberangriffe nicht vollständig vermieden werden können.

Mehr als drei Viertel der Organisationen sind der Ansicht, dass das Bewusstsein bei den Mitarbeiterinnen und Mitarbeitern unzureichend geschärft ist und noch weitere Maßnahmen zur Bewusstseinsbildung zu Cyberangriffen notwendig sind. Mehr als die Hälfte der Unternehmen glauben, über ihre Assets ausreichend Bescheid zu wissen, jedoch nur 16% sind der Ansicht diese auch ausreichend schützen zu können. Knapp die Hälfte haben keine dezidierte Cyber Security Mitarbeiterin bzw. Mitarbeiter und bei 63% ist der Themenkomplex in der IT-Abteilung angesiedelt (KPMG, 2016).

Wirtschafts- und Industriespionage in österreichischen Unternehmen 2015

Im Rahmen dieser Studie wurden in Österreich 15.000 Unternehmen aufgrund des Datenbestands der Wirtschaftskammer Österreich und der Industriellenvereinigung befragt, wovon 1.149 antworteten. Diese Organisationen wurden mittels standardisiertem Online-Fragebogen im Juni und Juli 2015 befragt. Die Ergebnisse wurden im Dezember 2015 veröffentlicht. Die Fragen umfassten die Themen Innovationen, Spionagevorfälle in der Vergangenheit und mögliche Fälle in der Zukunft, Präventionsmaßnahmen, sowie Erwartungen der Unternehmen. Bei den Fragestellungen zu bisherigen Ereignissen wurde ein Zeitraum von fünf

Jahren vorgegeben, um ein möglichst umfassendes Lagebild zu erhalten und im speziellen auf Folgeschäden eingehen zu können.

Es gaben 5,1% der befragten Unternehmen an, dass sie in den letzten fünf Jahren mindestens einmal Opfer von Wirtschafts- und Industriespionage waren. Bei fast jedem zweiten Fall wird eine Mitbewerberin oder ein Mitbewerber hinter dem Angriff vermutet. Von den betroffenen Unternehmen gab lediglich ein Viertel an, Behörden eingebunden zu haben. Neben den unmittelbaren Schäden waren in mehr als 70% der Fälle auch langfristige Schäden, wie Kundinnen-, Kunden-, Auftrags- oder auch Imageverluste zu verzeichnen. Etwa 30% der befragten Unternehmen schätzen die Hälfte ihrer Informationen als Geschäfts- und Betriebsgeheimnisse ein, wobei im Rahmen dieser Studie diese Einschätzung in Frage gestellt wird. Es konnten keine relevanten Unterschiede hinsichtlich der Unternehmensgröße festgestellt werden, wobei die Qualität der getroffenen Maßnahmen bei größeren Unternehmen tendenziell besser ist, als bei kleineren. Dies gilt auch für Branchen, welche durch Gesetze und Normen stark reguliert werden (Körmer & Langer, 2015).

1.4 Forschungsfrage und Hypothese

Das folgende Kapitel beschreibt die zentrale Forschungsfrage der vorliegenden Arbeit, sowie die forschungsleitenden Fragen und die Hypothese.

Forschungsfrage

Welche Themenschwerpunkte spielen in der gegenwärtigen Erforschung des Phänomens Wirtschafts- und Industriespionage anhand ausgewählter Studien eine relevante Rolle, welche Gemeinsamkeiten und Unterschiede weisen die Studien auf und inwieweit sind die ermittelten Schwerpunkte für die Praxis relevant?

Aufgrund dieser Forschungsfrage wurden folgende forschungsleitenden Fragen erarbeitet, um den Themenkomplex besser abzugrenzen und die relevanten Aspekte im Rahmen der vorliegenden Arbeit näher zu beleuchten. Die zuerst umfangreiche Forschungsfrage wurde in fünf forschungsleitende Fragen gegliedert, um jedem Schwerpunkt getrennt betrachten zu können.

Forschungsleitende Fragen

- Was sind die Charakteristika von Wirtschafts- und Industriespionage?
- Wie ist das Dunkelfeld bei Wirtschafts- und Industriespionage zu bewerten?
- Welche Studien können für einen Vergleich von Wirtschafts- und Industriespionage herangezogen werden?
- Welche Gemeinsamkeiten und Unterschiede können mithilfe einer systematischen Übersichtsarbeit zu Wirtschafts- und Industriespionage erhoben werden?
- Bilden die in den Studien untersuchten Kriterien, die Herausforderungen deutschsprachiger Unternehmen ab?

Aufgrund dieser Fragestellungen wurde folgende Hypothese abgeleitet.

Hypothese

H1: Die aus den Studien ermittelten Themenschwerpunkte decken sich mit den relevanten Problemen durch Wirtschafts- und Industriespionage in der Praxis.

1.5 Zielsetzung und Abgrenzung

Die vorliegende Arbeit hat vor allem zum Ziel, die Ergebnisse bestehender Studien zu dem Themenkomplex Wirtschafts- und Industriespionage hinsichtlich ihrer Relevanz in der Praxis zu prüfen. Außerdem soll damit auch erhoben werden, inwiefern mit diesen Informationen der Bedarf von Unternehmen gedeckt werden kann, oder welche Schwerpunkte bisher von den Studien zu wenig beleuchtet wurden.

Dazu werden im theoretischen Teil die Grundlagen für Übersichtsarbeiten, Wirtschafts- und Industriespionage, sowie Hell- und Dunkelfeldforschung aufgearbeitet. Anschließend werden die Studien analysiert, sowie deren Gemeinsamkeiten und Unterschiede dargestellt.

Im empirischen Teil wird aufgrund dieser Erkenntnisse ein Leitfadeninterview vorbereitet und mit mehreren Expertinnen und Experten aus der Praxis durchgeführt. Damit wird vor allem der Praxisbezug der Ergebnisse aktueller Studien verifiziert oder falsifiziert.

1.6 Aufbau der Arbeit

Die vorliegende Arbeit ist in fünf Abschnitte gegliedert. Das erste Kapitel beschreibt die Einleitung und den Kontext der vorliegenden Arbeit. Außerdem werden die Ziele und die Forschungsfrage erläutert.

Das nächste Kapitel beschreibt neben den zentralen Begriffen auch die zugrundeliegende Theorie. Dabei werden die Aspekte der systematischen Übersichtsarbeit, als auch die Grenzen dieser aufgezeigt. Außerdem erhält die Hell- und Dunkelfeldforschung besonderes Augenmerk.

Im dritten Kapitel wird neben der Anwendbarkeit der Theorie auf die Forschungsfrage auf die Auswahlkriterien eingegangen, welche bei der Recherche nach passenden Studien berücksichtigt wurden. Darauf aufbauend werden die Gemeinsamkeiten, Unterschiede, sowie Schwerpunkte der ausgewählten Studien dargestellt.

Im anschließenden empirischen Teil werden zu Beginn das Forschungsdesign, das Verfahren und die Messmethoden beschrieben. Danach werden die Operationalisierung und die Ergebnisse der Auswertung näher beleuchtet.

Im abschließenden Kapitel werden die Ergebnisse übersichtlich zusammengefasst, das Vorgehen der vorliegenden Arbeit nochmals reflektiert und Möglichkeiten für weitere Forschungen aufgezeigt.

1.7 Gender-Aspekt

In den vergangenen Jahren hat die gesellschaftliche Entwicklung bereits einige Schritte hin zu der Gleichberechtigung unterschiedlicher Geschlechter getan. Um diese Entwicklung auch im Rahmen der vorliegenden Arbeit zu unterstützen wird besondere Aufmerksamkeit auf eine geschlechterneutrale

Gestaltung gelegt. Dabei wird vor allem auf eine geschlechtergerechte Sprache geachtet, genauso wie auf entsprechende Abbildungen und Tabellen.

Ebenso ist es selbstverständlich, dass bei der Auswahl der Expertinnen und Experten das Geschlecht keine Rolle spielt. Abhängig von der Bereitschaft der potenziellen Interviewpartnerinnen und Interviewpartner wird eine gleichmäßige Geschlechterverteilung angestrebt.

Die Interviews werden nach den gleichen Maßstäben gestaltet, sodass auch diese gendersensible Fragestellungen und Formulierungen enthalten. Genauso wird auch bei den Workshops, Präsentationen und Vorträgen auf eine gendersensible Durchführung durch den Autor geachtet.

Der „Sprachleitfaden – Geschlechtergerechter Sprachgebrauch an der FH Campus Wien“ bildet die Basis für die entsprechenden Vorgaben, welche durch die vorliegende Arbeit zumindest erfüllt werden (Alker & Weilenmann, 2006, S. 7).

1.8 Gesellschafts- und Umweltaspekte

Der größte Nutzen der vorliegenden Arbeit ergibt sich einerseits für die weitere Forschung des Phänomens Wirtschafts- und Industriespionage. Dabei werden relevante Felder aufgezeigt, die bisher in Studien noch kaum behandelt wurden und noch weitere Forschung benötigen.

Andererseits zeigen die identifizierten Schwerpunkte der bestehenden Studien und die Prüfung deren Relevanz in der Praxis jene Themen auf, zu denen Entscheidungsträger von Unternehmen aussagekräftige Erkenntnisse benötigen. Die hohe Dunkelziffer legt außerdem noch einen großen Schleier auf die realen Angriffe und mögliche Risiken. Das Ergebnis der vorliegenden Arbeit gibt Aufschluss über Themen, welche für die Praxis bereits ausreichend dargestellt werden, aber vor allem auch, zu welchen noch mehr Informationen benötigt werden.

Wenn man zumindest dem Großteil der Studien zu Wirtschafts- und Industriespionage Glauben schenken darf, so belaufen sich die Schäden zumindest im deutschsprachigen Raum auf mehrere Milliarden Euro (Bachmann et al., 2015, S. 17; Corporate Trust, 2014, S. 8; F.A.Z. Institut et al., 2014, S. 3). Dabei ist der langfristige Schaden für Unternehmen, wie durch

Imageverlust oder sinkende Wettbewerbsfähigkeit noch gar nicht berücksichtigt. Damit werden Unternehmen geschwächt und das Risiko für die Mitarbeiterinnen und Mitarbeiter erhöht, dass der Arbeitgeber eventuell Konkurs anmelden muss.

Durch Wirtschafts- und Industriespionage werden Unternehmen zugunsten dem Vorteil anderer geschwächt, wobei dies mittel- und langfristig auch Auswirkungen auf das Land des Unternehmens haben kann. Der negative Einfluss dieser Angriffe wirkt sich damit auch indirekt auf die Wirtschaftsleistung des jeweiligen Landes aus.

Somit kann die vorliegende Arbeit im besten Fall einen kleinen Beitrag dazu leisten, das Risiko von Wirtschafts- und Industriespionage klarer darzustellen und damit die Erforschung des Themenkomplexes voranzutreiben. Dadurch können Unternehmen dieses Thema besser strukturieren und Entscheidungen vielmehr auf umfassende Fakten treffen, als aufgrund von Meldungen von Einzelfällen in den Medien.

2
Theoretischer Teil

Inhalt

2.1	BEGRIFFSDEFINITIONEN	35
2.2	THEORIE	38
2.2.1	SYSTEMATISCHE ÜBERSICHTSARBEIT	38
2.2.2	GRENZEN DER SYSTEMATISCHEN ÜBERSICHTSARBEIT UND KRITIK	40
2.2.3	HELL- UND DUNKELFELDFORSCHUNG	42

2.1 Begriffsdefinitionen

Dieses Kapitel beschreibt und erläutert die zentralen Begriffe der vorliegenden Arbeit, um ein möglichst einheitliches Verständnis zu ermöglichen.

Business Continuity Management (BCM)

Bei Business Continuity Management, kurz BCM, geht es darum, Unterbrechungen oder unerwünschte Verzögerungen von Geschäftsprozessen zu verhindern oder deren Risiken zu minimieren. Außerdem sollen damit die Auswirkungen von personellen und technischen Ausfällen, sowie von Elementarereignissen begrenzt werden. Nach einer Unterbrechung muss eine effiziente Wiederaufnahme und Fortführung der Geschäftsprozesse sichergestellt werden.

In mancher Literatur werden für BCM ausschließlich IT-relevante Schwerpunkte behandelt, welche jedoch die Ausmaße von Business Continuity Management nicht vollständig umfassen. Die Überlegungen und Maßnahmen zu BCM müssen Organisationen und deren Geschäftsprozesse, sowie die notwendigen Ressourcen dafür, vollständig erfassen (Kersten, Reuter & Schröder, 2013, S. 258-261).

Cybercrime

Unter dem Begriff Cybercrime sind Straftaten zu verstehen, welche mit Hilfe von Informationstechnologien und Kommunikationsnetzen begangen werden, wobei auch die Internetkriminalität hinzugezählt werden muss (KSÖ Kuratorium Sicheres Österreich, 2012, S. 116).

Hell- und Dunkelfeld

Das Hellfeld beschreibt das Ausmaß der bekannt gewordenen Kriminalität. Die entsprechenden Zahlen sind vor allem in den polizeilichen Kriminalstatistiken der einzelnen Länder erfasst und dokumentiert (Bundeskanzleramt Österreich, 2016, S. 8).

Das Dunkelfeld beschreibt jene kriminellen Vergehen, welche nicht bekannt sind. Der Hauptgrund dafür liegt oft darin, dass das Opfer eine Straftat nicht an die zuständige Behörde meldet. Die Dunkelziffer beschreibt somit die Anzahl der Fälle im Dunkelfeld zu einer bestimmten Straftat und kann im besten Fall nur geschätzt werden (Bundeskanzleramt Österreich, 2016, S. 8).

Industriespionage

Oft auch als Konkurrenzausspähung bezeichnet, steht die Industriespionage für das Ausspähen von Unternehmen durch andere Unternehmen. Das Ziel dahinter ist in den meisten Fällen die Beschaffung von schützenswerten Informationen zu Produkten, Entwicklungen oder Projekten (Schreiner, 2008, S. 28).

Kronjuwelen

Bei Kronjuwelen handelt es sich um Daten und Informationen eines Unternehmens, deren Vertraulichkeit, Integrität und Verfügbarkeit entscheidend für die Wettbewerbsfähigkeit sind. Damit sind die Kronjuwelen von besonderem Interesse für den Mitbewerb. Es ist unerlässlich, dass diese Daten von den Mitarbeiterinnen und Mitarbeitern des Unternehmens vertraulich behandelt werden und diese auch mit technischen Maßnahmen ausreichend abgesichert werden (Kasper, 2014, S. 67).

Security Incident

Bei Security Incidents handelt es sich um Ereignisse oder Zustände, welche sich direkt auf einzelne Personen, Organisationen oder Gesellschaften

beziehen und dabei einen Schaden verursachen, oder einen solchen begünstigen. Die Auswirkungen betreffen Personen, Eigentum oder auch Informationen (Talbot & Jakeman, 2009, S. 325).

Security Policy

Die Security Policy ist ein Grundsatzdokument für Organisationen und beschreibt dessen Werte, Prinzipien und den erstrebten Sicherheitsanspruch. Die Verantwortung für die Erstellung, Umsetzung und Pflege des Dokuments obliegt der Unternehmensleitung (Langer et al., 2011, S. 20).

Spionage

Dieser Begriff beschreibt gesamthaft alle Handlungen, durch welche versucht wird Staatsgeheimnisse zu erlangen oder ohne Berechtigung weiterzugeben. Unter Staatsgeheimnisse sind militärische, sicherheitspolitische oder nachrichtendienstliche Informationen zu verstehen. Der Fokus dieser Informationen liegt auf dem Schutz der betroffenen Nation oder des Landes (Schreiner, 2008, S. 27).

Systematische Übersichtsarbeit

Die systematische Übersichtsarbeit, oder auch systematisches Review genannt, besteht aus einer qualitativen Zusammenfassung der Ergebnisse einzelner Studien. Neben anderen Methoden der Aggregation von Informationen, zeichnet sich die systematische Übersichtsarbeit vor allem durch die definierten Ein- und Ausschlusskriterien aus. Es sollen unter Berücksichtigung dieser Kriterien möglichst alle relevanten Studien mit einbezogen werden. Einen besonderen Stellenwert hat auch die Beurteilung der methodischen Qualität der Einzelstudien und die Untersuchung der Gründe für eventuelle Unterschiede in den Ergebnissen (Ressing, Blettner & Klug, 2009, S. 457).

Wirtschaftsspionage

Dabei handelt es sich um staatlich gelenkte, von anderen Nachrichtendiensten ausgehende, Ausforschung von Organisationen. Die Motivation dahinter liegt darin, den Unternehmen des eigenen Landes oder Staates einen Vorteil zu verschaffen. Diese Schritte sind meist mittel- bis langfristig geplant und können unter Umständen auch als Industriespionage oder Konkurrenzausspähung getarnt werden (Schreiner, 2008, S. 27-28).

2.2 Theorie

Das folgende Kapitel beschreibt die Kerninhalte der gewählten Theorien, die im Rahmen der vorliegenden Arbeit herangezogen wurden, um das Verständnis für die weitere Betrachtung zu schaffen. Dabei wurde darauf geachtet, die Inhalte mit der notwendigen Tiefe zu betrachten.

2.2.1 Systematische Übersichtsarbeit

Um studienverarbeitende Verfahren durchführen zu können, gibt es unterschiedliche Möglichkeiten, wie die Literaturanalyse, Sekundäranalyse, systematische Übersichtsarbeit, als auch die Metaanalyse (Lueginger & Renger, 2013, S. 15). Systematische Übersichtsarbeiten gewähren einen Einblick in den aktuellen Stand der Forschung und ermöglichen die Beurteilung der Qualität der einzelnen Studien. Es wird dadurch eine Beurteilung der Ergebnisse, auch bei inkonsistenter Datengrundlage möglich. Durch systematische Übersichtsarbeiten werden die Unterschiede der Studien gewichtet und zu einem gemeinsamen Ergebnis zusammengeführt. Die Überlappungen werden berücksichtigt und jene Faktoren, die nur in einzelnen Studie angeführt werden, fließen dementsprechend geringer in das Ergebnis ein (Ressing et al., 2009, S. 456).

Die steigende Digitalisierung hat sich auch auf die Art und Weise von wissenschaftlichen Publikationen ausgewirkt. Einerseits steigt die Anzahl der wissenschaftlichen Studien und andererseits wird durch den Einsatz von elektronischen Mitteln die Recherche von solchen vereinfacht. Dadurch wird es deutlich aufwendiger einen Überblick über alle relevanten Studien zu behalten und es steigt damit der Bedarf an Übersichtsarbeiten, welche die Ergebnisse von Einzelstudien korrelieren. Zusammenfassungen werden vor allem dann eingesetzt, wenn die Ergebnisse von Einzelstudien zu einem bestimmten Themengebiet zwar vorhanden sind, aber die Ergebnisse unübersichtlich oder inkonsistent sind. Dadurch können Zusammenhänge hergestellt werden, welche durch die Betrachtung der Einzelstudien alleine nicht möglich wären. Je mehr Ergebnisse einer Übersichtsarbeit zugrunde liegen, desto fundierter werden die Erkenntnisse (Eisend, 2004, S. 1-2).

Bei Zusammenfassungen können unterschiedliche Ausprägungen unterschieden werden, nämlich narrative Reviews, systematische Übersichtsarbeiten, Metanalysen und Realanalysen.

Zusammenfassungen und Übersichtsarbeiten zu Einzelstudien ermöglichen Schlussfolgerungen, welche in den Einzelstudien aufgrund von zu geringer Datengrundlage nicht möglich sind. Systematische Übersichtsarbeiten ermöglichen einen Überblick über den Stand der Forschung zu einem bestimmten Themengebiet. Außerdem kann mithilfe von systematischen Übersichtsarbeiten die Qualität der betrachteten Einzelstudien bewertet werden und diese ermöglichen die Beurteilung von Ergebnissen, auch bei inkonsistenter Datenlage (Ressing et al., 2009, S. 456).

Gute Systematische Übersichtsarbeiten zeichnen sich durch mehrere Kriterien aus (Ressing et al., 2009, S. 457-458):

- Die Fragestellung wird a priori festgelegt.
- Es wurden Ausschlusskriterien definiert, nach denen die Literatur ausgewählt wird.
- Die Basis für die Literaturrecherche ist unabhängig von der gewählten Sprache der Quelle und umfasst unterschiedliche Quellen, wie Bibliotheken, Kongressbände oder Suchmaschinen im Internet.
- Die in den Publikationen dargestellten Informationen werden extrahiert.
- Die wichtigsten Charakteristika der Einzelstudien werden in einer übersichtlichen Form dargestellt, um die Unterschiede der untersuchten Daten zu verdeutlichen.
- Die mögliche Heterogenität der einzelnen Studien wird dargestellt und bei dem Vergleich berücksichtigt.
- Die verwendeten Methoden werden klar beschrieben.
- Die Limitationen und Rahmenbedingungen der Zusammenfassung werden diskutiert.

Sofern diese Kriterien bei der Betrachtung der Einzelstudien erfüllt werden, ist es möglich systematische Übersichtsarbeiten zu erstellen. Einerseits bieten diese einen guten Überblick zu dem betrachteten Themengebiet und

andererseits ermöglichen diese auch die Verarbeitung von Studien unterschiedlicher Ausprägungen.

Die Vergleichbarkeit von Einzelstudien und deren unterschiedlichen Betrachtungsgrößen wird bei einer systematischen Übersichtsarbeit durch die Effektschätzer erreicht. Somit erhalten die Studien unterschiedliche Gewichtungen, welche in die zusammenfassende Aussage einfließen. Dabei werden Aussagen zu bestimmten Einzelpunkten von Studien umso stärker bewertet, desto besser die Datenquellen sind. Aussagen von Studien mit einer Stichprobe von über 1.000 Interviewpartnerinnen und -partner werden eine höhere Gewichtung erhalten als andere, die ein Dutzend Interviewpartnerinnen und -partner vorweisen kann.

2.2.2 Grenzen der systematischen Übersichtsarbeit und Kritik

Die Charakteristika und Vorteile von systematischen Übersichtsarbeiten liegen auf der Hand und wurden in Kapitel 2.2.1 kurz vorgestellt. Durch das strukturierte Aufarbeiten und Aggregieren von Ergebnissen mehrerer Einzelstudien ergeben sich genauso auch Herausforderungen und Nachteile, welche folgend beleuchtet werden.

Uniformitätsproblem

Die ausgewählten Einzelstudien weisen in fast allen Fällen unterschiedliche Operationalisierungen, Stichproben oder Methoden zur Auswertung auf. Die Individualität der Studien und damit auch die daraus folgenden Auswirkungen auf die Ergebnisse erschwert die Vergleichbarkeit erheblich. Dieses Problem wird in der Literatur oft auch als „Apple and Oranges“- oder „Äpfel und Birnen“-Problem bezeichnet (Eisend, 2004, S. 20).

Im Laufe der Zeit haben sich zu diesem Diskussionspunkt zwei Lager gebildet. Die Befürworter der strengen Auswahl von Studien, die gleiche Charakteristika aufweisen, heben vor allem die erhöhte Vergleichbarkeit der Einzelstudien als erstrebenswerte Eigenschaft hervor. Dabei gilt es zu beachten, dass Studien mit gleichen Rahmenbedingungen sich im besten Fall anhand der Untersuchungspersonen und damit der Stichprobe unterscheiden. Demzufolge ist davon auszugehen, dass die Ergebnisse dieser Studien sehr ähnlich sein müssen und schlechtesten Falls eine Abweichung aufgrund eines Stichprobenfehlers aufweisen. Somit ist es sinnvoll, Studien in systemischen

Übersichtsarbeiten zu berücksichtigen, die im Sinne der Fragestellung entsprechende Rückschlüsse erlauben (Eisend, 2004, S. 20-21).

Integration von Studien unterschiedlicher Qualität

Je höher die Qualität der relevanten Studien ist, desto stärker sollten die Ergebnisse dieser Studien in der systematischen Übersichtsarbeit auch berücksichtigt werden. In der Literatur wird dieses Phänomen auch „garbage in – garbage out“ genannt. Dafür können die Erkenntnisse der methodisch besseren Einzelstudien mit höherer Qualität bewertet werden und sollten bei der Analyse auch entsprechend berücksichtigt werden. Eine weitere Möglichkeit für den Umgang mit Studien unterschiedlicher Qualität besteht darin, Studien mit niedrigerer Qualität von der weiteren Betrachtung auszuschließen. Dabei gilt es jedoch zu berücksichtigen, dass dieser Schritt auch gleichzeitig einen Informationsverlust für die Übersichtsarbeit bedeutet. Andererseits können diese Qualitätsunterschiede auch als Indikator für eine hohe Varianz der Studienergebnisse herangezogen werden (Eisend, 2004, S. 22).

Die Beurteilung ist dabei stark subjektiv und hängt damit maßgeblich von den Einschätzungen der Autorinnen und Autoren von Übersichtsarbeiten ab. Eine so eingeführte Moderatorvariable erlaubt die Aufarbeitung der unterschiedlichen Studienqualitäten zu verwertbaren Informationen, sodass vielmehr von „garbage in – information out“ gesprochen werden kann (Eisend, 2004, S. 23).

Verzerrung zugunsten signifikanter Ergebnisse

Eine große Herausforderung von Übersichtsarbeiten, vor allem auch von Metaanalysen, stellt der Selektionsmechanismus dar. Vor allem im Forschungs- und Publikationsprozess werden jene Studien, welche signifikante Ergebnisse aufweisen, stärker gefördert als jene mit weniger auffälligen Ergebnissen. Deshalb wird diese Problematik auch als „publication bias“ oder auch „file drawer problem“ bezeichnet, wobei eben jene unspektakulären Studien oft gar nicht veröffentlicht werden. So gilt es vor allem für Metaanalysen, aber auch für systematische Übersichtsarbeiten, Einzelstudien so auszuwählen, dass ein möglichst großer Querschnitt der vorhandenen Studien und den zugrundeliegenden Daten entsteht. Desto mehr Daten einer Studie zugrunde liegen, desto eher ist davon auszugehen, dass statistische Ausreißer und andere Verzerrungen kompensiert und minimal gehalten werden (Eisend, 2004, S. 23-25).

Integration von abhängigen Daten

Dieser Kritikpunkt wird in der Literatur auch als Effekt von „nonindependent effects“ bezeichnet. Dies bezieht sich auf die Tatsache, dass relevante Ergebnisse einer Studie zu einem bestimmten Thema bis zu einem gewissen Grad statistisch voneinander abhängig sind. Bei der Integration der Einzelergebnisse in einer Übersichtsarbeit werden diese Abhängigkeiten nur selten berücksichtigt. Um diesem Problem zu begegnen können die Ergebnisse in einer Studie aufgrund ihrer Abhängigkeiten zusammengefasst werden. Dabei verringert sich jedoch die Datenbasis dramatisch, weshalb in vielen Metaanalysen oder Übersichtsarbeiten darauf verzichtet wird (Eisend, 2004, S. 25-26).

Fehlende klare Auswahlkriterien

Es liegt in der Natur von Übersichtsarbeiten, die Ergebnisse von Einzelstudien zusammenzufassen und zu integrieren. Aus diesem Grund ist es unbedingt notwendig klar zu stellen, welche Kriterien für den Ein- oder Ausschluss der Studien herangezogen wurden, um diesen Prozess transparent und nachvollziehbar darzustellen. Diese Anforderungen erfüllen nicht alle veröffentlichten Übersichtsarbeiten, wobei auch zu beobachten ist, dass teilweise die Meinung der Autorinnen oder Autoren mit den Ergebnissen der Studien vermengt werden (Deppe, 2004, S. 39).

2.2.3 Hell- und Dunkelfeldforschung

Straftaten, welche von Personen oder Unternehmen zur Anzeige gebracht werden, finden sich in der polizeilichen Kriminalstatistik wieder. Solche Statistiken werden in vielen Ländern erfasst, vor allem auch in Deutschland, Schweiz und Österreich. Die entsprechenden Berichte werden jährlich veröffentlicht und stellen die Entwicklung der kriminellen Geschehen im jeweiligen Land dar (Bundesamt für Statistik BFS, 2016, S. 7; Bundeskanzleramt Österreich, 2016, S. 7; Bundeskriminalamt Deutschland, 2016, S. 1).

Das Hellfeld beschreibt jene Straftaten, welche als solche bei staatlichen Organisationen gemeldet werden und von diesen auch als solche erfasst werden, oder durch eigenständige Ermittlungstätigkeiten der Behörden. Somit stellt das Hellfeld die bekannt gewordene Kriminalität dar, wobei

vorausgesetzt werden muss, dass in den Statistiken auch alle staatlichen Organisationen die jeweils erfassten Straftaten einpflegen.

Das Dunkelfeld beschreibt die unbekannt gebliebene Kriminalität, wobei selbst Hell- und Dunkelfeld gemeinsam kaum das gesamte Maß des Kriminalitätsgeschehens abdecken können. Es ist davon auszugehen, dass das Hellfeld nur einen kleinen Teil des tatsächlichen Geschehens ausmacht. Die meisten Straftaten werden nicht beleuchtet, da sie entweder von den Geschädigten nicht zur Anzeige gebracht werden, oder von den staatlichen Organisationen nicht entdeckt werden. Die Erhebung von Zahlen aus dem Dunkelfeld gestaltet sich deutlich schwieriger als im Hellfeld, da dafür Einzelforschungen ausgewertet werden müssen (Neubacher, 2011, S. 43). Es wird zwischen dem relativen und dem absoluten Dunkelfeld unterschieden. Das relative Dunkelfeld kann durch gezieltes Fragen aufgehellt werden. Somit können mehr Informationen zu Straftaten bekannt werden, weshalb diese Fälle einige Gemeinsamkeiten mit jenen des Hellfelds aufweisen. Das absolute Dunkelfeld hingegen beschreibt jene Straftaten, welche vom Opfer nicht als solche empfunden werden, oder das Opfer selbst nicht berichten möchte oder kann. Die Grenzen zwischen Hell- und Dunkelfeld werden vor allem durch die Definition und die Kriterien einer Straftat bestimmt. Die rechtliche Wertung einer Tat wird maßgeblich von gültigen Gesetzen und Rechtsprechungen bestimmt (Neubacher, 2011, S. 34-35).

Eine weitere Form ist das doppelte Dunkelfeld. Dieses besteht aus Straftaten, welche weder angezeigt, noch durch die Dunkelfeldforschung erfasst werden. Damit sind die Straftaten der doppelten Dunkelfeldforschung ebenfalls nicht in den Kriminalstatistiken erfasst. Vor allem Tatbestände wie Wirtschaftsspionage, Konkurrenzausspähung und Datendiebstahl sind im Vergleich zu einfacheren Delikten wie Einbruch meist sehr komplex. Deshalb können die Opfer oft selbst kaum einschätzen, ob und in welchem Ausmaß sie Opfer eines Angriffs geworden sind.

Die bewährtesten Mittel um das Dunkelfeld, auch in Hinblick auf Wirtschafts- und Industriespionage, aufzuhellen und damit mehr Informationen zu erhalten, sind Befragungen der Opfer. Dafür werden die relevanten Organisationen anonym befragt, ob sie bereits Opfer von solchen Angriffen wurden. Auch im Hinblick auf das Hell- und Dunkelfeld von Wirtschafts- und Industriespionage wäre eine Erhebung der Information relevant, inwiefern nach einem erfolgten Angriff dieser auch zur Anzeige gebracht wurde und welche Informationen weitergegeben wurden. Durch die Betrachtung einer bestimmten Stichprobe

ist es möglich, die Ergebnisse und Erkenntnisse anschließend auf die Gesamtheit der Organisationen hochzurechnen (Kasper, 2014, S. 17-18).

Es gibt keine feste Relation zwischen den beiden Feldern, da die notwendigen Erfassungsfaktoren, wie Anzeigeverhalten oder Kontrollstrategien der Polizei, über lange Zeiträume hinweg konstant bleiben müssten. Die vergangenen Jahre haben gezeigt, dass diese Faktoren alles andere als gleichbleibend sind und damit eine Relation zwischen Hell- und Dunkelfeld unmöglich machen. Es ist vielmehr von einer Beziehungslosigkeit der beiden Felder auszugehen. Aufgrund dieser Beziehungslosigkeit zwischen Hell- und Dunkelfeld und der niedrigen Entdeckungsrate von Straftaten der Polizei durch eigenständige Kontrolltätigkeiten, ist das Anzeigeverhalten der Opfer der maßgebliche Treiber, um das Hellfeld zu erweitern (Neubacher, 2011, S. 36).

Mehrere Faktoren tragen zu der Entscheidung bei, eine Strafanzeige zu erstatten. Einerseits wägt ein Opfer im Rahmen einer Kosten-Nutzen-Analyse die Gründe ab, die für oder gegen eine Anzeige sprechen. Allen voran steht hier der materielle Nutzen, da Versicherungsunternehmen die entsprechenden Leistungen nur gegen Nachweis einer polizeilichen Anzeigebestätigung erbringen. Außerdem werden auch die immateriellen Werte und die möglichen sozialen Auswirkungen einer Anzeige oft bedacht. So werden etwa zwischen 80% und 90% aller Diebstähle von Kraftfahrzeugen angezeigt. Jedoch wird nur jeder zweite sexuelle Angriff zur Anzeige gebracht. Dabei handelt es sich um grobe Schätzungen, da das Dunkelfeld, vor allem bei Sexualdelikten, sehr hoch eingeschätzt wird. Ein weiterer Grund, eine Straftat nicht anzuzeigen, kann darin bestehen, dass das Opfer gar nicht erkennt, dass ein bestimmtes Verhalten strafbar ist. Vor allem beim Betrug ist die Grenzziehung für Juristinnen und Juristen schwierig und für Laien gar unmöglich (Neubacher, 2011, S. 38).

Auch die Exekutive kann mit Maßnahmen dazu beitragen Straftaten aus dem Dunkelfeld in das Hellfeld zu bringen. Allen voran können mit erhöhter Kontrolltätigkeit und Schwerpunktaktionen proaktiv auf Deliktarten eingegangen werden. Als Beispiel sei hier der illegale Drogenhandel angeführt, welcher kaum von Privatpersonen angezeigt wird und deshalb fast ausschließlich durch Maßnahmen der Exekutive aufgedeckt werden kann (Neubacher, 2011, S. 39).

3 Anwendung der Theorie auf die Forschungsfrage

Inhalt

3.1	Allgemeines und Rahmenbedingungen zu der Anwendbarkeit der Theorie auf die Forschungsfrage	45
3.2	Auswahlkriterien für die betrachteten Studien	45
3.3	Gemeinsamkeiten und Unterschiede der betrachteten Studien	47

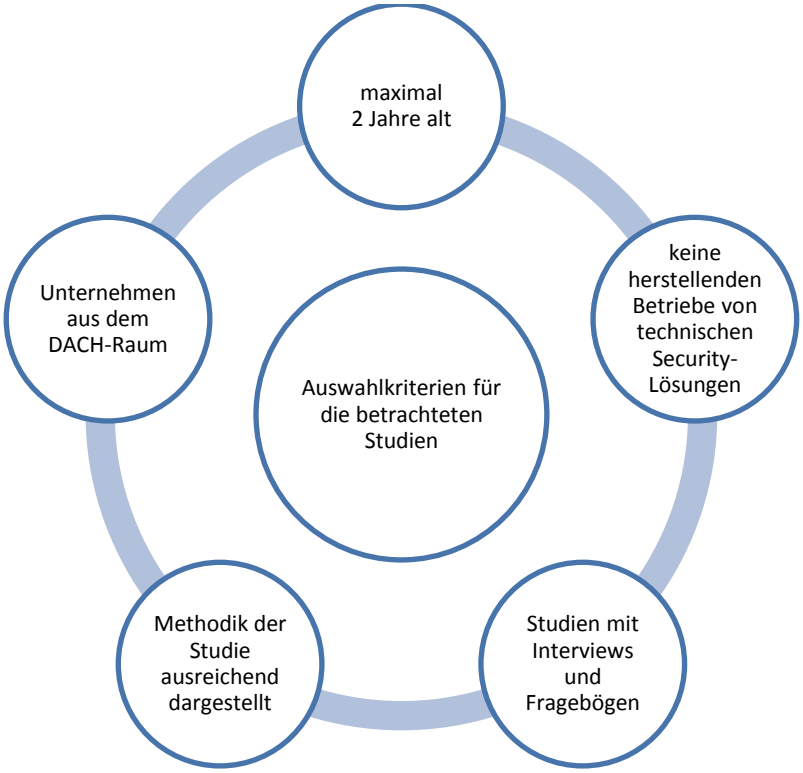
3.1 Allgemeines und Rahmenbedingungen zu der Anwendbarkeit der Theorie auf die Forschungsfrage

Die Basis für die Theorie bilden in der vorliegenden Arbeit die untersuchten Studien zu Wirtschafts- und Industriespionage. Das Kapitel beleuchtet einerseits die Ein- und Ausschlusskriterien der Studien für das systematische Review. Andererseits werden die identifizierten Gemeinsamkeiten und Unterschiede dieser Studien analysiert und detailliert dargestellt.

3.2 Auswahlkriterien für die betrachteten Studien

Für die Recherche von Studien zu dem Themenkomplex Wirtschafts- und Industriespionage wurden im Rahmen der vorliegenden Arbeit vor allem Online-Quellen herangezogen.

Abbildung 1: Übersicht der Auswahlkriterien für die Studien



Quelle: Eigene Darstellung

Eine erste grobe Analyse dazu hat gezeigt, dass einige Studien und Artikel unter den Begriffen „Cybercrime“ bzw. „Cybersecurity“ grundsätzlich auch das Risiko von Wirtschafts- und Industriespionage betrachten. Dabei liegt der Fokus vielmehr auf den technischen Angriffsvektoren als den realen Auswirkungen für Unternehmen. Die Folgekosten werden dabei gar nicht oder nur rudimentär betrachtet. Eine genauere Betrachtung dieser Quellen hat gezeigt, dass diese vor allem von herstellenden Betrieben solch technischer Produkte zur Abwehr der Angriffe veröffentlicht wurden. Die Objektivität und auch die umfassende Betrachtung des Themenkomplexes durch diese Quellen sind deshalb kritisch zu hinterfragen. Ein wichtiges Auswahlkriterium für Quellen im Rahmen dieser Arbeit war dementsprechend die fachliche Unabhängigkeit der Studien und Artikel. Der Einfluss von Herstellerinnen oder Herstellern und deren Motivation die eigenen Lösungen zu vermarkten, wurde damit weitestgehend vernachlässigt.

Der Fokus lag vor allem auf Studien, welche die Erkenntnisse aus Interviews und Fragebögen als Datengrundlage gewannen. Die einzelnen Punkte wurden über telefonische Interviews, sowie Online-Umfragen und schriftliche

Fragebögen abgedeckt. Quellen, deren Datengrundlage ausschließlich aus Incidents und technischen Reports bestehen, wurden von dieser Arbeit explizit ausgeschlossen, um eine umfassende Einschätzung der aktuellen Situation für Organisationen hinsichtlich Wirtschafts- und Industriespionage erhalten zu können. Eine Auswertung von Security-Incidents und –Reports würde ausschließlich jene Fälle widerspiegeln, welche bereits in Organisationen stattgefunden haben. Jedoch könnten damit keine Informationen zu dem Status quo der bestehenden, als auch der geplanten Sicherheitsmaßnahmen getroffen werden.

Im Rahmen dieser Arbeit werden ausschließlich Quellen betrachtet, deren Daten von Organisationen stammen, welche den Hauptsitz in Österreich, Deutschland oder Schweiz anführen, um die Ergebnisse auf den deutschsprachigen Raum anwenden zu können. Es werden ausschließlich Quellen berücksichtigt, welche ab Jänner 2014 veröffentlicht wurden. Damit soll gewährleistet werden, dass die gewonnenen Erkenntnisse dem aktuellen Stand entsprechen und nicht veraltet sind.

Ein weiteres wichtiges Auswahlkriterium der Quellen lag vor allem in der Transparenz der zugrundeliegenden Methodik. Somit wurden jene Studien berücksichtigt, in welchen die Vorgehensweise, der Umfang der Befragten, sowie deren Herkunft beschrieben wurden.

Die Recherche hat gezeigt, dass in einigen Studien der Themenkomplex Wirtschafts- und Industriespionage mit anderen Themenkreisen in Verbindung gebracht wird. Allen voran steht hier die IT im Vordergrund, wobei deren Ausprägung häufig gleichgesetzt wird mit dem Security-Niveau einer Organisation. Außerdem werden auch die Themen Business Continuity Management, Auslandsbeziehungen von Organisationen, als auch allgemeine IT-Trends in Verbindung gebracht.

3.3 Gemeinsamkeiten und Unterschiede der betrachteten Studien

Das folgende Kapitel beschreibt die Gemeinsamkeiten, als auch die Unterschiede jener Studien, welche in Kapitel 1.3.2 dargestellt wurden. Dafür wurden thematische Gruppen identifiziert und die relevanten Aspekte beleuchtet.

Betroffenheit

In allen betrachteten Studien wurde erhoben, ob die befragten Organisationen in den vergangenen Jahren bereits Angriffe in Verbindung mit Wirtschafts- oder Industriespionage verzeichnen konnten. Dabei wurde in mehreren Studien der mögliche Täterkreis beschrieben, wobei die Antworten divergieren. Diese reichen von organisierter Kriminalität, über Hacker, bis hin zum Mitbewerb, wobei sich Mitarbeiterinnen oder Mitarbeiter in fast allen Aufzählungen wiederfinden. Die einzelnen Deliktarten, als auch Ausprägungen von Wirtschafts- und Industriespionage wurden von zwei Studien beleuchtet, wobei der Ausfall der IT, der Verlust von Wettbewerbsvorteilen, als auch Plagiate und Patentrechtsverletzungen angeführt wurden.

Im Rahmen von zwei Studien wurden Organisationen nach den Ursachen für erfolgreiche Angriffe befragt. Die Antworten deuten auf eine starke Einbindung von Cyber-Angriffen hin, sodass neben dem gezielten Einsatz von Social Engineering vor allem fehlende Security-Patches auf Server und Clients, als auch das Ausnutzen von speziellen Schwachstellen der IT-Systeme genannt wurden. Die Antworten der beiden Studien stimmen größten Teils überein, wobei die Reihenfolge der Antworten variiert.

Der aktuelle Status zu den bereits erfolgten Angriffen von Wirtschafts- und Industriespionage wird von den Studien umfassend erfasst. Die Antworten variieren im Detail, doch grundsätzlich ist erkennbar, dass direkte Schäden vor allem durch den Diebstahl von IT-Geräten, der Unterbrechung von Prozessen und dem Abfluss von schützenswerten Informationen entstehen.

In fünf Studien wird festgestellt, dass in den letzten Jahren zwischen 27% und 55% der befragten Unternehmen bereits von Wirtschafts- oder Industriespionage direkt betroffen waren. Davon abweichend kommt eine Studie zu einem Wert von etwa 5%, welcher von den anderen deutlich abweicht. Dennoch scheint diese Information durchgehend erhoben zu werden.

Die Ergebnisse nach der Frage der betroffenen Abteilungen weisen teilweise gleiche Aussagen auf. Demnach sind vor allem die IT-Abteilung, als auch die Forschung und Entwicklung, sowie die Logistik der Unternehmen betroffen.

Starke Unterschiede in den Antworten gab es hinsichtlich der Branchen der betroffenen Organisationen. Dabei sind keine Übereinstimmungen vorhanden,

wobei diese Information ausschließlich von zwei Studien nachvollziehbar erhoben und dargestellt wurden.

Schäden

Der reale Schaden durch Wirtschafts- und Industriespionage in deutschsprachigen Organisationen wird durch die betrachteten Studien ausführlich beleuchtet. Große Einigkeit herrscht bei den Schadenshöhen der meisten Fälle, welche zwischen 10.000 Euro und 100.000 Euro liegt.

Die Aussagen zu den jährlichen Schäden pro Jahr sind nicht in dieser Ausführlichkeit abgefragt worden, gleichwohl diese einzelnen Ergebnisse medienwirksam kommuniziert wurden. Diese reichen von 1,6 Mrd. Euro für Österreich, über 11,8 Mrd. Euro oder sogar 51 Mrd. Euro für Deutschland.

Bei diesen Schäden handelt es sich sowohl um den direkten materiellen Schaden, als auch die Schätzungen zu den immateriellen Folgewirkungen. Die unterschiedlichen Ergebnisse zu der Fragestellung nach den Hinweisen zu materiellen oder immateriellen Schäden spiegelt diese schwierige Schätzung wider.

Kronjuwelen

Es wurde nur in zwei Studien nach den Kronjuwelen der Unternehmen gefragt. Die Fragen zielten vor allem auf den Bekanntheitsgrad der wichtigsten Assets des Unternehmens ab und in welchem Ausmaß diese bewusst geschützt werden. Aufgrund der Ergebnisse ist davon auszugehen, dass ein Großteil der Organisationen der Meinung ist, dass ihnen die eigenen Kronjuwelen bekannt sind. Hinsichtlich der Schutzmaßnahmen wird in einer Studie deutlich auf die Sensibilität der Mitarbeiterinnen und Mitarbeiter hingewiesen.

Management Attention

Die Aufmerksamkeit des Managements von Organisationen zu dem Thema Wirtschafts- und Industriespionage wird ausschließlich von einer Studie rudimentär betrachtet. Dabei wird die firmeninterne Kommunikation des Themenkomplexes auf Ebene der Entscheidungsträger abgefragt. In einer weiteren Studie wird hinterfragt, welches Budget für Präventionsmaßnahmen aufgewendet wird, um das Risiko von Spionage-Angriffen zu reduzieren.

Organisatorische Zuordnung des Informationsschutzes

Die eingesetzten Planstellen für den Themenkomplex des Informationsschutzes wurden im Rahmen von drei Umfragen erhoben. Die Ergebnisse zeigen einstimmig, dass sich in etwa der Hälfte der Organisationen zumindest eine Person ausschließlich diesem Thema widmet. Organisatorisch ist diese Person in den meisten Fällen der IT-Abteilung zugeordnet, in manchen Unternehmen direkt der Geschäftsführung.

Eine Studie weicht von diesem Ergebnis erheblich ab, wobei aufgrund dessen Antworten nur in 12% der Fälle eine solche Person mit den Aufgaben betraut wird.

Analyse und Reporting

Die Antworten von drei Umfragen zeigen unterschiedliche Aussagen zu den möglichen Ursachen für erfolgreiche Angriffe. Dabei werden entweder das Fehlverhalten von Mitarbeiterinnen und Mitarbeitern, gezielter Einsatz von Malware oder Hackerangriffe als häufigste Ursache gesehen. Diese Antworten sind die Aussagen der befragten Organisationen zu bereits durchgeführten Angriffen.

Die Erhebung der firmeninternen Berichterstattung zu möglichen Angriffen findet sich nur in einer Studie wieder, wobei 72% der befragten Unternehmen monatlich oder öfters berichten. Hingegen 23% überhaupt kein Reporting zu dieser Bedrohung durchführen.

Security-Policy

Gemäß den Aussagen in drei Studien gibt es in etwa 21% bis 45% der befragten Organisationen festgelegte Sicherheitsrichtlinien, welche auch umgesetzt und kontrolliert werden. Ebenso stellen zwei Arbeiten fest, dass zwischen 36% und 44% der Unternehmen eine Datenklassifizierung vorgeben, nach der die Daten einzuordnen und entsprechend der Klassifizierung auch zu behandeln sind.

Die Aspekte der technischen Umsetzung der Security-Policies werden in mehreren Studien erhoben, wobei sich auch die Fragen deutlich voneinander abgrenzen lassen. Vier der betrachteten Studien belegen, dass Unternehmen Verschlüsselungsmöglichkeiten bei der Übertragung von Daten einsetzen, wobei die Antworten von 36% bis 80% reichen. Die Verschlüsselung von

gespeicherten Daten wird von drei Umfragen erhoben und die Antworten liegen zwischen 36% und 52%. Gemäß zweier Studien liegt der Passwortschutz mit über 90% auf einem sehr hohen Niveau, wobei eine weitere Studie gezielt nach einem Passwortschutz auf allen Geräten fragt und das Ergebnis mit rund 56% deutlich niedriger ausfällt. Ebenfalls so viele Studien sind sich einig darüber, dass etwa ein Viertel bis ein Drittel der befragten Unternehmen eine erweiterte User-Identifikation einsetzt.

Physischer Schutz

Die physische Sicherheit vor Wirtschafts- und Industriespionage wird durch die ausgewählten Studien nur rudimentär betrachtet. Nur eine Studie hat die Frage gestellt, inwiefern der physische Zugriff oder Zutritt in Unternehmen gewährleistet ist, um einen unrechtmäßigen Zugriff auf Informationen oder Diebstahl von physischen Assets zu verhindern.

Zwei weitere Umfragen haben erhoben, ob ein unberechtigter Zutritt zu Assets verhindert werden kann. Die Antworten überschneiden sich teilweise, da etwaige bauliche Zutrittsbeschränkungen bei beiden Studien genannt wurden.

Technischer Schutz der IT

Der technische Schutz der IT von Unternehmen wird in den Studien ausführlich beleuchtet. Dabei werden Themen, wie Malware-Schutz, Firewalls oder Intrusion Prevention Systeme abgefragt. Vier der Studien erhoben den Einsatz von Firewalls und bescheinigen die entsprechende Nutzung in 86% bis 100% der untersuchten Organisationen. Drei Umfragen stellen fest, dass in 85% bis 100% ein umfassender Malware-Schutz auf den IT-Geräten eingesetzt wird. Das schließt vor allem Clients, Server und auch mobile Geräte ein. Ebenfalls die Abdeckung von aktuellen Patches und Updates wird von zwei Studien mit 65%, bzw. 74% ähnlich hoch ausgewiesen.

Im Gegensatz dazu unterscheiden sich die Ergebnisse von zwei Studien hinsichtlich der Wireless Security von Unternehmen mit 14% und 55% erheblich. Dabei sind aufgrund der Beschreibungen und den Fragestellungen unterschiedliche Auffassungen möglich. Auch die Antworten zu dem Einsatz von Intrusion Detection Systeme, Intrusion Prevention Systeme oder Data Loss Protection weisen mit 26% und 6% unterschiedliche Ergebnisse auf.

Prüfungen der Sicherheitsmaßnahmen

In fünf der sieben Studien wird erhoben, inwiefern die befragten Unternehmen Sicherheitsüberprüfungen durch externe Expertinnen und Experten oder durch die interne Revision durchführen lassen. Die Antworten bezeugen, dass zwischen 20% und 54% der Organisationen eine regelmäßige Überprüfung der Unternehmenssicherheit durchführen. Dabei werden die bereits eingesetzten Sicherheitsmaßnahmen des Unternehmens geprüft, um mögliche Sicherheitslücken oder Schwachstellen aufzudecken, welche von böswilligen Angreifern ausgenutzt werden könnten. Somit erhält das Unternehmen die Möglichkeiten diese Missstände weiter zu behandeln, einer Bewertung zuzuführen und bei Bedarf Gegenmaßnahmen einzusetzen.

Business Continuity Management

Im Rahmen von zwei Studien wurden Unternehmen gefragt, ob diese bereits ein Business Continuity Management einsetzen und ihm Bedarfsfall einsetzen können. Die Ergebnisse weichen deutlich voneinander ab, wobei 35% der Unternehmen antworteten festgelegte Maßnahmen für den Krisenfall definiert zu haben. Dem gegenüber steht ein anderes Studienergebnis, demnach 87% Sicherheitsmaßnahmen, wie Sicherheitsrichtlinien und Notfallpläne, einsetzen.

Gemäß den Ergebnissen von zwei anderen Studien besitzen etwa die Hälfte der Unternehmen einen Notfallplan für akute Fälle von Wirtschafts- und Industriespionage, um auf diese rasch und angemessen reagieren zu können. Dabei werden nicht nur technische Maßnahmen berücksichtigt, vor allem auch die Öffentlichkeitsarbeit, als auch Möglichkeiten zur Einleitung von forensischen Analysen.

Analyse von Aktivitäten auf IT-Systemen

Die ausgewählten Umfragen hinterfragen die Nutzung von Möglichkeiten, um Unregelmäßigkeiten in den Aktivitäten der Unternehmen feststellen zu können. Dabei werden einerseits technische Lösungen eingesetzt, welche Protokolldateien von IT-Systemen auswerten und mögliche Auffälligkeiten darstellen. Diese Möglichkeiten werden ausschließlich von einer Studie betrachtet und weisen einen niedrigen Wert von knapp 9% auf.

Andererseits werden allgemeine Möglichkeiten zur Erkennung von Abweichungen des erwünschten Verhaltens ebenfalls von zwei Studien abgefragt, wobei beide Ergebnisse um rund 40% liegen. Somit setzt jedes

vierte befragte Unternehmen auf Lösungen, um solch ein unerwünschtes Verhalten zu erkennen.

Eine einzige Studie beschäftigte sich mit der Frage um die laufende Analyse von Social Media Plattformen und privaten Cloud-Lösungen, um den unerwünschten Datenabfluss identifizieren zu können. Etwa 9% der von dieser einen Studie befragten Unternehmen setzen auf solch eine laufende Analyse.

Beziehungen mit ausländischen Unternehmen

Zwei Umfragen erhoben, mit welchen Ländern die befragten Unternehmen die meisten Geschäftsbeziehungen pflegen. Dabei kamen beide zu dem Schluss, dass Unternehmen aus Deutschland, Schweiz und Österreich vor allem mit Ländern in Westeuropa Geschäfte pflegen, als auch in Osteuropa und einige auch noch mit Asien.

Einschätzung der Effektivität bereits getroffener Maßnahmen

Für eine Einschätzung, der bereits getroffenen Maßnahmen zur Prävention von Wirtschafts- und Industriespionage, wurden im Rahmen von drei Studien die Organisationen befragt. Dabei wurde festgestellt, inwiefern diese selbst den aktuellen Status als angemessen oder ausreichend ansehen. Die Ergebnisse weisen einheitlich eine Selbsteinschätzung der Unternehmen aus, nach der 18% bis 20% die aktuellen Maßnahmen für nicht geeignet halten.

Eine Studie erhob die Angriffsvektoren, welche durch aktuelle Sicherheitsvorkehrungen am schlechtesten abgewendet werden könnten. Dabei wurden an erster Stelle Hackerangriffe genannt, dicht gefolgt von den Risiken durch Home Office, Smartphones und Tablets. Fast ebenso hoch wird das Risiko von Social Engineering eingeschätzt. Das Ergebnis einer anderen Studie kam zu einem anderen Ergebnis, wonach fast ausschließlich Social Engineering als Einfallstor für Angreifer eingeschätzt wird.

Planung weiterer Maßnahmen

Insgesamt betrachtet wurde die Frage nach zukünftig geplanten Maßnahmen von unterschiedlichen Studien auf der organisatorischen, der technischen und der personellen Ebene gestellt. Drei Studien befragten die Organisationen hinsichtlich geplanter organisatorischer Maßnahmen in nächster Zukunft. Dabei wurden unterschiedliche Antworten gegeben, wobei Security

Awareness Kampagnen mehrfach genannt wurden. Jeweils zwei Umfragen haben Informationen zu den geplanten Maßnahmen auf technischer und personeller Ebene erhoben. Dabei wurden Firewalls, Virenschutz und Identity and Access Management von zwei Studien dargelegt. Hinsichtlich personellen Präventionsmaßnahmen für die Zukunft herrschen stark unterschiedliche Meinungen vor, wobei sich keine relevanten Übereinstimmungen finden lassen. Es wurden dabei unterschiedliche Möglichkeiten genannt, welche vor allem die Sensibilität der Mitarbeiterinnen und Mitarbeiter bei dem Umgang mit besonders schützenswerten Daten erhöhen sollen.

In einer einzigen Studie wurde nach der Einschätzung hinsichtlich der aktuellen Loyalität der Mitarbeiterinnen und Mitarbeiter gefragt. Dabei schätzt knapp die Hälfte der befragten Unternehmen ihr Personal loyal ein. Mehr als ein Viertel kann dies nicht ausreichend einschätzen und rund 20% sehen sogar eine sinkende Loyalität.

Eine andere Umfrage hat Unternehmen die Frage gestellt, ob Versicherungen im Zusammenhang mit Wirtschafts- und Industriespionage, speziell im Cyber-Umfeld, zukünftig genutzt werden. Knapp 20% bejahten diese Frage, sodass bei diesen Organisationen die Versicherung von Cyber-Risiken für das kommende Jahr geplant ist.

4
Empirischer Teil

Inhalt

4.1	Forschungsfrage und Hypothese	55
4.2	Forschungsdesign	56
4.2.1	Grundlegende Entscheidungen für eine qualitative Forschung	57
4.2.2	Verfahren und Messmethode	58
4.3	Operationalisierung	64
4.4	Gestaltung und Anpassung des Interviewleitfadens	66
4.5	Durchführung der Erhebung	67
4.5.1	Auswahlkriterien und Rahmenbedingungen für die Experteninterviews	67
4.6	Ergebnisse	69
4.6.1	Anwendung der qualitativen Inhaltsanalyse	69
4.6.2	Ergebnisse der Experteninterviews	70
4.6.3	Beurteilung der Hypothese	74
4.7	Zusammenfassung und Interpretation	75

4.1 Forschungsfrage und Hypothese

Das folgende Kapitel beschreibt die zentrale Forschungsfrage der vorliegenden Arbeit, sowie die forschungsleitenden Fragen und die Hypothese.

Forschungsfrage

Welche Themenschwerpunkte spielen in der gegenwärtigen Erforschung des Phänomens Wirtschafts- und Industriespionage anhand ausgewählter Studien eine relevante Rolle, welche Gemeinsamkeiten und Unterschiede weisen die Studien auf und inwieweit sind die ermittelten Schwerpunkte für die Praxis relevant?

Aufgrund dieser Forschungsfrage wurden folgende forschungsleitenden Fragen erarbeitet, um den Themenkomplex besser abzugrenzen und die relevanten Aspekte näher zu beleuchten. Dabei werden relevante Studien zu

dem Themenkomplex Wirtschafts- und Industriespionage in deutschsprachigen Ländern berücksichtigt, als auch geltende Gesetze, Normen und EU-Richtlinien.

Forschungsleitende Fragen

- Was sind die Charakteristika von Wirtschafts- und Industriespionage?
- Wie ist das Dunkelfeld bei Wirtschafts- und Industriespionage zu bewerten?
- Welche Studien können für einen Vergleich von Wirtschafts- und Industriespionage herangezogen werden?
- Welche Gemeinsamkeiten und Unterschiede können mithilfe einer systematischen Übersichtsarbeit zu Wirtschafts- und Industriespionage erhoben werden?
- Bilden die in den Studien untersuchten Kriterien, die Herausforderungen deutschsprachiger Unternehmen ab?

Aufgrund dieser Fragestellungen wurde folgende Hypothese abgeleitet.

Hypothese

H1: Die aus den Studien ermittelten Themenschwerpunkte decken sich mit den relevanten Problemen durch Wirtschafts- und Industriespionage in der Praxis.

Die Hypothese prüft, inwiefern jene Themenschwerpunkte und Kriterien, welche in den Studien betrachtet wurden, in der Praxis maßgebliche Auswirkungen auf Organisationen haben.

4.2 Forschungsdesign

Das folgende Kapitel beschreibt die Planung und die grobe Struktur des Forschungsvorhabens der vorliegenden Arbeit. Die Vorgehensweise unterteilt sich in mehrere Teilschritte, welche folgend näher beleuchtet werden.

4.2.1 Grundlegende Entscheidungen für eine qualitative Forschung

Für die Durchführung von wissenschaftlichen Arbeiten bieten sich entweder quantitative oder qualitative Messmethoden zur Erhebung von Daten an. Die Unterscheidung zwischen diesen beiden Varianten ist absolut, sodass es für bestimmte Anforderungen auch Mischformen gibt. Es gilt jene Methoden zu wählen, welche bestmöglich geeignet sind, um die in Kapitel 1.4 beschriebenen forschungsleitenden Fragen zu beantworten und damit in Folge die in Kapitel 4.1 Hypothesen zu unterstützen oder zu widerlegen.

Die quantitative Forschung eignet sich vor allem für Umgebungen, in denen Standards vorherrschen, klare Zahlen und Fakten möglichst objektiv vorliegen und damit auch eine klare Vorgehensweise erlauben. Diese Eigenschaften begünstigen einen möglichst linearen Forschungsprozess. Nachdem ein Problem ausreichend identifiziert und von anderen Themen abgegrenzt wurde, erfolgt die Hypothesenbildung und danach erfolgt die Festlegung des Forschungsprozesses, sowie der Operationalisierung. Anschließend werden Daten erfasst, aufbereitet und ausgewertet. Diese Informationen bieten die Basis, um die im theoretischen Teil aufgestellte Hypothese zu unterstützen, oder abzulehnen (Baur & Blasius, 2014, S. 135-150). Dabei ist grundsätzlich keine Wiederholung der einzelnen Schritte vorgesehen, sondern diese haben sequenziell zu erfolgen (Baur & Blasius, 2014, S. 118). Außerdem versucht die quantitative Forschung die Subjektivität der Forscherinnen und der Forscher weitestgehend zu minimieren (Baur & Blasius, 2014, S. 46).

Die qualitative Forschung unterscheidet sich gegenüber der quantitativen vor allem durch ihre Zirkularität der einzelnen Teilschritte im Forschungsprozess (Baur & Blasius, 2014, S. 118). Die strikte Linearität ist hierbei nicht in dieser Ausprägung gegeben, sodass neu gewonnene Erkenntnisse eine Änderung der Forschungsfragen oder Hypothesen ermöglichen. Dadurch können die Phasen der Datenauswahl, Datenerhebung und Datenanalyse einander mit der theoretischen Reflexion abwechseln. Qualitative Forschung kann durch diese offene Zugangsweise näher und flexibler auf die zu untersuchenden Phänomene eingehen. Gerade diese Offenheit, für neue Erfahrungswelten und für das Unbekannte in dem scheinbar Bekannten, ist der Ausgangspunkt für eine gegenstandsbezogene Theoriebildung (Flick, 2008, S. 17). Außerdem werden die Forscherinnen und Forscher als Teil der Gesellschaft und erst durch ihr mitgebrachtes Verständnis, die Gewinnung von Erkenntnissen ermöglichen (Baur & Blasius, 2014, S. 47). Die qualitative Forschung zeichnet sich zusätzlich durch eine rekonstruktive Ausrichtung aus. Dabei wird etwas

rekonstruiert, was in sich bereits sinnhaft ist und dessen Sinn in wissenschaftliche Konzepte übertragen werden soll (Baur & Blasius, 2014, S. 118).

Im Rahmen der vorliegenden Arbeit wurden ein qualitativer Ansatz, sowie eine deduktive Vorgehensweise für den Forschungsprozess gewählt. Es wird jedoch nicht der Ansatz der gegenstandsbezogenen Theoriebildung verfolgt. Dabei wird aufgrund der forschungsleitenden Fragen, des aktuellen Standes der Forschung und der analysierten Studien eine entsprechende Hypothese abgeleitet. Diese Hypothese wird durch Interviews von Expertinnen und Experten überprüft.

Einen wichtigen Bestandteil der theoretischen Grundlagen bildet das systematische Review der aktuell verfügbaren Studien für den deutschsprachigen Raum im Kapitel 1.3.2. Die Erkenntnisse der Gemeinsamkeiten und Unterschiede aus Kapitel 3.3 sollen auf den Praxisbezug hin geprüft werden, wofür Interviews mit Sicherheitsexpertinnen und –experten aus Organisationen gewählt werden. Aufgrund der Informationen durch die Interviews sollen die Erkenntnisse der Studien auf ihren Praxisbezug hin überprüft werden.

Aufgrund der mangelnden theoretischen Grundlagen für die Vorgehensweise und fehlender Struktur der Erhebung von Wirtschafts- und Industriespionage war zu Beginn der vorliegenden Arbeit nicht abschließend auszuschließen, dass die definierten forschungsleitenden Fragen, die Schwerpunkte, als auch die Vorgehensweise das aktuelle Bild der Praxis von Wirtschafts- und Industriespionage für Organisationen angemessen und ausreichend widerspiegeln kann. Durch fehlende theoretische Konzepte und nicht standardisierte Messmethoden hinsichtlich Wirtschafts- und Industriespionage wird bereits zu Beginn der vorliegenden Arbeit von Anpassungen des Forschungsprozesses, aufgrund neuer Erkenntnisse während des Prozesses, ausgegangen. Diese Flexibilität kann mit einer quantitativen Forschung, mit ihren klar definierten Methoden, Standards und linearem Forschungsprozess nicht gewährleistet werden. Daher fiel die Wahl auf ein qualitatives Verfahren.

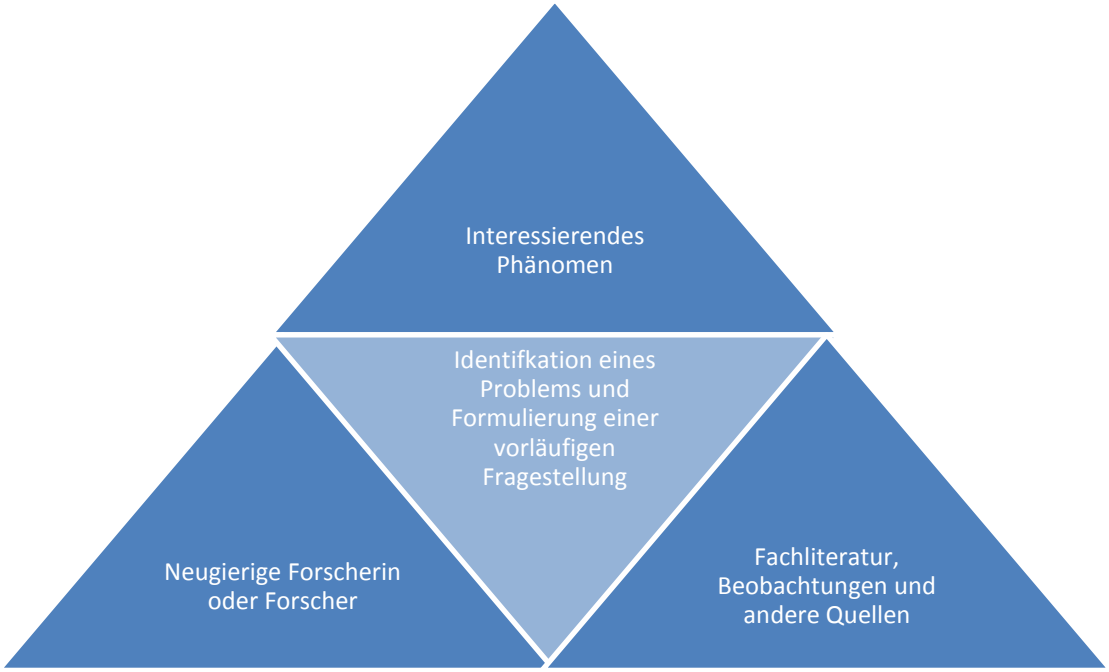
4.2.2 Verfahren und Messmethode

In Kapitel 1.3.2 wurden im Sinne der vorliegenden Arbeit relevante Studien zum Zweck der Hypothesenbildung erfasst und dargestellt. Diese stellen eine

wichtige Informationsquelle dar. Außerdem beleuchtet das Kapitel 3.3 die identifizierten Übereinstimmungen und genauso auch die Unterschiede der Ergebnisse dieser Studien.

Das Phänomen der Wirtschafts- und Industriespionage von Organisationen im deutschsprachigen Raum war ausschlaggebend für den Ansatz der vorliegenden Arbeit. Dabei stellen vor allem die mediale Berichterstattung von Einzelfällen, als auch das vermeintliche Dunkelfeld zu diesem Thema kaum einschätzbare Faktoren dar. Die identifizierten Studien wurden ausgewählt, um als theoretische Grundlage einen Überblick zu dem Themenkomplex zu erhalten. Die Schlussfolgerungen und Aussagen werden mittels Befragungen von Expertinnen und Experten hinsichtlich ihrer Relevanz in der Praxis überprüft. Außerdem ist eine neugierige Forscherin oder ein neugieriger Forscher notwendig, um diese Schritte durchzuführen. Die Abbildung 2 zeigt im Mittelpunkt der Forschungstrias zur Identifikation von Fragestellungen die Identifikation des Problems, sowie die Formulierung von vorläufigen Fragestellungen.

Abbildung 2: Forschungstrias zur Identifikation von Fragestellungen



Quelle: Eigene Darstellung nach (Baur & Blasius, 2014, S. 121)

Um diese Erkenntnisse auf die Relevanz in der Praxis hin zu prüfen gibt es unterschiedliche Möglichkeiten. Nach Meuser und Nagel (Meuser & Nagel, 1991, S. 442) bieten sich hierfür Interviews mit Expertinnen und Experten an. Im Gegensatz zu anderen Formen des offenen Interviews, wird durch Interviews von Expertinnen und Experten nicht die Person als Gesamtheit erfasst, sondern vielmehr die Expertise dieser Person zu dem gewählten Themenkomplex. Der Lebenszusammenhang der Person steht hierbei explizit nicht im Mittelpunkt, sondern stellt vielmehr nur einen Faktor dar. Dabei ist es sinnvoll, dass diese Personen keine beratenden Tätigkeiten, im Sinne von Consultants oder externen Prüferinnen und Prüfern ausüben, sondern selbst ein Teil des zu untersuchenden Handlungsfeldes sind.

In den meisten Fällen sind Expertinnen und Experten in einer Organisation nicht in der Ebene der Top-Führungskräfte anzutreffen, sondern vielmehr darunter. Jene Personen, die Sachverhalte erfassen, aufbereiten und für die Entscheiderinnen und Entscheider aufbereiten, besitzen das meiste Fachwissen zu einem Fachgebiet und sind in diesem Sinne als Expertinnen und Experten zu betrachten (Meuser & Nagel, 1991, S. 443-444).

Das Erfahrungswissen der Expertinnen und Experten wird im Rahmen der vorliegenden Arbeiten vor allem als Betriebswissen angesehen (Meuser & Nagel, 1991, S. 446). Wie bereits auch in den forschungsleitenden Fragen dargestellt wurde, gilt es zwar die Erfahrungen der Expertinnen und Experten mit den Ergebnissen der Studien zu vergleichen, doch vielmehr soll auch erhoben werden, zu welchem Grad die in den Studien erfassten Themen in der Praxis als relevant oder hilfreich angesehen werden. Außerdem sollen auch mögliche Schwerpunkte oder Sichtweisen der Expertinnen und Experten erfasst werden, welche bisher durch die betrachteten Studien nicht oder nur unzureichend dargestellt wurde.

Vor allem die Auseinandersetzung mit den Gemeinsamkeiten und Unterschieden der einzelnen Studien in Kapitel 3.3 hat gezeigt, dass unterschiedliche Schwerpunkte gesetzt werden, manche Themen in nahezu allen Studien angeführt werden und andere Aspekte nur in einzelnen betrachtet wird. Nun gilt es mit dem Kontextwissen der Expertinnen und Experten zu erheben, inwiefern die identifizierten Aspekte in der Praxis an Relevanz finden. Zusätzlich ist auch im Interesse der vorliegenden Arbeit festzuhalten und zu analysieren, inwiefern die Erkenntnisse der Studien sich mit den Erfahrungen der Expertinnen und Experten decken.

Kriterien für Expertinnen und Experten

Sofern eines der beiden folgenden Kriterien erfüllt ist, ist diese Person als Expertin oder Experte zu bezeichnen (Meuser & Nagel, 1991, S. 443).

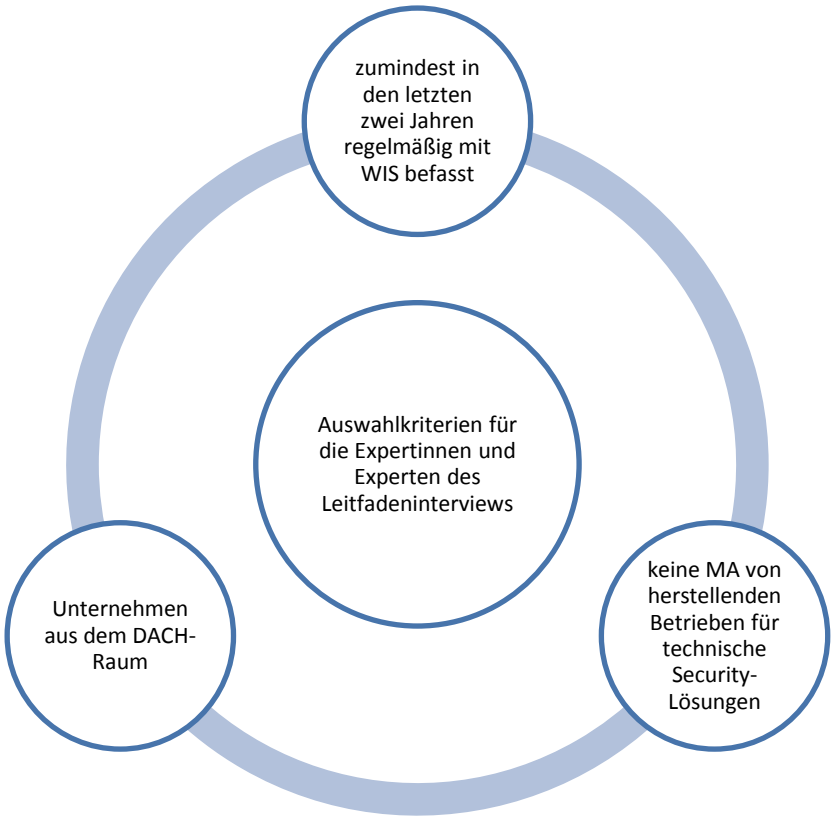
Die Person trägt Verantwortung für den Entwurf, die Implementierung oder die Kontrolle einer Problemlösung.

Die Person verfügt über einen privilegierten Zugang zu Informationen von Personengruppen oder Entscheidungsprozessen.

Im Kontext dieser Arbeit werden die Expertinnen und Experten in Organisationen voraussichtlich als Security Manager, Chief Information Security Officer oder auch Security Analyst bezeichnet. Vor allem bei Organisationen, welche nach ISO 27001 zertifiziert sind, ist davon auszugehen, dass diese Personen als Informationssicherheits-Manager bezeichnet werden (Austrian Standards Institute, 2008, S. 21).

Abgesehen von dieser Anforderung, werden für die Interviews ausschließlich Expertinnen und Experten befragt, welche den gleichen Anforderungen entsprechen, die in Kapitel 3.2 für die Studien festgelegt wurden.

Abbildung 3: Übersicht der Auswahlkriterien für die Expertinnen und Experten



Quelle: Eigene Darstellung

Die Expertin oder der Experte muss sich in den vergangenen zwei Jahren zumindest regelmäßig im beruflichen Kontext mit dem Thema Wirtschafts- und Industriespionage auseinandersetzen. Dabei ist es nicht relevant, wie die Rolle intern bezeichnet oder genannt wird. Es spielt außerdem auch keine Rolle, ob diese Position eine Personalführung bedingt, oder in welcher Organisationseinheit diese angesiedelt ist.

Analog zu den ausgewählten Studien müssen die Befragten für Unternehmen tätig sein, welche vorwiegend im DACH-Raum, also Deutschland, Schweiz oder Österreich, tätig sind. Es konnten ausschließlich Experten aus Österreich gefunden werden, die sich für das Interview bereit erklärten. Diese Auswahl entspricht dem Kriterium, jedoch befinden sich damit keine Expertinnen oder Experten aus Deutschland oder der Schweiz darunter.

Es werden keine Personen befragt, welche direkt für herstellende Betriebe von technischen Security-Lösungen tätig sind. Somit wird eine mögliche Motivation zur veränderten Sichtweise aufgrund von Unternehmenszielen ausgeschlossen.

Das Alter und das Geschlecht der Expertinnen und Experten sind für die Auswahlkriterien nicht relevant und werden dementsprechend bei der Auswahl nicht weiter berücksichtigt.

Aspekte der Interviews

Den Expertinnen und Experten werden mittels Leitfadeninterview offene Fragen zu dem Themenkomplex Wirtschafts- und Industriespionage gestellt. Entgegen geschlossenen Fragen, welche ausschließlich durch vorgegebene Möglichkeiten ein gewisses Spektrum an Antworten ermöglichen, wird durch Einsatz von offenen Fragen den Befragten weitestgehend eingeräumt ihr eigenes Verständnis des Themas darzustellen. Außerdem werden keine Suggestivfragen gestellt, welche eine vorangestellte Meinung bereits implizieren würden. Dadurch soll gewährleistet werden, dass die befragten Personen nach Möglichkeit ihre eigenen Meinungen, Ansichten und Erfahrungen darstellen und dabei durch das Interview möglichst wenig beeinflusst werden. Somit stellen die Expertinnen und Experten direkt die Zielgruppe dar und können Auskunft über ihr eigenes Handlungsfeld geben (Meuser & Nagel, 1991, S. 445).

Der Einsatz eines Leitfadeninterviews ermöglicht die grobe Ausrichtung des Interviews auf den Themenkomplex Wirtschafts- und Industriespionage. Dabei wird jedoch keine Einschränkung auf einzelne Teilaspekte ermöglicht. Darüber hinaus stellt ein leitfadenorientiertes Gespräch sicher, dass im Laufe der Befragung von der definierten Absicht nicht zu weit abgewichen wird. Nach Abschluss der Interviews kann somit eine generalisierte Auswertung der Antworten durchgeführt werden. Ein Leitfadeninterview unterstützt die Gesprächspartner dabei, nicht zu weit vom Thema abzuweichen und erlaubt gleichzeitig den Expertinnen und Experten die eigene Sichtweise darzustellen (Meuser & Nagel, 1991, S. 447-448).

Wichtige Eckpfeiler der Interviews

Im Rahmen des Interviews werden die Befragten um eine Einschätzung ihres Kenntnisstandes zu aktuellen Studien hinsichtlich Wirtschafts- und Industriespionage gebeten. Damit werden die Informationsquellen für

Expertinnen und Experten erhoben. In einem weiteren Schritt kann damit ausgewertet werden, inwiefern die, im Rahmen der vorliegenden Arbeit ausgewählten, Studien in der Praxis für Betroffene relevant sind. Dabei wird zuerst abgefragt, welche Berührungspunkte sie bisher mit Fällen in der Vergangenheit mit diesem Thema hatten.

Die Expertinnen und Experten wurden im Rahmen des Interviews nach ihrem Kenntnisstand von aktuellen Studien und dessen Ergebnissen befragt. Diese Einschätzung bietet einen Einblick darüber, welche Risiken von Informationssicherheits-Managerinnen und –Managern in der Praxis bewusst wahrgenommen werden. Dies bietet erst die Möglichkeit, dass Organisationen diese Risiken bewerten und entsprechend reagieren können. Der Vergleich zu den identifizierten Schwerpunkten der ausgewählten Studien kann weitere Einblicke hinsichtlich der Wahrnehmung von Wirtschafts- und Industriespionage bieten.

Die Befragten sollen ebenfalls aus ihrer Sicht darlegen, über welche Teilaspekte ausreichend Informationen vorliegen und für welche Fälle bisher zu wenig Information vorhanden sind.

4.3 Operationalisierung

Im Rahmen der Operationalisierung wurden die relevanten Elemente der Hypothesen in verschiedene Dimensionen zerlegt. Anschließend wurden Indikatoren und die zugehörigen Messgrößen definiert, um die Dimensionen messbar zu gestalten. Diese Indikatoren sollen vor allem durch die Antworten der Expertinnen und Experten im Zuge der Leitfadeninterviews beantwortet werden. Dadurch soll eine nachvollziehbare Beurteilung der in der vorliegenden Arbeit definierten Hypothese ermöglicht werden. Folgend wird die Hypothese nochmals dargestellt und anschließend werden die identifizierten Begriffe, Dimensionen und Indikatoren angeführt.

H1: Die aus den Studien ermittelten Themenschwerpunkte decken sich mit den relevanten Problemen durch Wirtschafts- und Industriespionage in der Praxis.

Tabelle 2: Operationalisierung der Hypothese H1

Begriff	Dimension	Indikator
B1 Wirtschafts- und Industrie-spionage	**D1** Vorfall	**I1** Erkennung
		I2 Erfahrung
		I3 Kurzfristige Schäden
		I4 Langfristige Schäden
	D2 Management Awareness	**I5** Kriterien zur internen Bewertung
		I6 Risikobewertung
		I7 Kommunikation
		I8 Bewusstsein bei Führungskräften
B2 Anwendbarkeit der Studien-ergebnisse in der Praxis	**D3** Relevanz in der Praxis	**I9** Hohe Relevanz
		I10 Keine Relevanz
		I11 Dunkelfeld
	D4 Unterschied Studien und Vorfälle	**I12** Relevanz von Studien und bekannten Fällen in der Praxis
		I13 Präferenz Studien oder Einzelfälle
	D5 Informations-bedarf	**I14** Verfügbare Informationen
		I15 Informationslücken
	D6 Ermittelte Themen-	**I16** Betroffenheit

	schwerpunkte der Studien	**I17** Kronjuwelen
		I18 Security-Policy
		I19 Physischer Schutz
		I20 Technischer Schutz der IT
		I21 Prüfungen der Sicherheitsmaßnahmen
		I22 Business Continuity Management
		I23 Analyse von Aktivitäten auf IT-Systemen
		I24 Beziehungen mit ausländischen Unternehmen
		I25 Einschätzung der Effektivität bereits getroffener Maßnahmen
		I26 Planung weiterer Maßnahmen

Quelle: Eigene Darstellung

4.4 Gestaltung und Anpassung des Interviewleitfadens

Auf Basis der in Tabelle 2 dargestellten Indikatoren wurde ein Interviewleitfaden entwickelt, um eine strukturierte Durchführung der Interviews zu begünstigen. Der Interviewleitfaden ist im Anhang B der vorliegenden Arbeit ersichtlich.

Die Interviews wurden möglichst offen geplant, um die Meinung und persönlichen Sichtweisen der Expertinnen und Experten nach Möglichkeit zu erfassen. Dabei wurden die ergänzenden Fragen abhängig von der Expertin, bzw. vom Experten gestellt, um den Interviewleitfaden bestmöglich

anzupassen. Außerdem sollte dadurch auch ein möglichst flüssiger Gesprächsverlauf ermöglicht werden. Außerdem wurden die Fragen an die Berufswelt der Expertinnen und Experten ausgerichtet, damit die Fragen von diesen leichter aufgenommen werden können (Gläser & Laudel, 2010, S. 151).

Die Basis für die Fragen liefert die bereits aufgearbeitete Literatur, wobei das Hauptaugenmerk auf die identifizierten Gemeinsamkeiten, Unterschiede und Schwerpunkte der betrachteten Studien das gelegt wurde.

Um vor allem die Verständlichkeit und die logische Abfolge der Fragen, als auch die Interviewdauer bewerten zu können, wurde vorab ein Pre-Test durchgeführt. Erstens hat dieser aufgezeigt, dass eine Erläuterung der Unterscheidung zwischen Industriespionage und Wirtschaftsspionage direkt nach der ersten Frage als sinnvoll erscheint, da dies dem Experten des Pre-Tests nicht bewusst war. Zweitens wurde die Reihenfolge der Fragen verändert, um diese logisch aufeinander besser aufzubauen. Drittens wurden aufgrund des Pre-Tests, die vertiefenden Fragen hinsichtlich der technischen, physischen und organisatorischen, bzw. personellen Sicherheit dahingehend angepasst, dass einleitend die Unterscheidung dieser drei Aspekte verdeutlicht wurde.

4.5 Durchführung der Erhebung

Das folgende Kapitel beschreibt die Erhebung der Daten aus den Leitfadeninterviews, um die Hypothese und die Forschungsfrage näher zu beleuchten. Expertinnen und Experten wurden im Rahmen der Interviews durch halbstandardisierte Interviewleitfäden befragt.

4.5.1 Auswahlkriterien und Rahmenbedingungen für die Experteninterviews

Die wichtigsten Auswahlkriterien für die Expertinnen und Experten wurden ausführlich im Kapitel 4.2.2 behandelt und in der Abbildung 3 übersichtlich dargestellt. Somit war es Voraussetzung, dass die Personen mindestens zwei Jahre einschlägige Berufserfahrung haben, im deutschsprachigen Raum tätig sind und aktuell nicht für herstellende Betriebe von Security-Produkten tätig

sind. Durch diese Kriterien soll sichergestellt werden, dass Expertinnen und Experten ausgewählt werden, an die auch die betrachteten Studien gerichtet sind.

Der Autor der vorliegenden Arbeit nutzte sein berufliches Netzwerk, um geeignete Expertinnen und Experten zu finden. Es erklärten sich sieben Personen bereit, das Interview zu führen. Aufgrund der bereits etablierten Gesprächsbasis wurde bei den Leitfadeninterviews auf das Siezen verzichtet. Dieser Umstand unterstützte eine entspannte Atmosphäre, um das Interview in Ruhe und der angebrachten Genauigkeit durchzuführen.

Der Autor steht mit den Expertinnen und Experten in keinem direkten Verhältnis und es handelt sich auch nicht um direkte Kooperationen, sodass eine entsprechende Beeinflussung ausgeschlossen werden kann (Gläser & Laudel, 2010, S. 56-57). Drei der sieben Interviews wurden telefonisch durchgeführt, da ein persönliches Gespräch in absehbarer Zeit nicht möglich war.

Die persönlichen Gespräche wurden mit einem Gerät zur Tonaufzeichnung digital mitgeschnitten und gespeichert. Die Telefonate wurden durch eine Software am Telefon des Interviewers aufgezeichnet. Bei allen Interviews wurden die interviewten Personen vor der Aufzeichnung, explizit auf die Tonaufzeichnung, sowie die anschließende Transkription hingewiesen. Alle Expertinnen und Experten waren damit einverstanden.

Tabelle 3: Übersicht der Rahmenbedingungen der Experteninterviews

Experte	Erfahrung	Übermittlung des Interview-leitfadens vorab	Persönlich oder telefonisch
E1	- Security Manager eines österr. Rechenzentrums - zw. 30 und 35 Jahre alt - etwa 5 Jahre Erfahrung mit Informationssicherheit	Ja	Persönlich
E2	- Security Manager eines österr. Energie-Unternehmens - zw. 40 und 45 Jahre alt - etwa 15 Jahre Erfahrung mit Informationssicherheit und Risikomanagement	Ja	Telefonisch

E3	- Risiko- und Security Manager eines Dienstleisters für Informations- und Kommunikationstechnologie - zwischen 25 und 30 Jahre alt - mehr als 8 Jahre Erfahrung in den Bereichen Risikomanagement und Informationssicherheit	Nein	Persönlich
E4	- Security Manager eines Unternehmens, welches in Österreich verantwortlich ist für "Einführung, Betrieb und Weiterentwicklung eines elektronischen Verwaltungssystems" - zwischen 35 und 40 Jahre alt - mehr als 10 Jahre Erfahrung als CISO	Nein	Persönlich
E5	- Security-Experte eines österr. Finanzdienstleisters - ca. 45 Jahre alt - etwa 15 Jahre Erfahrung mit Informationssicherheit	Nein	Persönlich
E6	- Security Manager eines österr. Finanzdienstleisters - ca. 40 Jahre alt - etwa 10 Jahre Erfahrung mit Informationssicherheit	Ja	Telefonisch
E7	- Risiko- und Security Manager eines österreichischen Dienstleisters für den öffentlichen Dienst - ca. 35-40 Jahre alt - etwa 15 Jahre Erfahrung mit Informationssicherheit	Nein	Telefonisch

Quelle: Eigene Darstellung

4.6 Ergebnisse

Auf Basis der durchgeführten Leitfadeninterviews und den beschriebenen Methoden zur Erhebung der Daten, werden in diesem Kapitel die zentralen Ergebnisse dargestellt und beschrieben.

4.6.1 Anwendung der qualitativen Inhaltsanalyse

Zur strukturierten Auswertung der Experteninterviews wurden die Tonaufzeichnungen mittels wortwörtlicher Transkription festgehalten.

Anschließend wurde das Allgemeinheitsniveau der Transkriptionen durch die zusammenfassende Inhaltsanalyse vereinheitlicht und schrittweise höher gesetzt (Mayring, 2016, S. 89-95). Der eingesetzte Verallgemeinerungsprozess besteht aus den folgenden sechs reduktiven Prozessen (Mayring, 2016, S. 95).

- Auslassen:
  Bedeutungsgleiche Aussagen, die sich an mehreren Stellen im Text wiederfinden, werden auf eine einzige Aussage reduziert.

- Generalisation:
  Die Aussagen werden auf ein einheitliches, abstraktes Niveau gehoben.

- Konstruktion:
  Mehrere Generalisierungen werden, abhängig vom jeweiligen Inhalt, zu einer globalen Aussage zusammengefasst.

- Integration.
  Eine Aussage, die bereits in einer globalen Konstruktion enthalten ist, kann wegfallen.

- Selektion:
  Sofern Aussagen essenzielle Informationen enthalten, werden diese unverändert beibehalten.

- Bündelung:
  Über den Text verstreute Aussagen, welche inhaltlich nah zusammenhängen, können in gebündelter Form wiedergegeben werden.

4.6.2 Ergebnisse der Experteninterviews

Im Folgenden werden die Ergebnisse der Experteninterviews näher beleuchtet. Es handelt sich dabei um die zweite Reduktion der Aussagen und der entsprechenden qualitativen Inhaltsanalyse, wie in Kapitel 4.6.1 beschrieben wurde. Die Aussagen orientieren sich an den Begriffen, Dimensionen und Indikatoren der Operationalisierung, welche im Kapitel 4.3 dargestellt wurden, wobei primär von den Dimensionen ausgegangen wird.

Die Reduktion und die Generalisierung können sich in jenen Fällen stark ähneln, wenn zu einem Indikator nur eine Aussage eines Experten oder einer Expertin vorhanden ist. Sofern mehrere Aussagen zu einem einzelnen Indikator vorhanden sind, werden diese Reduktionen in Form einer einzigen Generalisierung vereint.

Dimension 1: Vorfall

Die Experten waren größtenteils der Ansicht, dass die Erkennung von Angriffen durch Wirtschafts- und Industriespionage auf Organisationen eine große Herausforderung für diese darstellen. Dabei werden in den Organisationen unterschiedliche Schwerpunkte gelegt, wobei drei Interviews deutlich den Einsatz von technischen Tools für einen möglichen Lösungsansatz hervorhoben.

Die Erfahrung mit erfolgreichen Angriffen durch Wirtschafts- und Industriespionage ist bei den Interviewpartnern sehr differenziert. Im Fokus der Mehrheit der Aussagen steht jedenfalls der Schutz von unternehmenskritischen Daten.

Das Verständnis von kurzfristigen Schäden ist bei Unternehmen sehr unterschiedlich ausgeprägt. Hinter langfristigen Schäden wird durchwegs ein hohes Schadensausmaß vermutet, wobei zwei der befragten Experten den Verlust von Kundendaten und den damit verbunden Vertrauens- als auch Imageverlust angegeben haben.

Dimension 2: Management Awareness

Studien zu Wirtschafts- und Industriespionage werden von Experten einerseits aufgrund der zugeschriebenen Glaubwürdigkeit bewertet. Dabei stellt die mögliche Motivation der Autoren, die eigenen Lösungen oder Produkte zu verkaufen, den größten Aspekt dar. Andererseits wird die Fokussierung der Studien auf die Beantwortung spezieller Fragestellungen hervorgehoben.

Die Risikobewertung basiert auf gesetzlichen und regulatorischen Vorgaben, sowie Best Practices. Außerdem haben die Interviews gezeigt, dass das Risikomanagement auf die Anforderungen der jeweiligen Organisation angepasst sein muss.

Die Kommunikation zu den Risiken durch Wirtschafts- und Industriespionage gegenüber den Mitarbeiterinnen und Mitarbeitern, vor allem aber der Geschäftsführung stellt einen wesentlichen Faktor zur Sensibilisierung dar.

Drei Experten gaben außerdem an, dass das Bewusstsein bei den Führungskräften zu diesem Themenkomplex vor allem durch die Darstellung von bekannten Einzelfällen gesteigert werden kann. Als wichtiger Aspekt wurde hierbei genannt, dass die Darstellungen dieser Fälle nicht anonymisiert sein sollten, um die Aufmerksamkeit der Geschäftsführung oder des Vorstands zu erhalten.

Dimension 3: Relevanz in der Praxis

Einerseits dienen Studien, die einen Überblick zu aktuellen Entwicklungen im Themenkomplex Wirtschafts- und Industriespionage darstellen, als Orientierung, damit sich die Interviewpartner einen Überblick verschaffen können. Andererseits können Detailstudien, die auf spezielle, oft technische Aspekte eingehen, von Hilfe sein.

Hingegen bieten Studien, die keinen Bezug zu aktuellen Themen bieten, sowie eine starke Abhängigkeit zu herstellenden Betrieben von Security-Lösungen aufweisen, keinen Mehrwert für die befragten Experten.

Nur fünf Experten konnten sich mit dem Thema des Dunkelfelds identifizieren, wobei vier davon angaben, dass dieses in den Studien, als auch in der Praxis noch eine große Unbekannte ist und zu wenig beleuchtet wird.

Dimension 4: Unterschied Studien und Vorfälle

Die Ergebnisse aus Studien bilden, neben dem Informationsaustausch mit Kundinnen, Kunden und herstellenden Betrieben, sowie branchenspezifischen Abstimmungen mit anderen Organisationen, die Basis für weitere Entscheidungen.

Grundsätzlich wurde angemerkt, dass Detailberichte zu einzelnen Vorfällen den allgemeinen Studien vorgezogen werden, da dadurch die Bewertung von spezifischen Fragen und die interne Kommunikation damit unterstützt werden.

Dimension 5: Informationsbedarf

Fast alle Interviewpartner betonten, dass zu den technischen Aspekten, zur Abwehr von Angriffen durch Wirtschafts- und Industriespionage, ausreichend Informationen in Form von Studien vorhanden sind.

Organisationen haben einen Bedarf nach mehr Informationen zu umfassenden Security-Konzepten, Social Engineering, das potenzielle Schadensausmaß und den möglichen Auswirkungen durch solche Angriffe.

Dimension 6: Ermittelte Themenschwerpunkte der Studien

Hinsichtlich der ermittelten Themenschwerpunkte wurde darauf geachtet, dass diese von den Interviewpartnern ohne Beeinflussung des Interviewers genannt werden. Dementsprechend konnte nicht zu allen Indikatoren von jedem Experten eine Aussage erfasst werden.

Die Betrachtung der Betroffenheit von Wirtschafts- und Industriespionage in den Studien ist laut drei Experten nicht ausreichend transparent und es wird auch eine Unvollständigkeit dieser Sichtweise vermutet.

Drei Experten nannten den Aspekt der Kronjuwelen, wobei die Sichtweisen differenzieren. Die Klassifizierung von Kundendaten als Kronjuwelen wurde von zwei Experten erwähnt.

Die Regelungen der Security-Policy sollten praxisnah sein, sodass diese von Mitarbeiterinnen und Mitarbeitern nicht falsch interpretiert werden kann und haben damit einen hohen Stellenwert für Organisationen. Bestimmte Vorgaben müssen aufgrund von branchenspezifischen Gesetzen definiert und umgesetzt werden.

Hinsichtlich der physischen Sicherheit haben für Organisationen eine Videoüberwachung, eine Alarmanlage, Zutrittsmanagement und ein entsprechendes Zonenkonzept für das Personal und gegebenenfalls Kundinnen und Kunden eine hohe Bedeutung.

Antiviren-Lösung, Firewalls, Patches, User-Management, sowie sichere Authentifizierungsverfahren haben für Organisationen, aus technischer Sicht, eine hohe Bedeutung.

Regelmäßige Überprüfungen durch das interne Kontrollsystem, sowie technische Prüfungen durch Vulnerability Scanner und Penetration Tests werden von Organisationen größtenteils durchgeführt.

Vier Experten sind der Ansicht, die Verfügbarkeit von Services und Informationen nimmt in Organisationen einen ähnlich hohen, wenn nicht sogar höheren Stellenwert als etwaige Sicherheitsvorkehrungen ein.

Drei Interviewpartner äußerten sich zu der Beziehung mit ausländischen Organisationen und den damit verbundenen Einfluss auf Wirtschafts- und Industriespionage. Ein Experte zieht diesen Aspekt als relevante Basis für die interne Bewertung der Risiken heran.

Von den sieben Experten erwähnten zwei die eigene Einschätzung zur Effektivität der getroffenen Maßnahmen, wobei einer die technischen Maßnahmen als besonders effektiv hervorhob und der andere die Sensibilisierung der Mitarbeiterinnen und Mitarbeiter.

Fünf Experten waren der Ansicht, dass die Planung weiterer Maßnahmen zum Schutz vor Wirtschafts- und Industriespionage, neben der Analyse von Studien, vorrangig auf dem direkten Austausch mit anderen Organisationen, Kundinnen, Kunden und herstellenden Betrieben beruht.

4.6.3 Beurteilung der Hypothese

Die in Kapitel 4.6.2 dargestellten Ergebnisse der Leitfadeninterviews mit den Experten bilden die Basis für die Bewertung der Hypothese, um diese zu unterstützen, oder zu falsifizieren.

Tabelle 4: Übersicht der Rahmenbedingungen der Experteninterviews

Hypothese	**Bestätigung oder Falsifikation**
Die aus den Studien ermittelten Themenschwerpunkte decken sich mit den relevanten Problemen durch Wirtschafts- und Industriespionage in der Praxis.	**Bestätigt** Die meisten Themenschwerpunkte, welche in den Studien behandelt werden, stehen auch im Fokus der Security Manager in der Praxis.

Quelle: Eigene Darstellung

Aufgrund der erhobenen Daten konnte die Hypothese bestätigt werden und die Forschungsfrage damit beantwortet werden.

4.7 Zusammenfassung und Interpretation

Im Folgenden werden die wichtigsten Schwerpunkte der Studien aus Kapitel 3.3 und die relevanten Aussagen der Experten aus Kapitel 4.6.2 zusammengefasst und aufgrund dieser Erkenntnisse interpretiert.

Betroffenheit und Erkennung von Angriffen

Nur eine der betrachteten Studien hat konkret hinterfragt, ob Organisationen einen erfolgreichen Angriff überhaupt selbstständig erkennen können. Die anderen Studien greifen diese Frage gar nicht erst auf. Die Interviews zeigen ein ähnliches Bild, wobei die selbstständige Erkennung von Organisationen, dass sie angegriffen wurden, eine große Herausforderungen für Security-Experten darstellt. Einige Interviewpartner gehen davon aus, dass erst ein Hinweis einer staatlichen Stelle, oder die Veröffentlichung in den Medien den betroffenen Organisationen Aufschluss darüber gibt, dass sie erfolgreich angegriffen wurden.

Schäden, Folgekosten und das Dunkelfeld

Etwa die Hälfte der betrachteten Studien enthalten Aussagen zu Schäden und Folgekosten für Organisationen durch Wirtschafts- und Industriespionage. Dieser Aspekt wird auf unterschiedlichen Ebenen betrachtet, sei es der Schaden für ein gesamtes Land, oder für einzelne Organisationen pro Vorfall. Die dargestellten Informationen unterscheiden sich jedoch erheblich. Ähnlich verhält es sich auch mit den Aussagen der Experten, wobei diese den Fokus jeweils auf die eigene Organisation legen. Das Verständnis ist unterschiedlich ausgeprägt, kann jedoch grundsätzlich von keinem der Experten umfassend und vor allem belegbar festgehalten werden. Grundsätzlich wird ein hohes Schadenspotenzial vermutet, doch konnte dafür im Rahmen der Leitfadeninterviews niemand die zugrundeliegenden Überlegungen und Fakten darstellen.

Diese große Unbekannte lässt vermuten, dass es zwar immer wieder einzelne Informationen zu Vorfällen gibt, die öffentlich oder im Vertrauen bekannt werden. Das entspricht auch der fehlenden Darstellung des Dunkelfelds in

den betrachteten Studien, als auch den unterschiedlichen Aussagen der Experten zu diesem Aspekt.

Verständnis von Risikomanagement und Informationssicherheit

Insgesamt haben die Analyse der Studien und die Interviews mit den Experten gezeigt, dass es ein Verständnis auf fachlicher Ebene gibt, einzelne Aspekte betrachtet werden, dies aber selten im Rahmen vom einem koordinierten Risikomanagement-Prozess geschieht. Nur ein Experte zeigte im Rahmen des Interviews ein Verständnis der Integration eines Security Risk Management in ein unternehmensweises Risikomanagement. Ein weiterer Experte geht aufgrund von steigenden gesetzlichen Anforderungen davon aus, dass eine Risikobetrachtung in den nächsten Jahren für europäische Unternehmen zwingend erforderlich wird.

Security Management besteht aus der Kultur, den Prozessen und der Struktur, um Leistungen zu maximieren und unerwünschte Effekte zu minimieren, wobei dies auch die bewussten und unbefugten Aktionen von anderen gegen die Assets der Organisation inkludiert (Talbot & Jakeman, 2009, S. 11). Risikomanagement besteht aus der Kultur, den Prozessen und der Struktur, die zur Realisierung von Möglichkeiten beitragen und gleichzeitig unerwünschte Effekte behandeln. Somit ist Risikomanagement eine koordinierte Aktivität, um die Risiken einer Organisation zu lenken und zu steuern (Talbot & Jakeman, 2009, S. 12).

Im Rahmen der Leitfadeninterviews entstand der Eindruck, dass die Aufgaben des Risikomanagements und die des Security Managements streng voneinander getrennt werden. Einerseits werden diese Aufgaben organisatorisch unterschiedlichen Einheiten zugeordnet und damit bereits ein gewisser Abstand geschaffen. Andererseits beschäftigen sich die befragten Experten sehr stark mit der Behandlung von Angriffsmustern, welche in Studien, Medien und Interessensgruppen diskutiert werden. Eine gezielte Steuerung im Einklang der Unternehmensziele und den entsprechenden Risiken war nicht ersichtlich. Ein gesamtheitlicher Ansatz, welcher Security Management als einen Teil des Risikomanagements versteht, konnte nicht festgestellt werden.

Schwerpunkte der technischen und physischen Sicherheitsmaßnahmen

Die Erkenntnisse der Studien und der Interviews mit den Experten zeigen deutlich, dass die technischen Sicherheitsaspekte von Angriffen durch

Wirtschafts- und Industriespionage umfassend behandelt werden und die entsprechenden Studien auch den Informationsbedarf der Organisationen dahingehend abdecken. Vor allem die technischen Sicherheitsmaßnahmen werden regelmäßig in Form von Sicherheitsüberprüfungen, sogenannten „Penetration Tests“ durchgeführt.

Die physische Sicherheit nimmt für die Unternehmen ebenfalls eine wichtige Rolle ein, diese wird jedoch von den betrachteten Studien deutlich seltener behandelt. Dennoch wurde von den Interviewpartnern dieser Aspekt nicht genannt. Mehrere Experten merkten während der Interviews an, dass Maßnahmen zur Steigerung der physischen Sicherheit auf Anforderungen aus Gesetzen oder der Compliance heraus getrieben werden.

Die Sensibilisierung des Personals, vor allem des Top-Managements wurde im Rahmen der Interviews öfters erwähnt. Das Verständnis von möglichen Risiken und Folgen durch erfolgreiche Angriffe hat sowohl in den Studien, als auch bei den Experten einen hohen Stellenwert.

Kronjuwelen

Die Identifizierung und der angemessene Umgang mit den Kronjuwelen einer Organisation findet sich in den betrachteten Studien gar nicht wieder und auch nur drei der sieben Interviewpartner haben sich dazu geäußert. Dieser Umstand lässt die Vermutung zu, dass Kronjuwelen derzeit noch kaum in der Praxis behandelt werden. Gleichermaßen besteht aber ein großes vermutetes Schadenspotenzial hinter erfolgreichen Angriffen durch Wirtschafts- und Industriespionage bei den Experten.

Interne Kommunikation

Studien zu Wirtschafts- und Industriespionage werden von Experten unter anderem zur Verdeutlichung der eigenen Standpunkte und als Unterstützung bei internen Diskussionen und Entscheidungen rund um Informationssicherheit herangezogen. Das Bewusstsein hinsichtlich der Verfügbarkeit von Services und der Vertraulichkeit von schützenswerten Daten ist bei Führungskräften aufgrund der Expertenaussagen als hoch einzustufen, jedoch die Sensibilität bei Mitarbeiterinnen und Mitarbeitern nicht diesem hohen Niveau entspricht. Zur Verdeutlichung der entsprechenden Risiken durch die Experten gegenüber der Geschäftsführung oder dem Vorstand werden nach Möglichkeit Vorfälle herangezogen, welche nicht anonymisiert wurden.

Transparenz und Glaubwürdigkeit der Studien

Ein wichtiges Kriterium für die Bewertung von Studien stellt für die Experten die Transparenz der Studien dar. Dabei fließt auch die vermutete Motivation der Autoren stark ein. Autoren, welche primär für herstellende Betriebe von Security-Lösungen tätig sind, wird eine Motivation zugeschrieben, eben diese Lösungen auf dem Markt zu positionieren.

Durch die geografische Nähe der in den Studien betrachteten Organisationen kann zusätzlich die Glaubwürdigkeit der Studienergebnisse erhöht werden. Eine höhere Anzahl von Studien, welche auf Daten und Informationen aus dem deutschsprachigen Raum basieren, wurde von mehreren Experten während der Leitfadeninterviews als Wunsch geäußert. Es werden vorzugsweise Studien aus dem deutschsprachigen Raum herangezogen, sofern diese vorhanden sind. Andernfalls werden Alternativen gesucht, die mangels Alternativen auf Daten und Informationen anderer Länder basieren. Dieses Prinzip lässt sich auch bei der hohen Popularität von regionalen Nachrichtensendungen in den Medien beobachten. Je näher Vorfälle zu einer Person, bzw. im Kontext der vorliegenden Arbeit, zu einer Organisation passieren, desto eher fühlt sich diese betroffen (Hepp & Krotz, 2005, S. 147-149).

5 Conclusio

Inhalt

5.1	FAZIT	79
5.2	KRITISCHE REFLEXION DES FORSCHUNGSVORHABENS	81
5.2.1	EINHALTUNG QUALITATIVER GÜTEKRITERIEN	81
5.3	AUSBLICK UND KÜNFTIGER FORSCHUNGSBEDARF	83

5.1 Fazit

Nach der Analyse von Studien und den Leitfadeninterviews mit Experten konnte im Rahmen der vorliegenden Arbeit festgestellt werden, dass die behandelten Schwerpunkte in den Studien für die Praxis relevant sind. Vor allem die technischen Maßnahmen zum Schutz vor Wirtschafts- und Industriespionage werden umfassend behandelt. Die Anforderungen zur physischen Sicherheit erhalten die Organisationen in vielen Fällen durch gesetzliche oder Compliance-Vorgaben. Zur Gebäudesicherheit gibt es kaum offene Fragen bei den Security-Expertinnen und -Experten.

Umfassende Studien werden vor allem herangezogen, um einen Überblick zu aktuellen Angriffen und den Vorgehensweisen dahinter zu erhalten. Dabei werden Informationen von verschiedenen Instituten, aber auch Jahresberichte von staatlichen Organisationen, wie beispielsweise der Exekutive, herangezogen. Da solche Berichte zumeist jährlich von den gleichen Organisationen veröffentlicht werden und diese eine ähnliche Struktur zu den vorigen Berichten aufweisen, werden diese auch herangezogen, um Informationen zu langfristigen Entwicklungen zu erhalten.

Detailstudien geben den Expertinnen und Experten einen tiefen Einblick in spezielle Anforderungen, mit denen sie konfrontiert sind. Diese werden anlassbezogen herangezogen und helfen bei der Einschätzung von aktuellen Angriffen durch Wirtschafts- und Industriespionage.

Dabei werden die Studien primär anhand der vermuteten Motivation der Autorinnen und Autoren bewertet. Sofern Studien mit den Lösungen und Produkten eines Unternehmens in Verbindung gebracht werden können, erhöht sich die Skepsis der Expertinnen und Experten. Die damit verbundene Abhängigkeit einer Studie spielt eine wesentliche Rolle, ob diese von Organisationen für weitere Analysen herangezogen werden.

Vor allem die Leitfadeninterviews haben gezeigt, dass Studien nur einen Teil zu der Informationsbeschaffung für Expertinnen und Experten darstellen. Weitere wichtige Quelle für Organisationen sind die direkten Abstimmungen mit Kundinnen, Kunden, herstellenden Betrieben und vor allem anderen Unternehmen aus der gleichen Branche.

Die möglichst frühzeitige Erkennung der Angriffe durch Wirtschafts- und Industriespionage wird sowohl durch die Studien, als auch durch die Expertinnen und Experten als nicht ausreichend angegeben. Dieser Umstand verschärft die Betrachtung der möglichen Schäden und Folgekosten nach einem Angriff, da diese kaum bewertet werden können. Erschwerend kommt noch hinzu, dass die Einschätzung der Studien, hinsichtlich der Dunkelziffer, kritisch betrachtet wird. Somit werden auch Hochrechnungen von kumulierten Schadenssummen für ganze Länder durch Wirtschafts- und Industriespionage von Fachleuten kaum herangezogen.

Im Gegensatz dazu können Studien und Informationen zu Vorfällen im eigenen Land die Glaubwürdigkeit und die Akzeptanz in einer Organisation deutlich erhöhen, da durch die geografische Nähe das entsprechende Risiko stärker wahrgenommen wird.

Außerdem ist hervorzuheben, dass in einigen Organisationen Risikomanagement und Risk Management kaum interagieren. So gibt es Analysen und Einschätzungen zu möglichen Angriffen, welche aber zu selten in ein gesamtheitliches Risikomanagement eingebettet werden. Security Risk Management sollte als ein Teil von Risikomanagement verstanden werden, um eine umfassende Betrachtung, Bewertung und Abstimmung der Maßnahmen zu ermöglichen. Das Security Risk Management sollte mit jeder Aktivität des allgemeinen Risikomanagement einer Organisation verschränkt werden (Talbot & Jakeman, 2009, S. 12).

Sowohl die Studien, als auch die Aussagen der Expertinnen und Experten behandeln nur selten die Identifikation von Kronjuwelen und den

entsprechenden Umgang mit diesen. Außerdem unterscheiden sich die Sichtweisen und das Verständnis drastisch.

5.2 Kritische Reflexion des Forschungsvorhabens

5.2.1 Einhaltung qualitativer Gütekriterien

Die folgenden Gütekriterien für die qualitative Forschung nach Mayring wurden eingehalten (Mayring, 2016, S. 144-148). Nachstehend wird beschrieben, wie diese im Forschungsprozess der vorliegenden Arbeit berücksichtigt wurden.

1. Verfahrensdokumentation

Im Gegensatz zu quantitativer Forschung, bei der Messungen und Techniken oftmals standardisiert sind, gilt es bei der qualitativ orientierten Forschung das Vorgehen ausreichend detailliert zu dokumentieren, um die Nachvollziehbarkeit gewährleisten zu können (Mayring, 2016, S. 144-145).

Im Rahmen der vorliegenden Arbeit wurde der gesamte Forschungsprozess nachvollziehbar dokumentiert. Im Kapitel 2 wurde neben der Erläuterung der verwendeten Begriffe vor allem auf die Bedeutung der systematischen Übersichtsarbeit und dessen Einsatz in der vorliegenden Arbeit behandelt. Das Kapitel 3 beschreibt einerseits die Auswahlkriterien für die betrachteten Studien, als auch die identifizierten Gemeinsamkeiten, Unterschiede und Schwerpunkte dieser Studien. Die Auswertung dieser Ergebnisse, als auch die Vorgehensweise für die Leitfadeninterviews wurden im Kapitel 4 detailliert dargestellt. Die verwendeten Auswerteraster sind im Anhang C auszugsweise angeführt.

2. Argumentative Interpretationsabsicherung

Interpretationen lassen sich nicht wie mathematische Rechenoperationen nachrechnen, sondern benötigen andere Möglichkeiten, um deren Güte feststellen zu können. Somit ist es notwendig, dass Interpretationen argumentativ begründet werden müssen (Mayring, 2016, S. 145).

Die Identifizierung und Auswertung der Gemeinsamkeiten, Unterschiede und Schwerpunkte der Studien und der Transkriptionen der Interviewleitfaden, basiert auf vorher festgelegten Vorgehensweisen. Im Rahmen der Leitfadeninterviews ist kritisch zu betrachten, dass nicht alle Fachvokabel, die möglicherweise branchenspezifisch sind, vom Interviewer während der Gespräche nachgefragt wurden. Dabei ist anzumerken, dass sich diese Fälle auf Standards oder Normen bezogen, die nicht im Fokus der vorliegenden Arbeit liegen.

3. Regelgeleitetheit

Die qualitative Forschung ist zwar offen gegenüber dem Gegenstand und ermöglicht auch die Anpassung zuvor definierter Analyseschritte, jedoch hat dies mit systematischem Vorgehen zu erfolgen (Mayring, 2016, S. 145-146).

Das Forschungsdesign der vorliegenden Arbeit wurde ausführlich dokumentiert und orientiert sich an der Struktur empirischer sozialwissenschaftlicher Forschungsprozesse (Gläser & Laudel, 2010, S. 35). Außerdem wurde für die Durchführung der Interviews ein Leitfaden verwendet, welcher zuvor im Rahmen eines Pre-Tests überarbeitet wurde. Diese Veränderung wurde ebenfalls im Rahmen der vorliegenden Arbeit dokumentiert.

4. Nähe zum Gegenstand

Ein Ziel der qualitativen Forschung besteht darin, möglichst nahe an der Alltagswelt der beforschten Subjekte anzuknüpfen, also die natürliche Lebenswelt zu beforschen. Qualitative Forschung setzt an konkreten sozialen Problemen an und führt die Forschung auch für die Betroffenen durch. Nach der Forschung sollte nochmals geprüft werden, inwiefern diese Nähe erreicht werden konnte (Mayring, 2016, S. 146-147).

Die Expertinnen und Experten für das Leitfadeninterview wurden vom Autor aufgrund vorab definierter Kriterien ausgewählt, die ein Mindestmaß an Verständnis für das Thema voraussetzen. In der Einleitung zu den Interviews wurden die Rahmenbedingungen der vorliegenden Arbeit ausführlich erläutert, wodurch ein gleichberechtigtes und offenes Gesprächsklima bei den Interviews entstand.

5. Kommunikative Validierung

Durch die erneute Vorlage von Ergebnissen und Interpretationen den Beforschten gegenüber, kann die Korrektheit dieser bestätigt werden. Dies darf nicht das einzige Kriterium sein, da die Analyse sonst ausschließlich die subjektive Bedeutung erfassen würde (Mayring, 2016, S. 147).

Mit einem Interviewpartner konnte der Autor die angefertigte Transkription des Interviews nochmals abstimmen, um die Erkenntnisse zu validieren. Außerdem zeigten zwei weitere Experten Interesse an der vollständigen Arbeit. Im Rahmen der vorliegenden Arbeit war es nicht möglich mit allen Expertinnen und Experten die gewonnenen Erkenntnisse nochmals zu validieren, da dies den Rahmen der Arbeit erheblich übersteigen würde.

6. Triangulation

Durch eine Triangulation kann bei qualitativer Forschung eine Steigerung der Qualität erreicht werden, indem mehrere Analysegänge miteinander verbunden werden. Dabei soll die Fragestellung auf unterschiedlichen Wegen gelöst werden und die Ergebnisse zu vergleichen (Mayring, 2016, S. 147-148).

Im Rahmen der vorliegenden Arbeit wurden unterschiedliche Studien aus verschiedenen Ländern und Autoren gewählt. Zur Analyse der Studien wurde ein systematisches Review durchgeführt und die diese Ergebnisse mittels Leitfadeninterviews mit Expertinnen und Experten abgestimmt. Die Expertinnen und Experten wurden aus unterschiedlichen Branchen gewählt, um auch an dieser Stelle möglichst verschiedene Blickwinkel zu erhalten. Durch den Forschungsprozess wurden diese Ergebnisse strukturiert erarbeitet.

5.3 Ausblick und künftiger Forschungsbedarf

In der vorliegenden Arbeit wurden sowohl Studien, als auch Aussagen von Expertinnen und Experten zu Wirtschafts- und Industriespionage erhoben. Dabei handelt es sich um ein sehr umfassendes Themengebiet und deshalb wurden bewusst Grenzen gesetzt. Außerdem haben sich nach der Analyse der Ergebnisse noch weitere, interessante Themenkreise aufgetan, welche folgende kurz als Vorschlag für weitere Forschungen dargestellt werden.

Erkennung von Angriffen

Eines der zentralen Elemente, welche die Unschärfe bei der Einschätzung des Risikos von Wirtschafts- und Industriespionage bewirken, sind die kaum verfügbaren Informationen zur erfolgreichen Erkennung der Angriffe. Mehrere Experten gaben während der Leitfadeninterviews an, dass sie davon ausgehen, bei einem erfolgreichen Angriff, wohl erst Wochen oder Monate später durch die Medien oder staatliche Organisationen darüber zu erfahren. Eine bessere und vor allem frühzeitige Erkennung könnte langfristig auch zu einer genaueren Einschätzung des Risikos beitragen.

Transparenz der Schäden und Folgewirkungen steigern

Ein wichtiges Kriterium für die Bewertung der Studien hinsichtlich der dargestellten Schäden und Folgekosten ist gemäß der befragten Experten die Transparenz. Da die Studien anonymisiert sind, teilweise auf unpersönlichen Umfragen beruhen und nur selten für ein bestimmtes Land oder eine bestimmte Region erstellt werden, werden die dargestellten Ergebnisse kritisch hinterfragt. Zur Steigerung der Glaubwürdigkeit der dargestellten Schäden, könnte eine Analyse der Anforderungen von Organisationen und die Erstellung eines klaren Schemas zur Berechnung der Schäden beitragen.

Unterscheidung hinsichtlich der Angreifer

Organisationen unterscheiden kaum, ob es sich bei einem Angriff um Wirtschafts- oder Industriespionage handelt, oder ob Einzeltäter beteiligt sind. Die Maßnahmen zur Abwehr sind laut Aussagen der Interviews die gleichen. Dabei stellt sich die Frage, inwiefern sich die Intentionen der Angreifer in den Schäden niederschlagen und welche langfristigen Folgen dadurch entstehen. Im Rahmen der vorliegenden Arbeit konnte nicht festgestellt werden, inwiefern ein Angriff durch staatliche Organisationen oder Marktbegleiter in die Bewertung der Gegenmaßnahmen einfließen.

Leitfaden für entscheidungsrelevante Informationen

Die genaue Analyse der Informationsquellen von Organisationen zu Wirtschafts- und Industriespionage und den entsprechenden Gegenmaßnahmen, könnte Aufschluss darüber geben, welche Quellen schlussendlich in die Entscheidungen von Organisationen einfließen. Die Analyse der Quellen und eine strukturierte Aufbereitung der Entscheidungsfindung, könnten die Analyse und die Bewertung der Risiken

verbessern, als auch einen Leitfaden schaffen, an den sich andere Organisationen orientieren könnten.

Bibliographie

Alker, U. & Weilenmann, U. (2006). Sprachleitfaden - Geschlechtergerechter Sprachgebrauch an der FH Campus Wien.

Austrian Standards Institute. (2008). *ISO/IEC 27002:2005 - Leitfaden für das Informationssicherheits-Management*. Wien.

Baur, N. & Blasius, J. (Hrsg.). (2014). *Handbuch Methoden der empirischen Sozialforschung*. Wiesbaden: Springer VS.

Bundesamt für Statistik BFS. (2016). *Polizeiliche Kriminalstatistik (PKS). Jahresbericht 2015* (Statistik der Schweiz. Fachbereich 19, Kriminalität und Strafrecht). Neuchatel: Office federal de la statistique (OFS).

Eisend, M. (2004). *Metaanalyse. Einführung und kritische Diskussion* (Diskussionsbeiträge des Fachbereichs Wirtschaftswissenschaft der Freien Universität Berlin Betriebswirtschaftliche Reihe, Bd. 2004,8). Berlin: Hampp.

Flick, U. (Hrsg.). (2008). *Qualitative Forschung. Ein Handbuch* (Rowohlts Enzyklopädie, Bd. 55628, 6., durchges. u. aktualisierte Aufl.). Reinbek bei Hamburg: Rowohlt.

Gläser, J. & Laudel, G. (2010). *Experteninterviews und qualitative Inhaltsanalyse als Instrumente rekonstruierender Untersuchungen* (Lehrbuch, 4. Auflage). Wiesbaden: VS Verlag.

Hepp, A. & Krotz, F. (Hrsg.). (2005). *Globalisierung der Medienkommunikation: Eine Einführung* (Medien, Kultur, Kommunikation, 1. Aufl.). Wiesbaden: VS Verlag für Sozialwissenschaften.

Kasper, K. (2014). Wirtschaftsspionage und Konkurrenzausspähung - eine Analyse des aktuellen Forschungsstandes. Ergebnisbericht einer Sekundäranalyse.

Kersten, H., Reuter, J. & Schröder, K.-W. (2013). *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Der Weg zur Zertifizierung* (Edition <Kes>, 4., aktualisierte und erw. Aufl.). Wiesbaden: Springer Vieweg.

Köhler, T. R. (2014). *Vernetzt, verwanzt, verloren. Die unglaublichen Methoden der Wirtschaftsspionage*. Frankfurt/Main: Westend.

Langer, M., Jabinger, M. & Grasser, H. (2011). Wirtschafts- und Industriespionage. Handbuch Know-How-Schutz für die österreichische Wirtschaft.

Mayring, P. (2016). *Einführung in die qualitative Sozialforschung. Eine Anleitung zu qualitativem Denken* (Pädagogik, 6. Aufl.). Weinheim: Beltz.

Meuser, M. & Nagel, U. (1991). *Expertlnneninterviews - vielfach erprobt, wenig bedacht. Ein Beitrag zur qualitativen Methodendiskussion:* VS Verlag für Sozialwissenschaften.

Neubacher, F. (2011). *Kriminologie* (Nomos Lehrbuch). Baden-Baden: Nomos.

Ressing, M., Blettner, M. & Klug, S. J. (2009). Übersichtsarbeit - Systematische Übersichtsarbeiten und Metaanalysen-Teil 6 der Serie zur Bewertung wissenschaftlicher Publikationen. *Deutsches Ärzteblatt - Ärztliche Mitteilungen - Ausgabe B, 106* (27).

Schaaf, C. (2009). *Industriespionage. Der große Angriff auf den Mittelstand*. Stuttgart: Boorberg.

Schreiner, M. (2008). *Strategische Wirtschaftsspionage. Die HighTech-LowCost-Strategy der Volksrepublik China*. Saarbrücken: VDM Verlag Dr. Müller.

Talbot, J. & Jakeman, M. G. (2009). *Security risk management body of knowledge*. Hoboken, NJ: Wiley.

Online-Quellen

Bachmann, M., Shahd, M. & Grimm, F. (2015). Spionage, Sabotage und Datendiebstahl - Wirtschaftsschutz im digitalen Zeitalter. Zugriff am 31.08.2016. Verfügbar unter https://www.bitkom.org/Publikationen/2015/Studien/Studienbericht-Wirtschaftsschutz/150709-Studienbericht-Wirtschaftsschutz.pdf

Bundesamt für Sicherheit in der Informationstechnik. (2015). Cyber-Sicherheits-Umfrage 2015. Ergebnisse. Zugriff am 31.08.2016. Verfügbar unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/cybersicherheitslage/umfrage2015_ergebnisse.pdf?__blob=publicationFile&v=4

Bundeskanzleramt Österreich. (2016). Polizeiliche Kriminalstatistik Österreich. Sicherheit Österreich 2015. Zugriff am 31.08.2016. Verfügbar unter http://www.bmi.gv.at/cms/BK/publikationen/krim_statistik/2015/1342016_Web_Sicherheit__2015.pdf

Bundeskriminalamt Deutschland. (2016). Polizeiliche Kriminalstatistik Bundesrepublik Deutschland. Jahrbuch 2015. Zugriff am 31.08.2016. Verfügbar unter https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/PolizeilicheKriminalstatistik/2015/pks2015Jahrbuch.pdf?__blob=publicationFile&v=2

Corporate Trust. (2014). *Studie: Industriespionage 2014. Cybergeddon der deutschen Wirtschaft durch NSA & Co.?* Zugriff am 30.08.2016. Verfügbar unter https://www.corporate-trust.de/pdf/CT-Studie-2014_DE.pdf

Deppe, M. (2004). *Umsetzung der "evidence based medicine" anhand der perkutanen transforaminalen Sequestektomie*. Berlin, Freie Univ., Diss. Zugriff am 03.09.2016. Verfügbar unter http://www.diss.fu-berlin.de/diss/receive/FUDISS_thesis_000000001334

Europäische Kommission. (2016). NIS-Richtlinie. Richtlinie des europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union. Zugriff am 30.08.2016. Verfügbar unter http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52013PC0048

F.A.Z. Institut, forsa & Result Group. (2014). Kriminelle Risiken im Mittelstand. Gefahren, Schäden und Prävention - eine Studie. Zugriff am 30.08.2016. Verfügbar unter https://www.result-group.com/media/ResultGroup_KriminelleRisikenMittelstand-201.pdf

Körmer, C. & Langer, M. (2015). Wirtschafts- und Industriespionage. in österreichischen Unternehmen 2015. Zugriff am 30.08.2016. Verfügbar unter http://www.bmi.gv.at/cms/BMI_Verfassungsschutz/wis/files/Studienpublikation_RZ_111215_WEB.pdf

KPMG. (2016). Cyber Security in Österreich Studie IT-Advisory. Zugriff am 01.10.2016. Verfügbar unter https://www.kpmg.at/uploads/media/160321_KPMG_Studie_CyberSecurity.pdf

KSÖ Kuratorium Sicheres Österreich. (2012). Cybersicherheit in Österreich. Risikopotenziale und Handlungserfordernisse am Beispiel ausgewählter

Infrastruktursektoren. Zugriff am 02.09.2016. Verfügbar unter https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2015/02/Cyberrisikoanalyse.pdf

Lueginger, E. & Renger, R. (2013). Das weite Feld der Metaanalyse. Sekundärliteratur und metaanalytische Verfahren im Vergleich. *kommunikation. medien, 2nd Ed., 31.* Zugriff am 31.08.2016. Verfügbar unter http://journal.kommunikation-medien.at/wp-content/uploads/2013/05/Ausg2_Lueginger_Renger_2013.pdf

Schönherr, D., Mayerl, C. & Traunmüller, H. (2015). A1 IT-Security in heimischen Unternehmen. Zugriff am 30.08.2016. Verfügbar unter http://www.sora.at/fileadmin/downloads/projekte/2015_SORA-Endbericht_A1-IT-Security.pdf

Telekom Austria Group. (2016). *Geschäftsbericht nach IFRS 2015.* Zugriff am 03.10.2016. Verfügbar unter http://cdn1.telekomaustria.com/final/de/media/pdf/TAG_Geschaeftsbericht_2015.pdf

Abbildungsverzeichnis

ABBILDUNG 1: ÜBERSICHT DER AUSWAHLKRITERIEN FÜR DIE STUDIEN..... 46
ABBILDUNG 2: FORSCHUNGSTRIAS ZUR IDENTIFIKATION VON FRAGESTELLUNGEN59
ABBILDUNG 3: ÜBERSICHT DER AUSWAHLKRITERIEN FÜR DIE EXPERTINNEN UND EXPERTEN 62

Tabellenverzeichnis

TABELLE 1: ÜBERSICHT DER UNTERSUCHTEN STUDIEN 22
TABELLE 2: OPERATIONALISIERUNG DER HYPOTHESE H1 65
TABELLE 3: ÜBERSICHT DER RAHMENBEDINGUNGEN DER EXPERTENINTERVIEWS 68
TABELLE 4: ÜBERSICHT DER RAHMENBEDINGUNGEN DER EXPERTENINTERVIEWS 74
TABELLE 5: AUSZUG AUS DER EXTRAKTIONSTABELLE 95
TABELLE 6: OPERATIONALISIERUNG 99
TABELLE 7: AUSZUG AUS DER AUSWERTETABELLE FÜR DAS INTERVIEW 1 104
TABELLE 8: AUSZUG AUS DER AUSWERTETABELLE FÜR DAS INTERVIEW 2 105
TABELLE 9: AUSZUG AUS DER AUSWERTETABELLE FÜR DAS INTERVIEW 5 107

Anhang A: Auswertetabelle der systematischen Übersichtsarbeit der betrachteten Studien

Die folgende Tabelle 5 zeigt einen kurzen Auszug aus der Zusammenfassung der systematischen Übersichtsarbeit. Dabei wurden die betrachteten Studien hinsichtlich Gemeinsamkeiten, Unterschiede und allgemeine Schwerpunkte hin überprüft. Die vollständige Tabelle, sowie die gesammelten Ergebnisse liegen dem Autor vor.

Tabelle 5: Auszug aus der Extraktionstabelle

Gruppe	*Detail-beschreibung*	***IT-Security in heimischen Unternehmen***	***Spionage, Sabotage und Datendiebstahl – Wirtschaftsschutz im digitalen Zeitalter***	***Cyber-Sicherheits-Umfrage 2015***	***Industriespionage 2014: Cybergeddon der deutschen Wirtschaft durch NSA & Co.?***	***Kriminelle Risiken im Mittelstand: Gefahren, Schäden und Prävention – eine Studie***	***Cyber Security in Österreich Studie IT-Advisory***	***Wirtschafts- und Industriespionage in österreichischen Unternehmen 2015***
Allgemeines	*Bedrohungslage*			70% bewerten Cyber-Risiken als zunehmend	steigend	steigend, vor allem bei jenen Unternehmen, die bereits schon einmal Opfer wurden	92% glauben, dass Cyber Security kein Hype, sondern Alltag ist	Betroffenheit in den nächsten 5 Jahren: 71% gehen von keiner Gefährdung aus, 29% halten Betroffenheit für möglich
proaktive organisatorische Maßnahmen zur Absicherung vor WIS	*Eingesetzte Personal-Ressourcen für Security, bzw. Abteilung für Unternehmens-schutz vorhanden*			57% min. 1FTE		44%	45% kein Cyber-Security-MA	
Schaden	*Schaden / Land / Jahr*		DE: 51 Mrd.€		DE: 11,8 Mrd.€ AT: 1,6 Mrd.€			

Schaden	*Schaden / Org / Vorfall*				10k - 100k€	30%: 10k-50k		66%: 0-100k €, 16%: 100k-500k €, 7%: 500k-1Mio. €, 8%: 1Mio.-5Mio. €, 2%: höher
Schaden	*Hinweise auf konkreten, materiellen oder immateriellen Schaden*				33,45%			71%
Technischer Schutz vor Angriffen von außen, bzw. dem Internet	*Firewall eingesetzt*	86%	100%	99%	92,40%			
Technischer Schutz vor Angriffen von außen, bzw. dem Internet	*Mobile Security (technisch am Gerät)*	70%		44%				
Technischer Schutz vor Angriffen von außen, bzw. dem Internet	*Wireless Security (technisch)*	55%			14,40%			
Technischer Schutz vor Angriffen von außen, bzw. dem Internet	*Antivirus eingesetzt*	95%	100%	85%				
Technischer Schutz vor Angriffen von außen, bzw. dem Internet	*Updates/Patches regelmäßig*	74%		65%				
Technischer Schutz vor Angriffen von außen, bzw. dem Internet	*DLP & IDS/IPS*		26%		5,90%			

Quelle: Eigene Darstellung

Anhang B: Empirische Datenerhebung und Interviewleitfaden für die Experteninterviews

Im Folgenden wird der Interviewleitfaden dargestellt, der für die Durchführung der Experteninterviews herangezogen wurde. Es handelt sich dabei um die überarbeitete Version, wobei die Erkenntnisse aus dem Pre-Test bereits eingearbeitet wurden. Der kursive Text stellt die optionalen Fragen dar, welche aufgrund der Situation im Interview und der bisher abgehandelten Aspekte je nach Situation vom Autor gestellt wurden.

Begrüßung und Einführung (ca. 5 min)

- Information zum Ablauf des Interviews
- Einführung in die Zielsetzung der zugrundeliegenden Masterarbeit
- Einverständnis zur Audioaufnahme und Zusicherung der Anonymität (Unterfertigung der Einverständniserklärung)

Fachliche Fragen (ca. 50 min)

F1 Wie sind Sie bisher mit dem Themenkomplex WIS in Berührung gekommen? Welche Rolle spielt WIS in Ihrer Organisation?

Klarstellung WIS:

Industriespionage: Oft auch als Konkurrenzausspähung bezeichnet, steht die Industriespionage für das Ausspähen von Unternehmen durch andere Unternehmen. Das Ziel dahinter ist in den meisten Fällen die Beschaffung von schützenswerten Informationen zu Produkten, Entwicklungen oder Projekten.

Dabei handelt es sich um staatlich gelenkte, von anderen Nachrichtendiensten ausgehende Ausforschung von Organisationen. Die Motivation dahinter liegt darin, den Unternehmen des eigenen Landes oder Staates einen Vorteil zu verschaffen. Diese Schritte sind meist mittel- bis langfristig geplant und

können unter Umständen auch als Industriespionage oder Konkurrenzausspähung getarnt werden.

F2 Welche Maßnahmen in Ihrer Organisation tragen aus Ihrer Sicht maßgeblich zur Sicherheit vor WIS-Angriffen bei?

F3 Inwiefern können Sie Ergebnisse von Studien verwenden bzw. für Ihre Tätigkeit heranziehen und welche Rolle spielen diese Ergebnisse in Ihrer Organisation?

F4 Welche Themen werden aus Ihrer Sicht in den Studien ausreichend behandelt?

F5 Zu welchen Schwerpunkten in den Studien würden Sie sich mehr Informationen wünschen?

F6 Welche Studien ziehen Sie zur Recherche von Informationen heran? *Welche Studien bieten Ihnen dabei den größten Nutzen für Ihre Tätigkeiten? Worauf legen Sie bei der Auswahl besonders wert? Welche Kriterien für die Auswahl der Studien sind für Sie von besonderer Bedeutung? Welche Quellen sind für Ihre Bedürfnisse zur Informationsbeschaffung zu WIS geeignet?*

F7 Greifen Sie bei Ihrer täglichen Arbeit hinsichtlich WIS vermehrt auf umfassende Studien oder Detailberichte von einzelnen Vorfällen zurück? Welche Art von Information ist für Ihre weitere Arbeit am besten geeignet – Studien oder Detailberichte?

F8 Ist die Frage nach den Schäden und den Folge-Kosten für Organisationen aus Ihrer Sicht durch die Studien ausreichend behandelt?
Wie schätzen Sie die Glaubwürdigkeit der Angaben der Studien zu den Kosten ein? Inwiefern spielt die Glaubwürdigkeit der Studienergebnisse in Ihrer Organisation eine Rolle?

Hinweis: Die folgenden drei Fragen sind ähnlich aufgebaut und zielen auf die physische, technische, sowie personelle Sicherheit ab.

F9 Welche Maßnahmen zur Stärkung der physischen Sicherheit wurden in Ihrer Organisation getroffen?
Welchen Stellenwert nehmen diese bei Ihnen ein? Würden Sie hierzu gerne mehr Studienergebnisse sehen?

F10 Welche Maßnahmen zur Stärkung der technischen Sicherheit wurden in Ihrer Organisation getroffen?
Welchen Stellenwert nehmen diese bei Ihnen ein? Würden Sie hierzu gerne mehr Studienergebnisse sehen?

F11 Welche Maßnahmen zur Stärkung der organisatorischen, bzw. personellen Sicherheit wurden in Ihrer Organisation getroffen? *Welchen Stellenwert nehmen diese bei Ihnen ein? Würden Sie hierzu gerne mehr Studienergebnisse sehen?*

F12 Wenn Sie weitere Maßnahmen zum Schutz vor WIS planen, greifen Sie dabei auf Studienergebnisse zurück bzw. wo holen sie sich Ideen/Inspiration? Wenn nicht, welche Quellen ziehen Sie heran?

F13 Wir sind nun am Ende des Interviews angelegt. Gibt es aus Ihrer Sicht noch etwas, was Sie ergänzen möchten?

Abschluss des Interviews (ca. 5 min)

- Klärung offener Fragen
- Information zur weiteren Vorgehensweise der Masterarbeit und die weitere Verarbeitung der Informationen aus dem Interview
- Dank und Verabschiedung

Die Tabelle 6 zeigt die Operationalisierung, von den Begriffen, über die Dimensionen und entsprechenden Indikatoren, hin zu den Referenzen auf die einzelnen Fragen des Interviewleitfadens.

Tabelle 6: Operationalisierung

Begriff	Dimension	Indikator	Messinstrument
B1 Wirtschafts- und Industrie-spionage	**D1** Vorfall	**I1** Erkennung	**F1**
		I2 Erfahrung	**F1**
		I3 Kurzfristige Schäden	**F8**
		I4 Langfristige Schäden	**F8**

	D2 Management Awareness	**I5** Kriterien zur internen Bewertung	**F6**
		I6 Risikobewertung	**F6**
		I7 Kommunikation	**F3**
		I8 Bewusstsein bei Führungskräften	**F1**
B2 Anwend-barkeit der Studien-ergebnisse in der Praxis	**D3** Relevanz in der Praxis	**I9** Hohe Relevanz	**F3 / F4 / F5**
		I10 Keine Relevanz	**F3 / F4 / F5**
		I11 Dunkelfeld	**F5**
	D4 Unterschied Studien und Vorfälle	**I12** Relevanz von Studien und bekannten Fällen in der Praxis	**F7**
		I13 Präferenz Studien oder Einzelfälle	**F7**
	D5 Informations-bedarf	**I14** Verfügbare Informationen	**F4**
		I15 Informationslücken	**F5**
	D6 Ermittelte Themen-schwerpunkte der Studien	**I16** Betroffenheit	**F1**
		I17 Kronjuwelen	**F4 / F5**
		I18 Security-Policy	**F4 / F5**
		I19 Physischer Schutz	**F9**
		I20 Technischer Schutz der IT	**F10**
		I21 Prüfungen der Sicherheitsmaßnahmen	**F4 / F5**
		I22 Business Continuity Management	**F4 / F5**
		I23 Analyse von Aktivitäten auf IT-Systemen	**F4 / F5**
		I24 Beziehungen mit ausländischen Unternehmen	**F4 / F5**

		I25 Einschätzung der Effektivität bereits getroffener Maßnahmen	**F2**
		I26 Planung weiterer Maßnahmen	**F12**

Quelle: Eigene Darstellung

Anhang C: Auswertetabelle der qualitativen Inhaltsanalyse der Interviews

Die folgenden Teilanhänge C.1, C.2 und C.3 stellen Auszüge aus den Auswertetabellen der qualitativen Inhaltsanalyse der durchgeführt Interviews dar. Die vollständigen Interviewtranskriptionen, Auswertetabellen, sowie die entsprechenden Paraphrasierungen, Generalisierungen und Reduktionen liegen dem Autor vor.

Anhang C.1: Auszug aus der Auswertetabelle für das Interview 1

Tabelle 7: Auszug aus der Auswertetabelle für das Interview 1

Indikator	Paraphrase	Generalisierung	Reduktion
I9 Hohe Relevanz	„Das kommt bei dem Durchlesen der Studie heraus. Wenn sie zu technisch sind, ist es suboptimal – wenn sie zu oberflächlich sind, auch. Da ist immer so einen Mittelweg zu finden – das ist auch eine Kunst.“ (Interview1_20161103, Absatz 28)	Der Mittelweg zwischen Detailtiefe und Oberflächlichkeit von Studien bietet eine hohe Relevanz für den Einsatz in der Praxis.	Der Mittelweg zwischen Detailtiefe und Oberflächlichkeit von Studien bietet eine hohe Relevanz für den Einsatz in der Praxis.
I10 Keine Relevanz	„Umfassende Studien verwende ich für die tägliche Arbeit eher weniger. Eher wenn es so Adhoc-Themen gibt, die aufpoppen – irgendwelche aktuellen Themen“ (Interview1_20161103, Absatz 12)	Studien werden vor allem für kurzfristige Fragestellungen herangezogen, aber weniger für die tägliche Arbeit von Security-Expertinnen und -Experten	Studien werden vor allem für kurzfristige Fragestellungen herangezogen, aber weniger für die tägliche Arbeit von Security-Expertinnen und -Experten
I11 Dunkelfeld	„Da könnte mehr Fokus daraufgelegt werden können.“ (Interview1_20161103, Absatz 40)	Auf das Dunkelfeld könnte ein größerer Fokus gelegt werden.	Auf das Dunkelfeld könnte ein größerer Fokus gelegt werden.

Quelle: Eigene Darstellung

Anhang C.2: Auszug aus der Auswertetabelle für das Interview 2

Tabelle 8: Auszug aus der Auswertetabelle für das Interview 2

Indikator	Paraphrase	Generalisierung	Reduktion
I12 Relevanz von Studien und bekannten Fällen in der Praxis	„Richtung Studien selber, so als zusätzlicher Themenbereich, dass man einfach einmal schaut, ja ok, was ist eigentlich gewesen, wo gibt es Schwerpunkte, von dem her, finde ich am interessantesten den vom BSI, wo oftmals eine gute Studie herausgegeben wird, dann das Bundesministerium für Inneres für den Bereich und sonst gesehen direkt vom BVT, also vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung.“ (Interview2_20161118, Absatz 16)	Studien von BSI, BMI und BVT dienen vor allem zur Orientierung der Schwerpunkte bei Security	Studien dienen vor allem zur Orientierung der Schwerpunkte, wobei die entscheidungskritischen Informationen aus dem eigenen Sektor kommen.
	„Wir beziehen uns eigentlich immer auf die Branche selber und kritische Infrastruktur, die die Messlatte für uns selber ist.“ (Interview2_20161118, Absatz 58)	Die Vorgaben aus der eigenen Branche heraus bilden die Messlate für Organisationen.	
	„Abschließend wäre noch zu sagen, dass ich eigentlich eher weniger auf solche Studien verlasse, die zwar schon auch Input-gebend sind, aber jetzt nicht der wichtigste Teil für Entscheidungen“ (Interview2_20161118, Absatz 66)	Studien werden bei Entscheidungsfindungen als zusätzlicher Input eingesetzt.	

I13 Präferenz Studien oder Einzelfälle	„da ist es sicher dann interessant ... wobei das sind dann wieder Detailberichte und die haben nicht den Charakter einer Studie, die ich dann in Anspruch nehme.“ (Interview2_20161118, Absatz 32)	In Organisationen werden verstärkt Detailberichte eingesetzt, als umfassende Studien.	In Organisationen werden verstärkt Detailberichte eingesetzt, als umfassende Studien.
I14 Verfügbare Informationen	„Fühle ich mich eigentlich auch ausreichend informiert.“ (Interview2_20161118, Absatz 56)	Im Allgemeinen ist die Verfügbarkeit von Informationen auf einem guten Niveau.	Im Allgemeinen ist die Verfügbarkeit von Informationen auf einem guten Niveau.

Quelle: Eigene Darstellung

Anhang C.3: Auszug aus der Auswertetabelle für das Interview 5

Tabelle 9: Auszug aus der Auswertetabelle für das Interview 5

Indikator	Paraphrase	Generalisierung	Reduktion
I5 Kriterien zur internen Bewertung	„Wir sind ein IT-Provider eines Finanzdienstleisters. Bei uns geht es eher um Vertrauen, wenn man das so locker formulieren will. Wir leben vom Vertrauen, dass unsere Kunden uns Geld anvertrauen“ (Interview5_20161122, Absatz 4)	Die Wahrung des von Kundinnen und Kunden entgegengebrachten Vertrauens trägt maßgeblich zur Ausrichtung der Sicherheit von IT-Providern bei.	Die Wahrung des von Kundinnen und Kunden entgegengebrachten Vertrauens trägt maßgeblich zur Ausrichtung der Sicherheit von IT-Providern bei.
I6 Risikobewertung	„Das ist in der Security eine wichtige Frage, mit wieviel Risiko möchte ich leben. Geht es hier um das Ergebnis um jeden Preis? Auch wenn das wirtschaftlich unvernünftig ist?“ (Interview5_20161122, Absatz 18)	Die Risikobereitschaft ist grundlegend für die Entscheidung, ob Risiken eingegangen werden sollen.	Eine Risikobewertung muss die Risikobereitschaft, die Marktposition, die Klassifizierung der Daten, sowie bekannte Schwachstellen berücksichtigen.
	„Bin ich der Billigst-Anbieter zu Kampfpreisen, wo die Kunden alles hinnehmen, Hauptsache der Preis stimmt, dann wird das mit der Security wohl egal sein. Aber dann muss ich halt auch ... Da habe ich halt dafür die Kostenführerschaft.“ (Interview5_20161122, Absatz 22)	Die Marktposition einer Organisation gibt zumindest ein grobe Richtung der erwarteten Security durch die Kundinnen und Kunden bekannt.	
	„Datenklassifizierung, wo kann ich mir einen Breach überhaupt leisten, wo will ich mir keinen leisten, wo ist es mir egal“ (Interview5_20161122, Absatz 26)	Eine Datenklassifizierung zeigt jene Daten auf, die geschützt werden müssen.	

	„Dann braucht man die Risikoabschätzung, ist das eine Lücke, ein Zero Day Exploit, wie schnell ist der eigentlich auswertbar?“ (Interview5_20161122, Absatz 32)	Bekannte Schwachstellen müssen bewertet werden, um deren Risiko für die Organisation einschätzen zu können.	
I7 Kommunikation	„Je nachdem, wie halt die eigenen Kunden sind, kann eine glaubwürdige Security, oder ein professioneller Umgang mit Breaches dazu führen, dass sich die Kundenbeziehung verstärkt, oder nicht. Das hängt davon ab, was bin ich für ein Unternehmen.“ (Interview5_20161122, Absatz 22)	Nach einem erfolgreichen Angriff kann ein professioneller Umgang damit die Kundenbeziehung unter Umständen verstärken.	Nach einem erfolgreichen Angriff kann ein professioneller Umgang damit die Kundenbeziehung unter Umständen verstärken.

Quelle: Eigene Darstellung