Bundeskriminalamt

Wirtschaftsspionage und Konkurrenzausspähung – eine Analyse des aktuellen Forschungsstandes

Ergebnisbericht einer Sekundäranalyse

Karsten Kasper

Stand: April 2014

Das Kriminalistische Institut des Bundeskriminalamts ist zertifiziert nach DIN EN ISO 9001 (TÜV Nord CERT, Zertifikat-Registrier-Nr. 44 100 081125)

Inhaltsverzeichnis

Tabellen- und Abbildungsverzeichnis

Abkürzungsverzeichnis

ASW	Arbeitsgemeinschaft für Sicherheit der Wirtschaft
BDI	Bundesverband der Deutschen Industrie
BfV	Bundesamt für Verfassungsschutz
BIP	Bruttoinlandsprodukt
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation u. neue Medien
BKA	Bundeskriminalamt
BMI	Bundesministerium des Inneren
BMWi	Bundesministerium für Wirtschaft
BND	Bundesnachrichtendienst
BSI	Bundesamt für Sicherheit in der Informationstechnik
BVT	Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Österreich)
COD	Computergestütztes Dokumentationssystem
COMPINT	Computer Intelligence
CT	Corporate Trust
DATAINT	Data Intelligence
DIHK	Deutscher Industrie- und Handelskammertag
E&Y	Ernst & Young
e. V.	Eingetragener Verein
F&E	Forschung und Entwicklung
HUMINT	Human Source Intelligence
IKT	Informations- und Kommunikationstechnologien
IT	Informationstechnik
KA	Konkurrenzausspähung
KMU	Kleine und mittlere Unternehmen
LfV	Landesamt für Verfassungsschutz
NSA	National Security Agency (USA)
PKS	Polizeiliche Kriminalstatistik
PwC	PricewaterhouseCoopers
SiFo	Programm Sicherheitsforschung der Bundesregierung
TECHINT	Technical Intelligence
VDI	Verein Deutscher Ingenieure
VdS	Vertrauen durch Sicherheit
VSW	Verband für Sicherheit in der Wirtschaft
Wikri	Wirtschaftskriminalität
WS	Wirtschaftsspionage

Zusammenfassung

Der vorliegende Bericht stellt die Ergebnisse einer Sekundäranalyse zum Thema Wirtschaftsspionage und Konkurrenzausspähung dar. Im Fokus der Analyse standen aktuelle Beiträge aus der Fachliteratur sowie empirische Studien, in deren Rahmen Unternehmensbefragungen durchgeführt worden sind.

Geleitet wurde die Analyse von der zentralen Frage, wie sich die Phänomene Wirtschaftsspionage und Konkurrenzausspähung aus Sicht deutscher Unternehmen aktuell darstellen. Anlass zu dieser Frage bieten u. a. sowohl die intensive und zum Teil überspitzte mediale Berichterstattung zu diesem Thema als auch die relativ wenigen Erkenntnisse zur Phänomenologie der Wirtschaftsspionage und Konkurrenzausspähung der Strafverfolgungsbehörden. Auch umfangreiche Abfragen im Auftrag des Bundesministeriums des Innern bei deutschen und ausländischen Behörden und Dienststellen im Hinblick auf eine Verbesserung des Kenntnisstandes haben nicht die erwünschten Ergebnisse erbracht (vgl. Ziercke 2008: 11). Auf der Grundlage der Hellfelderfassung sowie der medialen Berichterstattung können jedoch keine zuverlässigen Erkenntnisse zu der Phänomenentwicklung gewonnen und polizeiliche Maßnahmen zur Prävention und Repression begründet werden.

Zur Beantwortung der zentralen Fragestellung wurden schwerpunktmäßig empirische Studien mit Hilfe einer qualitativen Text- und Datenanalysesoftware systematisch ausgewertet. Da sich die betrachteten Unternehmensbefragungen in Vorgehen und methodischer Qualität sowie bei den thematischen Schwerpunkten und Zielsetzungen zum Teil stark unterscheiden, sollten die im Rahmen dieser Analyse gewonnen Erkenntnisse eher als Anhaltspunkte und Tendenzen verstanden werden denn als feste statistische Größen.

Folgende zentrale Ergebnisse können aus der Sekundäranalyse abgeleitet werden:

- Die strafrechtlich relevante Unterscheidung zwischen Wirtschaftsspionage und Konkurrenzausspähung ist für Unternehmen weniger bedeutsam.
- Die Mehrheit der Unternehmen schätzt die von Ausforschungsaktivitäten ausgehende Bedrohung für die deutsche Wirtschaft als hoch bis sehr hoch ein und geht zudem von einem zukünftig weiteren Anstieg der Bedrohung aus.
- Im Durchschnitt gibt ungefähr jedes vierte Unternehmen an, bereits Opfer von Ausforschungshandlungen geworden zu sein.

- Nur ein kleiner Teil der Unternehmen bringt entsprechende Vorfälle zur Anzeige.
- Etwa jeder dritte Fall von Ausforschung wurde rein zufällig entdeckt.
- Die Sicherheitsbehörden spielen eine untergeordnete Rolle bei der Aufdeckung von Ausforschungsverdachtsfällen.
- Aktuelle und ehemalige Mitarbeiter bilden die wichtigste Tätergruppe, sie können sowohl bewusst als auch unbewusst zu Tätern werden.
- Schätzungen zum jährlichen finanziellen Schaden durch Ausforschung in Deutschland reichen von ein- bis zu dreistelligen Milliardenbeträgen. Im Gegensatz dazu wird nach Hochrechnungen auf der Grundlage der Schadensangaben der befragten Unternehmen „lediglich“ von einstelligen Milliardenbeträgen ausgegangen.
- Unternehmen kooperieren bei der Abwehr von Wirtschaftsspionage und Konkurrenzausspähung häufiger mit privaten Akteuren als mit Behörden. Sie sind auch häufiger mit den Informations- und Beratungsangeboten von privaten Einrichtungen zufrieden.
- Viele Unternehmen sehen die Notwendigkeit von organisatorischen, personellen, technischen und IT-spezifischen Sicherheitsvorkehrungen. Sie sind sich aber häufig nicht der schwerwiegenden Auswirkungen bewusst, die ein Angriff zu Ausforschungszwecken für das Unternehmen haben kann – somit werden vielfach nur Mindestvorkehrungen getroffen.
- Die Entwicklungen im Bereich der Informations- und Kommunikationstechnologien (IKT) führen zu neuen Risiken und erhöhen die Wahrscheinlichkeit, dass deutsche Unternehmen Opfer von Ausforschung werden.

Ferner ergeben sich aus der Sekundäranalyse mehrere Schlussfolgerungen: Die verschiedenen behördlichen Akteure im Bereich Wirtschafts- und Informationsschutz sollten ihre Kräfte und Anstrengungen zusammenführen, wie es in der vom Bundesverband der Deutschen Industrie (BDI), des Deutschen Industrie- und Handelskammertags (DIHK) und des Bundesministeriums des Inneren (BMI) unterzeichneten „Erklärung für eine Nationale Wirtschaftsschutzstrategie“ vorgesehen ist (vgl. BMI 2013a: 1). Die Festlegung eines gemeinsamen Ansprechpartners für die Wirtschaft sowie die Bündelung von Informations- und Beratungsangeboten und von wissenschaftlichen Tätigkeiten der staatlichen Akteure sind weitere notwendige Maßnahmen.

Zudem ist es wichtig, dass die Sicherheitsbehörden mit anderen Akteuren im Wirtschaftsschutz (Kammern, Verbände, private Dienstleister, Forschungsinstitute etc.) zusammenarbeiten. Besonders wichtig als Kooperationspartner sind die Kammern der Industrie und des Handels sowie des Handwerks, die den Unternehmen häufig am nächsten stehen und deshalb zu ihren wichtigsten Ansprechpartnern zählen.

Auch zusätzliche großangelegte repräsentative Opferbefragungen können den Sicherheitsbehörden relevante Informationen zu den Phänomenen Wirtschaftsspionage und Konkurrenzausspähung liefern. Dabei wäre es von Vorteil, wenn die Sicherheitsbehörden *eigene* Dunkelfeld- und Opferbefragungen in Auftrag geben, um auf diese Weise die Berücksichtigung der eigenen Perspektive, Interessenslage und Fragestellungen gewährleisten zu können. Allgemein besteht der Bedarf an weiterer empirischer Forschung in diesem Themenfeld.

Abstract

This report examines and summarises German papers and empirical studies dealing with economic and industrial espionage. It thereby focuses on German businesses' perspectives of these two phenomena with regard to their respective threat perception, their victimisation, the identified damages, the detected and suspected offenders, their preventive and repressive security measures, their cooperation with the respective law enforcement and intelligence agencies, and lastly their perception of relevant public and private actors. On the one hand one can observe broad, yet mostly superficial media coverage on economic and industrial espionage; on the other hand law enforcement authorities still lack profound expertise in the crime fields' phenomenologies. The literature review contributes to this domain by providing a systematic and comprehensive synopsis which is mainly based on empirical findings.

1. Einleitung und Begrifflichkeiten

> *„Wir wollen unsere Unternehmen vor Wirtschafts- und Konkurrenzspionage aus aller Welt schützen und eine nationale Strategie für den Wirtschaftsschutz erarbeiten*“ (Bundesregierung 2013: 145).

> *„Damit [durch ein rechtlich verbindliches Abkommen zum Schutz vor Spionage; der Verf.] sollen die Bürgerinnen und Bürger, die Regierung und die Wirtschaft vor schrankenloser Ausspähung geschützt werden. Wir stärken die Spionageabwehr*“ (Bundesregierung 2013: 149).

Diese Zitate aus dem Koalitionsvertrag der aktuellen Bundesregierung verdeutlichen die Bedeutung und das Bedrohungspotenzial von Wirtschaftsspionage und Konkurrenzausspähung (vgl. Bundesregierung 2013).

Der Begriff „Spionage“ ist kein eigener Straftatbestand im Strafgesetzbuch, er bezeichnet lediglich einen Phänomenbereich. In der für die zuständigen Behörden geltenden Definition wird Spionage als die Auskundschaftung und Erlangung fremder Geheimnisse oder geschützten Wissens durch fremde Staaten und deren Nachrichtendienste definiert. Neben Politik, Verwaltung, Militär und Forschung zählt auch die Wirtschaft zu den „klassischen“ Spionagezielen. Die einschlägigen gesetzlichen Strafbestimmungen sind hier der Landesverrat (§ 94 StGB), das Offenbaren von Staatsgeheimnissen (§ 95 StGB), die landesverräterische Ausspähung und das Auskundschaften von Staatsgeheimnissen (§ 96 StGB), die Preisgabe von Staatsgeheimnissen (§ 97 StGB) sowie die landesverräterische (§ 98 StGB) und die geheimdienstliche Agententätigkeit (§ 99 StGB).

Somit zählt der Phänomenbereich Wirtschaftsspionage zu den Staatsschutzdelikten, die politisch motivierte Straftaten umfassen, bei denen die äußere Sicherheit der Bundesrepublik Deutschland angegriffen wird und nicht nur das jeweilige betroffene Unternehmen.

Für die Verfolgung geheimdienstlicher Agententätigkeit, auch in dem Bereich Wirtschaft, ist der Generalbundesanwalt zuständig. Das Bundesamt für Verfassungsschutz (BfV)

definiert Wirtschaftsspionage als „…die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben“ (BfV 2008: 9).

Das Bundesamt und die Landesämter für Verfassungsschutz haben den Auftrag, Unternehmen präventiv vor der Ausforschung, insbesondere durch ausländische Nachrichtendienste, aufzuklären und zu schützen (vgl. BfV 2008: 9). Wichtigstes Ziel dabei ist die Erhöhung der Wahrnehmung der Bedrohung und der Sensibilität für das Thema. Abgesehen davon sind Unternehmen jedoch immer erstmals selbst in der Pflicht, ausreichend und geeignete Sicherheitsmaßnahmen zu treffen. Die Bekämpfung der Ausforschung durch Wettbewerber oder Einzeltäter gehört nicht zum Aufgabenbereich der Verfassungsschutzbehörden (vgl. Warnecke 2010: 256).

Während der Verfassungsschutz vornehmlich präventiv agiert, nehmen die Strafverfolgungsbehörden eine repressive Funktion bei der Bekämpfung von Wirtschaftsspionage und Konkurrenzausspähung ein.

Die Wirtschaftsspionage muss von der Konkurrenzausspähung (manchmal auch als Betriebs-, Industrie- oder Konkurrenzspionage bezeichnet) abgegrenzt werden, die nach einschlägiger Definition der Sicherheitsbehörden für die Ausforschung eines Unternehmens durch andere Unternehmen, Einzelpersonen oder organisierte Gruppen steht. Die Verfolgung obliegt der Justiz der Länder und fällt in die Zuständigkeit der Wirtschaftskriminalität. Die Konkurrenzausspähung ist u. a. als Verstoß gegen die §§ 17 ff. UWG (Verrat von Betriebs- und Geschäftsgeheimnissen), §§ 202a-c StGB (Ausspähen, Abfangen von Daten und Vorbereitungshandlungen), §§ 303a-b StGB (Datenveränderung, Computersabotage) sowie §§ 242 ff. StGB (Diebstahl) strafbar (vgl. Többens 2000: 511). Geschädigte Unternehmen haben die Möglichkeit, Anzeige bei den Strafverfolgungsbehörden zu erstatten.

In beiden Kriminalitätsbereichen wird das gleiche Ziel verfolgt: Wirtschaftsspionage und Konkurrenzausspähung, dienen dazu, unbemerkt und unter Verwendung von „unehrlichen“ Mitteln (vgl. Niemantsverdriet 2011: 26) an Know-how und Informationen (neue Technologien, Produktionsabläufe, Strategiepapiere, Kunden-/Lieferantenlisten etc.) zu gelangen, die die Wirtschaftskraft des eigenen Unternehmens oder des eigenen Landes verbessern und

zudem rechtzeitig über unerwartete technische Entwicklungen informieren (vgl. Warnecke 2010: 257).

Die Unterschiede zwischen Wirtschaftsspionage und Konkurrenzausspähung erschließen sich erst im Laufe von Ermittlungen und sind für eine erste Zuordnung im Schadensfall nicht zielführend. Die Frage nach dem/den Täter/n ist Dreh- und Angelpunkt nach einer ersten Tatortbewertung und steht im Zentrum der kriminalpolizeilichen Ermittlungsarbeit. Bezüglich der Opfer oder der angewandten Methoden lassen sich weniger augenscheinliche Unterschiede feststellen.

Die Unterscheidung zwischen Wirtschaftsspionage einerseits und Konkurrenzausspähung andererseits ist für die Sicherheitsbehörden, vor allem in Bezug auf die Zuständigkeiten, relevant. Für die meisten Unternehmen jedoch scheint diese Unterscheidung sehr viel weniger bedeutsam. Bei einem festgestellten Vorfall ist es für viele Unternehmen zunächst nicht wichtig, ob der Angriff von einem Wettbewerber oder einem ausländischen Nachrichtendienst ausging, sondern vielmehr, wie der Schaden für das Unternehmen behoben und so gering wie möglich gehalten werden kann. Die definitorische Unterscheidung zwischen Wirtschaftsspionage und Konkurrenzausspähung scheint daher für viele Unternehmen eher eine akademische als eine praktische Bedeutung zu haben und es wird regelmäßig gefordert, dass die verschiedenen Zuständigkeiten zusammengeführt werden (vgl. BfV 2008: 9).

Dass diese Unterscheidung für die Wirtschaft weniger relevant ist als für die Sicherheitsbehörden, wird auch dadurch ersichtlich, dass in den vorliegenden Unternehmensbefragungen keine terminologische Trennung vorgenommen wird und somit begrifflich nicht zwischen den Phänomenen Wirtschaftsspionage und Konkurrenzausspähung unterschieden wird. Stattdessen wird in manchen Studien z. B. lediglich *ein* Begriff verwendet der beide Phänomene abdeckt[1]. In anderen Studien werden die Phänomene Wirtschaftsspionage und Konkurrenzausspähung synonym verwendet, ohne Berücksichtigung der Unterschiede[2]. In wieder anderen Studien werden anstelle der Begriffe Wirtschaftsspionage und Konkurrenzausspähung andere Begriffe verwendet, wie z. B. unfreundlicher Know-how-Verlust oder Datendiebstahl, die in den jeweiligen Studien aber durchaus für Wirtschaftsspionage und

[1] In den Corporate Trust-Studien steht der Begriff Industriespionage gleichzeitig für Wirtschaftsspionage und Konkurrenzausspähung. In den KPMG-Studien zu e-Crime wird der Begriff Wirtschaftsspionage überwiegend genutzt, weil er in der Öffentlichkeit häufig als Begriff für alle Formen der Ausforschung in der Wirtschaft verwendet wird (vgl. KPMG 2010a: 20).

[2] Z. B. in den Ernst & Young-Befragungen, wo die Begriffe austauschbar verwendet werden.

Konkurrenzausspähung stehen: So benennt z. B. das Sicherheitsforum Baden-Württemberg in seiner Studie, die im Rahmen des Programms Sicherheitsforschung der Bundesregierung (SiFo) gefördert wurde, den Verrat oder das Ausspähen von Geschäfts- und Betriebsgeheimnissen als „die am meisten verbreitete Form der Wirtschafts- und Industriespionage“ (Sicherheitsforum 2010: 45).

In der vorliegenden Arbeit sollen die verschiedenen Begrifflichkeiten folgendermaßen verwendet werden: Sofern allgemein von auf wirtschaftliche Vorteile ausgerichteter Auskundschaftung die Rede ist und es nicht relevant ist (und/oder möglich ist herauszufinden), ob es sich um Wirtschaftsspionage (und somit um einen ausländischen Nachrichtendienst als Täter/Auftraggeber) oder um Konkurrenzausspähung (und somit um einen Wettbewerber als Täter/Auftraggeber) handelt, werden im Folgenden die Phänomene Wirtschaftsspionage und Konkurrenzausspähung gemeinsam und im Singular (als ein Begriff) mit der Abkürzung WS/KA verwendet. Ist die Unterscheidung wichtig (und/oder möglich), wird jeweils der zutreffende Begriff Wirtschaftsspionage oder Konkurrenzausspähung verwendet.

Der Begriff der Ausforschung wird verwendet, wenn allgemein von einem ungewollten Verlust unternehmensinterner Daten gesprochen wird und es zunächst nicht feststellbar ist, wer die Daten gestohlen, weitergeleitet oder gefunden hat. Dieser Begriff bezieht sich gleichzeitig auf WS/KA sowie auf die anderen in den Befragungen genannten Methoden der Auskundschaftung, wie z. B. Datenklau, Abhören und Abfangen von Daten, Verrat von Geschäfts- und Betriebsgeheimnissen, Angriffe auf die IT zu Ausforschungszwecken etc.

Wirtschaftsspionage und Konkurrenzausspähung sind nicht gleichzusetzen mit e-Crime, Cybercrime oder mit Wirtschaftskriminalität – in mehreren Studien werden sie als ein Teil dieser breiteren Kriminalitätsphänomene gesehen.

Sicherheitsbehörden, Massenmedien, Sicherheitsexperten aus Kammern, Verbänden und Beratungsunternehmen, Politik und Unternehmen selbst sind sich einig: Auf wirtschaftliche Vorteile ausgerichtete Ausforschung ist eine ernstzunehmende Bedrohung für die deutsche Wirtschaft, die den technologischen Vorsprung Deutschlands gefährdet, das Wirtschafts-

wachstum bremst, deutsche Arbeitsplätze bedroht und beinahe jedes Unternehmen treffen kann (vgl. Blume 2008: 11).

Die mediale Berichterstattung zum Thema Wirtschaftsspionage und Konkurrenzausspähung ist beträchtlich und hat sich seit den Enthüllungen durch Edward Snowden weiter intensiviert. Besonders beunruhigend für die Öffentlichkeit sind die bislang ungeahnten technischen Möglichkeiten der Ausforschung sowie die Tatsache, dass nachrichtendienstliche Wirtschaftsspionage nicht nur von Ländern wie Russland, Nordkorea oder China, sondern auch von den engsten Verbündeten ausgehen kann (vgl. Peil 2013: 14).
Kammern, Verbände und Behörden reagieren auf das gestiegene Interesse seitens der Unternehmen an diesem Themenbereich mit einer Vielzahl von Seminaren, Workshops und Fortbildungsveranstaltungen.

Gesellschaftliche Entwicklungen, wie z. B. die hohe Zahl der Leiharbeitnehmer in vielen Unternehmen, die sich tendenziell weniger mit einem Arbeitgeber identifizieren als Stammpersonal, oder die schnell wachsende Zahl wirtschaftlich erfolgreicher Unternehmen in Schwellenländern erhöhen die Bedrohung. Die Gefahr für deutsche Unternehmen wächst aber vor allem mit den Fortschritten im IKT-Bereich. Angriffe über das Internet können relativ einfach und risikoarm bei mehreren tausend Unternehmen gleichzeitig durchgeführt werden, Daten können in kürzester Zeit von einem Ende der Welt zum anderen verschickt werden und auf kleinste Speichermedien passen enorme Datenmengen.

Ausforschung für wirtschaftliche Vorteile ist eine reale Gefahr und die Bedrohung nimmt weiterhin zu. Trotz der umfangreichen Berichterstattung und der hohen Bedrohungswahrnehmung, lassen sich in den Medien und der Fachliteratur nur relativ wenige eindeutige Angriffe auf deutsche Unternehmen feststellen. Dieser Widerspruch spiegelt sehr gut die Situation wider, in der sich die Strafverfolgungsbehörden befinden: obwohl sie davon ausgehen, dass die Bedrohung für deutsche Unternehmen u. a. aus den oben genannten Gründen weiter ansteigen wird, benötigen die Behörden weitere Erkenntnisse zur Phänomenologie der Wirtschaftsspionage und Konkurrenzausspähung. Das Dunkelfeld gilt in diesen Deliktsbereichen als erheblich und kann sogar als „doppeltes Dunkelfeld“ bezeichnet werden (vgl. Kapitel 4.1). Denn einerseits werden Fälle von Wirtschaftsspionage und Konkurrenzausspähung in einem nicht bekannten Ausmaß gar nicht bemerkt oder die Unternehmen sind andererseits oftmals nicht bereit, die Ausforschung anzuzeigen.

Um adäquate präventive und repressive Maßnahmen zur Abwehr von Wirtschaftsspionage und Konkurrenzausspähung entwickeln zu können, müssen sich die Strafverfolgungsbehörden auf zuverlässige empirische Erkenntnisse stützen, da das Hellfeld und die Medienberichterstattung hierfür nicht ausreichend sind. Hier kann die Dunkelfeldforschung durch repräsentative Opferbefragungen nützliche und verlässlichere Informationen generieren. Im Rahmen einer solchen Befragung haben Unternehmen die Möglichkeit, sich anonym zu dem Thema zu äußern, und können gleichzeitig davon profitieren: erstens können ihnen die Ergebnisse helfen, die eigene Bedrohungslage besser einzuschätzen und zweitens können sie überprüfen, ob die eigenen Sicherheitsvorkehrungen ausreichend sind.

Der Schwerpunkt der vorliegenden Arbeit liegt auf der Analyse von Opferbefragungen zu Erfahrungen der Unternehmen mit Wirtschaftsspionage und Konkurrenzausspähung. Zentrale Frage dieser Ausarbeitung ist, wie sich die Phänomene Wirtschaftsspionage und Konkurrenzausspähung in Deutschland aus Sicht der Unternehmen und anhand des aktuellen Forschungsstandes darstellen.

Nach einer kurzen Erläuterung der Ziele der Sekundäranalyse und des methodischen Vorgehens folgt ein Kapitel mit theoretischen Anmerkungen. Im Anschluss daran werden die zentralen Ergebnisse der Sekundäranalyse differenziert u. a. nach der Betroffenheit, der Bedrohungswahrnehmung, den Schäden, den wichtigsten Kooperationspartnern der Unternehmen sowie den getroffenen Sicherheitsvorkehrungen präsentiert.

2. Ziele der Sekundäranalyse

Ziel der Sekundäranalyse ist die Aufarbeitung des aktuellen Forschungsstandes in den Kriminalitätsbereichen Wirtschaftsspionage und Konkurrenzausspähung auf der Grundlage öffentlich zugänglicher Quellen. Dadurch soll gezeigt werden, wie sich die Phänomene Wirtschaftsspionage und Konkurrenzausspähung in Deutschland darstellen.

Der Schwerpunkt der Ausarbeitung liegt auf der Sichtweise deutscher Unternehmen. Ihre Einschätzungen, Wahrnehmungen und Aussagen zur Bedrohung durch Wirtschaftsspionage und Konkurrenzausspähung, der eigenen Betroffenheit, den entstandenen Schäden, identifizierten Tätern, Kooperationsformen mit anderen Einrichtungen sowie den implementierten Sicherheitsvorkehrungen sind die zentralen Aspekte der Analyse. Das bedeutet, dass

neben Beiträgen aus der Fachliteratur (u. a. Monographien, Sammelbänden, Fachzeitschriften und Veröffentlichungen wichtiger privater und staatlicher Akteure) schwerpunktmäßig empirische Studien ausgewertet werden, in deren Rahmen Unternehmensbefragungen durchgeführt wurden.

3. Methodisches Vorgehen

3.1 Literaturrecherche

In einem ersten Schritt wurde eine systematische schlagwortgestützte Recherche nach thematisch relevanten Forschungsprojekten, Studien, Doktor- und Diplomarbeiten, Fachartikeln, Tagungsbeiträgen und Publikationen durchgeführt. Mit im Vorfeld festgelegten Suchbegriffen wurde online (u. a. in Bibliothekskatalogen und auf den Websites relevanter Institutionen) sowie in polizeilichen Fachdatenbanken recherchiert.

Mit der größten Anzahl an Suchbegriffen[3] wurde im *computergestützten Dokumentationssystem (COD) für Literatur* des Bundeskriminalamts (BKA) recherchiert. Durch die Verwendung eines Trunkierungszeichens[4] konnte eine größere Abdeckung des Suchraums gewährleistet werden. Mit Hilfe dieser schlagwortgestützten Recherche konnten ca. 440 auswertungsrelevante Quellen ab dem Erscheinungsjahr 1999 identifiziert werden. Aus diesen wurden für die weitere Auswertung nur Quellen ab 2007 mit unmittelbarem Themenbezug und wissenschaftlichem Charakter ausgewählt. Mit Hilfe dieser Kriterien konnte die Zahl der auswertungsrelevanten Quellen auf 148[5] reduziert werden.

Nach einer ersten Sichtung des Materials konnte festgestellt werden, dass die oben beschriebene, sehr breit gefasste Stichwortsuche nicht nötig ist, um thematisch relevante Artikel zu identifizieren. Behandelt eine Quelle das Thema Wirtschaftsspionage oder Konkur-

[3] Suchbefehl: .spionage. o .ausspähung. o technologietransfer. o technologischer. transfer. o Unternehmensschutz o Unternehmenssicherheit o Know-how-Schutz. o Know-how-Verlust. o Know-how-Abfluss. o Know-how-Diebstahl. o Datendiebstahl. o .Nachrichtendienst. o Informationsgewinnung. o IT-Sicherheit. o Spionageattacke. o Informationssicherheit. o Informationsabfluss. o Informationsschutz.

[4] „.“ wurde als Platzhalter für Buchstaben und Wortteile genutzt – somit wurden mit dem Suchbegriff „.spionage.“ auch Artikel gefunden, die die Wörter Konkurrenzspionage, Spionagegefahr, Wirtschaftsspionage etc. enthielten.

[5] Die identifizierten Beiträge stammen u. a. aus folgenden Fachzeitschriften: IT-Sicherheit - Management und Praxis, KES – Die Zeitschrift für Informations-Sicherheit, WIK – Zeitschrift für die Sicherheit der Wirtschaft, W&S - Das Sicherheitsmagazin, DNP - Die Neue Polizei, Die Polizei, Kriminalistik.

renzausspähung, so werden diese Begriffe im Regelfall auch in dieser Quelle verwendet, sodass die Anzahl der Suchworte für die weitere Suche reduziert werden konnte.[6] Mit Hilfe der Auswahlkriterien „zeitliche Begrenzung", „thematische Relevanz" und „wissenschaftlicher Charakter" wurden auch die Ergebnisse aus den anderen Katalogen/Datenbanken/Suchmaschinen[7] bewertet: bei thematischem Bezug (Wirtschaftsspionage und/oder Konkurrenzausspähung ist zentrales Thema der Quelle) und wissenschaftlichem Charakter wurden Quellen ab 2007 berücksichtigt. Auf diese Weise konnten ca. 70 weitere relevante Quellen identifiziert werden.

Über die so recherchierten Quellen sollten Hinweise auf empirische Studien mit Unternehmensbefragungen gesammelt werden. Ferner wurde auf den Websites mehrerer einschlägiger Institutionen[8] nach empirischen Studien recherchiert. Es konnten insgesamt ca. 70 potenziell relevante empirische Studien gefunden werden. Auch hier wurden die zu untersuchenden Studien anhand mehrerer im Voraus festgelegter Kriterien bestimmt: im Rahmen der Studie waren deutsche Unternehmen per Fragebogen befragt worden, es wurden maximal die drei aktuellsten Studien einer Institution ausgewählt, es waren Unternehmen befragt worden (nicht Sicherheitsdienstleister oder Politiker), Studien ab 2007 (bei besonders relevanten Studien auch älter), die Unternehmen mussten sich in mindestens einer Frage zum Thema Wirtschaftsspionage und/oder Konkurrenzausspähung äußern[9]. Insgesamt wurden auf diese Weise 27 auswertungsrelevante empirische Studien identifiziert[10], die sich hinsichtlich Umfang, Qualität, methodischer Transparenz, Zielgruppe, Vorgehen bei der Auswahl der Unternehmen für die Stichprobe (Stichprobenkonstruktion), thematischen und geografi-

[6] Es wurde nur noch mit folgenden Stichworten gesucht: Wirtschafts-/Konkurrenz-/Betriebs-/Industriespionage und Konkurrenzausspähung.

[7] U. a. Online-Bibliothekskatalog Bundeskriminalamt, Bibliothekskatalog Kriminologische Zentralstelle, Katalog Institut für Kriminologie Universität Tübingen, link.springer.com, books.google.de, Katalog Leibniz-Institut für Sozialwissenschaften, HeBIS-Portal, Katalog Freie Universität Berlin, oclc.org/oaister.

[8] U. a. Europäische Kommission, European Cyber Crime Centre, EU Agency for Network and Information Security, Bundesamt für Verfassungsschutz, Landesämter für Verfassungsschutz, Bundesamt für Sicherheit in der Informationstechnik, Statistisches Bundesamt, ASW e. V., Bundeszentrale für politische Bildung, Bundesverband mittelständische Wirtschaft, Bundesverband der Deutschen Industrie, Bundesverband der Sicherheitswirtschaft, Deutscher Mittelstandsbund, DIHK, Zentralverband des Deutschen Handwerks, PwC, KPMG, Ernst & Young, Kötter Services, Ebner Stolz, Rödl & Partner, BDO Deutschland, ectacom, BITKOM, McAfee.

[9] Hierbei gab es drei Möglichkeiten der thematischen Ausrichtung: a) Hauptthema der Befragung ist Wirtschaftsspionage/Konkurrenzausspähung (WS/KA), b) Wirtschaftsspionage/Konkurrenzausspähung wird im Rahmen eines anderen Hauptthemas (z. B. Cybercrime oder Know-how-Verlust) thematisiert, c) eine Ausforschungsmethode (z. B. Datenklau oder Verrat von Betriebsgeheimnissen) wird im Rahmen eines anderen Hauptthemas angesprochen.

[10] Durchgeführt/beauftragt von Unternehmensberatungen und Sicherheitsdienstleistern, Sicherheitsbehörden, Bundesministerien, Hochschulen, Wirtschaftsinteressensverbänden, der IHK u. a.

schen Schwerpunkten etc. unterscheiden. Auch die Erhebungsinstrumente (Fragebögen) variieren bezüglich ihrer Qualität, des Umfangs, der Gestaltung etc. Diese Unterschiede erschweren den Vergleich der Ergebnisse der einzelnen Befragungen, ihre Existenz muss vor allem beim Sichten der Ergebnisse der Studien berücksichtigt werden. Widersprüchliche Ergebnisse mögen durchaus dem unterschiedlichen Forschungsdesign einzelner Studien geschuldet sein und weniger dem Einfluss anderer unabhängiger Variablen. Der in dieser Arbeit vorgenommene Vergleich der Ergebnisse der Studien sowie die berechneten „Durchschnittswerte", die sich auf mehrere Studien beziehen, sollen daher nicht als statistische Ergebnisse verstanden werden, sondern als Tendenzen und Anhaltspunkte. Ferner sollte auch bedacht werden, dass private Unternehmen oder Netzwerke (wie Unternehmensberatungen oder Hersteller von Computersicherheitssoftwares) mit ihren Befragungen spezifische Eigeninteressen verfolgen können und dementsprechend möglicherweise andere Schwerpunkte setzen und Empfehlungen aussprechen als öffentliche Einrichtungen.

Alle hier untersuchten Studien sind Teilerhebungen umfassender Forschungsvorhaben mit unterschiedlicher Vorgehensweise bei der Konstruktion der jeweiligen Stichprobe. In manchen Studien wurden die Teilnehmer über eine Zufallsauswahl bestimmt, in anderen über eine bewusste Auswahl nach Quoten (systematische Stichprobenziehung), während es in weiteren Befragungen keine Teilnahmebegrenzung gab und alle interessierten Unternehmen teilnehmen konnten. In vielen Studien wird angegeben, dass repräsentative Befragungen durchgeführt worden sind. Dies kann bei einigen Befragungen jedoch angezweifelt und bei den meisten Studien aufgrund einer nicht vorhandenen vollständigen methodischen Transparenz nicht überprüft werden, weswegen die Aussagekraft der meisten Studien für alle deutsche Unternehmen eingeschränkt ist und Hochrechnungen nicht möglich sind.[11]

3.2 Erhebung und Auswertung

Zur systematischen Erhebung der für die Sekundäranalyse zentralen Punkte wurde ein Auswerteraster/Codesystem bestehend aus mehreren Über- und Unterkategorien entwickelt. Im Rahmen eines Pretests wurden fünf Studien mit dem Auswerteraster bearbeitet. Im Anschluss an den Pretest wurde das Auswerteraster angepasst und optimiert. Das endgültige

[11] Ein Überblick über die Studien befindet sich in Tabelle 10, S. 90.

Auswerteraster besteht aus rund 90 Über- und Unterkategorien (Codes und Subcodes), die mit Codierregeln und Codierbeispielen versehen wurden, um eine möglichst eindeutige Codierung zu gewährleisten.

Nach dem Pretest wurden das angepasste Auswerteraster sowie alle empirischen Studien und mehrere weitere Quellen (u. a. Beiträge aus Fachzeitschriften) in MAXQDA, einer Software zur computergestützten qualitativen Daten- und Textanalyse, eingespeist, wo ihre systematische Bearbeitung möglich war.

Nach Abschluss der Codierungsphase wurden die Daten für die weitere Auswertung in eine Excel-Tabelle exportiert. In der tabellarischen Darstellung lassen sich Muster, Gemeinsamkeiten, Unterschiede und Veränderungen zwischen den einzelnen Studien leichter erkennen. Ähnliche Codierungen aus verschiedenen Studien oder Fachbeiträgen können so miteinander in Verbindung gebracht und interpretiert werden.

4. Theoretischer Hintergrund

4.1 Dunkelfeld und Dunkelfeldforschung

Ein zentrales Ergebnis der kriminologischen Dunkelfeldforschung ist die Feststellung, dass das Dunkelfeld bei allen bislang untersuchten Delikten größer ist als das Hellfeld[12] (vgl. Schwind 2013: 54). Dies trifft auch auf die Phänomene Wirtschaftsspionage und Konkurrenzausspähung zu. Eine weitere Erkenntnis ist, dass die Größe des Dunkelfeldes von Delikt zu Delikt variiert (vgl. Schwind 2013: 54). Bei den Phänomenen Wirtschaftsspionage und Konkurrenzausspähung wird das Dunkelfeld in der Fachliteratur und in mehreren Studien als besonders groß geschätzt und sogar als „doppeltes Dunkelfeld“ bezeichnet. Ein doppeltes Dunkelfeld besteht aus Straftaten, die weder der Polizei bekannt bzw. angezeigt werden, noch durch die Dunkelfeldforschung vollständig erfasst werden können (vgl. Schwind 2013: 47). Dies liegt u. a. daran, dass ein Angriff zum Zwecke der Ausforschung auch von den betroffenen Unternehmen nicht immer bemerkt wird oder dass die Unternehmen auch in entsprechenden Befragungen aufgrund der Angst, dass der Vorfall an die Öffentlichkeit gelangt,

[12] Das Hellfeld wird hierbei definiert als die Gesamtheit aller amtlich registrierten Straftaten.

nicht jeden Ausforschungsvorfall ansprechen. Angriffe, die der Polizei nicht gemeldet werden, können folglich auch nicht in der Polizeilichen Kriminalstatistik (PKS) registriert werden (vgl. Meissinger 2005: 25).

Ferner können Tatbestände wie Wirtschaftsspionage, Konkurrenzausspähung, Datendiebstahl, Verrat von Geschäftsgeheimnissen etc. im Vergleich zu Tatbeständen wie Einbruch oder Körperverletzung so kompliziert sein, dass die Opfer nur schwer einschätzen können, ob und in welchem Umfang sie überhaupt geschädigt wurden.

Das gebräuchlichste Verfahren, um das Dunkelfeld in den Phänomenen Wirtschaftsspionage und Konkurrenzausspähung aufzuhellen und um opferbezogene Erkenntnisse zu gewinnen, sind Opferbefragungen (Schwind 2013: 47). Dabei werden (repräsentative) Stichproben (z. B. alle deutschen kleinen und mittleren Unternehmen (KMU) oder alle Global Player mit Hauptsitz in Baden-Württemberg) anonym darüber befragt, ob sie während eines gewissen Zeitraums Opfer von bestimmten (angezeigten und nicht angezeigten) Delikten, die im Zusammenhang mit WS/KA stehen könnten, geworden sind. In einigen der hier untersuchten Studien ist zudem das Anzeigeverhalten der Unternehmen und die zugrundeliegenden Motivationen analysiert worden und es konnten Informationen über den Zusammenhang zwischen Hellfeld, Dunkelfeld und Anzeigeverhalten gewonnen werden. Wurden die Teilnehmer einer Opferbefragung über eine repräsentative Zufallsstichprobe identifiziert, können die Ergebnisse aus der Stichprobe auf die Grundgesamtheit hochgerechnet werden.

Folglich liegt der Fokus des vorliegenden Berichts auf Unternehmensbefragungen. Direkte Aussagen von (betroffenen) Unternehmen bieten, bei korrekter methodischer Durchführung der Befragung, verlässlichere Erkenntnisse als auf Erfahrungen basierende Schätzungen oder theoretische Annahmen von Experten.

4.2 Methoden der Informationsbeschaffung

In der Fachliteratur werden im Zusammenhang mit Wirtschaftsspionage und Konkurrenzausspähung mehrere Methoden der Informationsbeschaffung genannt (vgl. Warnecke 2010: 259).

Human Source Intelligence (HUMINT) bezeichnet das Vorgehen, bei dem Informationen durch den Einsatz oder die Abschöpfung menschlicher Quellen erlangt werden. Wettbewerber oder Nachrichtendienste, die interessiert am Know-how eines bestimmten Unternehmens sind, könnten z. B. einen Spion in dieses Unternehmen einschleusen oder eine Quelle im Unternehmen anwerben (vgl. Sicherheitsforum 2010: 27). Die Informationsbeschaffung über menschliche Akteure gelingt oft bereits durch eine einfache legale Gesprächsabschöpfung, bei der betriebsinterne Informationen unbedachten Mitarbeitern entlockt werden (vgl. Warnecke 2010: 259). Eine weitere personengebundene Methode, um an Unternehmensinterna zu gelangen, ist das Social Engineering, eine Art soziale Manipulation. Hier erfinden Ausforscher falsche Tatsachen und nutzen Eigenschaften wie Hilfsbereitschaft, Angst, Respekt oder Vertrauen der Mitarbeiter des auszuspähenden Unternehmens aus, um unberechtigt an unternehmensinterne Informationen zu gelangen. Oftmals werden diese Informationen für die weitere Ausforschung benötigt (vgl. Sicherheitsforum 2010: 29).

Werden Informationen mit Hilfe technischer Mittel oder Methoden erlangt, spricht man von Technical Intelligence (TECHINT) (vgl. Sicherheitsforum 2010: 29). Dazu zählt z. B. das Hacken von IKT, das Abhören von Telefongesprächen oder das Belauschen von vertraulichen Besprechungen mit Hilfe von Wanzen (vgl. Warnecke 2010: 261). Auch drahtlose Verbindungen wie Bluetooth- und WLAN-Technologie können zum Zweck der illegalen Informationsbeschaffung missbraucht werden.

Informationen können aber auch durch das Eindringen in bzw. die Nutzung von Computersystemen gesammelt werden. Diese Methoden werden als Computer Intelligence (COMPINT) oder Data Intelligence (DATAINT) bezeichnet. Darunter fällt vor allem die Einführung von Schadsoftware, wie z. B. Viren, Würmer oder Trojaner in die Technik eines Unternehmens, um Unbefugten Zugriff auf Datenmaterial, Dokumente, Netzwerkinformationen etc. zu ermöglichen. Schadsoftware kann relativ leicht über das Internet z. B. über manipulierte E-Mail-Anhänge oder verseuchte Websites in das Unternehmensnetzwerk eingeschleust werden. Wie geschickt und unbemerkt man hier vorgehen kann, zeigen uns die Enthüllungen von Edward Snowden. Aber auch von USB-Sticks, CDs und anderen Datenspeichern können Schadprogramme in das Unternehmensnetzwerk gelangen (vgl. Sicherheitsforum 2010: 31).

Häufig beschränken sich Ausforscher aber nicht nur auf eine einzige der beschriebenen Methoden, sondern kombinieren mehrere miteinander.

4.3 Lagedarstellung

Zahlen zur Betroffenheit der Unternehmen von Wirtschaftsspionage oder Konkurrenzausspähung finden sich weder in der PKS noch in den Verfassungsschutzberichten. In der PKS werden aber Deliktsformen aufgeführt, die zumindest teilweise, jedoch nicht ausschließlich, für Wirtschaftsspionage und/oder Konkurrenzausspähung stehen können, wie zum Beispiel der Verrat von Geschäfts- und Betriebsgeheimnissen nach § 17 UWG oder das Ausspähen und Abfangen von Daten nach §§ 202a-c StGB. Die in der PKS aufgeführten Fälle des Verrats von Geschäfts- und Betriebsgeheimnissen sind zwischen 2008 und 2012 um ca. 30 Prozent (28,7 Prozent) von 408 auf 525 Fälle gestiegen. Insgesamt wurden den Strafverfolgungsbehörden zwischen 2008 und 2012 2.627 Fälle bekannt (vgl. Tabelle 1).

Tabelle 1: PKS-Fallentwicklung Verrat von Betriebs- und Geschäftsgeheimnissen

Verrat von Betriebs- und Geschäftsgeheimnissen nach § 17 1-4 UWG (Straftatenschlüssel 715300 und 715400)	Erfasste Fälle
2012	525
2011	500
2010	646
2009	548
2008	408
2008 – 2012	**2.627**

Quelle: Eigene Darstellung. Vgl. PKS Jahresberichte 2008 – 2012.

Ein deutlicher Anstieg kann auch bei den Fällen von Ausspähen und Abfangen von Daten einschl. Vorbereitungshandlungen beobachtet werden: zwischen 2008 und 2012 kann ein Anstieg um 117 Prozent auf 16.794 Fälle festgestellt werden. Insgesamt wurden den Strafverfolgungsbehörden in diesem Zeitraum 66.928 Fälle bekannt (vgl. Tabelle 2).

Tabelle 2: PKS-Fallentwicklung Ausspähen, Abfangen von Daten

Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen (Straftatenschlüssel 678000)	Erfasste Fälle
2012	16.794
2011	15.726
2010	15.190
2009	11.491
2008	7.727
2008 – 2012	**66.928**

Quelle: Eigene Darstellung. Vgl. PKS Jahresberichte 2008 – 2012.

Die Zahlen aus der PKS sind lediglich ein Indikator für die Entwicklung von Delikten, die auch auf die Begehung von Wirtschaftsspionage und/oder Konkurrenzausspähung abzielen können, sie spiegeln allerdings nicht die tatsächliche Fallzahlenentwicklung in den beiden Phänomenbereichen wider.

Aus den den Sicherheitsbehörden vorliegenden Fallzahlen zu neu eingeleiteten Ermittlungsverfahren in den Bereichen Spionage/Proliferation oder wegen des Verdachts geheimdienstlicher Agententätigkeit bzw. wegen Landesverrats für die Jahre 2008 bis 2012 können keine eindeutigen Informationen zu Wirtschaftsspionageverfahren abgeleitet werden, da eine deliktische Aufschlüsselung nach Jahren oder nach der Anzahl der Verfahren nicht möglich ist.

5. Ergebnisse der Auswertung

In den folgenden Unterkapiteln werden die zentralen Ergebnisse der Sekundäranalyse vorgestellt. In einem ersten Schritt (Kapitel 5.1) wird auf die Bedrohungswahrnehmung deutscher Unternehmen eingegangen. Halten sie es für wahrscheinlich, selbst Opfer von Ausforschung zu werden? Wie wird die allgemeine Gefahr für die deutsche Wirtschaft eingeschätzt? Stellen Wirtschaftsspionage und Konkurrenzausspähung aus Sicht der Unternehmen ein ernstzunehmendes Risiko dar? Im Anschluss an dieses Unterkapitel, in dem allgemein die subjektive Einschätzung der Unternehmen präsentiert wird, folgt Kapitel 5.2 mit konkreten Angaben der Unternehmen zur Betroffenheit von Ausforschung (tatsächlich berichtete Kriminalitätsbelastung). In den Kapiteln 5.3 und 5.4 werden die zentralen Ergebnisse der Unternehmensbefragungen bezüglich der Schäden durch Ausforschung sowie der festgestellten Täter vorgestellt. Es folgt Kapitel 5.5, in dem die von den Unternehmen getroffenen Sicherheitsvorkehrungen erläutert werden. In den Kapiteln 5.6 und 5.7 wird gezeigt, ob und wie die Unternehmen mit den Sicherheitsbehörden kooperieren und welche Institutionen aus Sicht der Unternehmen zu den wichtigsten Akteuren im Bereich der Abwehr von Ausforschung gehören.

5.1 Bedrohungswahrnehmung deutscher Unternehmen

Die Bedrohung, die für deutsche Unternehmen von Angriffen zum Zweck der Ausforschung ausgeht, ist real und es kann davon ausgegangen werden, dass nicht nur weltweit tätige Unternehmen, sogenannte Global Player, sondern auch und vielleicht vor allem mittlere und kleine Unternehmen besonders bedroht sind. Zu dieser Einschätzung kommen Experten aus den Sicherheitsbehörden und der privaten Sicherheitsbranche. Das Risiko, dass ein Unternehmen infiltriert, abgehört oder auf elektronischem Wege ausgespäht wird, um an unternehmenskritisches Know-how zu gelangen, ist vor allem für deutsche Unternehmen, die als besonders innovativ und produktiv gelten, als hoch einzustufen (vgl. George 2013: 23). Die Bedrohungslage nimmt nicht zuletzt aufgrund der steigenden und globalen Vernetzung der IKT weiter zu (vgl. BMWi 2012: 30). Die Gefährdung der Unternehmen ist in Teilen auch auf die hohe Leistungskraft ausländischer Nachrichtendienste zurückzuführen (vgl. Bätz/Claaßen 2009: 38 f.).

Die häufig geäußerte Kritik, dass Unternehmen die Gefahren von Ausforschung unterschätzen (vgl. George 2013: 23), muss auf der Grundlage der Ergebnisse der Befragungen differenzierter betrachtet werden. In der Mehrheit der Befragungen schätzte mehr als die Hälfte der Unternehmen das Risiko für die *Gesamt*wirtschaft sehr hoch ein – es waren aber oft deutlich weniger Unternehmen, die das *individuelle* Risiko gleich hoch bewerteten wie das für die Gesamtwirtschaft. Das Bewusstsein für die Gefahren von WS/KA ist durchaus vorhanden, es wirkt sich aber nicht immer auf die Schutzvorkehrungen der Unternehmen aus.

Es ist unerlässlich, dass sich ein Unternehmen ein Bild von den wichtigsten Gefahren (Korruption, Sabotage, Diebstahl, Ausforschung etc.) macht, denen es ausgesetzt ist und die den geregelten Ablauf im Unternehmen beeinträchtigen können. Diese Gefahren und ihre Auswirkungen sollten von dem Unternehmen identifiziert, analysiert und bewertet werden. Nur so können effektive Schutzvorkehrungen implementiert und begründet werden.

5.1.1 Aktuelle Bedrohung

Die Sensibilität der deutschen Unternehmen für die Gefahren von Ausforschung ist hoch. So schätzten im Durchschnitt der Befragungen[13] ca. 60 Prozent der Unternehmen (vgl. Tabelle 3) die Bedrohung durch Ausforschung[14] für ihr eigenes Unternehmen als bedeutsam ein.

Die Ergebnisse mehrerer Studien verweisen zudem auf einen Anstieg der Bedrohungswahrnehmung im Laufe der letzten Jahre. Während in der 10. WIK-Sicherheits-Enquête rund 52 Prozent der Unternehmen das Risiko, das von WS/KA für das eigene Unternehmen ausgeht als relevant betrachteten (vgl. WIK 2011/2: 13), waren es in der Folgestudie bereits 60 Prozent (vgl. WIK 2013/2: 11). Auch in den von Ernst & Young (E&Y) in 2011 und 2013 durchgeführten Befragungen kann ein leichter Anstieg der Einschätzung des Gefahrenniveaus beobachtet werden. 2011 schätzten 61 Prozent und 2013 63 Prozent der Unternehmen die Bedrohung, die von WS/KA und Datenklau ausgeht, als mäßig bis sehr groß für das eigene Unternehmen ein (vgl. E&Y 2011: 5 und E&Y 2013: 4).

[13] In insgesamt 20 von 27 Befragungen machten die Unternehmen Angaben zur Bedrohungswahrnehmung.

[14] In manchen Studien wurde direkt nach der Bewertung der Bedrohung durch Wirtschaftsspionage/Konkurrenzausspähung gefragt, während in anderen Studien (z. B. Studien mit dem Hauptthema Wirtschaftskriminalität, Cybercrime) lediglich nach der Bedrohungswahrnehmung einzelner Tathergänge, Angriffsformen oder Delikten gefragt wurde (wie z. B. Datendiebstahl, Verrat von Geschäfts- und Betriebsgeheimnissen), die aber mit WS/KA in Verbindung stehen.

Tabelle 3: Wahrnehmung der aktuellen Bedrohung durch Ausforschung

Einschätzung der Bedrohung durch Ausforschung für das eigene Unternehmen	Anteil der Unternehmen	Konkret genanntes Risiko	Quelle
besonders bedrohlich	51 %	Diebstahl von geschäfts-kritischem Know-how	KPMG 2010a: 10
relevant	51,6 %	WS/KA	WIK 2011/1: 13
relevant	60,2 %	WS/KA	WIK 2013/2: 11
mäßig bis sehr groß	61 %	WS/KA	E&Y 2011: 5
mäßig bis sehr groß	63 %	WS/KA	E&Y 2013: 4
hoch bis sehr hoch	61 %	Datendiebstahl/ Datenmissbrauch	KPMG 2013b: 38
hoch bis sehr hoch	81 %	Verrat von Geschäfts- und Betriebsgeheimnissen	KPMG 2013b: 38
Arithmetisches Mittel	**61 %**		
Median[15]	**61 %**		

Quelle: Eigene Darstellung.

Bei der Bedrohungswahrnehmung bestimmter Angriffsformen ergibt sich ein ähnliches Bild: In der e-Crime-Studie 2010 von KPMG wurde der Diebstahl von geschäftskritischem Know-how von 51 Prozent der befragten Unternehmen als besonders bedrohliches e-Crime-Risiko mit hohem Schadenspotenzial für das eigene Unternehmen eingestuft, wobei wesentliche Unterschiede zwischen den verschiedenen Branchen festgestellt werden können. Überdurchschnittlich häufig bewerteten Unternehmen aus der Maschinenbaubranche (78 Prozent), aus der Automobilindustrie (75 Prozent) und aus der Elektronik- und Software-Branche (73 Prozent) den Diebstahl von geschäftskritischem Know-how als besonders bedrohliches Risiko (vgl. KPMG 2010: 10). Im Secure Mobile Computing Report 2013 ging die große Mehrheit der befragten Unternehmen davon aus, dass Unternehmen aus der Automobilbranche, der zivilen Luft- und Raumfahrt, der Rüstungsindustrie und der Chemie- und Pharmabranche einer höheren Bedrohung durch Ausforschung ausgesetzt sind als Unternehmen aus anderen Branchen (vgl. Secusmart 2013: 2 f.).

[15] Die in diesem und den folgenden Kapiteln vorgenommenen Berechnungen der Mittel- und Zentralwerte für die im Rahmen der vorliegenden Arbeit zusammengetragenen empirischen Werte können durchaus als problematisch angesehen werden, da sich die verschiedenen Werte u. a. auf teilweise unterschiedliche Zeiträume und Methoden der Ausforschung beziehen. Die Mittel- und Zentralwerte können deshalb nicht als statistisch belastbare Zahlen verstanden werden, sondern vielmehr als Tendenzen oder Anhaltspunkte, die lediglich ein besseres Verständnis und einen leichteren Überblick ermöglichen sollen.

In der Wirtschaftskriminalität-Studie 2013 von KPMG sollten die Unternehmen die Risiken bewerten, die von 9 wirtschaftskriminellen Handlungen ausgehen. Durchschnittlich stuften 56 Prozent der mittelständischen Unternehmen das Risiko, Opfer einer dieser Handlungen zu werden, als hoch bis sehr hoch ein. Das größte Risiko sahen die Unternehmen bei dem Delikt Datendiebstahl/Datenmissbrauch – hier schätzten 81 Prozent der mittelständischen Unternehmen das Risiko, Opfer zu werden, als hoch bis sehr hoch ein. Aber auch die Verletzung von Geschäfts- und Betriebsgeheimnissen wurde von der Mehrheit der mittelständischen Unternehmen (61 Prozent) als große bis sehr große Bedrohung empfunden. Im Vergleich zu diesen zwei Delikten, die zur Ausforschung eines Unternehmens geeignet sind, werden bis auf die Verletzung von Schutz- und Urheberrechten (Risiko wurde von 80 Prozent der Unternehmen als hoch bis sehr hoch eingestuft) alle anderen wirtschaftskriminellen Handlungen wie z. B. Korruption (59 Prozent der Unternehmen), Diebstahl/Unterschlagung (53 Prozent), Betrug/Untreue (50 Prozent) und Geldwäsche (36 Prozent) als weniger bedrohlich eingeschätzt (vgl. KPMG 2013b: 38).

Die Bedrohung durch Ausforschung wurde ferner auch im direkten Vergleich mit anderen unternehmerischen Sicherheitsrisiken als relativ hoch eingeschätzt.

In der 10. und 11. WIK-Sicherheits-Enquête wurde die Gefährdung durch WS/KA unter fünf unternehmerischen Sicherheitsrisiken[16] jeweils als zweitwichtigste Bedrohung gesehen, gleich nach Angriffen auf die IT und Telekommunikation und noch vor der allgemeinen Kriminalität (vgl. WIK 2011/1: 12 und WIK 2013/1: 8).

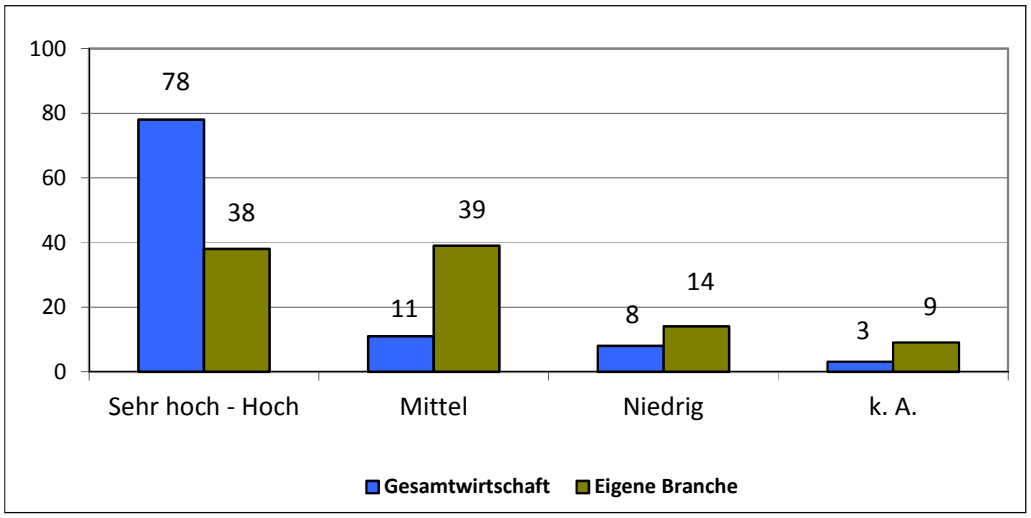
In der <kes>/Microsoft-Sicherheitsstudie 2012 befand sich Wirtschaftsspionage/unbefugte Kenntnisnahme/Informationsdiebstahl (also WS/KA) auf Rang 4 von insgesamt 12 verschiedenen Gefahrenbereichen für Unternehmen[17] und rückte in der Prognose für 2014 sogar auf Rang 3 (vgl. kes 2012/4: 5).

Welche Auswirkungen hat die NSA-Überwachungs- und Spionageaffäre auf die Bedrohungswahrnehmung der Unternehmen? In der Wirtschaftskriminalität-Studie von PricewaterhouseCoopers (PwC) ging die Mehrheit der Unternehmen von einer unveränderten Gefahrenlage aus. Nur ein Viertel war der Meinung, dass das Risiko, dass Geschäfts- und Betriebs-

[16] Angriffe auf die IT und Telekommunikation, Konkurrenzausspähung/Wirtschaftsspionage, Kriege und Militäreinsätze, Kriminalität, politischer Extremismus/Terrorismus.
[17] Rang 1: Irrtum/Nachlässigkeit eigener Mitarbeiter, Rang 2: Malware, Rang 3: Software-Mängel/-Defekte.

geheimnisse ausgespäht werden, aktuell höher ist als vor Bekanntwerden der Affäre (vgl. PwC 2013: 20). In einer Befragung des BDI (vgl. Abbildung 1) von 2013 schätzten jedoch 78 Prozent der Unternehmen die Wahrscheinlichkeit, dass die deutsche Industrie von der NSA ausspioniert wurde, als hoch bis sehr hoch ein. Lediglich 38 Prozent der Unternehmen sahen das gleiche Risiko für die eigene Branche (vgl. BDI 2013: 3). Auf diese Diskrepanz zwischen individueller und allgemeiner Risikowahrnehmung wird in Kapitel 5.1.3 eingegangen.

Abbildung 1: Einschätzung der Betroffenheit von NSA-Abhörmaßnahmen



Anteil der Unternehmen (in Prozent), die das Risiko, dass die deutsche Wirtschaft bzw. die eigene Branche von der NSA ausspioniert wurde, als niedrig, mittel oder hoch bis sehr hoch einschätzten. Quelle: Eigene Darstellung nach BDI 2013: 3.

Im Vergleich zu Unternehmen aus anderen europäischen Ländern[18] gaben deutsche Firmen am häufigsten an (19,5 Prozent), dass Ausforschung ein *wichtiges* Mittel ist, um in der jeweiligen Branche Informationen über Konkurrenten zu erhalten[19] (vgl. Europäische Kommission 2013a: 125). Im europäischen Durchschnitt stimmten dieser Aussage „lediglich" 8,9 Prozent der Unternehmen zu. Diese Zahlen zeigen, dass das Problembewusstsein deutscher Unternehmen im europäischen Vergleich überdurchschnittlich hoch ist, was die Vermutung zulässt, dass sie auch überdurchschnittlich oft von Ausforschung betroffen sein könnten. Im europäischen Durchschnitt stuften am häufigsten Unternehmen aus der Automobil- und aus

[18] Studie im Auftrag der Europäischen Kommission zu Geschäftsgeheimnissen und vertraulichen Geschäftsinformationen im Binnenmarkt. Teilnehmende Länder an der Umfrage: Österreich, Belgien, Tschechische Republik, Frankreich, Deutschland, Ungarn, Italien, Niederlande, Polen, Spanien, Schweden, Schweiz, Vereinigtes Königreich. Insgesamt 537 Unternehmen, davon 41 deutsche.

[19] Folgende andere Mittel werden ebenfalls häufig als „wichtig" bezeichnet um in der jeweiligen Branche an Informationen über Konkurrenten zu gelangen (europäischer Durchschnitt in Klammern): Kunden 39 (34,6) Prozent, von Regulierungsbehörden geforderte Offenlegungen 22 (12,1) Prozent, Arbeitnehmermobilität 17,1 (16,6) Prozent und Nachkonstruktion 17,1 (13,4) Prozent.

der Pharmabranche (39 bzw. 21 Prozent) Ausforschung als *wichtiges* Mittel zur Informationsbeschaffung ein (vgl. Europäische Kommission 2013b: 12 f.).

5.1.2 Künftige Bedrohung

Deutsche Unternehmen schätzten nicht nur die aktuelle Gefahr, die von Ausforschung ausgeht, als relevant ein. So gingen im Durchschnitt der Studien knapp 60 Prozent (vgl. Tabelle 4) der Unternehmen davon aus, dass das zukünftige Risiko, ausgeforscht zu werden, ansteigen wird.

Tabelle 4: Einschätzung der zukünftigen Bedrohung durch Ausforschung

Einschätzung des Anstiegs der Bedrohung für das eigene Unternehmen	Anteil der Unternehmen	Konkret genanntes Risiko	Quelle
leichter bis starker Anstieg	33,7 %	WS/KA	CT 2007: 39
leichter bis starker Anstieg	52,3 %	WS/KA	CT 2012: 49
Ausforschung als bedeutendstes zukünftiges unternehm. Risiko	53,1 %	WS/KA	CT 2010: 9
etwas bis stark zunehmendes Risiko	40 %	WS/KA	kes 2012/4: 8
Anstieg	70 %	WS/KA	WIK 2011/1: 3
Anstieg	64,4 %	WS/KA	WIK 2013/1: 3
(starker) Anstieg	65 %	WS/KA	E&Y 2011: 5
(starker) Anstieg	76 %	WS/KA	E&Y 2013: 5
Arithmetisches Mittel	**56,8 %**		
Median	**58,8 %**		

Quelle: Eigene Darstellung.

In der <kes>/Microsoft-Sicherheitsstudie 2012 sollten die Unternehmen eine Prognose darüber abgeben, wie sich die Bedeutung verschiedener Gefahrenbereiche entwickeln wird. Ca. 40 Prozent der befragten Unternehmen gaben an, dass die Bedeutung von Wirtschaftsspionage und unbefugter Kenntnisnahme (WS/KA) zunehmen wird. Nur bei den Gefahrenbereichen Malware und Hacking gingen sie häufiger von einer zunehmenden Bedeutung (ca. 50 Prozent und etwas mehr als 40 Prozent) aus (vgl. kes 2012/4: 8).

Auch das Gefahrenbarometer 2010, in dem die Sicherheitsrisiken für den deutschen Mittelstand bewertet werden, kam zu einem ähnlichen Ergebnis. Spiona-

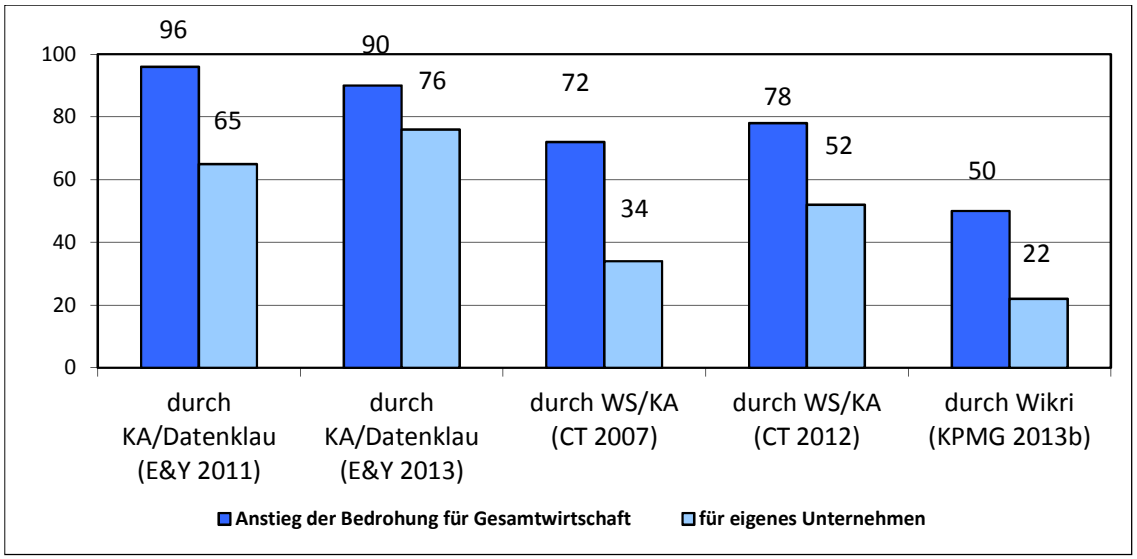
ge/Informationsabfluss (WS/KA) wurde von mehr als der Hälfte (53,1 Prozent) der Unternehmen als bedeutendstes unternehmerisches Risiko in den kommenden Jahren bewertet (vgl. CT 2010: 25).

Noch häufiger erwarteten die in der 10. und 11. WIK-Sicherheits-Enquête befragten Unternehmen einen Anstieg der künftigen Gefährdung durch WS/KA: 2011 gingen 70 Prozent und 2013 ca. 64 Prozent der Unternehmen von einer Zunahme der allgemeinen Gefährdung der deutschen Wirtschaft durch WS/KA aus (vgl. WIK 2011/2: 14 und WIK 2013/2: 12). Auch wenn der Wert zwischen 2011 und 2013 sinkt, waren es immer noch fast zwei Drittel aller Unternehmen, die eine Zunahme der Bedrohung erwarteten. Ferner bildet die Sicherheits-Enquête in dieser Hinsicht eine Ausnahme, denn in mehreren anderen Studien konnte gezeigt werden, dass der Anteil der Unternehmen, die von einer steigenden Bedrohung ausgingen, zunimmt.

5.1.3 Individuelles vs. gesamtwirtschaftliches Risiko

In mehreren Studien konnte eine Diskrepanz zwischen der individuellen und der gesamtwirtschaftlichen Bedrohungswahrnehmung der Unternehmen festgestellt werden: Die Mehrheit der Unternehmen ging von einer aktuell hohen oder einer steigenden Bedrohung für die Gesamtwirtschaft aus – aber deutlich weniger Unternehmen schätzten ihr eigenes Risiko bzw. das Risiko für die eigene Branche ähnlich hoch ein wie das der Gesamtwirtschaft. Viele Unternehmen gingen folglich davon aus, dass ihr individuelles Risiko geringer sei als das der Gesamtwirtschaft (vgl. CT 2012: 49). Sie nahmen also durchaus ein allgemeines Risiko wahr, wähnten sich selbst jedoch in Sicherheit (vgl. KPMG 2013a: 13).

Abbildung 2: Bedrohungswahrnehmung



Unternehmen (in Prozent), die von einem Bedrohungsanstieg durch Ausforschung oder Wirtschaftskriminalität für die Gesamtwirtschaft bzw. für sich selbst ausgingen. Darstellung der Befragungsergebnisse ausgewählter Studien. Quelle: Eigene Darstellung.

Dies zeigt sich u. a. in den Befragungen von E&Y von 2011 und 2013. 2011 gaben 96 Prozent der Unternehmen an, dass die Bedrohung durch Industriespionage und Datenklau (WS/KA) für die Gesamtwirtschaft ansteigen wird, während es „nur" 65 Prozent der Unternehmen auch für sich selbst so einschätzten (vgl. E&Y 2011: 4 f.). Auch in der Befragung von 2013 bewerteten die Unternehmen das allgemeine und das individuelle Risiko unterschiedlich hoch (vgl. Ernst & Young 2013: 5 f.). Im Vergleich zur Studie von 2011 befürchteten in der Folgestudie jedoch mehr Unternehmen einen Anstieg der individuellen Bedrohung, was dazu führte, dass die Diskrepanz zwischen individueller und gesamtwirtschaftlicher Bedrohungswahrnehmung abnahm.

Obwohl die Werte aus den Industriespionage[20]-Studien von Corporate Trust (CT) niedriger sind als die Werte der E&Y-Studien, weisen sie ein ähnliches Muster auf. 2007 gaben ca. 72 Prozent der befragten Unternehmen an, dass die Bedrohung durch WS/KA für die Gesamtwirtschaft steigen wird, nur rund 34 Prozent glaubten jedoch, dass die Bedrohung auch für das eigene Unternehmen steigt (vgl. CT 2007: 39). Auch hier rechneten in der Folgestudie deutlich mehr Unternehmen damit, dass die Bedrohung durch WS/KA für sie selbst in den kommenden Jahren zunehmen wird, an den hohen Wert der Bedrohung für die Gesamtwirtschaft reichte diese Einschätzung aber dennoch nicht heran (vgl. CT 2012: 49).

[20] Obwohl der Titel der Studien „Industriespionage" lautet, beziehen sich die Herausgeber der Studie auf die beiden Phänomene Wirtschaftsspionage und Konkurrenzausspähung.

Die individuelle Risikoeinschätzung fiel aber auch in anderen Deliktsbereichen geringer aus als die allgemeine Gefahreneinschätzung. In der KPMG-Studie zu Wirtschaftskriminalität schätzten 67 Prozent der befragten Unternehmen das generelle Risiko, von Wirtschaftskriminalität[21] betroffen zu sein, als hoch bis sehr hoch ein und 50 Prozent erwarteten, dass das Risiko in den kommenden zwei Jahren weiter steigen wird. Im Gegensatz dazu gingen nur 17 Prozent der Befragten von einem gegenwärtig hohen bis sehr hohen Gefahrenpotenzial für das *eigene* Unternehmen aus und nur 22 Prozent nahmen an, dass das Gefahrenpotenzial für das *eigene* Unternehmen in den kommenden zwei Jahren ansteigen wird (vgl. KPMG 2013b: 37).

Eine Erklärung für diese Diskrepanz in der Bedrohungswahrnehmung der Unternehmen, also für die Annahme, dass Ausforschung eher die anderen betrifft als das eigene Unternehmen, ist, dass sich viele Unternehmen nicht als Angriffsziel einschätzen (vgl. IHK Nord 2013: 15). Das Unternehmenswissen wird womöglich nicht als ausreichend relevant dafür empfunden, dass Nachrichtendienste oder Konkurrenten einen hohen Aufwand betreiben, um an es heranzukommen. Theoretische Ansätze zur Risikoeinschätzung[22] gehen davon aus, dass die Wahrnehmung eines Risikos u. a. davon abhängt, ob Menschen annehmen, dass ein Risiko durch eigenes Handeln kontrolliert und somit reduziert werden kann. Diese Annahme verleitet viele Menschen dazu, unrealistisch optimistisch zu sein, da sie glauben, dass sie aufgrund ihrer Handlungsfähigkeit einem geringeren Risiko ausgesetzt sind als der Durchschnitt (vgl. Wiedemann/Mertens 2005: 40). Das Risiko Dritter, deren Sicherheitsvorkehrungen einem nicht genauer bekannt sind, bewertet man somit subjektiv höher als das eigene, auf das man in einem gewissen Maße z. B. durch adäquate Schutzvorkehrungen Einfluss nehmen kann.

5.1.4 Zusammenfassung Bedrohungswahrnehmung

- Im Durchschnitt der Studien schätzten ca. **60 Prozent** der Befragten die **Bedrohung** durch Ausforschung für ihr eigenes Unternehmen als bedeutsam ein.
- Der Anteil der Unternehmen, die die Bedrohung durch Ausforschung für sich selbst als bedeutsam einstuften, **stieg** während der letzten Jahre **an**.

[21] Darunter fallen auch Wettbewerbsdelikte wie Diebstahl vertraulicher Kunden- und Unternehmensdaten und die Verletzung von Geschäfts- oder Betriebsgeheimnissen, die zur Ausspähung genutzt werden können.
[22] Vgl. u. a. Slovic 1999.

- Je nach **Branche** bewerteten die Unternehmen die Bedrohung durch Ausforschung unterschiedlich. Als besonders bedrohlich wurde das Risiko von Unternehmen aus der Maschinenbau- und der Automobilbranche eingestuft.
- Im **europäischen Vergleich** gingen deutsche Unternehmen überdurchschnittlich oft davon aus, dass Ausforschung genutzt wird, um Informationen über Konkurrenten zu erhalten.
- Im Durchschnitt der Befragungen gingen knapp **60 Prozent** der Unternehmen davon aus, dass das zukünftige Risiko, ausgeforscht zu werden, (stark) **ansteigen** wird.
- Unternehmen schätzten das **individuelle** Risiko, von Ausforschung betroffen zu sein geringer ein als das Risiko der **Gesamtwirtschaft**.

5.2 Betroffenheit deutscher Unternehmen

Es steht außer Frage, dass deutsche Unternehmen aufgrund ihrer Leistungs- und Innovationskraft und ihrer Bemühungen im Bereich Forschung und Entwicklung (F&E) anhaltend im Fokus der nationalen und internationalen Konkurrenz und von ausländischen Nachrichtendiensten stehen (vgl. Karden 2011: 18). In 23 von 27 Befragungen konnten die teilnehmenden Unternehmen angeben, ob und wie oft sie während eines bestimmten vorangegangenen Zeitraums (ein bis zehn Jahre) mit Angriffen zu Ausforschungszwecken konfrontiert waren. In den Studien wurde den Unternehmen Anonymität gewährt. Dies erhöht die Wahrscheinlichkeit, dass die befragten Unternehmen ohne größere Vorbehalte u. a. Angaben zur Betroffenheit machen. Aufgrund der Anonymität der Befragungen kann auch davon ausgegangen werden, dass die Unternehmen mehr Vorfälle angaben, als sie bei der Polizei angezeigt hatten.

In diesem Unterkapitel werden die Aussagen der Unternehmen zur tatsächlichen Betroffenheit zusammengefasst dargestellt, um auf folgende Fragen zu antworten: Wie häufig waren deutsche Unternehmen konkret von Angriffen zu Ausforschungszwecken (Vorfälle und konkrete Verdachtsfälle) betroffen? Hatte die Unternehmensbranche oder die Größe eines Unternehmens einen Einfluss darauf? Wie veränderte sich die Betroffenheit über die letzten Jahre? Wie wurden die Unternehmen auf die Angriffe aufmerksam?

5.2.1 Betroffenheit von unterschiedlichen Arten der Ausforschung

Zuerst muss angemerkt werden, dass in den Studien sehr unterschiedlich hohe Betroffenheitswerte festgestellt werden konnten: so lag der Anteil der Unternehmen, die in mindestens einem Fall eine Ausforschung feststellen konnten, zwischen 7 und 85 Prozent.

Diese breite Streuung kann u. a. auf Unterschiede in den Forschungsdesigns der verschiedenen Befragungen zurückgeführt werden. So bezogen sich die Studien zum Teil auf unterschiedliche Grundgesamtheiten, wie z. B. baden-württembergische Unternehmen, norddeutsche Unternehmen, kleine und mittlere Unternehmen (KMU), mittelständische Unternehmen etc. Ferner können Unterschiede bzgl. der Auswahlmethode, also der Stichprobenbestimmung, festgestellt werden und somit auch hinsichtlich der Repräsentativität. Auch lassen sich zwischen den Studien Unterschiede bzgl. des inhaltlichen Schwerpunkts feststellen[23], die dazu führen können, dass unter den Teilnehmern besonders viele Unternehmen sind, die bereits eine gewisse Sensibilität für Ausforschung aufweisen.

Da die Werte in dieser Form für eine Bewertung zu ungenau sind, müssen die verschiedenen Angriffe auf die Unternehmen differenzierter betrachtet werden. Hierfür wurden die Vorfälle unter drei Oberbegriffen zusammengefasst, die sich an dem Wortlaut der Befragungen orientieren: erstens Verrat von Geschäfts- und Betriebsgeheimnissen, zweitens Datendiebstahl (darunter auch Know-how-Verlust, Ausspähen/Abfangen von Daten, Abhören von Daten) und drittens WS/KA (in diesem Fall wird ausdrücklich nach der Betroffenheit von Wirtschaftsspionage und/oder Konkurrenzausspähung gefragt). Im Anschluss an diese Aufteilung werden Mittel- und Zentralwert (Median) gebildet, damit ein besseres Verständnis und ein leichterer Überblick möglich sind.

Im Durchschnitt der aktuellsten Studien[24] verzeichnete zwischen 2010 und 2013 laut eigener Angabe ca. jedes vierte Unternehmen mindestens einen Fall von Verrat von Geschäfts- und Betriebsgeheimnissen[25], ebenfalls ca. jedes vierte Unternehmen mindestens einen Fall von

[23] Ist es eine Studie konkret zum Thema WS/KA oder wird die Betroffenheit von Ausforschung nur im Rahmen von Wirtschaftskriminalität oder e-Crime abgefragt?

[24] Nur Befragungen zwischen 2010 und 2013, wobei jeweils nur die letzte Befragung einer Institution berücksichtigt wurde (n = 11).

[25] In drei Befragungen (Median: 21 Prozent, Arithmetisches Mittel: 28,3 Prozent). Vgl. Tabelle 5.

Datendiebstahl[26] und ca. jedes sechste Unternehmen meldete mindestens einen Fall von WS/KA[27].

Aufgrund der immer noch teils großen Streuung der Einzelwerte in diesen Gruppen sowie der unterschiedlichen Zeiträume, auf die sich die Befragungen beziehen, können diese Zahlen aber nur als Tendenz und Anhaltspunkt betrachtet werden. Beispielhaft sollen ausgewählte Ergebnisse aus den verschiedenen Studien dargestellt werden.

Verrat von Geschäfts- und Betriebsgeheimnissen

Tabelle 5: Betroffenheit von Verrat von Geschäfts- und Betriebsgeheimnissen

Konkret genannter Vorfall	Anteil der Unternehmen	Zeitraum	Quelle
Verrat von Geschäfts- und Betriebsgeheimnissen	16 %	in verg. 2 Jahren	KPMG 2013a: 15
Verrat von Geschäfts- und Betriebsgeheimnissen	21 %	in verg. 2 Jahren	KPMG 2013b: 33
Verrat von Geschäfts- und Betriebsgeheimnissen	48 %	in verg. 4 Jahren	Sicherheitsforum 2010: 47
Arithmetisches Mittel	**28,3 %**		
Median	**21 %**		

Quelle: Eigene Darstellung.

Von Verrat von Geschäfts- und Betriebsgeheimnissen waren in der SiFo-Studie des Sicherheitsforums Baden-Württemberg 18 Prozent der Unternehmen in den vergangenen vier Jahren mindestens einmal sicher betroffen gewesen und weitere 30 Prozent verzeichneten in dieser Zeit einen oder mehrere konkrete Verdachtsfälle (vgl. Sicherheitsforum 2010: 45 f.). Somit musste sich knapp jedes zweite Unternehmen in Baden-Württemberg zwischen 2006 und 2010 näher mit einem potentiell schädlichen Know-how-Abfluss befassen.

In der e-Crime-Studie von KPMG verzeichneten 16 Prozent der von e-Crime betroffenen Unternehmen zwischen 2011 und 2013 mindestens einen sicheren Fall von Verrat von Geschäfts- und Betriebsgeheimnissen (vgl. KPMG 2013a: 15). Die Unternehmen konnten bei dieser Befragung keine Angaben zu konkreten Verdachtsfällen machen.

In der Wirtschaftskriminalität-Studie von KPMG waren zwischen 2010 und 2012 21 Prozent der von Wirtschaftskriminalität betroffenen Unternehmen in mindestens einem

[26] In acht Befragungen (Median: 23,5 Prozent, Arithmetisches Mittel: 30,61 Prozent). Vgl. Tabelle 6.
[27] In vier Befragungen (Unter den aktuellen Befragungen sind dies: Ernst & Young 2013, PwC 2013b, BMWi 2012, Corporate Trust 2012) (Median: 9,5 Prozent, Arithmetisches Mittel: 18,65 Prozent). Vgl. Tabelle 7.

Fall Opfer von Verrat von Geschäfts- und Betriebsgeheimnissen (vgl. KPMG 2013b: 33). Auch in dieser Befragung wurden konkrete Verdachtsfälle nicht erhoben.

Datendiebstahl

Tabelle 6: Betroffenheit von Datendiebstahl[28]

Konkret genannter Vorfall	Anteil der Unternehmen	Zeitraum	Quelle
Datendiebstahl	8 %	k. A.	BMWi 2012: 55
Datendiebstahl	15,8 %	im letzten Jahr	IHK Nord 2013: 9
Entwendung von Geschäftsgeheimnissen	17,1 %	in verg. 10 Jahren	Europäische Kommission 2013b: 19
Diebstahl vertraulicher Daten	20 %	in verg. 2 Jahren	PwC 2013: 18
Ausspähen, Abfangen von Daten	27 %	in verg. 2 Jahren	KPMG 2013a: 15
Datendiebstahl/ Datenmissbrauch	31 %	in verg. 2 Jahren	KPMG 2013b: 33
Vertraulichkeitsbruch/ Datendiebstahl	53 %	in verg. 2 Jahren	kes 2012/4: 10
Ausspähung und Abhörangriffe	73 %	in verg. 2 Jahren	WIK 2013/2: 12
Arithmetisches Mittel	**30,61 %**		
Median	**23,5 %**		

Quelle: Eigene Darstellung.

In der Studie des Sicherheitsforums Baden-Württemberg von 2004 gab ca. die Hälfte der Unternehmen[29] an, zwischen 1994 und 2004 mindestens einmal einen Fall von unfreundlichem Informationsabfluss festgestellt zu haben (vgl. Sicherheitsforum 2004: 51 und 63).

In der Cybercrime-Studie der IHK Nord waren es deutlich weniger Unternehmen, die einen unfreundlichen Informationsabfluss feststellen konnten. Nur knapp 16 Prozent der von Cybercrime betroffenen norddeutschen Unternehmen gaben an, dass unternehmensrelevante Daten gestohlen wurden (vgl. IHK Nord 2013: 9).

[28] Auf manche Werte wird erst in den Kapiteln 2.2.2 bzw. 2.2.3 näher eingegangen.
[29] Nicht in Tab. 7 „Betroffenheit von Datendiebstahl“ aufgeführt, da die Studie vor 2010 durchgeführt wurde. Der Anteil der betroffenen Unternehmen wirkt sich somit nicht auf den Mittel- oder Modalwert aus.

Wirtschaftsspionage und Konkurrenzausspähung

Tabelle 7: Betroffenheit von Wirtschaftsspionage/Konkurrenzausspähung allgemein[30]

Konkret genannter Vorfall	Anteil der Unternehmen	Zeitraum	Quelle
WS/KA allgemein	1 %	k. A.	BMWi 2012: 55
WS/KA allgemein	7 %	in verg. 3 Jahren	E&Y 2013: 18
WS/KA allgemein	12 %	in verg. 2 Jahren	PwC 2013: 17 f.
WS/KA allgemein	54,6 %	in verg. 3 Jahren	CT 2012: 13
Arithmetisches Mittel	**18,65 %**		
Median	**9,5 %**		

Quelle: Eigene Darstellung.

Auch bei den Angaben zur Betroffenheit von WS/KA können größere Unterschiede zwischen den einzelnen Studien festgestellt werden. 2010 gab knapp jedes fünfte (18 Prozent) von e-Crime betroffene Unternehmen[31] an, in den vergangen drei Jahren von WS/KA betroffen gewesen zu sein (vgl. KPMG 2010a: 21). Auch nach der Studie von CT, die sich ausschließlich mit dem Thema WS/KA befasst, entdeckte ca. jedes fünfte Unternehmen zwischen 2009 und 2012 mindestens einen Fall von Ausforschung. Dazu kamen weitere ca. 30 Prozent mit mindestens einem konkreten Verdachtsfall, was bedeutet, dass sich etwa die Hälfte der befragten Unternehmen ausführlicher mit der Bedrohung von WS/KA beschäftigen musste (vgl. CT 2012: 13).

Die Ergebnisse einer Studie des österreichischen Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT)[32], die sich ebenfalls ausschließlich mit dem Phänomenbereich Wirtschaftsspionage/Konkurrenzausspähung befasst, verweisen auf eine noch höhere Betroffenheitsrate: hier gab knapp ein Drittel der befragten österreichischen Unternehmen[33] an, mindestens einmal Opfer von WS/KA geworden zu sein (vgl. BVT 2010: 11).

Im Vergleich zu den Studien, die sich nicht ausschließlich mit den Phänomenbereichen Wirtschaftsspionage und Konkurrenzausspähung befassen, war der Anteil der Unter-

[30] Auf manche Werte wird erst in den Kapiteln 2.2.2 bzw. 2.2.3 eingegangen.
[31] Nicht in Tab. 8 „Betroffenheit von WS/KA allgemein“ aufgeführt, da 2013 eine Folgestudie erschien, die bereits in Tab. 7 „Betroffenheit von Datendiebstahl“ aufgeführt ist. Der Anteil der betroffenen Unternehmen wirkt sich somit nicht auf den Mittel- oder Modalwert aus.
[32] In Österreich erfolgt keine Trennung in der Zuständigkeit zur Bekämpfung von Wirtschaftsspionage und Konkurrenzausspähung.
[33] Nicht in Tab. 8 „Betroffenheit von WS/KA allgemein“ aufgeführt, da deutsche Unternehmen nicht befragt wurden. Der Anteil der betroffenen Unternehmen wirkt sich somit nicht auf den Mittel- oder Modalwert aus.

nehmen, die in der CT- und BVT-Studie angaben, bereits von Wirtschaftsspionage und/oder Konkurrenzausspähung betroffen gewesen zu sein, relativ hoch. Dies könnte u. a. daran liegen, dass Unternehmen, die bereits für die Thematik sensibilisiert sind (z. B. aufgrund von Verdachtsfällen im Unternehmen), eher an einer Befragung zum Thema Wirtschaftsspionage und/oder Konkurrenzausspähung teilnehmen als andere Unternehmen.

In der Wirtschaftskriminalität-Studie von PwC gaben lediglich 2 Prozent der Unternehmen an, dass sie mindestens einen Fall von WS/KA in den vergangenen zwei Jahren feststellen konnten, und weitere 10 Prozent gaben mindestens einen konkreten Verdachtsfall an (vgl. PwC 2013: 17). Im Vergleich zu den Ergebnissen aus den Studien von KPMG, BVT und CT erscheinen diese Werte sehr niedrig. In der gleichen PwC-Studie gaben aber weitere 20 Prozent der Unternehmen an, dass ihnen sicher oder vermutlich vertrauliche Kunden- und Unternehmensdaten gestohlen wurden (vgl. PwC 2013: 17). Somit erhöht sich der Anteil der von *einer Form* von Ausforschung betroffenen Unternehmen deutlich und nähert sich den Werten aus den anderen Studien an.

Ein ähnliches Muster lässt sich im Gefahrenbarometer 2010 von CT feststellen: auch hier gab nur ein kleiner Teil der Unternehmen an (knapp 6 Prozent)[34], in den vorhergehenden drei Jahren von WS/KA betroffen gewesen zu sein. Dazu kamen aber weitere rund 14 Prozent, die Opfer von Hackerangriffen wurden sowie ca. 20 Prozent, die mindestens einen Diebstahl/Einbruch/Überfall festgestellt haben – beides Angriffsformen, über die ein Unternehmen ausgeforscht werden kann (vgl. CT 2010: 17). Aus diesen weiteren im Gefahrenbarometer gemachten Angaben kann geschlossen werden, dass WS/KA wohl öfter stattfindet als nur bei den 6 Prozent der Unternehmen, die sie als solche bezeichnet haben. Viele Unternehmen scheinen ein veraltetes Bild von WS/KA zu haben, welches z. B. Ausforschung mittels Hackerangriffen nicht impliziert (vgl. KPMG 2010a: 21). Demnach muss berücksichtigt werden, dass auch das Erhebungsinstrument einen nicht unbedeutenden Einfluss auf das Antwortverhalten haben kann – so haben z. B. sich thematisch überschneidende Antwortmöglichkeiten einen negativen Effekt auf die Betroffenheitsrate.

Das Gleiche gilt auch für die Studie des Bundesministeriums für Wirtschaft und Technologie (BMWi) von 2012. Nur 1 Prozent der 952 befragten Unternehmen, die Erfahrungen mit IT-Sicherheitsproblemen gemacht haben, gab an, Opfer von WS/KA geworden zu sein.

[34] Nicht in Tab. 8 „Betroffenheit von WS/KA allgemein“ aufgeführt, da 2013 eine Folgestudie von Corporate Trust erschien, die bereits in Tab. 8 „Betroffenheit von WS/KA allgemein“ aufgeführt ist. Der Anteil der betroffenen Unternehmen wirkt sich somit nicht auf den Mittel- oder Modalwert aus.

Dazu kommen aber weitere 8 Prozent, die mindestens einen Fall von Datendiebstahl (durch externe oder interne Unbefugte) feststellen konnten und weitere 51 Prozent der Unternehmen, die mehrere Virenangriffe verzeichneten (vgl. BMWi 2012: 55). Der geringe Wert bei WS/KA bedeutet somit nicht, dass tatsächlich nur 1 Prozent der Unternehmen ausgeforscht wurde. Die Unternehmen waren gleichzeitig von anderen Angriffen betroffen, deren Hintergrund ebenfalls die Ausforschung des Unternehmens sein kann, die aber zum Teil nur anders ausgewiesen wurden. Ferner sollte bei dieser Studie berücksichtigt werden, dass ca. zwei Drittel der befragten Unternehmen weniger als 100 Mitarbeiter haben, was dazu führt, dass der Anteil von Kleinst- und Kleinunternehmen im Vergleich zu anderen im Rahmen der Sekundäranalyse untersuchten Studien vier- bis fünfmal höher liegt. Damit ist die Studie des BMWi eine der Studien mit dem höchsten Anteil an Kleinst- und Kleinunternehmen und gleichzeitig die Studie, in der der geringste Grad an Betroffenheit von WS/KA feststellt wird. Für Kleinst- und Kleinunternehmen ist es aber häufig deutlich schwieriger als für Großunternehmen, Angriffe zu Ausforschungszwecken überhaupt zu identifizieren.

5.2.2 Bedeutung von Unternehmensgröße und Branche

Unternehmensgröße

In mehreren Studien wurde im Ergebnis darauf hingewiesen, dass die Unternehmensgröße Einfluss auf die Betroffenheit hat: so gaben in sieben Befragungen größere Unternehmen deutlich häufiger als kleine Unternehmen an, dass sie Opfer von Ausforschung wurden.

Während in der e-Crime Studie 2010 von KPMG 18 Prozent aller Unternehmen in den vergangenen drei Jahren mindestens einen Fall von WS/KA zu verzeichnen hatten, waren es bei den Unternehmen mit einem Jahresumsatz von mehr als drei Milliarden Euro sogar 30 Prozent (vgl. KPMG 2010a: 21). Im Cyber Security Report von 2012 waren die Unternehmen mit einem Jahresumsatz von mehr als 500 Millionen Euro dreimal so oft „häufig“ von Ausforschung über die IT betroffen (18 Prozent) als Unternehmen mit einem Umsatz von weniger als 100 Millionen Euro (6 Prozent). Bei letzteren konnte sogar jedes dritte Unternehmen mit Gewissheit angeben, noch nie von solch einer Art von Ausforschung betroffen gewesen zu sein, nur 2 Prozent der großen Unternehmen konnten diese Aussage für sich bestätigen (vgl. Deutsche Telekom 2012: 11). Der Einfluss der Unternehmensgröße auf die Betroffenheit eines Unternehmens kann auch anhand der Ergebnisse der CT-Studie von 2012 beobachtet

werden: Unter den Unternehmen, die mindestens einen Fall von WS/KA festgestellt haben, waren elf Prozent Kleinunternehmen (10-50 Mitarbeiter) und 89 Prozent mittelständische oder große Unternehmen (mehr als 50 Mitarbeiter) (vgl. CT 2012: 14).

Die Rolle der Größe eines Unternehmens kann auch bei Wirtschaftskriminalität im Allgemeinen festgestellt werden. KPMG zeigte diesbezüglich, dass mehr als jedes zweite befragte deutsche Großunternehmen (56 Prozent) in den vergangenen zwei Jahren von einer Form der Wirtschaftskriminalität betroffen war, während bei den mittelständischen Unternehmen „nur" jedes vierte Unternehmen (24 Prozent) einen Vorfall feststellen konnte (vgl. KPMG 2013b: 13 und 33).

Jedoch sollte die Annahme, je größer ein Unternehmen, desto höher die Wahrscheinlichkeit, dass es auch Opfer von Ausforschung wird (vgl. Sicherheitsforum 2004: 66), differenzierter betrachtet werden. Zwar entdeckten in vielen Studien Kleinst- und Kleinunternehmen deutlich weniger festgestellte oder vermutete Fälle von Ausforschung als mittlere und große Unternehmen. Dies bedeutet jedoch nicht, dass sie auch tatsächlich seltener betroffen waren als größere Unternehmen. Ein Grund kann sein, dass sie weniger Kapazitäten haben als größere Unternehmen, um Vorfälle zu identifizieren. Es ist möglich, dass Kleinstunternehmen mit weniger als zehn Mitarbeitern seltener Opfer von WS/KA werden als kleine und mittlere Unternehmen. Dass große Unternehmen grundsätzlich häufiger betroffen sind als mittlere Unternehmen kann aber durchaus angezweifelt werden. Vielmehr sollte davon ausgegangen werden, dass andere Aspekte als die Unternehmensgröße einen bedeutenderen Einfluss darauf haben, wie sehr ein Unternehmen im Fokus der internationalen und nationalen Konkurrenz oder ausländischer Nachrichtendienste steht. Das können z. B. die Innovationsfähigkeit eines Unternehmens, die Bemühungen im F&E-Bereich oder auch der relative Wert seiner Produkte für die Konkurrenz oder andere Staaten sein (vgl. Sicherheitsforum 2004: 69).

Zum Beispiel konnte in mehreren Studien festgestellt werden, dass forschungsintensive Unternehmen häufiger Opfer von Ausforschung wurden als Unternehmen, die wenig oder keine F&E betreiben (vgl. BMWi 2012: 23). Von den Unternehmen mit intensiver F&E verzeichneten 27 Prozent in den vorhergehenden vier Jahren mindestens einen Fall von Verrat von Geschäfts- und Betriebsgeheimnissen, bei Unternehmen mit wenig bzw. keiner F&E waren es demgegenüber nur 15 Prozent (vgl. Sicherheitsforum 2010: 45).

Zusätzlichen Einfluss auf die Betroffenheit eines Unternehmens kann auch der Umgang mit den eigenen Mitarbeitern haben. Fehlende Sensibilisierung der Mitarbeiter für die

Gefahren eines unbewussten Informationsabflusses sowie fehlende firmeninterne Sanktionierung im Falle absichtlicher Weitergabe von geheimem Know-how erhöhen die Wahrscheinlichkeit, dass ein Unternehmen ausgeforscht wird (vgl. KPMG 2010a: 25 und KPMG 2013a: 32).

Branchenzugehörigkeit

Ferner hat die Branchenzugehörigkeit Einfluss auf die Betroffenheit der Unternehmen. In mehreren Studien waren überdurchschnittlich häufig Unternehmen aus der Automobil-, der Luftfahrt-, der Maschinenbau- und der Pharma-/Chemiebranche von Ausforschungsaktivitäten betroffen.

In der CT-Industriespionage-Studie von 2012 waren besonders oft Unternehmen aus der Automobil-/Luftfahrzeug-/Schiffs- und Maschinenbaubranche (ca. 30 Prozent) und aus dem Bereich Banken/Finanzdienstleistungen/Versicherungen (ca. 22 Prozent) von Ausforschung betroffen.

In der EU-Studie zu Geschäftsgeheimnissen und vertraulichen Geschäftsinformationen wurde in den vergangenen zehn Jahren ca. jedem dritten Unternehmen aus der Chemiebranche (35,7 Prozent) und aus der Automobilbranche (33,3 Prozent) unternehmensrelevantes Know-how entwendet. Von allen befragten Unternehmen waren demgegenüber insgesamt „nur“ rund 20 Prozent betroffen (vgl. Europäische Kommission 2013b: 19).

Diese Ergebnisse bedeuten nicht, dass sich Unternehmen aus weniger gefährdeten Branchen nicht vor Ausforschung schützen müssen (vgl. CT 2012: 15). Vielmehr sollte jedes Unternehmen die Wahrscheinlichkeit von Angriffen zu Ausforschungszwecken anhand seiner Position im Verhältnis zu Konkurrenten und in Bezug auf die Einschätzung, wie relevant unternehmerisches Know-how für andere Unternehmen bzw. Länder sein kann selbst bewerten. Die jeweilige Branchenzugehörigkeit kann bei solch einer individuellen Bewertung der Gefährdung eines Unternehmens einen Anhaltspunkt darstellen.

5.2.3 Längsschnittvergleich der Betroffenheit

Sieben Institutionen[35] haben Unternehmen mehr als einmal zu dem gleichen Thema befragt, was einen Längsschnittvergleich der Betroffenheitswerte der Unternehmen ermöglicht (vgl. Tabelle 8).

Tabelle 8: Betroffenheit im Längsschnittvergleich

Studien	Konkret genannter Vorfall	Jahr (Zeitraum)	Anteil der Unternehmen	Veränderung
Corporate Trust 2007 und 2012	WS/KA	2007 (k. A.)	54 %	↑
		2012 (3 Jahre)	54,6 %	
kes 2010 und 2012	Vertraulichkeitsbruch/ Datendiebstahl	2010 (2 J.)	84 %	↑
		2012 (2 J.)	85 %	
PwC 2011 und 2013	Diebstahl vertraulicher Daten	2011 (2 J.)	35 %	↓
		2013 (2 J.)	20 %	
	WS/KA	2011 (2 J.)	18 %	↓
		2013 (2 J.)	12 %	
KPMG 2010b und 2013b	Datendiebstahl/ Datenmissbrauch	2010 (3 J.)	53 %	↓
		2013 (2 J.)	31 %	
	Verrat von Geschäfts- und Betriebsgeheimnissen	2010 (3 J.)	24 %	↓
		2013 (2 J.)	21 %	
KPMG 2010a und 2013a	Datendiebstahl	2010 (3 J.)	61 %	↓
		2013 (3 J.)	24 %	
	Verrat von Geschäfts- und Betriebsgeheimnissen	2010 (3 J.)	51 %	↓
		2013 (3 J.)	16 %	
	Ausspähen, Abfangen von Daten	2010 (3 J.)	44 %	↓
		2013 (3 J.)	27 %	
Ernst & Young 2011 und 2013	WS/KA	2011 (3 J.)	10 %	↓
		2013 (2 J.)	7 %	
WIK 2011 und 2013	Ausspähen	2011 (2 J.)	51,2 %	=
		2013 (2 J.)	51 %	
	Abhören	2011 (2 J.)	10 %	↑
		2013 (2 J.)	22 %	

Quelle: Eigene Darstellung.

In Kapitel 5.1.2 wurde gezeigt, dass die Mehrheit der Unternehmen von einem Anstieg der Bedrohung durch Ausforschung ausging. Auch in der Fachliteratur wird seit mehreren Jahren vor einem Anstieg der Zahl der ausgeforschten Firmen gewarnt (vgl. Sarin 2010: 73).

Diese Wahrnehmungen und Prognosen decken sich jedoch nicht mit den Aussagen der Unternehmen zur Anzahl tatsächlich festgestellter Vorfälle von Ausforschung. Vergleicht man die von den Unternehmen gemachten Angaben zur konkreten Betroffenheit von Aus-

[35] Corporate Trust: Industriespionage 2007 und 2012, kes/Microsoft Sicherheitsstudie 2010 und 2012, KPMG Wirtschaftskriminalität 2010 und 2013, KPMG e-Crime 2010 und 2013, PwC Wirtschaftskriminalität 2011 und 2013, Ernst & Young Datenklau 2011 und 2013, WIK Sicherheits-Enquête 2011 und 2013.

forschung zu unterschiedlichen Zeitpunkten lässt sich vielmehr feststellen, dass die Anzahl der Vorfälle und konkreten Verdachtsfälle in den letzten Jahren tendenziell abgenommen hat.

Ein leichter Anstieg der Fälle kann lediglich in drei Studien beobachtet werden. In der WIK-Sicherheits-Enquête 2011 konnten 10 Prozent der Unternehmen in den vergangenen zwei Jahren mindestens einen *Abhör*versuch feststellen (vgl. WIK 2011/2: 14), 2013 waren es bereits 22 Prozent der Unternehmen, die *abgehört* wurden (vgl. WIK 2013/2: 12). Demgegenüber veränderte sich in den gleichen Studien der Anteil der *ausgespähten* Unternehmen zwischen 2011 und 2013 jedoch nicht – in beiden Jahren gab ca. die Hälfte der befragten Unternehmen an, bereits *ausgespäht* worden zu sein (vgl. WIK 2011/2: 14 und WIK 2013/2: 12).

Ebenfalls ein leichter prozentualer Anstieg kann bei der Häufigkeit von Vertraulichkeitsbrüchen in der kes/Microsoft-Sicherheitsstudie zwischen den Jahren 2010 und 2012 beobachtet werden. 2010 gaben 30 Prozent der Unternehmen an, dass Unbefugte in den vergangenen zwei Jahren erwiesenermaßen auf die eine oder andere Weise Zugriff auf schutzwürdige Daten erlangen konnten und bei 54 Prozent der Befragten war das vermutlich der Fall. Somit waren insgesamt 84 Prozent der Unternehmen von einem Vertraulichkeitsbruch betroffen (vgl. kes 2010/4: 10). Dieser Wert stieg in der Studie von 2012 auf 85 Prozent (vgl. kes 2012/4: 13).

Eine weitere geringe Zunahme kann in der Industriespionage-Studie von CT zwischen 2007 und 2012 beobachtet werden. Einen konkreten Fall von WS/KA haben in der Studie von 2007 18,9 Prozent und in der Studie von 2012 21,4 Prozent der befragten Unternehmen feststellen können. Addiert man dazu die konkreten Verdachtsfälle, ergibt sich für 2007 ein Wert von 54 Prozent, der auf 54,6 Prozent in 2012 ansteigt (vgl. CT 2007: 13 und CT 2012: 13). Diese drei Beispiele einer leichten Zunahme der Ausforschung sind jedoch die Ausnahme.

Vielmehr wird in der Mehrheit der Studien festgestellt, dass der Anteil der von Ausforschung betroffenen Unternehmen zum Teil stark rückläufig ist. Dies ist z. B. der Fall in den Wirtschaftskriminalität- und e-Crime-Studien von KPMG, nach denen zwischen 2010 und 2013 ein deutlicher Rückgang bei Vorfällen wie Datendiebstahl, Verrat von Geschäfts- und Betriebsgeheimnissen und dem Ausspähen und Abfangen von Daten vorliegt. So konnten in der

e-Crime Studie von 2010 44 Prozent der von e-Crime betroffenen Unternehmen einen Fall von Ausspähen/Abfangen von Daten feststellen (vgl. KPMG 2010a: 21) während der Anteil in der Studie von 2013 nur noch bei 27 Prozent der Unternehmen lag (vgl. KPMG 2013a: 15).

Und während in der Wirtschaftskriminalität-Studie von KPMG in 2010 53 Prozent der Unternehmen von Datendiebstahl/Datenmissbrauch betroffen waren (vgl. KPMG 2010b: 8), waren es in der Folgestudie von 2013 nur noch 31 Prozent (vgl. KPMG 2013b: 33).

In der E&Y-Studie konnte bereits im Jahr 2011 nur jedes zehnte Unternehmen einen Vorfall bzw. konkreten Verdachtsfall von WS/KA feststellen (vgl. E&Y 2011: 9). In der Befragung von 2013 lag dieser Wert bei sieben Prozent der befragten Unternehmen und somit noch niedriger (vgl. E&Y 2013: 18).

Auch nach der Wirtschaftskriminalität-Studie von PwC kann zwischen 2011 und 2013 eine abnehmende Betroffenheitsrate beobachtet werden: bei sicher festgestelltem Diebstahl von Kunden- und Unternehmensdaten von 35 auf 20 Prozent sowie bei WS/KA-Vorfällen von 18 auf 12 Prozent[36].

Die Ergebnisse der Studien verweisen somit auf einen gleichen Trend: In den letzten Jahren ist die Betroffenheitsrate vornehmlich gesunken oder zumindest gleich geblieben. In der Mehrzahl der Längsschnittvergleiche stellten in den aktuellsten Studien prozentual weniger Unternehmen Vorfälle bzw. konkrete Verdachtsfälle fest als in den Vorgängerstudien.

Die Autoren der Studien liefern mehrere Erklärungsansätze für diese Entwicklung. Eine Erklärung ist, dass die Abnahme der Häufigkeit von Ausforschungsvorfällen mit einer verbesserten Deliktskenntnis und Analysefähigkeit der Unternehmen zusammenhängt. Das bedeutet, dass die Unternehmen die Vorfälle präziser zu Deliktstypen zuordnen können und somit Redundanzen vermeiden, wobei die tatsächliche Anzahl der Vorfälle jedoch konstant geblieben ist (vgl. KPMG 2013a: 14).

Der Rückgang der von den Unternehmen festgestellten Vorfälle könnte zudem auf das Vorhandensein von Compliance Management Systemen in den Unternehmen zurückzuführen sein. In den letzten Jahren haben Unternehmen vermehrt solche Systeme eingeführt und sind dadurch und nicht zuletzt aufgrund einer gesteigerten Sensibilisierung auf Fälle gestoßen, die ohne Compliance Management System unentdeckt geblieben wären. Nach

[36] Jeweils bestätigte Fälle und konkrete Verdachtsfälle addiert.

mehreren Jahren des erfolgreichen Wirkens solcher Systeme treten die Unternehmen dann in die sogenannte Präventionsphase ein, in der die neu eingeführten präventiven und repressiven Maßnahmen greifen und ein weiterer Anstieg der Kriminalität im und gegen das Unternehmen verhindert werden kann (vgl. PwC 2013: 16).

Die Verfasser anderer Studien sind der Meinung, dass die Ausforschung deutscher Unternehmen in den letzten Jahren professioneller und zielgenauer geworden ist (vgl. KPMG 2013a: 14). Eine weitere Begründung könnte somit sein, dass nicht die Anzahl der Vorfälle rückgängig ist, sondern dass die Täter immer professioneller vorgehen und somit viele Angriffe den Unternehmen nicht oder erst sehr spät bekannt werden.

Möglicherweise besteht aber auch ein Zusammenhang zwischen dem weiter oben thematisierten Anstieg der Bedrohungs*wahrnehmung* und dem Rückgang der tatsächlich festgestellten Ausforschungsvorfälle, da eine gesteigerte Bedrohungswahrnehmung und die damit einhergehende erhöhte Sensibilisierung der Unternehmen für mögliche Ausforschungsaktivitäten zu einer Abnahme der Betroffenheit führen können. Es kann davon ausgegangen werden, dass Unternehmen, die für eine bestimmte Bedrohung sensibilisiert sind, tendenziell eher konkrete Abwehrmaßnahmen treffen werden, als solche Unternehmen, die diese Bedrohung weder wahrnehmen noch bewerten.

Nach den Ergebnissen der Studien besteht Einigkeit darin, dass aufgrund rückläufiger Häufigkeiten keine Entwarnung gegeben werden kann, da die Unternehmen angeben, dass ca. ein Drittel der Ausforschungsangriffe nur per Zufall entdeckt wurde. Ein Rückgang der festgestellten Vorfälle bedeutet somit nicht automatisch, dass auch das Dunkelfeld kleiner wird (vgl. PwC 2011: 19). Auch mit den von den Unternehmen gemachten Angaben zur Betroffenheit von Ausforschung gelingt es nicht, die gesamte Bedrohungslage korrekt abzubilden.

Auch in der Fachliteratur geht man davon aus, dass Wirtschaftsspionage und Konkurrenzausspähung von den Unternehmen nicht unterschätzt werden dürfen, da von der Anzahl der entdeckten Fälle nicht (immer) auch auf die Anzahl der tatsächlich durchgeführten Angriffe geschlossen werden kann. Dies verdeutlicht folgendes Beispiel: die systematische Auswertung der Akten des DDR-Staatssicherheitsdienstes zeigt, dass obwohl Wirtschaftsspionage gegen Westdeutschland in einem unerwartet hohen Ausmaß betrieben wurde, diese jedoch nur in den wenigsten Fällen entdeckt wurde. Erst viel später konnte nachgewiesen

werden, dass viele westdeutsche Unternehmen von Agenten infiltriert waren und dass über beinahe jedes bedeutende Unternehmen Akten geführt wurden (vgl. Nathusius 2001: 61).

Zudem verweisen Sicherheitsexperten und die Verfassungsschutzberichte darauf, dass die Bedrohungslage für deutsche Unternehmen aufgrund der weltweit wachsenden Vernetzung der IKT stetig zunimmt (vgl. BMWi 2012: 23). Zwar finden sich auch in der Fachliteratur keine gesicherten Erkenntnisse zum Umfang der elektronischen Ausforschung deutscher Unternehmen, es ist aber davon auszugehen, dass mit der Verdichtung der elektronischen Vernetzung in der Wirtschaft auch die elektronischen Angriffsmöglichkeiten weiter zunehmen (vgl. Even 2013b: 9). So wird die Anzahl immer effektiverer und zielgerichteter elektronischer Angriffe zur Ausforschung der Unternehmen weiterhin zunehmen, was damit zusammenhängt, dass solche Angriffe vergleichsweise günstig und wenig risikobehaftet sind (vgl. Klingelhöller 2008: 31). Die Ausforschung verlagert sich vermehrt auf das Internet, wo sie weltweit durchgeführt werden kann und was dazu führt, dass potenziell beinahe jedes Unternehmen ausgeforscht werden kann (vgl. BVT 2010: 5).

5.2.4 Erkennen von Ausforschung

Es gibt eine Vielzahl von möglichen Risiken für den Abfluss geheimen Unternehmens-Know-hows. Oft werden diese Risiken vor allem von betroffenen kleinen und mittleren Unternehmen nicht oder aber zu spät erkannt bzw. nicht ausreichend ernst genommen (vgl. CT 2010: 48). Auch der Verfassungsschutz stellt fest, dass viele Unternehmen den ungewollten Know-how-Verlust gar nicht (vgl. Even 2013b: 7) oder erst dann bemerken, wenn der Angriff bereits stattgefunden hat (vgl. George 2013: 23) und sie von Dritten darauf hingewiesen werden (vgl. Niemantsverdriet 2011: 26). Ein häufiger Indikator, der darauf schließen lässt, dass Know-how aus dem Unternehmen abgeflossen ist, sind Fälle, bei denen Mitbewerber über unternehmensinterne Informationen verfügen, wie z. B. die Ergebnisse vertraulicher Gespräche des Vorstands, die Forschungsergebnisse aus der F&E-Abteilung oder die Preisgestaltung, die sie nur durch eine Quelle im betroffenen Unternehmen gewonnen haben können (vgl. Leiner 2008: 40). Der Verlust von solch sensiblen Unternehmensdaten kann den Aktienkurs eines Unternehmens beeinflussen, seine Marktpräsenz verringern und im äußersten Fall bis zur Insolvenz führen (vgl. Leiner 2008: 40).

Von Ausforschung geht auch deswegen eine besondere Gefahr für die Unternehmen aus, da viele Angriffe nur zufällig entdeckt werden (vgl. Sarin 2010: 73). Die Unternehmens-

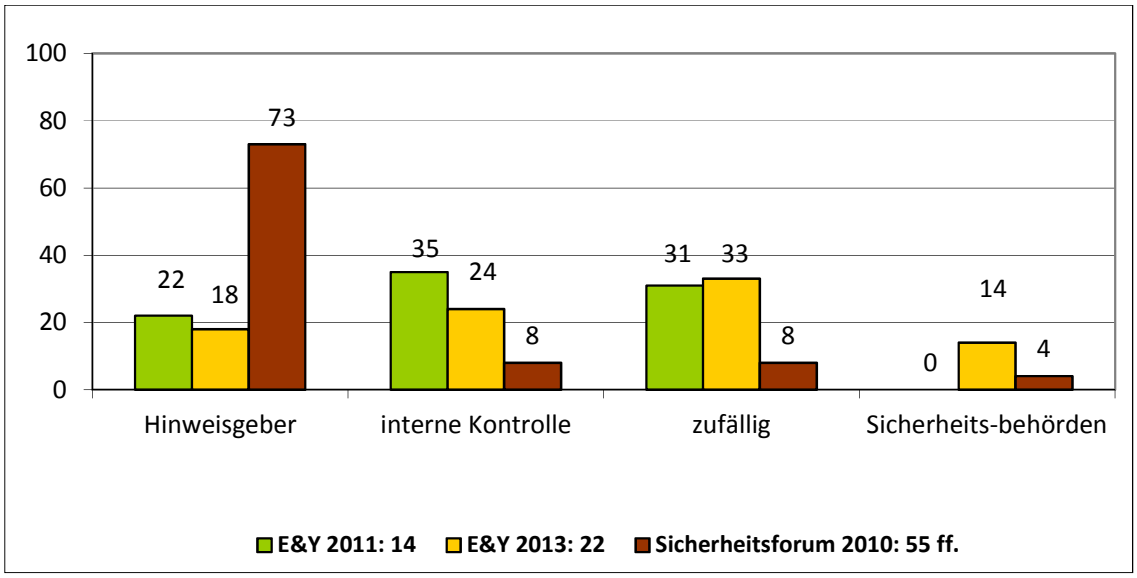
befragungen bestätigen das: In der Mehrheit der Studien wurde ca. jeder dritte Fall von Ausforschung rein zufällig entdeckt und somit *nicht* durch interne Kontrollmechanismen, Routineprüfungen oder Hinweise der Sicherheitsbehörden. Das bedeutet gleichzeitig, dass viele Angriffe unentdeckt bleiben und die Unternehmen somit nicht darauf reagieren können. Häufig bemerkten Unternehmen einen Know-how-Abfluss erst dann, wenn es für eine Intervention bereits zu spät ist.

Die Verfasser der Studie des Sicherheitsforums Baden-Württemberg von 2004 zu Know-how-Verlusten und die der Studie vom österreichischen BVT von 2010 kommen zu sehr ähnlichen Ergebnissen bezüglich der wichtigsten Verdachtsmomente/Indikatoren von Vorfällen im Zusammenhang mit Ausforschung. In beiden Studien wurden die Unternehmen am häufigsten durch das Auftauchen von Teilinformationen bei Mitbewerbern darauf aufmerksam, dass eine Ausforschung stattgefunden hat. In der österreichischen Studie betraf dies knapp jeden zweiten Vorfall (46 Prozent) (vgl. BVT 2010: 9) und in der Studie aus Baden-Württemberg machte das etwas mehr als ein Viertel der Nennungen aus (vgl. Sicherheitsforum 2004: 55). Auch der nicht erklärbare Verlust von Aufträgen wurde von vielen Unternehmen in direktem Zusammenhang mit WS/KA gesehen: bei ca. 30 Prozent der Vorfälle in der Studie aus Österreich und bei rund 20 Prozent der Nennungen in der Studie des Sicherheitsforums. Auch das Auftauchen von ähnlichen Konkurrenzprodukten war für viele Unternehmen ein relativ häufiger Indikator dafür, dass sie ausgeforscht wurden – für ca. 30 Prozent der österreichischen Unternehmen (vgl. BVT 2010: 9) und bei ca. 17 Prozent der Nennungen aus Baden-Württemberg (vgl. Sicherheitsforum 2004: 55). Zudem bemerkten die Unternehmen in der österreichischen Studie ca. jeden vierten Vorfall dadurch, dass ein neuer Mitbewerber plötzlich am Markt auftauchte und jeden dritten Vorfall von Ausforschung, weil ein verdächtiges Unterbieten durch Mitbewerber stattfand[37] (vgl. BVT 2010: 9).

Während in der Folgestudie des Sicherheitsforums Baden-Württemberg von 2010 die meisten Angriffe auf Geschäfts- und Betriebsgeheimnisse erst durch Tipps von Hinweisgebern aufgedeckt wurden, spielte der Zufall bei der Entdeckung von Ausforschung in den E&Y-Studien eine bedeutendere Rolle (vgl. Abbildung 3)

[37] Mehrfachnennungen möglich.

Abbildung 3: Aufdeckung von Angriffen zu Ausforschungszwecken



Anteil der Unternehmen (in Prozent), die durch Hinweisgeber, unternehmensinterne Kontrollen, Zufall oder Sicherheitsbehörden einen Vorfall von Ausforschung bemerkt haben. Quelle: Eigene Darstellung.

Diese Ergebnisse zeigen, dass der Zufall bei der Aufdeckung von Ausforschung eine nicht zu unterschätzende Rolle spielt. Ferner sollten die Unternehmen davon ausgehen, dass sie nur relativ selten von den Sicherheitsbehörden auf Angriffe aufmerksam gemacht werden. Die Unternehmen sind somit größtenteils auf sich selbst gestellt, was durchaus kritisch eingeschätzt werden kann, wenn man bedenkt, dass deutlich mehr Ausforschungsvorfälle durch Hinweise von externen oder internen Informanten aufgedeckt werden als durch die unternehmenseigenen Kontrollsysteme oder die interne Revision.

Ähnlich verhält es sich in den weitergefassten Deliktsbereichen Wirtschaftskriminalität und Cybercrime. Auch hier waren die Strafverfolgungsbehörden/Aufsichtsbehörden nur selten Initiator der Entdeckung wirtschaftskrimineller Handlungen: bei 13 Prozent (vgl. KPMG 2013b: 40) bzw. bei ca. 10 Prozent (vgl. PwC 2013: 83) der betroffenen Unternehmen. Zudem gaben besonders viele Unternehmen an, dass Informationen interner[38] und externer[39] Hinweisgeber zur Entdeckung wirtschaftskrimineller Handlungen führten. In der KPMG-Studie gab rund jedes zweite Unternehmen an, dass wirtschaftskriminelle Handlungen nur zufällig entdeckt wurden, während der Faktor Zufall bei den in der PwC-Studie befragten Unternehmen deutlich weniger ins Gewicht fiel (5 Prozent). Auch die interne Revision spielte

[38] Bei 50 Prozent (vgl. KPMG 2013b: 40) bzw. 38 Prozent (vgl. PwC 2013: 83) der befragten Unternehmen.
[39] Bei 40 Prozent (vgl. KPMG 2013b: 40) bzw. 22 Prozent (vgl. PwC 2013: 83) der befragten Unternehmen.

in der KPMG-Studie (40 Prozent der Unternehmen) eine bedeutendere Rolle als in der von PwC durchgeführten Befragung (8 Prozent der Unternehmen).

5.2.5 Zusammenfassung Betroffenheit

- Im Durchschnitt der aktuellsten Studien verzeichnete zwischen 2010 und 2013 ca. **jedes vierte Unternehmen** mindestens einen Fall von Verrat von Geschäfts- und Betriebsgeheimnissen, ebenfalls ca. **jedes vierte Unternehmen** mindestens einen Fall von Datendiebstahl und ca. **jedes sechste Unternehmen** mindestens einen Fall von WS/KA.
- Aufgrund unterschiedlicher **Forschungsdesigns** der Befragungen ist ein direkter Vergleich der Ergebnisse nur eingeschränkt möglich, sodass die o. g. Betroffenheitswerte nur als eine Tendenz betrachtet werden können. So kann zum Beispiel vermutet werden, dass ein sehr niedriger Wert von Ausforschung betroffener Unternehmen u. a. darauf zurückzuführen ist, dass ausschließlich kleine Unternehmen befragt wurden (→ Auswirkungen der Festlegung der *Grundgesamtheit* auf die Ergebnisse der Befragung). Demgegenüber kann ein hoher Wert von betroffenen Unternehmen darauf hinweisen, dass sich hauptsächlich Unternehmen an der Befragung beteiligt haben, die bereits für das Thema sensibilisiert waren (→ Auswirkungen der Zusammenstellung der *Stichprobe* auf die Ergebnisse der Befragung).
- In sieben Befragungen gaben **größere Unternehmen** deutlich häufiger als kleine Unternehmen an, dass sie Opfer von Ausforschung wurden. Diese Ergebnisse sollten jedoch nicht zu der Annahme führen, dass die Wahrscheinlichkeit der Ausforschung mit der Größe eines Unternehmens zunimmt, dass also kleinere Unternehmen weniger gefährdet sind als große.
- Vielmehr gibt es weitere Aspekte, die die Wahrscheinlichkeit von Wirtschaftsspionage und/oder Konkurrenzausspähung erhöhen können, wie zum Beispiel die Investitionen eines Unternehmens in die **Forschung und Entwicklung** oder seine Bemühungen bzgl. der **Sensibilisierung der Mitarbeiter**.
- In mehreren Studien konnte gezeigt werden, dass die **Branchenzugehörigkeit** eines Unternehmens Einfluss auf die Wahrscheinlichkeit nimmt, ausgeforscht zu werden. Überdurchschnittlich häufig waren Unternehmen aus der Automobil-, der Luftfahrt-, der Maschinenbau- und der Pharma-/Chemiebranche Opfer von Ausforschung.

- Im Gegensatz zur Bedrohungswahrnehmung der Unternehmen, die während der letzten Jahre zugenommen hat, nahmen die **Betroffenheitswerte** der Unternehmen ab. Es wurden tendenziell weniger Unternehmen ausgeforscht als noch in den direkten Vorgängerstudien.
- Dieser in den Studien festgestellte Rückgang der Angriffe zu Ausforschungszwecken auf deutsche Unternehmen hängt *nicht notwendigerweise* mit einem Rückgang der tatsächlichen Ausforschungsaktivitäten zusammen. Er könnte auch darauf zurückzuführen sein, dass Angreifer immer professioneller werden und Vorfälle somit unbemerkt bleiben. Eine weitere Ursache könnten auch die gestiegene Bedrohungswahrnehmung und die damit einhergehende größere Sensibilisierung der Unternehmen für Ausforschung sein.
- Diese Ergebnisse geben jedoch **keine Entwarnung**. Weder die Herausgeber der Studien noch die Sicherheitsbehörden oder die Fachliteratur gehen davon aus, dass die Gefahr von Ausforschung zukünftig abnehmen wird. Begründet wird dies u. a. dadurch, dass neue technische Entwicklungen sowie die immer stärkere elektronische Vernetzung der Wirtschaft die Ausforschung eher erleichtern.
- Wichtigste **Verdachtsmomente**, die auf einen bereits eingetretenen Ausforschungsvorfall hindeuteten, waren das Auftauchen von Teilinformationen bei Mitbewerbern, der nicht erklärbare Verlust von Aufträgen sowie das Erscheinen von ähnlichen Konkurrenzprodukten.
- In der Mehrheit der Studien wurde etwa jeder dritte Angriff zu Ausforschungszwecken lediglich durch **Zufall** entdeckt. Nur selten wurden die Unternehmen von den **Sicherheitsbehörden** aufmerksam gemacht.
- **Unternehmensinterne Kontrollen** deckten nur einen kleinen Teil der Angriffe auf. Häufig entdeckten Unternehmen den Verlust von sensiblem Know-how erst aufgrund von Hinweisen von internen oder externen **Tippgebern**.

5.3 Schäden

Durch Ausforschung erhalten Wettbewerber wichtige Informationen über deutsche Firmen, was zur Folge haben kann, dass der deutschen Industrie große Aufträge entgehen. Auch der Diebstahl von Forschungs- und Entwicklungsergebnissen führt zu einem erheblichen finanziellen Verlust bei den bestohlenen Unternehmen, da auf jahrelange und kostenintensive F&E nicht die erwarteten Gewinne folgen, weil Konkurrenten mit den erlangten Erkenntnissen

kostengünstigere Produktkopien auf den Markt bringen können als das geschädigte Unternehmen (vgl. Schaaf 2009: 62). Die von den Unternehmen getätigten Investitionen rechnen sich dann nicht mehr und ihr Umsatz bricht ein. Wird öffentlich bekannt, dass ein Unternehmen Opfer von Ausforschung wurde und sensible Daten entwendet werden konnten, verliert dieses zudem an Ansehen und Reputation, was mittel- und langfristig zu (weiterem) finanziellen Schaden führen kann (vgl. IHK Nord 2013: 15). Die Ausforschung eines Unternehmens kann letztlich dazu führen, dass das Unternehmen Insolvenz anmelden muss und es somit zu einem Verlust von Arbeitsplätzen kommt: in Deutschland sind laut dem Bayerischen Landesamt für Verfassungsschutz jährlich über 50.000 Arbeitsplätze mittelbar durch Ausforschung gefährdet[40] (vgl. George 2013: 23 und Proschko 2010: 19).

5.3.1 Materielle und immaterielle Schäden

Ein von Ausforschung betroffenes Unternehmen kann direkte finanzielle (materielle) Schäden und indirekte Auswirkungen (immaterielle Schäden) erfahren. Immaterielle Schäden, wie z. B. Imageschäden bei Kunden und Geschäftspartnern, negative Medienberichterstattung, sinkende Attraktivität als Arbeitgeber, Transfer von Forschungswissen etc. sollten nicht unterschätzt werden, da sie zum Teil schwerwiegendere Konsequenzen haben können, als die direkten finanziellen Schäden (vgl. Sicherheitsforum 2010: 49).

In der CT-Studie von 2012 benannten rund zwei Drittel der geschädigten Unternehmen hohe Kosten für Rechtsstreitigkeiten als konkrete Schädigung durch WS/KA und bei ca. 60 Prozent führte das Bekanntwerden der Ausforschung zu Imageschäden und Vorbehalten bei Kunden und Lieferanten. Ca. ein Drittel der Unternehmen erlitt durch WS/KA konkrete Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen. Zudem musste sich etwa jedes fünfte Unternehmen im Anschluss an einen Ausforschungsvorfall mit negativer Medienberichterstattung auseinandersetzen und weitere ca. 20 Prozent wurden mit den gestohlenen Daten erpresst (vgl. CT 2012: 24).

Wie in der CT-Studie von 2012, werden auch in der SiFo-Studie von 2010 konkrete Umsatzeinbußen seltener als andere Schäden als eine Konsequenz von ungewolltem Know-how-Abfluss genannt. Jedes zweite ausgeforschte Unternehmen stellte fest, dass durch den Verrat von Geschäfts- und Betriebsgeheimnissen Wettbewerber strategische Vorteile erlangen konnten. Etwa ein Drittel der Unternehmen bewertete die benötigte Zeit und die Kosten

[40] Die Berechnungsgrundlage für diese Einschätzung wird von den Autoren nicht genannt.

für die betriebsinterne Bearbeitung des Vorfalls als besonders großen Schaden und ca. ein Viertel der Unternehmen berichtete über einen großen zeitlichen und finanziellen Aufwand für die Rechtsverfolgung. Ca. jedes fünfte Unternehmen erlitt konkrete Umsatzeinbußen und ebenfalls ca. jedes fünfte Unternehmen konnte einen Reputationsverlust für die betroffene Marke bzw. das Produkt feststellen (vgl. Sicherheitsforum 2010: 49 f.).

Nach der kes-Sicherheitsstudie führte die Ausforschung eines Unternehmens zu missbräuchlicher Verwendung von Unternehmens-Know-how durch Dritte (bei 29 Prozent der geschädigten Unternehmen), zu Imageschäden (27 Prozent) und zu verlorenen Kunden/Aufträgen (21 Prozent) (vgl. kes 2012/4: 14).

Die möglichen negativen Auswirkungen der Ausforschung sind somit vielfältig und nicht ausschließlich finanzieller Natur. Zudem wurden die verschiedenen Auswirkungen von den Unternehmen unterschiedlich bewertet und wahrgenommen. Für manche Unternehmen war der Verlust wichtiger Kunden der erheblichste Schaden. Andere bezeichneten den Verlust von Forschungsergebnissen und somit die Verschlechterung ihrer Innovationssituation als bedeutendsten Schaden. Für manche ausgeforschte Unternehmen war die negative Medienberichterstattung der größte spürbare Schaden, wieder andere konnten sofort erhebliche Umsatzeinbußen feststellen, weil sie zum Beispiel eine Ausschreibung verloren haben. Welche Schäden einem Unternehmen durch Ausforschung entstanden sind, hing zum Teil auch von der Branche ab (vgl. KPMG 2010a: 18).

5.3.2 Schätzungen des finanziellen Schadens

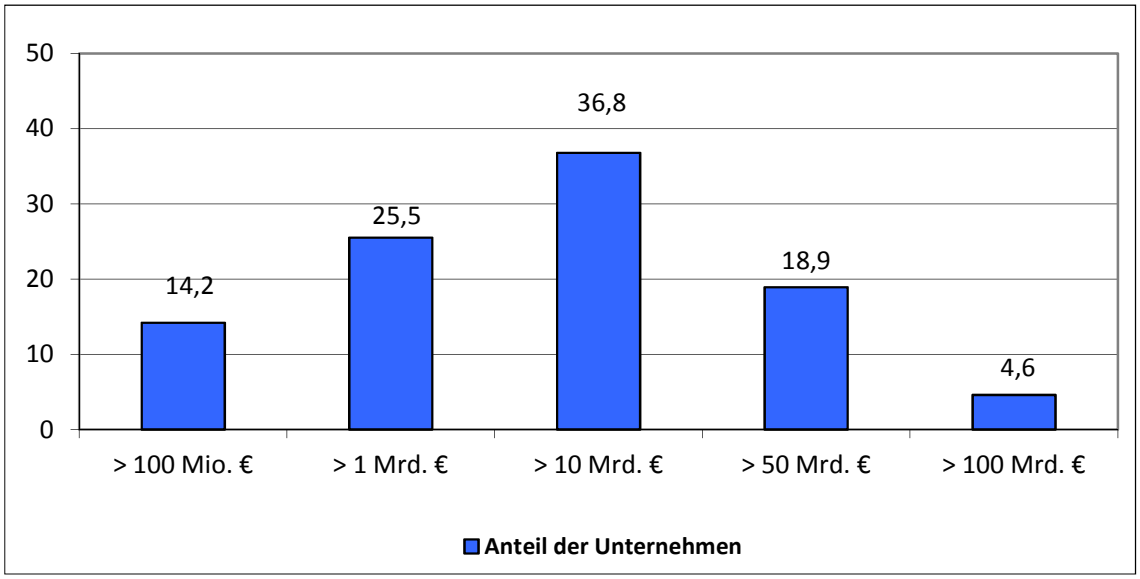
Auch wenn die tatsächlichen wirtschaftlichen Auswirkungen von Wirtschaftsspionage und/oder Konkurrenzausspähung auf die deutsche Wirtschaft nur schwer bestimmt werden können (vgl. Sicherheitsforum 2010: 48), werden sie in der Öffentlichkeit mehrheitlich als sehr bedeutsam eingeschätzt. Meistens wird jedoch nicht näher erläutert, wie diese Schätzungen zustande gekommen und welche Elemente in die Berechnung eingeflossen sind. So bewerteten im Cyber Security Report 2012 37 Prozent der befragten Entscheidungsträger aus Politik und Wirtschaft den durch Ausforschung verursachten jährlichen Schaden für die deutsche Wirtschaft als *sehr groß* und 43 Prozent als *groß* (vgl. Deutsche Telekom 2012: 27).

Auch in der Presse wurden regelmäßig Schadensschätzungen genannt: u. a. wurde der jährliche Schaden für die deutsche Wirtschaft auf 20 bis 50 Milliarden Euro (vgl. Heise

2011), mehrfach auf 50 Milliarden Euro (vgl. u. a. Handelsblatt 2013, Reuters 2013, Balser 2014) und auf 80 Milliarden Euro (vgl. Nuri 2009) geschätzt. Der Verein Deutscher Ingenieure (VDI) ging sogar von einem jährlichen Schaden in Höhe von 100 Milliarden Euro aus (vgl. u. a. RP Online 2014, Focus Online 2014). 100 Milliarden Euro hätten im Jahr 2013 rund 3,65 Prozent des deutschen Bruttoinlandsproduktes (BIP) ausgemacht (vgl. Statistisches Bundesamt 2014: 1).

Im Secure Mobile Computing Report von Secusmart[41] und TeleTrusT[42] von 2013 sollten die Unternehmen schätzen, wie viele Euro der deutschen Wirtschaft jährlich durch WS/KA verloren gehen (vgl. Abbildung 4): Etwa ein Viertel der Befragten geht von einem Schaden von über 50 Milliarden Euro aus (vgl. Secusmart 2013: 1).

Abbildung 4: Schätzung des Schadens durch WS/KA für die deutsche Wirtschaft



Schätzung des Schadens durch befragte Unternehmen (Angaben in Prozent). Eigene Darstellung nach Secusmart 2013: 1.

Im Auftrag des Cabinet Office der britischen Regierung führte das Wirtschaftsberatungsunternehmen Detica im Jahr 2011 eine Studie zu den Kosten von Cybercrime durch. Der wirtschaftliche Schaden, der den britischen Unternehmen durch den Diebstahl von geistigem Eigentum und durch WS/KA entsteht, wird laut dieser Studie mit jährlich 21 Milliarden Pfund (ca. 26 Milliarden Euro) beziffert und der Schaden für Bürger und die Regierung mit jeweils ca. drei Milliarden Pfund (ca. vier Milliarden Euro) (vgl. Detica 2011: 24). Experten und die britische Öffentlichkeit reagierten sehr skeptisch auf diese Ergebnisse. Vor allem der hohe

[41] Unternehmen für abhörsichere Sprachkommunikation.
[42] Der Bundesverband IT-Sicherheit e.V. ist der größte Kompetenzverbund für IT-Sicherheit in Europa.

jährliche Schaden der britischen Unternehmen wurde stark angezweifelt und viele Experten vermuteten, dass die Gefahr hochgespielt wurde (vgl. Anderson u. a. 2012: 2). Die Zweifel an den Ergebnissen dieser Studie veranlassten das britische Verteidigungsministerium, eine weitere Studie in Auftrag zu geben, in der die Kosten von Cybercrime erneut gemessen und die Ergebnisse von Detica überprüft werden sollten. Die Autoren dieser Nachfolgestudie kommen zu dem Ergebnis, dass der finanzielle Schaden, der den Unternehmen durch Cyber-*Ausforschung* entstand, im Gegensatz zu anderen Cyber-Straftaten nicht in die Berechnung einfließen kann, da es dazu *keine* verlässlichen Zahlen für das Vereinigte Königreich gibt (vgl. Anderson u. a. 2012: 18).

Wie im Vereinigten Königreich, sollten auch in Deutschland die Schätzungen zum finanziellen Schaden durch Ausforschung für die deutsche Wirtschaft kritisch betrachtet werden. Manche Autoren gehen sogar davon aus, dass keine der Schätzungen für Deutschland annähernd verlässlich sein kann (vgl. Huber 2009: 40). Da zudem viele der vorliegenden Studien in Bezug auf Erhebung, Analyse und Interpretation der Ergebnisse Unsicherheiten aufweisen, ist es nicht ohne weiteres möglich, von den Angaben zum finanziellen Schaden durch Ausforschung auf zukünftige Entwicklungen zu schließen (vgl. Staron/Tempel 2014: 16).

5.3.3 Hochrechnungen des finanziellen Schadens

Aussagekräftiger als reine (Experten-) Schätzungen der Höhe der finanziellen Schäden durch Ausforschung sind die Angaben von betroffenen Unternehmen. Aber selbst die Angaben der Unternehmen beruhen häufig nur auf groben Schätzungen, da sie einen Verlust von kritischem Unternehmens-Know-how oft überhaupt nicht quantifizieren können (vgl. Staron/Tempel 2014: 17). Das führt dazu, dass je nach Unternehmen unterschiedliche Kriterien zur Schadensbestimmung herangezogen werden (vgl. Röder 2011: 14). Somit sollen auch die folgenden Hochrechnungen *nicht* als endgültige Größen und Maßstäbe verstanden werden, sondern dienen vielmehr als Größenorientierung (vgl. Huber 2010: 112).

Unternehmen konnten nur in wenigen Befragungen Angaben zu der Höhe des finanziellen Schadens durch Ausforschung machen. Mit den so erlangten Daten gehen die Verfasser der Studien unterschiedlich um: Manche berechneten lediglich den durchschnittlichen finanziellen Schaden der befragten Unternehmen und einige wenige versuchten, den durchschnittlichen finanziellen Schaden auf die gesamte deutsche Wirtschaft hochzurechnen. In anderen Studien wurde nur der durchschnittliche Schaden pro Angriffsform berechnet.

Finanzieller Schaden für die Gesamtwirtschaft

Nur wenige Institutionen rechnen den von den Unternehmen in den Befragungen bezifferten Schaden durch Ausforschung auf die deutsche Gesamtwirtschaft hoch.

Die in der ersten Studie des Sicherheitsforums Baden-Württemberg befragten Unternehmen bezifferten den Schaden durch ungewollte Informationsverluste mit 52 Millionen Euro. Auf dieser Grundlage wurde anschließend eine Hochrechnung für die deutsche Gesamtwirtschaft vorgenommen[43], die ergibt, dass der Schaden durch Know-how- und Informationsverluste für die deutsche Wirtschaft bei ca. sieben bis acht Milliarden Euro liegt (vgl. Sicherheitsforum 2004: 63). Leider wird nicht näher erläutert, auf welchen Zeitraum sich der Schaden bezieht (wahrscheinlich auf die vergangenen zehn Jahre), weswegen die Angaben zur Schadenshöhe nur eingeschränkt aussagekräftig sind.

Eine weitere Hochrechnung auf die deutsche Gesamtwirtschaft nahm Corporate Trust in der Studie „Industriespionage" vor. Auf der Grundlage der Schadensangaben der betroffenen Unternehmen[44] kamen die Autoren der Studie 2007 zu dem Ergebnis, dass der deutschen Wirtschaft durch WS/KA ein Gesamtschaden von ca. 2,8 Milliarden Euro entstand[45] (vgl. CT 2007: 17). Leider ist auch hier unklar, für welchen Zeitraum die Gesamtschadensangabe gültig ist. Die Verfasser der 2012 erschienenen Folgestudie schlossen nach den Angaben der Unternehmen[46] auf einen jährlichen Schaden in Höhe von 4,2 Milliarden Euro für die deutsche Wirtschaft[47] (vgl. CT 2012: 55), was in 2012 ca. 0,16 Prozent des deutschen BIP ausgemacht hätte (vgl. Statistisches Bundesamt 2014: 1). Dabei gab ca. jedes zweite Unternehmen an, dass der Schaden unter 100.000 Euro lag und ca. jedes fünfte Unternehmen konnte den Schaden durch WS/KA auf zwischen 100.000 und einer Million Euro beziffern.

[43] Geschädigte Unternehmen beziffern einen Schaden in Höhe von 52 Millionen Euro. Dieser wird auf alle 400 befragten Unternehmen hochgerechnet (= 110 Millionen Euro). Der Umsatz der befragten Unternehmen entspricht 1/10 des BIP Baden-Württembergs (10 x 110 Millionen = 1,1 Milliarden Euro Schaden für Baden-Württemberg). Baden-Württemberg macht ca. 1/7 des BIP Deutschlands aus (7 x 1,1 Milliarden = 7,7 Milliarden Euro Schaden für Deutschland) (vgl. Sicherheitsforum 2004: 60).

[44] Ca. 64 Prozent der geschädigten Unternehmen hatten einen finanziellen Schaden zu verzeichnen (vgl. Corporate Trust 2007: 17).

[45] Schäden der betroffenen Unternehmen werden anhand des prozentualen Anteils der Unternehmen auf ca. 65.000 Unternehmen in Deutschland hochgerechnet (vgl. Corporate Trust 2007: 17).

[46] Ca. 83 Prozent der geschädigten Unternehmen hatten einen finanziellen Schaden zu verzeichnen (vgl. Corporate Trust 2012: 55).

[47] Für die Befragung wurden nur Unternehmen mit mind. 10 Mitarbeitern bzw. einem jährlichen Umsatz über einer Million Euro ausgewählt. Für Deutschland ergibt sich eine Referenzgröße von ca. 65.000 Unternehmen. Schäden der betroffenen Unternehmen wurden anhand des prozentualen Anteils auf die zu referierenden 65.000 Unternehmen hochgerechnet und der Gesamtschaden anschließend bereinigt (vgl. Corporate Trust 2012: 19).

Etwa 10 Prozent der geschädigten Unternehmen verzeichneten durch WS/KA sogar einen Schaden von mehr als einer Million Euro (vgl. CT 2012: 20).

Auch in der KPMG-Studie „Wirtschaftskriminalität“ von 2013 errechneten die Wissenschaftler einen Gesamtschaden für Deutschland auf der Grundlage der von den Unternehmen gemachten Angaben. Wirtschaftskriminelle Handlungen (darunter fielen auch Ausforschungshandlungen wie Datendiebstahl und Verrat von Geschäfts- und Betriebsgeheimnissen) kosteten ein Unternehmen pro Jahr durchschnittlich ca. 320.000 Euro. Der durchschnittliche Schaden pro Einzelfall lag bei ca. 30.000 Euro. Der deutschen Wirtschaft entsteht somit hochgerechnet ein jährlicher Schaden durch *Wirtschaftskriminalität* in Höhe von ca. 20 Milliarden Euro (vgl. KPMG 2013b: 35). Berücksichtigt man, dass darin auch der finanzielle Schaden durch Korruption, Diebstahl und andere wirtschaftskriminelle Handlungen eingeschlossen war, dann lag der Schaden, der alleine von Ausforschungshandlungen ausging (deutlich) unter den errechneten 20 Milliarden Euro und war somit auch in dieser Studie recht weit entfernt von den 50 bis 100 Milliarden Euro, die häufig in den Medien genannt werden.

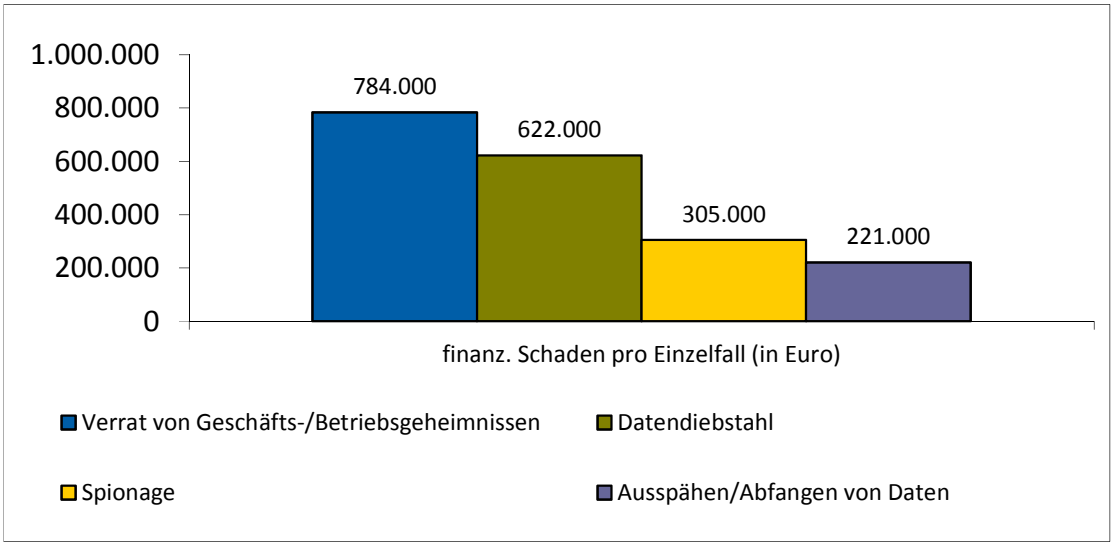
Der österreichischen Wirtschaft entsteht durch WS/KA ein hochgerechneter jährlicher Schaden von rund 880 Millionen Euro (vgl. BVT 2010: 4), was in 2010 ca. 0,31 Prozent des österreichischen BIP ausgemacht hätte (vgl. Eurostat 2014: 1). Rund jedes zweite betroffene österreichische Unternehmen gab an, dass der durchschnittliche Schaden von Ausforschung unter 100.000 Euro liegt. Ein Drittel verzeichnete Schäden zwischen 100.000 und 500.000 Euro und ca. jedes fünfte geschädigte Unternehmen gab an, dass Angriffe zu Ausforschungszwecken für Schäden von über 500.000 Euro verantwortlich waren (vgl. BVT 2010: 8).

Finanzieller Schaden pro Einzelfall einer Deliktsform

In der e-Crime-Studie 2010 von KPMG wurde auf der Grundlage der Aussagen der geschädigten Unternehmen der durchschnittliche Schaden pro *Einzelfall* in bestimmten Deliktsformen berechnet (vgl. Abbildung 5). Wurde ein Unternehmen Opfer von WS/KA, führte dies zu einem durchschnittlichen Schaden von 305.000 Euro *pro Vorfall* und ausgespähte oder abgefangene Daten führten zu einem durchschnittlichen Schaden von 221.000 Euro pro Vorfall. Bei einem Datendiebstahl entstand im Durchschnitt ein Schaden von 622.000 Euro und ein

Fall von Verrat von Geschäfts- und Betriebsgeheimnissen verursachte sogar einen durchschnittlichen Schaden von 784.000 Euro (vgl. KPMG 2010a: 18 f.).

Abbildung 5: Durchschnittlicher Schaden pro Einzelfall einer bestimmten Deliktsform



Quelle: Eigene Darstellung nach KPMG 2010a: 18.

In der Folgestudie von 2013 konnten die Unternehmen lediglich angeben, welchen Anteil die Ermittlungs- und Folgekosten am durchschnittlichen Gesamtschaden pro Deliktstyp einnahmen. Die Ermittlungs- und Folgekosten lagen im Durchschnitt aller e-Crime-Deliktstypen bei ca. 100.000 Euro pro Fall und sie verursachten ein Viertel des durchschnittlichen Gesamtschadens. Im Deliktsbereich Ausspähen/Abfangen von Daten machten sie 19 Prozent, bei Datendiebstählen 17 Prozent und bei Fällen von Verrat von Geschäfts- und Betriebsgeheimnissen 12 Prozent des Gesamtschadens aus (vgl. KPMG 2013a: 22).

In der SiFo-Studie des Sicherheitsforums Baden-Württemberg bezifferten die geschädigten Unternehmen den finanziellen Schaden pro Fall von „Verrat von Geschäfts- und Betriebsgeheimnissen“ im Durchschnitt mit 171.000 Euro und somit deutlich niedriger als in der e-Crime Studie 2010 von KPMG, laut deren Ergebnisse der Verrat von Geschäfts-/Betriebsgeheimnissen die kostenintensivste Form von Ausforschung war und ein Vorfall zu einen durchschnittlichen Schaden von 784.000 Euro führte. Allerdings verzeichneten forschungsintensive Unternehmen in der SiFo-Studie einen durchschnittlich höheren Schaden – pro Fall von Verrat von Geschäfts- und Betriebsgeheimnissen entsteht ihnen ein Schaden in Höhe von 259.000 Euro. Etwa jedes fünfte geschädigte Unternehmen bewertete diese Kosten als beträchtlich für das Unternehmen, was zeigt, dass die aus Ausforschung resultieren-

den finanziellen Verluste Unternehmen empfindlich treffen können (vgl. Sicherheitsforum 2010: 48).

Im Vergleich mit anderen wirtschaftskriminellen Handlungen verursachten Wettbewerbsdelikte, zu denen die Verfasser der PwC-Studie u. a. den Diebstahl vertraulicher Kunden- und Unternehmensdaten und WS/KA zählten, den Unternehmen besonders hohe finanzielle Schäden. So machten Wettbewerbsdelikte zwar nur ca. ein Drittel der identifizierten wirtschaftskriminellen Vorfälle aus, sie waren aber für den Großteil der angegebenen finanziellen Schäden verantwortlich: Lag der durchschnittliche Schaden pro Unternehmen bezogen auf *alle* wirtschaftskriminellen Delikte bei ca. drei Millionen Euro, so belief er sich *allein* bei den Wettbewerbsdelikten auf ca. 20 Millionen Euro pro Unternehmen (vgl. PwC 2013: 68).

5.3.4 Zusammenfassung Schäden

- Die Ausforschung deutscher Unternehmen schadet nicht nur dem jeweils betroffenen Unternehmen, sondern sie kann sich auch negativ auf die deutsche **Gesamtwirtschaft** auswirken. So sind jährlich über 50.000 Arbeitsplätze mittelbar durch WS/KA gefährdet.
- Die möglichen negativen Auswirkungen eines Angriffs zu Ausforschungszwecken auf ein Unternehmen können sehr vielfältig sein. Ein betroffenes Unternehmen kann **direkte finanzielle Schäden** (z. B. Ermittlungskosten) verzeichnen und/oder **immaterielle Schäden** (z. B. Imageschäden), die den finanziellen Schaden indirekt erhöhen können.
- Unternehmen, die Opfer von Ausforschung wurden, verzeichneten häufiger immaterielle Schäden als direkte Umsatzeinbußen.
- Die Schäden, die der deutschen Wirtschaft durch Ausforschung entstehen, werden in der Öffentlichkeit (von politischen und wirtschaftlichen Entscheidungsträgern, Presse etc.) mehrheitlich als sehr bedeutsam **eingeschätzt**. In der Presse finden sich regelmäßig Schadensschätzungen zwischen 20 bis 100 Milliarden Euro. Auch viele Unternehmen gingen davon aus, dass der jährliche finanzielle Schaden für die deutsche Wirtschaft mehr als 10 Milliarden Euro beträgt. Jedoch beruhen solche Schätzungen häufig nicht auf verlässlichen Zahlen und sollten deswegen eher **kritisch** bewertet werden.
- **Hochrechnungen** auf die Gesamtwirtschaft auf der Grundlage der Schadensangaben der Unternehmen ergaben Schadenshöhen, die zwischen jährlich 2,8 Milliarden und deutlich unter 20 Milliarden Euro liegen und somit weit niedriger sind als die in den Medien oder

den Unternehmen genannten Schätzungen. Die Hochrechnungen stehen in keinem Verhältnis zu den Schätzungen, die sich in den Medien finden oder den Schätzungen der Unternehmen selbst, sie liegen zum Teil zehn- bis zwanzigmal niedriger. In manchen Studien wurde nicht der gesamtwirtschaftliche Schaden, sondern der durchschnittliche Schaden für ein Unternehmen pro **Vorfall** beziffert.

- Unternehmen wurden nur in wenigen Studien aufgefordert, den finanziellen Schaden durch Ausforschung zu beziffern. Da den Unternehmen für die **Schadensberechnung** oft keine einheitliche Grundlage zur Verfügung stand und es diesbezüglich auch kaum Vorgaben in den Befragungen gab, konnten viele die Höhe des finanziellen Schadens nicht richtig beziffern. Die errechneten Schadenshöhen sollten somit nicht als feste Größen, sondern eher als Anhaltspunkte verstanden werden.
- Dennoch bieten die Schadensangaben aus **Unternehmensbefragungen** bei methodisch sauberem Vorgehen eine gute Möglichkeit, um eine Berechnungsgrundlage für die Gesamtwirtschaft zu schaffen.

5.4 Täter

5.4.1 Festgestellte Täter

Bei WS/KA ist es oft schwer, den oder die Täter sofort und eindeutig zu bestimmen. Dies ist vor allem bei der Ausforschung über das Internet der Fall (vgl. KPMG 2013a: 24). In der Fachliteratur geht man davon aus, dass ein großer Teil der Angriffe zu Ausforschungszwecken auf deutsche Unternehmen – bei manchen Autoren bis zu 90 Prozent der Angriffe (vgl. Blume 2008: 34) – von Wettbewerbern, Kunden und Lieferanten erfolgt und nur ein geringer Teil von ausländischen Nachrichtendiensten durchgeführt wird. Diese Einschätzung kann sich aber im Zuge der NSA Überwachungs- und Spionageaffäre und den Enthüllungen durch Edward Snowden ändern und es ist daher wahrscheinlich, dass auch Unternehmen ausländische Nachrichtendienste vermehrt als Bedrohung wahrnehmen werden.

In den meisten Befragungen wurden am häufigsten aktuelle bzw. ehemalige Mitarbeiter als Täter identifiziert. In mehreren Studien konnten die befragten Unternehmen nationale und internationale Wettbewerber als zweithäufigste Tätergruppe feststellen. Weitere häufig ge-

nannte Tätergruppen waren Kunden, Lieferanten und Kooperationspartner und somit Personen, die den Unternehmen persönlich bekannt waren. Ausländische Nachrichtendienste wurden in vielen Studien nur zu einem geringen Teil als Angreifer identifiziert.

Nicht alle Angriffe zu Ausforschungszwecken auf und über IKT lassen sich ausschließlich von außerhalb durchführen, viele brauchen zusätzlich die wissentliche oder unwissentliche Unterstützung von Innentätern (vgl. Huber 2009: 40). In vielen Fällen arbeiten externe Täter mit willigen Unternehmensangehörigen zusammen oder sie versuchen mit Hilfe von Social Engineering über Mitarbeiter an wichtiges internes Know-how zu gelangen. Weitere Möglichkeiten, wie Mitarbeiter unbewusst zu Tätern werden können, sind der Verlust von mobilen elektronischen Endgeräten oder die leichtfertige Weitergabe von internen Informationen auf Reisen oder in sozialen Netzwerken (vgl. CT 2012: 8). Sie können aber auch aus eigener Motivation das Unternehmen ausforschen und mit Unternehmensinterna an Wettbewerber herantreten (vgl. Sicherheitsforum 2010: 22). Eigene Mitarbeiter können somit beabsichtigt und unbeabsichtigt zu Tätern werden.

Aufgrund gesellschaftlicher Veränderungen kann davon ausgegangen werden, dass aktuelle oder ehemalige Mitarbeiter weiterhin eine wichtige und sogar zunehmende Rolle beim Verlust von sensiblem Know-how spielen werden: die Anzahl der Zeitarbeiter in Unternehmen nimmt zu und es kann angenommen werden, dass sich viele von ihnen weniger stark mit dem Unternehmen identifizieren als fest angestellte Mitarbeiter. Das Gleiche gilt für unbezahlte „ewige“ Praktikanten (vgl. Huber 2009: 40). Eine geringe Identifizierung mit dem Arbeitgeber und dadurch häufig bedingt ein geringeres Verantwortungsbewusstsein können teilweise erklären, warum Mitarbeiter zu Tätern werden.

In der CT-Studie von 2012 waren eigene Mitarbeiter in 58 Prozent aller Fälle mittelbar oder unmittelbar an der Ausforschung des Unternehmens beteiligt. Bei ca. jedem vierten Ausforschungsvorfall konnten die Unternehmen konkurrierende nationale oder internationale Unternehmen identifizieren und an ca. jedem fünften Vorfall waren Kunden oder Lieferanten beteiligt. Ausländische Nachrichtendienste konnten nur in 14 Prozent[48] der Fälle als Täter festgestellt werden (vgl. CT 2012: 27).

[48] Mehrfachnennungen möglich.

Auch in der Studie des österreichischen BVT spielten eigene Mitarbeiter in der Mehrheit der Vorfälle eine zentrale Rolle. Rund die Hälfte der ausgeforschten Unternehmen gab an, dass die Täter ehemalige Mitarbeiter waren, die beim Wechsel des Arbeitgebers sensibles Know-how zur Konkurrenz mitgenommen haben. Bei 9 Prozent der von WS/KA betroffenen Unternehmen waren aktive Mitarbeiter für die Ausforschung verantwortlich. Inländische und ausländische Konkurrenten konnten ebenfalls von beinahe jedem zweiten betroffenen Unternehmen[49] identifiziert werden. Nur rund 2 Prozent der geschädigten Unternehmen konnten einen ausländischen Nachrichtendienst als Urheber des Spionageangriffs erkennen (vgl. BVT 2010: 8 f.).

Das Sicherheitsforum Baden-Württemberg kam ebenfalls zu dem Ergebnis, dass vor allem Unternehmensangehörige zu den Tätern bei Ausforschung gehörten. Sie handelten aus eigener Motivation, wurden durch Konkurrenten oder ausländische Nachrichtendienste aktiv angeworben oder von diesen durch Social Engineering manipuliert (vgl. Sicherheitsforum 2010: 22). So gaben die geschädigten Unternehmen an, dass über 70 Prozent der Täter aus den eigenen Reihen kamen. Sie verteilten sich über alle Positionen und Ränge im Unternehmen. Nationale und internationale Wettbewerber konnten hingegen nur in ca. jedem fünften Vorfall festgestellt werden. Auch in dieser Studie spielten ausländische Nachrichtendienste lediglich eine untergeordnete Rolle – sie konnten nur in 6 Prozent der Angriffe als Täter identifiziert werden. Ferner zeigen die Ergebnisse der Studie, dass zwischen den geschädigten Unternehmen und den Tätern im Vorfeld der Ausforschung sehr häufig irgendeine Art von Geschäftsbeziehung existierte und dass sich dadurch in 90 Prozent der Fälle Täter und Opfer vor der Tat kannten (vgl. Sicherheitsforum 2010: 67 f.).

In der Befragung von E&Y von 2013 identifizierten jeweils 45 Prozent der betroffenen Unternehmen aktuelle und ehemalige Mitarbeiter sowie konkurrierende ausländische Unternehmen als Täter. Etwa ein Viertel der Unternehmen nannte ausländische oder inländische Kunden/Lieferanten als Täter (vgl. E&Y 2013: 21).[50]

In der Studie der Europäischen Kommission identifizierten deutsche Firmen etwas häufiger als andere europäische Firmen aktuelle und ehemalige Mitarbeiter als Täter (D: ca. 67 Prozent, EU: ca. 64 Prozent). Zudem nannten deutsche Unternehmen deutlich häufiger als europäische Unternehmen Wettbewerber als Täter (D: ca. 67 Prozent, EU: ca. 53 Prozent). Dafür spielten im europäischen Durchschnitt die Kunden eine deutlich größere Rolle

[49] Mehrfachnennungen möglich.
[50] Mehrfachnennungen möglich.

bei Ausforschung als in Deutschland (D: ca. 11 Prozent, EU: ca. 31 Prozent). Somit bestätigt auch der europäische Vergleich, dass die größte Gefahr für ein Unternehmen von den eigenen aktuellen oder ehemaligen Mitarbeitern ausgeht, gefolgt von nationaler/internationaler Konkurrenz sowie Kunden, Zulieferern und Kooperationspartnern. Hauptverantwortlich für den Know-how-Abfluss waren somit auch im europäischen Vergleich unternehmensnahe Täter (vgl. Europäische Kommission 2013b: 21).

Auch in der KPMG e-Crime-Studie von 2010 wurde die wichtige Rolle von eigenen Mitarbeitern bei der Ausforschung des Unternehmens betont. Sie machten bei Datendiebstahl und bei Verletzungen von Geschäfts- oder Betriebsgeheimnissen jeweils 62 Prozent der Täter aus. Bei anderen e-Crime-Handlungen lag der Anteil eigener Mitarbeiter bei 48 Prozent. Auch bei e-Crime-Handlungen konnte der Täter somit häufig im unmittelbaren Umfeld des Unternehmens gefunden werden (vgl. KPMG 2010a: 13).

Auch wenn ausländische Nachrichtendienste nur selten von den Unternehmen als Angreifer identifiziert werden konnten, bedeutet das jedoch nicht, dass sie nicht ebenfalls in die Ausforschung deutscher Unternehmen involviert sind. Man kann davon ausgehen, dass sie aufgrund einer besseren finanziellen und materiellen Ausstattung professioneller vorgehen und deswegen seltener als Täter erkannt werden (vgl. Schaaf 2009: 23). Zudem muss bedacht werden, dass bereits identifizierten Tätern nicht immer eine Verbindung zu einem ausländischen Nachrichtendienst nachgewiesen werden kann (vgl. Glitza 2012: 118).

5.4.2 Herkunft der Täter

Laut Verfassungsschutz geht Wirtschaftsspionage vor allem von russischen und chinesischen Nachrichtendiensten aus (vgl. George 2013: 24 und BMI 2013b: 382 ff.). Es sollte aber nicht ausgeschlossen werden, dass auch Nachrichtendienste westlicher Staaten deutsche Unternehmen ausspionieren. So kann angenommen werden, dass auch von der US-amerikanischen NSA, dem britischen GCHQ (vgl. Peil 2013: 14) und den französischen Geheimdiensten Wirtschaftsspionage gegen deutsche Unternehmen betrieben wird (vgl. Le Figaro 2011).

Die Mehrheit der befragten Unternehmen vermutete, dass Wirtschaftsspionage und Konkurrenzausspähung hauptsächlich von Nachrichtendiensten und Unternehmen aus China, anderen asiatischen Ländern, den USA und Russland ausgehen (vgl. E&Y 2011: 6, E&Y

2013: 15, KPMG 2013a: 23). In der CT-Studie von 2012 und in der SiFo-Studie des Sicherheitsforums Baden-Württemberg sollten die Unternehmen Angaben zu der Herkunft der festgestellten Täter machen. Überraschenderweise war hier der Anteil der chinesischen und asiatischen Täter im Vergleich zu anderen Nationalitäten relativ gering (vgl. Sicherheitsforum 2010: 64 und CT 2012: 17). Z. B gaben in der SiFo-Studie ca. 70 Prozent der Unternehmen an, dass deutsche Täter am illegalen Abfluss von Geschäfts- und Betriebsgeheimnissen beteiligt waren. Lediglich etwa jedes fünfte Unternehmen konnte einen Täter aus Asien identifizieren (vgl. Sicherheitsforum 2010: 65).

Diese Angaben zeigen, dass Angreifer aus Deutschland nicht unterschätzt werden sollten und dass nicht nur ausländische Konkurrenz Industriespionage betreibt. Auch deutsche Unternehmen können sich gegenseitig ausforschen. Zudem sollte nicht außer Acht gelassen werden, dass von der (deutschen) Nationalität der Tatausführenden nicht unbedingt auf die Nationalität der Auftraggebenden geschlossen werden kann. Auf der Grundlage dieser Ergebnisse kann somit auch nicht unterstellt werden, dass Täter aus China oder dem restlichen Asien tatsächlich eine untergeordnete Rolle bei der Ausforschung deutscher Unternehmen spielen. Es ist z. B. denkbar, dass Angriffe aus Asien besonders professionell durchgeführt und deswegen seltener von den Unternehmen entdeckt werden.

5.4.3 Motive

Am ausführlichsten wurden die Motive interner Täter für Ausforschung in der SiFo-Studie des Sicherheitsforums Baden-Württemberg beschrieben. Als wichtigster Grund für die Weitergabe von unternehmensinternem Know-how konnten bei Einzeltätern und bei Tätern, die durch Dritte angeheuert wurden, finanzielle und materielle Anreize gesehen werden. Die betroffenen Unternehmen gaben an, dass dies der Hauptgrund in ca. 80 Prozent der Fälle von Verrat von Geschäfts- und Betriebsgeheimnissen war. Die Befragten übten zudem Kritik an den unternehmenseigenen Sicherheitsvorkehrungen: in 77 Prozent der Fälle konnten unzureichende interne Kontrollen als wichtigste Motivation des internen Täters identifiziert werden. In zwei Drittel der Fälle spielte auch berufliche Enttäuschung eine wichtige Rolle für den Verrat von Unternehmensinterna. Bei jedem dritten Fall wurde der interne Täter bestochen oder erpresst. Ideologische Überzeugungen oder persönliche Bindungen wurden von Unternehmen nur selten als Tatgrund festgestellt (vgl. Sicherheitsforum 2010: 68 f.).

In der E&Y-Studie von 2013 vermutete jedes zweite Unternehmen, dass Angreifer das Ziel verfolgen, sich einen Wettbewerbsvorteil zu verschaffen. Ca. 40 Prozent der Unternehmen konnten als Motivation das Erlangen eines finanziellen Vorteils erkennen und etwa jedes zehnte betroffene Unternehmen ging davon aus, dass eigene Mitarbeiter durch Unwissenheit zu einem Abfluss von geheimem Unternehmens-Know-how beigetragen haben (vgl. E&Y-2013: 24).

Ist ein Mitarbeiter bereit, dem Unternehmen durch Ausforschung Schaden zuzufügen (z. B. durch den Verkauf von sensiblem Unternehmens-Know-how aufgrund persönlichem finanziellen Druck), sieht er sein Handeln als gerechtfertigt an (krisenbedingte Entlassung wird als unfair empfunden) und bietet sich ihm schließlich die Gelegenheit dazu (leichter Zugriff auf sensible Daten, da fehlende interne Kontrolle), sind alle drei Voraussetzungen (Motivation, Rechtfertigung und Gelegenheit) des sogenannten Betrugs-Dreiecks („Fraud Triangle“)[51]erfüllt und die Wahrscheinlichkeit, dass der Mitarbeiter zur Tat schreitet, ist zumindest aus theoretischer Sicht relativ hoch (vgl. KPMG 2010a: 15).

5.4.4 Zusammenfassung Täter

- Bei Ausforschung ist es oft schwer, einen Täter sofort und eindeutig zu bestimmen. Dies ist vor allem bei der Ausforschung über das Internet der Fall.
- In den meisten Befragungen wurden am häufigsten aktuelle bzw. ehemalige **Mitarbeiter** als Täter identifiziert. Diese arbeiteten absichtlich mit externen Tätern zusammen oder sie wurden über **Social Engineering** unbeabsichtigt zu Mittätern.
- Nationale und internationale **Wettbewerber** wurden des Öfteren als zweithäufigste Tätergruppe festgestellt.
- Häufig bestand zwischen geschädigtem Unternehmen und Tätern im Vorfeld der Ausforschung irgendeine Art von **Geschäftsbeziehung** (Mitarbeiter, Kunden, Lieferanten, Partner).
- **Ausländische Nachrichtendienste** konnten nur selten als Angreifer identifiziert werden. Dies bedeutet jedoch nicht, dass sie nicht auch versuchen würden, an Know-how aus deutschen Firmen zu gelangen. Vielmehr ist nicht auszuschließen, dass sie aufgrund einer besseren finanziellen und materiellen Ausstattung professioneller vorgehen und deswegen seltener als Täter erkannt werden. Laut Verfassungsschutz geht Wirtschaftsspionage vor

[51] Theorie entwickelt von Donald Ray Cressey (vgl. Cressey 1973: 30).

allem von russischen und chinesischen Nachrichtendiensten aus, es sollte aber nicht ausgeschlossen werden, dass auch Nachrichtendienste westlicher Staaten spionieren.

- Die Gefahr, die von **deutschen Wettbewerbern** ausgeht, sollte nicht unterschätzt werden.
- Zu den **Gründen**, die die Weitergabe von unternehmensinternem Know-how begünstigten, zählten u. a. finanzielle und materielle Anreize, unzureichende interne Kontrollen, berufliche Enttäuschung, Erpressung oder Bestechung.
- Sind alle drei Voraussetzungen des **Betrug-Dreiecks** erfüllt (Motivation, Rechtfertigung und Gelegenheit), ist die Wahrscheinlichkeit hoch, dass ein Mitarbeiter seinem Unternehmen, z. B. durch das Weiterleiten von unternehmensinternen Daten an Dritte, Schaden zufügt.

5.5 Sicherheitsvorkehrungen der Unternehmen

Viele Unternehmen in Deutschland verfügen über Spitzentechnologie von wegweisender globaler Marktbedeutung. Wie bereits gezeigt, stehen nicht nur große Unternehmen, sondern auch KMU im Fokus der nationalen und internationalen Konkurrenz und von ausländischen Nachrichtendiensten. Manche KMU stehen auch aufgrund ihrer Funktion als Technologielieferanten für große Unternehmen im Fokus von Ausforschungsaktivitäten (vgl. Bernd-Striebeck 2012: 18).

Ein effektiver Schutz vor Ausforschung erscheint vielen Unternehmen wie der sprichwörtliche „Kampf gegen Windmühlenflügel“: Häufig sind eigene Mitarbeiter am Know-how-Verlust beteiligt und technische Entwicklungen und Prozesse bieten Angreifern neue Möglichkeiten, um Unternehmen auszuforschen. Zwar ist maximale Sicherheit nicht praktikabel, das soll aber nicht als Grund gesehen werden, überhaupt keine Sicherheitsvorkehrungen zu treffen, da sonst die Existenz eines Unternehmens gefährdet ist (vgl. Litzcke 2010: 76). Es gibt eine Reihe von sehr effektiven Möglichkeiten, das eigene Unternehmen zu schützen und es Angreifern so schwer wie möglich zu machen. Die Autoren des Verizon Data Breach Investigations Report 2011 fanden heraus, dass 96 Prozent der „data breaches“[52] mit Hilfe einfacher Sicherheitsvorkehrungen vermeidbar gewesen wären (vgl. Verizon 2011: 3 und 65 ff.).

[52] Gemeint sind Datenkompromittierungen durch Angriffsformen wie Cyber-Ausforschung, Hacking, Malware etc.

In der Fachliteratur wird häufig kritisiert, dass es vielen deutschen Unternehmen an ausreichenden präventiven Maßnahmen, die Ausforschungsvorfälle deutlich erschweren würden, fehlt (vgl. Leiner 2008: 40). Vor allem das IT-Sicherheitsniveau vieler KMU in Deutschland ist demnach stark verbesserungsbedürftig (vgl. BMWi 2012: 9). Deswegen werden Unternehmen regelmäßig aufgefordert, mehr für die Abwehr von Ausforschung zu tun. Sie sollten nicht abwarten, bis es tatsächlich zu einem Know-how-Verlust kommt, sondern eine Vielzahl präventiver Maßnahmen ausschöpfen und diese auch ständig weiterentwickeln, hinterfragen, begutachten und wenn nötig verbessern (vgl. Proschko 2010: 19).

Dabei wird stets betont, dass eine verlässliche Abwehr nur durch einen *ganzheitlichen* Ansatz, also durch ein integriertes Know-how-Schutzkonzept sichergestellt werden kann, der zugleich Technik, Prozesse und Mitarbeiter umfasst.[53] Die Sicherheitsmaßnahmen aus diesen drei Bereichen sollen sich gegenseitig ergänzen. Gleichzeitig sollte Informationsschutz ein wichtiger Bestandteil der Unternehmensstrategie sein (vgl. Proschko 2010: 19). Um einen dauerhaften Schutz darstellen zu können, sollten präventive Maßnahmen gegen Ausforschung eine langfristige Perspektive verfolgen (vgl. Litzcke 2010: 78).

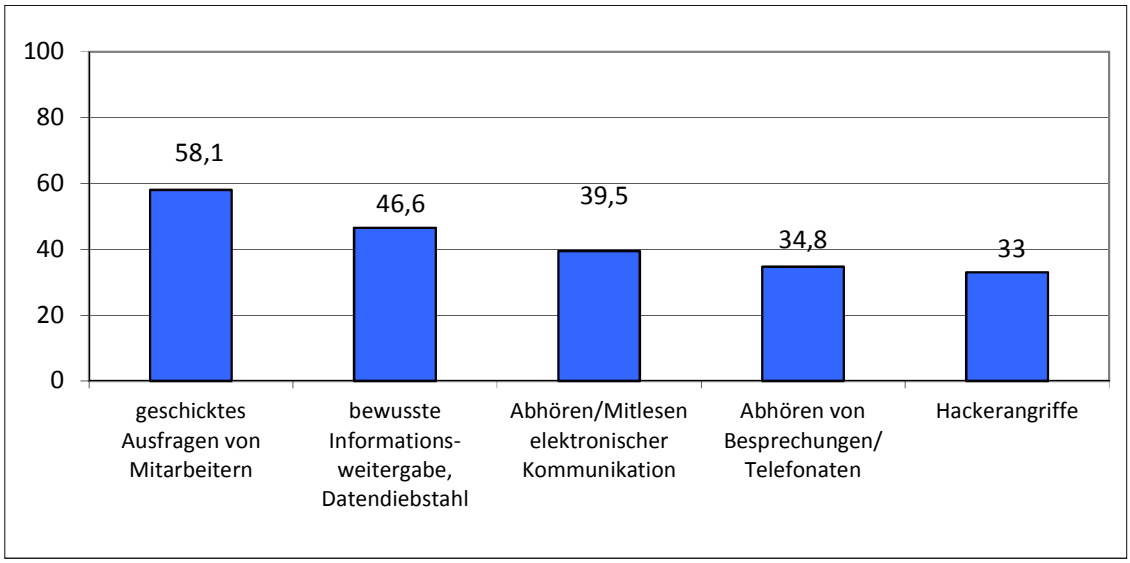
Bevor ein Unternehmen aber über adäquate Sicherheitsvorkehrungen in den verschiedenen Unternehmensbereichen entscheidet, sind mehrere vorbereitende Schritte notwendig. Als erstes sollte im Unternehmen im Rahmen einer Schutzbedarfsanalyse Klarheit darüber geschaffen werden, welches spezielle Know-how für den eigenen Wettbewerbsvorteil/-vorsprung ausschlaggebend ist und an welchen Stellen im Unternehmen es sich befindet (beispielsweise Produktionsprozesse, Arbeitsmethoden, Kunden-/Lieferantenbeziehungen, Strategien, Fertigkeiten etc.) (vgl. Sicherheitsforum 2004: 4 f., Leiner 2008: 40). Bei vielen Unternehmen gehören etwa fünf Prozent aller Daten zum schutzwürdigen Kern-Know-how und sind für das Unternehmen überlebenswichtig. Dagegen sind etwa 80 Prozent aller Informationen frei verfügbar und benötigen keinen besonderen Schutz (vgl. George 2013: 24). Ferner sollte das Unternehmen wissen, wie und wo dieses erfolgskritische Know-how gespeichert ist, wer Zugriff darauf hat und welche Kommunikationswege es nimmt (vgl. Bernd-Striebeck 2012: 18). Es ist nicht notwendig, dass für alle Informationen das gleiche Sicherheitsniveau gilt, vielmehr sollten sich die Schutzmaßnahmen an der Vertraulichkeit der jeweiligen Informationen orientieren (vgl. CT 2012: 32). In einem zweiten Schritt sollte das

[53] Vgl. u. a. Arends/Kranawetter 2011: 52, Bätz/Claaßen 2009: 46, Bernd-Striebeck 2012: 1, Blume 2008: 34, Litzcke 2010: 78, Proschko 2010: 19.

Unternehmen dokumentieren, welche Sicherheitsmaßnahmen gegen Ausforschung in den verschiedenen Unternehmensbereichen bereits implementiert wurden. In einem dritten Schritt muss geprüft werden, ob sich diese Sicherheitsmaßnahmen bewährt haben. Auf dieser Grundlage können im Anschluss mehrere Handlungsempfehlungen für die verschiedenen Bereiche formuliert werden, in einem Maßnahmenkatalog zusammengefasst und nach Priorität geordnet werden (vgl. Bernd-Striebeck 2012: 18).

In mehreren Studien sollten die Befragten einschätzen, ob die eigenen präventiven Sicherheitsvorkehrungen gegen Ausforschung aus der Sicht des Unternehmens ausreichend sind. Exemplarisch werden hier die Ergebnisse der CT-Studie von 2012 präsentiert. Es fällt auf, dass zum Teil deutlich mehr als jedes dritte Unternehmen die eigenen Sicherheitsvorkehrungen als nicht ausreichend einstufte (vgl. Abbildung 6).

Abbildung 6: Selbsteinschätzung zu unternehmensinternen Schutzvorkehrungen



Unternehmen (in Prozent), die die eigenen Schutzvorkehrungen für bestimmte Bedrohungen als nicht ausreichend einstuften. Quelle: Eigene Darstellung nach Corporate Trust 2012: 52.

Mehr als 90 Prozent der Unternehmen nannten *mehrere* Bedrohungen, für die keine ausreichenden Schutzvorkehrungen existierten, und bei jeder dieser Bedrohungen hält sich mindestens ein Viertel der Unternehmen für angreifbar (vgl. CT 2012: 52). Diese Selbsteinschätzung verdeutlicht anschaulich die Gefährdungslage der deutschen Wirtschaft.

Im Folgenden wird aufgezeigt, welche Maßnahmen zur Abwehr von Ausforschung die befragten Unternehmen getroffen haben und ob sie aus Sicht der für die Studien verantwortli-

chen Institutionen ausreichen. Der Schwerpunkt liegt hierbei eher auf präventiven als auf repressiven Maßnahmen, da ihnen eine besondere Bedeutung zukommt: Ist kritisches Unternehmens-Know-how erst einmal abgeflossen, ist es oftmals schwierig, einen weiteren Missbrauch mit den gestohlenen Informationen zu verhindern oder einen angemessenen Ersatz für den Schaden zu erwirken (vgl. Blume 2008: 34). Es werden hauptsächlich die Ergebnisse aus Studien präsentiert, in denen die Unternehmen speziell nach Maßnahmen zur Abwehr von Ausforschung und nicht allgemein zum Schutz vor Wirtschaftskriminalität oder Cybercrime befragt wurden.

5.5.1 Strukturelle und organisatorische Maßnahmen

In vielen Studien wurde empfohlen, den Know-how-Schutz nicht ausschließlich bei der IT-Abteilung zu verorten. Obwohl Ausforschung zunehmend über Kommunikations- und Informationstechnologien und das Internet stattfindet, sollte nicht nur der IT-Bereich eines Unternehmens, sondern die gesamte Unternehmenssicherheit im Bereich der Abwehr von Ausforschung aktiv werden. Es besteht die Gefahr, dass Unternehmen den Schwerpunkt der Sicherheitsvorkehrungen zu stark auf Ausforschung über IT legen und dabei andere Bedrohungen, wie z. B. das Abschöpfen menschlicher Quellen vernachlässigen (vgl. Blume 2008: 33).

Die Verfasser mehrerer Studien kamen zu dem Ergebnis, dass nur wenige Unternehmen ein System der integrierten Unternehmenssicherheit implementiert haben. So zeigen die Ergebnisse der E&Y-Studien 2011 und 2013, dass bei rund drei Viertel der Unternehmen lediglich die IT-Abteilung für die Abwehr von Ausforschung zuständig war.

Ferner sollten sich die Verantwortlichkeiten und Aufgaben innerhalb eines Unternehmens in einem Informationsschutzkonzept widerspiegeln. Den Beschäftigten sollte verständlich dargestellt werden, warum bestimmte Sicherheitsmaßnahmen implementiert werden und wie im Verdachtsfall gehandelt werden soll.

Die Ergebnisse der CT-Studie zeigen, dass 2012 lediglich 20 Prozent der Unternehmen über ein Informationsschutzkonzept verfügten (vgl. CT 2012: 42) und auch in der WIK-Sicherheits-Enquête 2011 gab nur etwa ein Drittel der Unternehmen an, über ein Know-how-Schutzkonzept zu verfügen. Rund jedes fünfte Unternehmen war sogar der Meinung, dass ein solches Schutzkonzept nicht gebraucht wird (vgl. WIK 2011/1: 5). In den Studien von

2011 und 2013 gab jeweils ca. ein Drittel der von E&Y befragten Unternehmen an, über ein Informationsschutzkonzept zu verfügen (vgl. E&Y 2013: 12). Zu einem ähnlichen Ergebnis kamen die Autoren der Studie des BMWi, nach der nur 37 Prozent der Unternehmen über schriftlich fixierte IT-Sicherheitsregeln verfügten und mehr als jedes zweite Unternehmen der Meinung war, dass dies nicht notwendig sei (vgl. BMWi 2012: 9). Ein deutlich größerer Anteil an Unternehmen mit einem Konzept für den Informationsschutz kann in der kes-Sicherheitsstudie festgestellt werden. Hier verfügten drei Viertel der befragten Unternehmen über eine schriftliche Strategie zur Informationssicherheit (vgl. kes 2012/5: 25).

Es ist wichtig, dass einem Unternehmen bewusst ist, welche die wichtigsten Daten im Unternehmen sind und dass diese besonders geschützt werden müssen. Diese wettbewerbsentscheidenden Daten sind die „Kronjuwelen" eines Unternehmens und von besonderem Interesse für die Konkurrenz. Die Daten sollten als geheim oder vertraulich gekennzeichnet werden, damit für alle Mitarbeiter, die Zugriff auf diese Daten haben, unmissverständlich klar ist, dass es sich um *interne* Informationen handelt (vgl. Leiner 2008: 40). Die Schutzbedarfsanalyse sollte als Ausgangspunkt für alle weiteren Anstrengungen im Bereich Informationssicherheit und als Grundlage für eine erfolgreiche Abwehr von Ausforschung gesehen werden.

Die Herausgeber der CT-Studie verweisen aber darauf, dass etwa 45 Prozent der Unternehmen keine Schutzbedarfsanalyse durchgeführt haben und sie somit häufig nicht genau bestimmen konnten, welche Informationen besonderen Schutz brauchen. Lediglich jedes fünfte Unternehmen hatte eine solche Analyse bereits durchgeführt und ein Viertel der Unternehmen war zum Erhebungszeitpunkt gerade mit der Erstellung beschäftigt (vgl. CT 2012: 32). Das BSI kommt in seiner Studie zur IT-Sicherheit in KMU zu einem ähnlichen Ergebnis: Lediglich die Hälfte der befragten Unternehmen hatte risikobehaftete Daten im Unternehmen identifiziert und klassifiziert (vgl. BSI 2011: 59).

Unternehmen sollten zudem über klare Regelungen verfügen, wie mit schützenswerten Informationen umgegangen werden soll bei Speicherung, Vervielfältigung, Weitergabe oder Vernichtung. Fehlen diese, besteht die Gefahr, dass Beschäftigte mit schützenswerten Daten nicht umsichtig genug umgehen bzw. solche Informationen böswillig weitergeben und sich im Nachhinein darauf berufen können, dass ihnen die Vertraulichkeit der Dokumente nicht klar gewesen sei.

Nach der CT-Studie 2012 hat nur ca. jedes dritte Unternehmen klare Regelungen verfasst, die bestimmen, wie mit sensiblen Informationen umgegangen werden soll (vgl. CT 2012: 42). In den von E&Y durchgeführten Studien lag der Anteil der Unternehmen mit klaren Regeln für den Umgang mit schützenswerten Informationen in 2011 und 2013 mit jeweils ca. 80 Prozent deutlich höher (vgl. E&Y 2013: 12).

Ferner wird empfohlen, dass Unternehmen in den verschiedensten Bereichen über Reaktionspläne verfügen, in denen festgelegt wird, wie im Notfall gehandelt und auf Ausforschungsversuche reagiert werden soll.

Zwei Drittel der Unternehmen haben solche Sicherheitsstandards mit Notfallplänen im Bereich IT-Sicherheit erstellt, lediglich ein Viertel im Bereich Informationsschutz (CT 2010: 20). Dadurch besteht die Gefahr, dass im Angriffsfall wichtige Zeit verlorengeht, in der weiterer Schaden von dem Unternehmen hätte abgewandt werden können.

Wie wirksam präventive Maßnahmen sind, hängt größtenteils davon ab, wie hoch die Entdeckungswahrscheinlichkeit ist. Folglich ist es wichtig, dass Kontrollmaßnahmen im Unternehmen allgemein bekannt sind, da sie die Wahrscheinlichkeit der Entdeckung einer Straftat aus subjektiver Sicht der Täter erhöhen (vgl. Sicherheitsforum 2010: 55).

5.5.2 Personelle Maßnahmen

Um sich effektiv vor Angriffen zu Ausforschungszwecken zu schützen, ist es wichtig, dass Unternehmen die eigenen Beschäftigten in die Sicherheitsstrategie einbeziehen und diese ausreichend für die Sicherheitsbelange der Firma sensibilisieren. Auf diese Weise kann bereits ein Großteil der Angriffe abgewehrt werden (vgl. Staron/Tempel 2014: 18). Schutzvorkehrungen in der IT, der Gebäudesicherheit oder im organisatorischen Bereich können nur in Kombination mit personellen Maßnahmen greifen.

Unternehmen können eine Vielzahl von präventiven Maßnahmen im personellen Bereich implementieren, z. B. indem Beschäftigte bereits bei der Einstellung sicherheitsüberprüft werden, sie hinsichtlich der Gefahren von Social Engineering sensibilisiert werden, Zugriffe und Zugänge beschränkt werden, die Entdeckungswahrscheinlichkeit von Ausforschung erhöht wird und im Falle eines Verstoßes gegen Unternehmensregeln strafrechtliche

und/oder betriebliche Sanktionen konsequent umgesetzt werden. Im Folgenden werden lediglich die Angaben der Unternehmen zu ausgewählten Schutzmaßnahmen vorgestellt.

Vor allem Bewerber auf Stellen in sensiblen Bereichen, wie z. B. die IT-Abteilung oder F&E, sollten vor der Einstellung bestimmte Verfahren durchlaufen, in denen sie Seriosität und Zuverlässigkeit unter Beweis stellen können.

80 Prozent der befragten Unternehmen in der CT-Studie integrierten Geheimhaltungsverpflichtungen in alle Arbeitsverträge, aber nur 6 Prozent führten Integritätstests für neue Mitarbeiter durch (vgl. CT 2012: 39). Auch in den E&Y Studien sicherte sich die große Mehrheit der Unternehmen (ca. neun von zehn Unternehmen) mit Geheimhaltungsverpflichtungen in den Arbeitsverträgen ab und etwa jedes fünfte Unternehmen führte Integritätstests für neue Bewerber durch (vgl. E&Y 2013: 11).

Häufig werden Mitarbeiter unbeabsichtigt zu Tätern, indem sie z. B. ohne es zu merken durch Social Engineering manipuliert werden oder indem sie unvorsichtig mit sensiblen Daten umgehen. Um diese Gefahren so gering wie möglich zu halten, ist es notwendig, dass die Beschäftigten eines Unternehmens für die Gefahren von Ausforschung sensibilisiert werden und dass sie ein Bewusstsein für Social Engineering und die Richtungen, aus denen Angriffe kommen können, entwickeln (vgl. Niemantsverdriet 2011: 27).

74 Prozent der in der CT-Studie von 2012 befragten Unternehmen gaben an, dass es für ihre Beschäftigten keine regelmäßigen Schulungen gibt, um auf die Gefahren von Social Engineering aufmerksam zu machen (vgl. CT 2012: 38) und nur bei 13 Prozent der Unternehmen wurden Beschäftigte bereits zu den Gefahren von Ausforschung geschult (u. a. Vorgehen der Nachrichtendienste und empfohlenes Verhalten im Ausland). Etwa jedes zweite Unternehmen der E&Y-Studien gab an, eigene Beschäftigte bereits für die Gefahren von Ausforschung sensibilisiert zu haben (vgl. E&Y 2013: 11). In der SiFo-Studie des Sicherheitsforums Baden-Württemberg hatte weniger als die Hälfte der Unternehmen (42 Prozent) bisher Schulungen zur Sensibilisierung der Beschäftigten für den Schutz von Unternehmens-Know-how durchgeführt (vgl. Sicherheitsforum 2010: 77), was für die Initiatoren der Studie durchaus bedenklich ist.

Durch Schulungen und Loyalitätssteigerung können Beschäftigte vom Sicherheitsrisiko zum Sicherheitsfaktor werden (vgl. George 2013: 24). Somit ist der Aufbau von Loyalität zu dem Unternehmen eine andere Möglichkeit, um zu verhindern, dass sich Beschäftigte gegen das Unternehmen richten und beabsichtigt Know-how weiterleiten. Loyale Beschäftigte sind seltener bereit, sensibles Unternehmens-Know-how an Wettbewerber zu verkaufen. Zudem gehen sie verantwortlicher mit kritischem Unternehmenswissen um und sind auch aufmerksamer, wenn es darum geht, auf Unregelmäßigkeiten oder dem Unternehmen schadende Verhaltensweisen von anderen Beschäftigten hinzuweisen (vgl. CT 2012: 39). Dieser informellen Sozialkontrolle kommt eine wichtige Funktion zu, denn eine Unternehmenskultur, in der Kommunikationsbereitschaft und Transparenz von vielen Beschäftigten gelebt wird, hemmt potentielle Täter (vgl. Sicherheitsforum 2010: 57).

Rund 37 Prozent der von CT befragten Unternehmen gaben an, personalfördernde Maßnahmen zur Steigerung der Loyalität der Beschäftigten durchzuführen (vgl. CT 2012: 39). In den E&Y-Studien führte sogar etwa jedes zweite Unternehmen solche Maßnahmen durch (vgl. E&Y 2013: 11).

Weitere in der Fachliteratur genannte Sicherheitsvorkehrungen für den Personalbereich sind u. a. regelmäßige Kontrollen, um Beschäftigte, die über Zugriff auf sensibles Know-how verfügen, für WS/KA unempfänglich zu machen, Zugangsbeschränkungen zu bestimmten Bereichen im Unternehmen sowie Zugriffsbeschränkungen nach dem „Need-to-know-Prinzip“ (Kenntnis nur bei Bedarf)[54] auf sensible Unternehmensdaten (vgl. Blume 2008: 34).

So gaben 58 Prozent der Unternehmen, die sich an der Befragung des Sicherheitsforums beteiligt haben, an, dass sie über Zugriffsbeschränkungen verfügen und sensibles Wissen nur den Beschäftigten zur Verfügung steht, die es auch wirklich im Rahmen ihrer Tätigkeiten brauchen (Sicherheitsforum 2010: 78). In der CT-Studie waren es lediglich 28 Prozent, die die Zugriffsmöglichkeiten der Beschäftigten reglementiert haben (vgl. CT 2012: 35).

Viele Täter sind den Unternehmen vor der Straftat persönlich bekannt, die Gefahr geht somit auch von Kunden und Lieferanten und sogar von Geschäftspartnern aus. Dementsprechend findet sich in der Fachliteratur eine Vielzahl von Vorschlägen, auf die die Unternehmen ebenfalls achten sollten, wie z. B. Geheimhaltungsverpflichtungen für Geschäftspartner.

[54] Mitarbeiter bekommen nur Zugriff auf Informationen, die sie unmittelbar für die Erfüllung konkreter Aufgaben benötigen (vgl. Blume 2008: 34).

In der Industriespionage-Studie verfügten etwa 56 Prozent der befragten Unternehmen über Geheimhaltungsverpflichtungen für Geschäftspartner (CT 2012: 42). In den E&Y-Befragungen gaben 2011 69 Prozent und 2013 80 Prozent der Unternehmen an, Geheimhaltungsverpflichtungen mit ihren Geschäftspartnern abzuschließen (vgl. E&Y 2013: 12).

5.5.3 Technische/IT-Maßnahmen

Sehr häufig wird in der Fachliteratur darauf verwiesen, dass umfangreiche technische Maßnahmen in den Bereichen IT-Sicherheit oder Gebäude- und Raumsicherheit (Zäune, Alarmanlagen, Kameras, Zutrittssysteme) notwendig sind.[55] Unternehmen wird empfohlen, in regelmäßigem Abstand die Möglichkeiten der Umgehung dieser Sicherheitsvorkehrungen zu untersuchen und zu bewerten. Auch zu diesen Punkten konnten die Unternehmen in mehreren Studien Angaben im Zusammenhang mit der Bedrohung durch Ausforschung machen.[56]

Wegen der zunehmenden Ausforschung über IKT und da diese Angriffe für die Täter oftmals sehr risikoarm und kostengünstig sind, sollten die Unternehmen neben strukturellen und personellen vor allem auch IT-Sicherheitsmaßnahmen für die Abwehr von Ausforschung berücksichtigen. Auch hierzu finden sich vielfältige Handlungsempfehlungen in der Fachliteratur. Zum Teil gestaltet sich der Schutz von kritischen Daten vor Angriffen über IKT als recht komplexe Herausforderung für die Unternehmen (vgl. Höfer 2009: 45). Im Folgenden soll nur auf eine kleine Auswahl eingegangen werden.

Die Ergebnisse aller Studien zeigen, dass technische Standardmaßnahmen wie Passwortschutz auf allen Geräten, Firewalls, Spamfilter oder Virenschutzsoftware von den Unternehmen beinahe flächendeckend eingesetzt wurden. Häufig wandten rund 90 Prozent der Unternehmen diese Vorkehrungen an (vgl. E&Y 2013: 9, CT 2012: 35, BMWi 2012: 24).

Umfassendere IT-Schutzvorkehrungen werden von den Unternehmen deutlich seltener eingesetzt. Über die Auswertung von Log-Daten können Unternehmen auf ungewollte Zugriffe auf ihre IT-Systeme aufmerksam werden. Zudem sind Log-Daten häufig die einzigen Informationen, die für eine forensische Analyse zur Verfügung stehen (vgl. Gogolinski 2013: 10). Da-

[55] Vgl. u. a. Bernd-Striebeck 2012: 20, Sack 2008/01: 20 und Sack 2008/02: 20, Warnecke 2010: 307 ff., Schubert 2010: 41 ff.

[56] Technische- sowie IT-Maßnahmen werden u. a. in folgenden Studien ausführlicher thematisiert: CT 2012: 35 ff.; E&Y 2013: 9; IHK Nord 2013: 15 ff.; KES 2012/6: 44; BSI 2011: 44, 58 ff., 65 f.; Sicherheitsforum 2010: 75.

mit eine umfassende Übersicht über alle Systeme in einem Unternehmen gewährleistet werden kann, müssen Log-Daten in regelmäßigen Abständen und ohne konkreten Anlass ausgewertet und auf Sicherheitsvorfälle und Funktionsstörungen überprüft werden (vgl. BSI 2011: 58).

Die Verfasser mehrerer Studien kommen zu dem kritischen Ergebnis, dass nur ein kleiner Teil der befragten Unternehmen solch ein kontinuierliches Monitoring durchführte, was dazu führt, dass Informationsabflüsse meist nur durch Zufall entdeckt werden (vgl. CT 2012: 34). Zwar werteten 97 Prozent der vom BSI befragten Unternehmen ihre Log-Daten grundsätzlich aus, jedoch gaben nur 17 Prozent an, das kontinuierlich durchzuführen (vgl. BSI 2011: 59). Nur jedes fünfte von CT befragte Unternehmen gab an, die Log-Daten mit Hilfe eines kontinuierlichen Monitorings zu überprüfen (vgl. CT 2012: 35). Auch in den E&Y-Studien kontrollierte nur eine Minderheit der Unternehmen sämtliche EDV-Daten, in der Befragung von 2013 waren es nur 30 Prozent (vgl. E&Y 2013: 9).

Das Verbot der Nutzung von USB-Sticks, CD-Brennern oder portablen Festplatten ist eine relativ einfach umsetzbare Sicherheitsmaßnahme in einem Unternehmen. Sie ist zudem sehr effektiv, da sie dazu beiträgt, die Wahrscheinlichkeit zu verringern, dass Beschäftigte unbewusst oder absichtlich zu Tätern werden. Wenn dieses Verbot im Unternehmen klar kommuniziert wird, dann kann sich das Unternehmen auch auf die soziale Kontrolle unter den Beschäftigten verlassen. Trotzdem nutzte im Durchschnitt der Studien nur eine Minderheit der befragten Unternehmen (zwischen rund 20 und 30 Prozent) dieses Verbot (vgl. CT 2012: 35, E&Y 2013: 9, BMWi 2012: 24).

Technisch aufwendiger ist die Verschlüsselung des E-Mail-Verkehrs, der Festnetz- oder der mobilen Telefonie. Aufgrund des zum Teil hohen Nutzens für ein Unternehmen wird in der Fachliteratur häufig zu Verschlüsselungen geraten. Im Durchschnitt der Studien verfügten jedoch nur ca. 18 bis 27 Prozent der Unternehmen über Verschlüsselungslösungen für den E-Mail-Verkehr (vgl. CT 2012: 35, BMWi 2012: 24, BSI 2011: 44, KES 2012/6: 11).

Obwohl sich in mehreren Bereichen Verbesserungspotenzial erkennen lässt, schätzten viele Unternehmen die getroffenen Sicherheitsvorkehrungen im IT-Bereich als ausreichend ein. So fühlte sich z. B. die große Mehrheit der von E&Y befragten Unternehmen vor der Ausfor-

schung über das Internet sicher: 82 Prozent der Unternehmen gaben an, dass die präventiven Vorkehrungen im Unternehmen ausreichend seien, um sich wirkungsvoll gegen einen Informationsabfluss zu schützen (vgl. E&Y 2013: 8). Im Gegensatz dazu sahen die Autoren der Studien vor allem in Bezug auf die IT-Schutzvorkehrungen erhebliches Verbesserungspotenzial bei vielen Unternehmen. Zwar verfügten die meisten Unternehmen über ein hohes Bewusstsein bzgl. der Relevanz der IT-Sicherheit, es fehlte aber häufig an der Einsicht, dass Ausforschung im IT-Bereich die Geschäftstätigkeit nachhaltig stören und dadurch zu großen Schäden führen kann (vgl. BMWi 2012: 9).

Das Verhalten der Unternehmen kann aber nicht als irrational bezeichnet werden, da sie die Prioritäten nach Abwägung rationaler Kriterien festlegen. So wird oftmals die Erhöhung des IT-Sicherheitsniveaus aus wirtschaftlichen Gründen anderen Unternehmenszielen untergeordnet (vgl. BMWi 2012: 60).

5.5.4 Zusammenfassung Sicherheitsvorkehrungen

- Aus der Fachliteratur und der Selbsteinschätzung der Unternehmen geht hervor, dass bei vielen deutschen Unternehmen die Schutzvorkehrungen gegen Ausforschung **verbesserungsbedürftig** sind.
- Damit ein Unternehmen weiß, welche Sicherheitsvorkehrungen getroffen werden müssen, sollte es mehrere **vorbereitende Schritte** befolgen: Schutzbedarfsanalyse (Bestimmung des schutzwürdigen Kern-Know-hows des Unternehmens), Dokumentation und anschließend Evaluierung der bereits implementierten Sicherheitsmaßnahmen, Formulierung von Handlungsempfehlungen im Rahmen eines Maßnahmenkatalogs.
- Das Abschöpfen **menschlicher Quellen** (Beschäftigte, Kooperationspartner eines Unternehmens) sollte als ernstzunehmende Bedrohung wahrgenommen werden.
- Nur wenige Unternehmen haben ein System der **integrierten Unternehmenssicherheit** implementiert. Eine verlässliche Abwehr kann aber nur durch einen ganzheitlichen Ansatz (Know-how-Schutzkonzept) sichergestellt werden, der zugleich Technik, Prozesse und Beschäftigte umfasst. In vielen Unternehmen ist jedoch lediglich die IT-Abteilung für die Abwehr von Ausforschung zuständig.
- Häufig verfügte weniger als ein Drittel der Unternehmen über ein schriftlich fixiertes **Informationsschutzkonzept**, in dem die Verantwortlichkeiten und Aufgaben im Bereich der

Abwehr von Ausforschung sowie Handlungsempfehlungen im Falle eines Ausforschungsvorfalls aufgeführt werden.

- Rund die Hälfte der Unternehmen hatte keine **Schutzbedarfsanalyse** durchgeführt, mit deren Hilfe seine „Kronjuwelen“ (wettbewerbsentscheidende Daten) bestimmt werden können.
- Zwischen 30 und 80 Prozent der Unternehmen verfügten über **schriftlich verfasste Vorgaben**, die den richtigen Umgang mit schützenswerten Informationen regeln.
- Vor allem **Bewerber** auf Stellen in sensiblen Bereichen sollten vor der Einstellung bestimmte Sicherheitsüberprüfungen durchlaufen: Zwischen 80 und 90 Prozent der Unternehmen integrierten **Geheimhaltungsverpflichtungen** in die Arbeitsverträge aller Beschäftigten. Deutlich weniger Unternehmen (zwischen 6 und 20 Prozent) führten **Integritätstests** für neue Bewerber durch.
- Es ist wichtig, dass die Beschäftigten eines Unternehmens für die Gefahren von Wirtschaftsspionage und Konkurrenzausspähung **sensibilisiert** werden und dass sie ein Bewusstsein für „Social Engineering“ und die Richtungen, aus denen die Ausforschung kommen kann, entwickeln. Jedoch sensibilisierten lediglich zwischen 13 und rund 50 Prozent der Unternehmen ihre Beschäftigten für die Gefahren von Ausforschung.
- Durch **Loyalitätssteigerung** und die Identifikation mit einem Unternehmen kann das Risiko, dass Beschäftigte absichtlich Unternehmensinterna weiterleiten, gesenkt werden. Ca. 40 bis 50 Prozent der Unternehmen haben Maßnahmen zur Steigerung der Loyalität der Beschäftigten durchgeführt.
- Eine weitere wichtige Maßnahme sind **Zugangsbeschränkungen** zu bestimmten Bereichen im Unternehmen sowie **Zugriffsbeschränkungen** auf sensible Unternehmensdaten. Rund 30 bis 60 Prozent der Unternehmen gaben an, dass sie die Zugriffsmöglichkeiten der Beschäftigten reglementieren.
- Eine weitere Vorkehrung, um sich vor Know-how-Verlust zu schützen, sind **Geheimhaltungsverpflichtungen** für Geschäftspartner. Zwischen 56 und 80 Prozent der Unternehmen gaben an, dass sie solche Verpflichtungen mit ihren Geschäftspartnern eingegangen sind.
- Während **technische Standardmaßnahmen** zum Schutz vor Ausforschung bei der großen Mehrheit (rund 90 Prozent) der Unternehmen Anwendung finden, setzten deutlich weniger Unternehmen *umfassendere* IT-Schutzvorkehrungen um.

- Über die Auswertung von **Log-Daten** können Unternehmen auf ungewollte Zugriffe auf ihre IT-Systeme aufmerksam werden. Zudem sind Log-Daten häufig die einzigen Informationen, die für eine forensische Analyse zur Verfügung stehen. Nur ein kleiner Teil der Unternehmen (17 bis 30 Prozent) führte ein **kontinuierliches Monitoring** dieser Daten durch.
- Nur wenige Unternehmen (20 bis 30 Prozent) verboten die Nutzung von USB-Sticks, CD-Brennern etc., obwohl dieses Verbot relativ einfach umzusetzen wäre.
- Die technisch aufwendigere **Verschlüsselung** des E-Mail-Verkehrs, die einen sehr effektiven Schutz vor Ausforschung bieten kann, wurde von 18 bis 27 Prozent genutzt.

5.6 Kooperation der Unternehmen mit den Sicherheitsbehörden

Werden die Sicherheitsbehörden von den Unternehmen in Kenntnis gesetzt, wenn sie einen Ausforschungsvorfall oder einen konkreten Verdachtsfall festgestellt haben? In der Fachliteratur geht man davon aus, dass in den meisten Fällen von Ausforschung die betroffenen Unternehmen zur Aufklärung des Vorfalls eher ein privates Sicherheitsunternehmen einschalten als die Polizei (vgl. Schaaf 2009: 25). Das läge daran, dass viele Unternehmen nicht wirklich an der Bekämpfung von Wirtschaftsspionage und Konkurrenzausspähung interessiert seien, was dazu führe, dass die Polizei eher durch Zufälle zu den Fällen geführt werde als durch Informationen von den Unternehmen selbst (vgl. Nathusius 2001: 56). Sprechen bei einem Angriff die Hinweise dafür, dass die Täter Wettbewerber sind, schalten die betroffenen Unternehmen sehr häufig erst einmal ein professionelles Sicherheitsunternehmen ein. Auf diese Weise können sie sicherstellen, dass sie selbst bestimmen, wie mit den Ermittlungserkenntnissen umgegangen wird und ob eine Anzeige gestellt werden soll. Die Entscheidungshoheit bleibt somit bei dem betroffenen Unternehmen (vgl. Schaaf 2009: 25). Ferner wird in der Fachliteratur auch häufig angezweifelt, dass geschädigte Unternehmen immer eine umfassende Hilfestellung vonseiten der Behörden erhalten können (vgl. Nathusius 2001: 56) und dass die Strafverfolgungsbehörden in jedem Fall auch die Interessen des Unternehmens wahren können und somit aus Sicht der Unternehmen auch die richtigen Ansprechpartner sind (vgl. Schaaf 200: 24). Den Unternehmen wird von den Autoren empfohlen, sich in einem festgestellten oder vermuteten Fall von Ausforschung erst einmal an die zuständige Verfassungsschutzbehörde zu wenden (vgl. Schaaf 2009: 15), da diese nicht dem Legalitätsprinzip unterliegt und einen Vorfall vertraulich behandeln kann, ohne

dass Ermittlungen eingeleitet werden (vgl. CT 2012: 29). Das komme den Unternehmen entgegen, da es meistens nicht in ihrem Interesse liege, dass Vorfälle zur Anzeige gebracht werden (vgl. Schaaf 2009: 24). Gemäß dem Legalitätsprinzip sind die Strafverfolgungsbehörden verpflichtet, bei Kenntnis einer Straftat tätig zu werden. Für die Staatsanwaltschaft bestehen jedoch auch gesetzlich geregelte Ausnahmen vom Verfolgungszwang (vgl. Der Generalbundesanwalt beim Bundesgerichtshof, ohne Jahresangabe). Staatsanwaltschaft und Polizei ist es wichtig, den betroffenen Unternehmen den Handlungsspielraum aufzuzeigen und eine abgestimmte Vorgehensweise zu erarbeiten.

Werden Ausforschungsvorfälle ausschließlich von privaten Sicherheitsunternehmen oder dem Verfassungsschutz behandelt, ohne dass sie im Anschluss daran zur Anzeige gebracht werden, erscheinen sie nicht in der Polizeilichen Kriminalstatistik.

Es ist jedoch wichtig, dass sich die betroffenen Unternehmen auch an die Strafverfolgungsbehörden wenden, da eine konsequente Strafverfolgung ihre Glaubwürdigkeit nach innen und nach außen unterstützt und auch bei den eigenen Beschäftigten zu einem verbesserten Unrechtsbewusstsein führt (vgl. Sicherheitsforum 2010: 62). Dies ist vor allem vor dem Hintergrund wichtig, dass in vielen Studien den Beschäftigten in einem Unternehmen eine wichtige Rolle bei der Ausforschung zukommt und die in der SiFo-Studie befragten Unternehmen angaben, dass in 92 Prozent der Vorfälle das mangelnde Werte- und Unrechtsbewusstsein der Täter für ihre Taten ausschlaggebend ist (vgl. Sicherheitsforum 2010: 70).

Eine geringe Anzeigebereitschaft bei Wirtschaftsspionage oder Konkurrenzausspähung vergrößert das Dunkelfeld in diesem Bereich erheblich und je größer die Dunkelziffer ist, desto schwieriger wird eine adäquate Lageeinschätzung durch die Ermittlungsbehörden. Dies erschwert es den Sicherheitsbehörden auch, sich an die besonderen Bedürfnisse der Wirtschaft anzupassen, da sie auf der Grundlage von Schätzungen und Hochrechnungen Personalaufbau und Budgeterhöhung zum Zweck der Bekämpfung von Wirtschaftskriminalität nur schwer begründen können (vgl. IHK Nord 2013: 16). Zudem kann nur auf der Grundlage der Rückmeldungen der Unternehmen eine genaue Einschätzung des Risiko- und Schadenspotenzials von WS/KA durch die Strafverfolgungsbehörden vorgenommen werden (vgl. Even 2013: 39). Effektive und effiziente Bekämpfungsmaßnahmen benötigen das Feedback der Unternehmen und können nicht auf der Grundlage von Vermutungen konzipiert werden.

Werden die Strafverfolgungsbehörden von Ausforschungsvorfällen in Kenntnis gesetzt, kann auch verhindert werden, dass Kriminelle mit der gleichen Vorgehensweise mehrere Unternehmen schädigen. Zudem können Fälle, bei denen Täter mehrere Unternehmen angegriffen haben, möglicherweise schneller aufgeklärt werden, wenn die Strafverfolgungsbehörden Erkenntnisse aus unterschiedlichen Fällen sammeln.

Es liegt somit durchaus auch im eigenen Interesse der Unternehmen, dass sie Vorfälle den Strafverfolgungsbehörden mitteilen, denn diese können mit ihren Ermittlungen dazu beitragen, dass die Täter gefasst werden und weiterer Schaden von dem Unternehmen abgewandt wird. Die Kooperation mit den Strafverfolgungsbehörden führt zudem auch zu einer vollständigeren Lagebeschreibung, die wiederum den Unternehmen helfen kann, kostenintensive Sicherheitsvorkehrungen gegen nicht bestehende Bedrohungen, einzusparen (vgl. Oelmaier 2012: 27).

5.6.1 Meldebereitschaft der Unternehmen

Wie in der Fachliteratur von vielen privaten und öffentlichen Akteuren dargestellt zeigt auch der Vergleich der Studienergebnisse, dass die Meldebereitschaft der Unternehmen bei Ausforschung sehr niedrig ist. In keiner Studie gab mehr als ein Drittel der befragten Unternehmen an, sich im Verdachts- oder Schadensfall an die Sicherheitsbehörden[57] zu wenden. In den meisten Studien war dieser Anteil sogar deutlich niedriger.

Die Herausgeber der Studie zu Know-how- und Informationsverlusten des Sicherheitsforums Baden-Württemberg kommen zu dem Ergebnis, dass nur ca. 8 Prozent der befragten Unternehmen die Schadensfälle mit externen Sicherheitsberatern oder den Sicherheitsbehörden bearbeitet haben (vgl. Sicherheitsforum 2004: 78). In der Nachfolgestudie stellten die befragten Unternehmen immerhin in jedem dritten Fall von Verrat von Geschäfts- und Betriebsgeheimnissen eine Strafanzeige (vgl. Sicherheitsforum 2010: 60). Auch der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) kam 2008 zu einem ähnlichen Ergebnis, nach dem nur 4 Prozent der von WS/KA betroffenen Unternehmen die Sicherheitsbehörden kontaktierten (vgl. Schnaas 2014: 9). Das Beratungsunternehmen CT konnte sogar einen Rückgang bei der Meldebereitschaft der Unternehmen feststellen. Gab 2007 noch etwa jedes vierte befragte Unternehmen an, bei einem Vorfall

[57] In den meisten Studien werden die Verfassungsschutz- und die Strafverfolgungsbehörden zusammen aufgeführt.

oder einem Verdacht auf WS/KA den Verfassungsschutz oder die Strafverfolgungsbehörden eingeschaltet zu haben, war es 2012 nur noch jedes fünfte Unternehmen (vgl. CT 2012: 29).

Im Lagebericht zur Informationssicherheit gibt rund ein Drittel der Unternehmen, die einen Vertraulichkeitsbruch[58] festgestellt haben, an, Strafanzeige gegen die Verursacher zu erstatten (vgl. kes 2012/4: 14).

Zu ähnlichen Ergebnissen zur Meldebereitschaft der Unternehmen kommt die IHK Nord. In ihrer Befragung norddeutscher Unternehmen zur Betroffenheit von Cybercrime zeigte nur etwa jedes zehnte von Cybercrime betroffene Unternehmen alle oder einige Angriffe an, während rund 60 Prozent den Strafverfolgungsbehörden keinen einzigen Angriff meldeten (vgl. IHK Nord 2013: 11).

KPMG kann mit seinen Studien zu den Themen Wirtschaftskriminalität und Cybercrime als einzige Institution eine deutlich höhere Meldebereitschaft bei den Unternehmen und geringe Berührungsängste zu den Strafverfolgungsbehörden nachweisen. So gaben rund 90 Prozent der zum Thema e-Crime befragten Unternehmen an, die Strafverfolgungsbehörden, *nach eingehender Abwägung* der Vor- und Nachteile, bei einem e-Crime-Vorfall einzubeziehen und 64 Prozent der von e-Crime betroffenen Unternehmen zeigten die Delikte auch an (vgl. KPMG 2010: 30).[59] Für die e-Crime-Studie 2013 liegen keine Zahlen zu der Anzeigebereitschaft von Unternehmen vor. Aber auch in den Befragungen zur Wirtschaftskriminalität gab jeweils die Mehrheit der Unternehmen an, die Strafverfolgungsbehörden bei der Fallaufklärung eingeschaltet zu haben: 2013 schalteten 51 Prozent der betroffenen mittelständischen Unternehmen aus Deutschland die Strafverfolgungsbehörden bei der Fallaufklärung ein, 2010 waren es 54 Prozent und 2006 56 Prozent (vgl. KPMG 2013b: 42). Da sich die Anzeigebereitschaft der Unternehmen in den Befragungen mit dem Schwerpunkt Wirtschaftskriminalität auch auf andere Kriminalitätsformen, wie z. B. Diebstahl, Betrug, Untreue, Korruption und Geldwäsche bezog, kann aufgrund der niedrigen Anzeigebereitschaft bei Fällen von Ausforschung, die in den anderen Studien beobachtet werden kann, vermutet werden, dass der hohe Wert in den weiter gefassten Studien zu Wirtschaftskriminalität und Cybercrime mit den anderen Kriminalitätsformen zusammenhängt. Dies würde bedeuten,

[58] Zugriff auf unternehmensinterne Informationen/Know-how durch Social Engineering, Verlust/Diebstahl von Speichermedien, Online-Angriffe, Abhören/Mitlesen von Kommunikation etc.

[59] Die Anzeigebereitschaft der Unternehmen bezieht sich neben eindeutigen Ausforschungshandlungen wie Datendiebstahl, Verrat von Geschäfts- und Betriebsgeheimnissen oder Ausspähen/Abfangen von Daten unter anderem auch auf Betrug und Verletzung von Schutz- und Urheberrechten.

dass die von (Wirtschafts-) Kriminalität betroffenen Unternehmen vor allem Vorfälle von Diebstahl, Betrug etc. den Strafverfolgungsbehörden meldeten statt Ausforschungsvorfälle.

5.6.2 Gründe der geringen Meldebereitschaft der Unternehmen

Fehlende Kenntnis der Ansprechpartner und ihrer Zuständigkeiten

Ein Grund, dass die Unternehmen bei Ausforschungsvorfällen eher selten die Sicherheitsbehörden einschalten, ist, dass sie die Zuständigkeiten, Aufgaben und Sicherheitsangebote der Behörden nicht ausreichend gut kennen. Viele Unternehmen waren sich der Möglichkeiten, die ihnen Behörden bieten, nicht bewusst. Aber auch ungenaue oder falsche Vorstellungen vom Ablauf der Ermittlungen können ausschlaggebend für die mangelnde Anzeigebereitschaft seitens der Unternehmen sein (vgl. Ziercke 2012: 109). Dies kann auch von der Größe eines Unternehmens abhängen und der Anzahl der Beschäftigten, die speziell im Sicherheitsbereich des Unternehmens arbeiten. Zumindest diese Beschäftigten sollten die Aufgaben der Sicherheitsbehörden und die relevanten Ansprechpartner jedoch kennen.

In der ersten Studie des Sicherheitsforums Baden-Württemberg von 2004 gab jedes zweite befragte Unternehmen an, dass ihm die Arbeit der Sicherheitsbehörden nicht bekannt ist und eine Zusammenarbeit für unnötig erachtet wird. Diese Meinung hatte etwa die Hälfte der KMU (bis 200 Millionen Euro Jahresumsatz), doch nur 20 Prozent der großen Unternehmen (über 500 Millionen Euro Jahresumsatz). Nur ca. 13 Prozent der befragten Unternehmen gaben an, die Hilfe der Sicherheitsbehörden zu benötigen, obwohl ihnen deren Arbeitsweise weitgehend unbekannt war. Erneut schätzten die großen Unternehmen die Rolle der Sicherheitsbehörden beim Informationsschutz als wichtiger ein: 40 Prozent von ihnen gaben an, dass ihnen die Arbeit der Sicherheitsbehörden nicht bekannt war, sie diese aber für nötig halten (vgl. Sicherheitsforum 2004: 66). Hinzu kommt, dass nur jedem zehnten befragten Unternehmen die Ansprechpartner bei den Sicherheitsbehörden im Bereich Informationsschutz bekannt waren. Auch hier lässt sich wieder ein Unterschied bezüglich der Größe der Unternehmen feststellen, denn mehr als die Hälfte der großen Unternehmen kannte die relevanten Ansprechpartner (vgl. Sicherheitsforum 2004: 71 ff.).

In der WIK-Sicherheits-Enquête gab lediglich ein Drittel der Unternehmen an, die staatlichen Sensibilisierungsaktivitäten und -maßnahmen im Wirtschaftsschutz (Schutz vor Ausspähung und Spionage) zu kennen. Aber auch bei den Unternehmen, die in den vorhergehenden 24 Monaten von Wirtschaftsspionage und/oder Konkurrenzausspähung betroffen

gewesen sind, kannte nur eine Minderheit (39 Prozent) die Angebote und Aktivitäten der Sicherheitsbehörden (vgl. WIK 2011/2: 15).

In der Befragung der IHK Nord gab ca. jedes fünfte Unternehmen an, Cybercrime-Angriffe den Sicherheitsbehörden nicht gemeldet zu haben, da ihnen nicht bekannt war, an wen sie sich hätten wenden sollen (IHK Nord 2013: 12).

Auch in einer Studie des österreichischen BVT wird die seltene Einbeziehung der Sicherheitsbehörden in Fällen von Ausforschung damit begründet, dass nur die wenigsten Unternehmen ihre Angebote kennen: 85 Prozent der befragten Unternehmen gaben an, die genaue Arbeit der Sicherheitsbehörden und ihre Unterstützungsmaßnahmen im Bereich der Wirtschaftsspionage und Konkurrenzausspähung nicht zu kennen (vgl. BVT 2010: 11).

Angst vor Reputationsverlust

Ein weiterer Grund, sich bei einem Vorfall nicht an die Behörden zu wenden, ist die Befürchtung, dass der Fall dadurch an die Öffentlichkeit gelangt (vgl. CT 2012: 13) und dem Unternehmen hierdurch ein Reputationsschaden entsteht, dessen Auswirkungen größer sind als der durch den eigentlichen Know-how-Abfluss entstandene Schaden (vgl. Schaaf 2009: 23 f.). Um einen Imageverlust bzw. Reputationsschaden zu vermeiden, unterließen die in der SiFo-Studie 2010 befragten Unternehmen in 53 Prozent der Fälle von Know-how-Abfluss eine Strafanzeige (vgl. Sicherheitsforum 2010: 60). Auch um die Geschäftsbeziehungen mit anderen Unternehmen nicht zu beeinträchtigen, verzichteten in der gleichen Befragung 43 Prozent der Unternehmen auf eine Strafanzeige (vgl. Sicherheitsforum 2010: 60). Als Grund gaben die Befragten an, dass im Falle der Herstellung von Öffentlichkeit die Geschäftspartner befürchten könnten, dass bereits sensible Daten entwendet worden sind, und darunter das Vertrauen der Geschäftspartner und Kunden leide.

In der IHK-Studie zum Thema Betroffenheit von Cybercrime hatten sich die befragten Unternehmen deutlich seltener aus Reputationsgründen gegen eine Anzeige der Vorfälle entschieden. Nur ca. 5 Prozent der Unternehmen gaben an, Angriffe nicht anzuzeigen, weil sie einen Ruf- und Imageschaden befürchteten (vgl. IHK Nord 2013: 12).

Zu hoher Aufwand und geringer Nutzen

Mehr als die Hälfte der in der IHK Nord-Studie befragten Unternehmen gab an, dass sie sich aufgrund des hohen Aufwands gegen eine Anzeige entschieden hatten. Das kann evtl. daran

liegen, dass den Unternehmen nur ein geringfügiger Schaden entstanden ist und sie den Vorfall nicht hochspielen wollen. Es ist aber auch möglich, dass sie die Abläufe und Methoden der Arbeit der Sicherheitsbehörden nicht ausreichend gut kennen, was erneut auf mangelnden Kontakt mit den Behörden zurückgeführt werden könnte. Bei ca. einem Drittel der Unternehmen war der Zweifel am Erfolg ausschlaggebend dafür, dass sie den Cyberangriff nicht angezeigt hatten (vgl. IHK Nord 2013: 11).

Der geringe Nutzen einer Strafanzeige für das Unternehmen wurde von den in der SiFo-Studie befragten Unternehmen als wichtigster Grund für das Unterlassen einer strafrechtlichen Anzeige angegeben: in 82 Prozent der Vorfälle wurde dies als Hauptgrund genannt. In 77 Prozent der Vorfälle entschieden sich die Unternehmen gegen eine Anzeige, da ihnen der Ausgang der Strafverfolgung zu unsicher erschien und in etwas mehr als jedem zweiten Fall, weil sie befürchteten, dass die Strafverfolgung zu langwierig verlaufen könnte (vgl. Sicherheitsforum 2010: 16).

Die Ergebnisse aus den Unternehmensbefragungen zeigen, dass sich nur wenige Unternehmen, die einen unfreundlichen Informationsabfluss festgestellt haben, an die Sicherheitsbehörden wenden. Wenn es zu einem Austausch mit den Sicherheitsbehörden kommt, dauert dieser meist nur so lange an, bis der Vorfall aufgeklärt ist. An einem längerfristigen Austausch mit den Sicherheitsbehörden sind jedoch nur wenige Unternehmen interessiert (vgl. Nathusius 2001: 56). Viele Unternehmen sind nicht bereit, sich gegenüber den Sicherheitsbehörden zu öffnen, z. B. um gemeinsame Sicherheitskonzepte zu erarbeiten oder um an der Aufklärung eines eingetretenen Ausforschungsvorfalls kooperativ mit den Sicherheitsbehörden zusammenzuarbeiten. Dies liegt u. a. daran, dass die Wahrung ihres Rufes und die Schadensbegrenzung für viele Unternehmen wichtiger sind als die Täterermittlung (vgl. Ziercke 2008: 11). Viele Unternehmen vermuten weiterhin, dass ihre Interessen und Belange von den Sicherheitsbehörden nicht ausreichend berücksichtigt werden können (vgl. BKA 2014: 5).

Es ist wichtig, dass diese Vermutungen und Ängste durch einen stetigen gegenseitigen Informations- und Erfahrungsaustausch abgebaut werden, denn Verfassungsschutz- und Strafverfolgungsbehörden verfügen durchaus über Möglichkeiten, auf Belange der Unternehmen einzugehen: Da der Polizei die Furcht der Firmen vor einem kostspieligen Imageschaden bekannt ist, wurden die polizeilichen Maßnahmen entsprechend angepasst – die

Polizei legt z. B. großen Wert auf vertrauensvolle Zusammenarbeit mit den Unternehmen und bei Cyber-Ausforschung stehen den Unternehmen Fachdienststellen für Cybercrime-Delikte zur Verfügung, die in mehreren Bundesländern eingerichtet wurden (vgl. Ziercke 2008: 11). Ferner ist es der Polizei wichtig, dass im Rahmen der Ermittlungs- und Tatortarbeit keine unnötige firmeninterne oder öffentliche Aufmerksamkeit erregt oder die Geschäfts- und Betriebsabläufe übermäßig gestört werden (vgl. BKA 2014: 18 f.). Die Strafverfolgungsbehörden kennen die Sorgen der Unternehmen vor einem möglichen Imageschaden und ihren Wunsch nach Diskretion und es ist ihnen möglich, diese in ihren Maßnahmen entsprechend zu berücksichtigen, z. B. indem nur so viele (nicht uniformierte) Beamte vor Ort erscheinen, wie für die Durchführung der polizeilichen Maßnahmen notwendig sind und sie sich, wenn nötig, an der Pforte als Geschäftstermin anmelden. Bei Cyber-Ausforschung besteht zudem die Möglichkeit, dass vor Ort eine Spiegelung der als beweisrelevant eingeschätzten Daten stattfindet, was den laufenden Betrieb des Unternehmens nur geringfügig beeinträchtigt (vgl. ebd.).

Auch bei einer Kooperation mit den Verfassungsschutzbehörden können die Unternehmen davon ausgehen, dass ihre Informationen vertraulich behandelt werden (vgl. secure-it 2008: 14). Zudem muss ein Ausforschungsvorfall nicht aktenkundig gemacht und der Staatsanwaltschaft übergeben werden und gelangt somit auch nicht automatisch an die Öffentlichkeit (vgl. Blass 2011: 1). Darüber hinaus verfügt der Verfassungsschutz über ein umfangreiches Angebot von Präventions- und Informationsangeboten für Unternehmen (vgl. George 2013: 25).

5.6.3 Zusammenfassung Kooperation

- Es ist wichtig, dass sich Unternehmen, die Opfer von Ausforschung wurden, an die Strafverfolgungsbehörden wenden, da eine konsequente **Strafverfolgung** die Glaubwürdigkeit des Unternehmens nach innen und nach außen fördert und auch bei den eigenen Beschäftigten zu einem besseren Werte- und Unrechtsbewusstsein führt.
- Eine geringe Anzeigebereitschaft bei Ausforschungsvorfällen vergrößert das **Dunkelfeld** und erschwert es den Behörden, die Lage adäquat einzuschätzen. Eine verbesserte **Lagebeschreibung** kann den Unternehmen u. a. aber dabei helfen, kostenintensive und nicht unbedingt notwendige Sicherheitsvorkehrungen einzusparen.

- Wie in der Fachliteratur dargestellt zeigt auch der Vergleich der Studienergebnisse, dass die **Meldebereitschaft** der Unternehmen bei einem Fall von Ausforschung sehr niedrig ist. In den Studien gaben zwischen 4 und 33 Prozent der Unternehmen an, sich im Verdachts- oder Schadensfall an die Sicherheitsbehörden gewandt zu haben.
- Ein Grund für die Zurückhaltung der Unternehmen beim Einschalten der Sicherheitsbehörden bei Fällen von Ausforschung war die **mangelnde Kenntnis** über die Zuständigkeiten, Aufgaben und Sicherheitsangebote der Behörden. Diese Begründung nannten zwischen 33 und 50 Prozent der deutschen und 85 Prozent der österreichischen Unternehmen.
- Ein weiterer Grund für die geringe Kooperation war die Furcht, dass der Ausforschungsvorfall dadurch an die Öffentlichkeit gelangt und dem Unternehmen ein **Reputationsschaden** entstehen könnte. Diese Begründung nannte rund die Hälfte der Unternehmen.
- Ferner unterließen rund 50 Prozent der Unternehmen die Meldung eines Vorfalls, da ihnen der **Aufwand** zu hoch und der **Nutzen** zu gering erschienen.

5.7 Wichtige Akteure im Bereich der Abwehr von Ausforschung und im Informationsschutz

Im Kapitel 5.2 konnte gezeigt werden, dass deutsche Unternehmen, u. a. aufgrund ihrer Innovation und Technologieorientierung im Fokus von Wirtschaftsspionage und Konkurrenzausspähung stehen. Das Risiko, Opfer eines ungewollten Informationsabflusses zu werden, nimmt durch mehrere Entwicklungen, wie

- dem verschärften internationalen Wettbewerb durch aufstrebende Schwellenländer,
- einer nach dem Kalten Krieg neuen Aufgabenstellung ausländischer Geheimdienste,
- veränderter Formen inner- und zwischenbetrieblicher Kooperation
- dem Fortschritt im Bereich der IKT

weiter erheblich zu (vgl. Röder 2011: 4). Vor dem Hintergrund dieser Entwicklungen erscheint es als unabdingbar, dass sich Unternehmen im Sinne wirkungsvoller Schutzmaßnahmen vor Ausforschung mit anderen Akteuren austauschen und mit ihnen kooperieren. Beratungs- und Informationsangebote im Bereich Abwehr von Ausforschung werden von unterschiedlichen Akteuren[60] – von der Privatwirtschaft, von Behörden und Verbänden – bereit-

[60] Private Unternehmen für IT-Sicherheit, für Objektsicherheit, für Schulungen; Arbeitsgemeinschaft für Sicherheit in der Wirtschaft, Sicherheitsforum Baden-Württemberg; Bundesministerium für Wirtschaft und Technolo-

gestellt. Unternehmen können somit auf eine große Bandbreite an Beratungsmöglichkeiten zurückgreifen, die ihnen dabei helfen, Kenntnisse zu Handlungsoptionen zu verbessern und vorhandene Kooperationsnetzwerke besser zu nutzen (vgl. Sicherheitsforum 2010: 83). Eine effektive Abwehr kann weder von Sicherheitsbehörden, noch von Wirtschaftsverbänden und Unternehmen alleine geleistet werden. Die Aktivitäten der verschiedenen Akteure müssen vernetzt, aufeinander abgestimmt und harmonisiert werden (vgl. BMI 2013a: 1). Ein regelmäßiger Erfahrungsaustausch schafft Vertrauen und ist eine notwendige Voraussetzung für eine wirkungsvolle Abwehr von Wirtschaftsspionage und Konkurrenzausspähung (vgl. BMI 2008: 335 und Even 2013: 39).[61]

Unternehmen können auf eine Vielzahl an Unterstützungsangeboten aus der Privatwirtschaft, von Behörden oder Verbänden zurückgreifen. Interessant ist festzustellen, von wem sie sich unterstützen lassen und ihre Bewertung dieser Angebote (vgl. Sicherheitsforum 2010: 83). In den Studien gab die Mehrheit der Unternehmen an, dass sie im Bereich der präventiven und repressiven Abwehr von Ausforschung bevorzugt mit privaten Institutionen zusammenarbeitet. So kontaktierten betroffene Unternehmen im Verdachts- oder eingetretenen Schadensfall häufiger private Anbieter als öffentliche und griffen auch eher auf deren Informations- und Beratungsangebote zurück.

In der SiFo-Studie des Sicherheitsforums Baden-Württemberg gaben fast zwei Drittel der befragten Unternehmen an, Beratungs- und Informationsangebote privater Einrichtungen in Anspruch zu nehmen. Lediglich 30 Prozent der Unternehmen griffen auf Beratungs- und Informationsangebote von öffentlichen Einrichtungen zurück[62] und weitere 30 Prozent der Unternehmen nutzten weder die Angebote von privaten noch von öffentlichen Einrichtungen (vgl. Sicherheitsforum 2010: 83). Ein Grund für die geringe Nutzung von externen Angeboten kann die Angst der Unternehmen vor einem Reputationsverlust bei Kunden, Kooperationspartnern und Unternehmensangehörigen sein (vgl. Sicherheitsforum 2010: 85). Dass beinahe jedes dritte Unternehmen auf keine externen Beratungsangebote zurückgegriffen hat, kann durchaus als kritisch bewertet werden und es zeigt, dass im Bereich des Wirt-

gie, Bundeskriminalamt, Bundesamt für Verfassungsschutz, Landesamt für Verfassungsschutz Baden-Württemberg, Bundesamt für Sicherheit in der Informationstechnologie.

[61] Einen guten Überblick über die Kooperationsformen der Unternehmen mit Behörden und Verbänden bietet u. a. Sicherheitsforum 2010b: SiFo-Studie 2009/2010 Handlungsempfehlungen für Unternehmen, S. 29-34.

[62] Mehrfachnennungen möglich.

schaftsschutzes Unternehmen weiterhin für die zahlreichen Hilfestellungen der verschiedenen Akteure sensibilisiert werden müssen.

Unter den öffentlichen Einrichtungen kontaktierten die Unternehmen an erster Stelle das BSI (25 Prozent der Unternehmen), um Beratungsangebote zum Know-how-Abfluss durch WS/KA zu erhalten. An das BKA wandten sich 24 Prozent der befragten Unternehmen, an die Landesämter für Verfassungsschutz 16 Prozent und an das Bundesamt für Verfassungsschutz 13 Prozent. Deutlich häufiger griffen die Unternehmen auf Angebote privater Akteure zurück. 55 Prozent informierten sich bei privaten Unternehmen für IT-Sicherheit, 47 Prozent bei privaten Unternehmen für Objektsicherheit und 28 Prozent bei privaten Schulungsunternehmen (vgl. Sicherheitsforum 2010: 84). Dies kann u. a. daran liegen, dass es deutlich mehr private als öffentliche Einrichtungen im Bereich Wirtschaftsschutz und Spionageabwehr gibt, die dementsprechend auf das jeweilige Unternehmen zugeschnittene Angebote erarbeiten können.

Zwar wurden in der SiFo-Studie Beratungs-, Betreuungs- und Informationsangebote privater Anbieter von den Unternehmen deutlich häufiger in Anspruch genommen als Angebote öffentlicher Anbieter, die Angaben zum *Nutzen* der Angebote dieser Akteursgruppen unterschieden sich aber weniger stark. So überwog bei allen genannten öffentlichen *und* privaten Anbietern eine gemischte Bewertung (teils sehr hilfreich/teils nicht hilfreich) bezüglich der Frage, ob ihre Angebote hilfreich für das Unternehmen waren. Relativ häufig wurden die Angebote des BSI (36 Prozent der Unternehmen, die die Angebote genutzt haben), des LfV Baden-Württemberg und des BfV (jeweils 33 Prozent), privater Unternehmen für IT-Sicherheit (32 Prozent), der ASW (25 Prozent) und privater Unternehmen für Objekt-Sicherheit (24 Prozent) als *sehr hilfreich* bewertet (vgl. Sicherheitsforum 2010: 85). Nur ca. ein Drittel der befragten Unternehmen, die die Angebote der Behörden in Anspruch genommen hatten, empfand diese als hilfreich (vgl. Sicherheitsforum 2010: 84). Auch wenn die absoluten Zahlen relativ niedrig und somit nicht repräsentativ sind, sollten diese Ergebnisse Beachtung finden.

Die Sicherheits-Enquête 2011 kommt zu ähnlichen Ergebnissen. Auch in dieser Studie wird ersichtlich, dass Unternehmen im Bereich des Wirtschafts- und Informationsschutzes eher mit privaten Einrichtungen als mit staatlichen Behörden kooperierten. Von allen befragten

Unternehmen hatten nur ca. 18 Prozent[63] Kontakt zu den für Wirtschafts- und Informationsschutz zuständigen Behörden. Aber auch die Unternehmen, die in den vorangegangenen 24 Monaten Opfer von Ausforschung geworden sind, standen nicht sehr viel häufiger in Kontakt mit den Sicherheitsbehörden – lediglich 22,6 Prozent der Unternehmen, die bereits Opfer von Ausforschung wurden, hatten bereits Kontakt mit den Sicherheitsbehörden während weitere rund 34 Prozent der geschädigten Unternehmen ausschließlich mit privaten Dienstleistern in Kontakt standen (vgl. WIK 2011/2: 15).

Im Gegensatz zu den in der SiFo-Studie vorgenommenen Bewertungen schnitten in der Sicherheits-Enquête die Sicherheitsbehörden generell schlechter ab als private Anbieter oder Verbände. So bewerteten die Unternehmen in den Befragungen von 2011 und 2013 die Informationen, die sie von den Behörden erhalten haben durchweg als befriedigend oder schlechter. Die von den Polizeibehörden zur Verfügung gestellten Informationen zu Sicherheitsfragen wurden von den Unternehmen auf einer Skala von eins (sehr gut) bis sechs (ungenügend) mit einer 3,0, die von den Verfassungsschutzbehörden bereitgestellten Informationen mit einer 3,5 bewertet. Besser schnitten die VdS Schadenverhütung GmbH (2,5), Anbieter von Sicherheitstechnik (2,5), ASW/VSW (2,6), der Bundesverband Sicherheitstechnik e. V. (2,7) und der Bundesverband Deutscher Wach- und Sicherheitsunternehmen e. V. (2,8) ab (vgl. WIK 2013/2: 11).

In der Befragung des BMWi von 2012 wurden private Akteure häufiger als geeignete Partner bei der Erhöhung der IT-Sicherheit (u. a. um einer Ausforschung des Unternehmens vorzubeugen) bezeichnet als öffentliche Akteure. 64 Prozent der Unternehmen bewerteten jeweils Anbieter von IT-Sicherheitslösungen und die Industrie- und Handelskammern/Handwerkskammern als geeignete Kooperationspartner, um die IT-Sicherheit im Unternehmen zu erhöhen. Als weitere geeignete Institutionen bewerteten 60 Prozent der Unternehmen externe Dienstleister und Berater und 45 Prozent kooperierten gerne mit Initiativen der Wirtschaft (z. B. ASW).

Deutlich seltener wurden von den Unternehmen öffentliche Institutionen als geeignete Kooperationspartner bewertet. So waren 54 Prozent der Ansicht, dass das BSI ein wichtiger Ansprechpartner im Themenfeld IT-Sicherheit ist. Eine entsprechende Unterstützung

[63] Davon gaben 46 Unternehmen an, welche Behörde sie konkret kontaktierten: 31 Unternehmen kontaktierten die Verfassungsschutzbehörden, 26 das BKA oder ein LKA, vier das Bundesministerium für Wirtschaft (BMWi), je zwei das BSI bzw. den Bundesnachrichtendienst (BND) (Mehrfachnennungen möglich).

durch die Polizei und die Verfassungsschutzbehörden wurde nur von ca. jedem fünften Unternehmen als geeignet eingeschätzt (vgl. BMWi 2012: 44).

5.7.1 Zusammenfassung Wichtige Akteure

- Eine effektive Abwehr von Ausforschung kann weder von Sicherheitsbehörden noch von Wirtschaftsverbänden und Unternehmen allein geleistet werden. Unternehmen profitieren von Kooperationen und Netzwerken zum **Erfahrungsaustausch.**
- Die Ergebnisse der Studien zeigen, dass Unternehmen im Bereich der Abwehr von Ausforschung häufiger mit **privaten Akteuren** zusammenarbeiteten als mit Behörden.
- Etwa zwei Drittel der Unternehmen nutzten **Beratungs- und Informationsangebote** privater Einrichtungen, während die Angebote öffentlicher Einrichtungen nur von rund 30 Prozent der Unternehmen in Anspruch genommen wurden. Von den Unternehmen, die bereits Opfer von Ausforschung geworden sind, kontaktierten ca. 20 Prozent die für den Wirtschafts- und Informationsschutz zuständigen Behörden, während ein Drittel ausschließlich mit privaten Dienstleistern kooperierte.
- Die Hilfestellungen privater Akteure wurden von den Unternehmen deutlich besser oder zumindest ähnlich gut/schlecht **bewertet** wie die Angebote öffentlicher Akteure.
- So wurden die Informationen von Behörden in einer Studie durchweg mit den Schulnoten 3,0 oder schlechter bewertet, während die Angebote von Verbänden oder privaten Dienstleistern immer besser als 3,0 abschnitten. Während ca. 60 Prozent der Unternehmen die Angebote privater Akteure als geeignet zur **Erhöhung der IT-Sicherheit** einstuften, wurden die Angebote der Sicherheitsbehörden von nur 20 Prozent der Unternehmen als hilfreich bewertet.

6. Resümee und Empfehlungen

Im Anschluss an die systematische Auswertung relevanter Fachliteratur und empirischer Studien, in deren Rahmen Unternehmen zu ihren Erfahrungen mit Ausforschungsangriffen befragt wurden, konnte in der vorliegenden Ausarbeitung gezeigt werden, wie sich die Phänomene Wirtschaftsspionage und Konkurrenzausspähung aus Sicht deutscher Unternehmen aktuell darstellen.

Folgende zentrale Ergebnisse können aus der Sekundäranalyse abgeleitet werden:

Die strafrechtlich relevante Unterscheidung zwischen Wirtschaftsspionage und Konkurrenzausspähung ist für Unternehmen weniger bedeutsam: Für viele hat sie eher eine akademische als eine praktische Bedeutung. Gleichwohl verfügen die zuständigen Sicherheitsbehörden über ein anderes Verständnis: Während Wirtschaftsspionage als die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung bzw. Aufklärung von Wirtschaftsunternehmen und Betrieben definiert wird, steht die Konkurrenzausspähung ausschließlich für die Ausforschung, die ein konkurrierendes Unternehmen oder eine Einzelperson gegen ein anderes Unternehmen betreibt.

Die Mehrheit der Unternehmen schätzt die Bedrohung durch Ausforschung für die deutsche Wirtschaft als hoch bis sehr hoch ein und geht zudem von einem zukünftigen Anstieg der Bedrohung aus. Das eigene Risiko wird von den Unternehmen dabei tendenziell niedriger eingeschätzt als das Risiko der Gesamtwirtschaft.

Über die aktuellsten Befragungen verteilt verzeichnete zwischen 2010 und 2013 laut eigener Aussage ca. jedes vierte Unternehmen mindestens einen Fall von Verrat von Geschäfts- und Betriebsgeheimnissen, ebenfalls ca. jedes vierte Unternehmen mindestens einen Fall von Datendiebstahl und ca. jedes sechste Unternehmen meldete mindestens einen Fall von WS/KA. Der Längsschnittvergleich zeigt, dass die Betroffenheitswerte der Unternehmen im Laufe der letzten Jahre mehrheitlich sanken oder stagnierten. Viele Autoren verweisen aber in ihren Studien darauf, dass die rückläufigen Tendenzen nicht unbedingt darauf hindeuten, dass die Ausforschung deutscher Unternehmen auch tatsächlich weniger wurde, sondern nennen andere Ursachen, wie z. B. eine genauere Identifizierung und Klassifizierung der verschiedenen Straftaten durch die Unternehmen. Dieser Rückgang der festgestellten Ausforschungsvorfälle, kann auch auf die gestiegene Bedrohungs*wahrnehmung* zurückzuführen sein: Unternehmen, die eine Bedrohung durch Ausforschung wahrnehmen und für mögliche Gefahren sensibilisiert sind, sind potentiell auch eher bereit, Schutzvorkehrungen zu treffen.

Etwa jeder dritte Fall von Ausforschung wurde rein zufällig entdeckt. Die Sicherheitsbehörden spielen eine untergeordnete Rolle bei der Aufdeckung, da in den meisten Fällen interne oder externe Hinweisgeber auf die Vorfälle aufmerksam machten.

Aktuelle und ehemalige Beschäftigte sind die wichtigste Tätergruppe, sie können bewusst oder unbewusst zu Tätern werden. Ausforschung geht zudem ebenfalls häufig von

Kunden, Lieferanten und Kooperationspartnern aus, was bedeutet, dass den Unternehmen in vielen Fällen die Täter persönlich bekannt sind. Ausländische Nachrichtendienste wurden in allen Studien hingegen nur von einem kleinen Teil der betroffenen Unternehmen als Täter identifiziert.

Schätzungen zum jährlichen finanziellen Schaden durch Ausforschung reichen von ein- bis zu dreistelligen Milliardenbeträgen. Im Gegensatz dazu wird nach Hochrechnungen auf der Grundlage der unternehmenseigenen Schadensangaben „lediglich" von einstelligen Milliardenbeträgen ausgegangen. Aber auch diese Zahlen sind nicht sehr verlässlich, da Unternehmen der Bestimmung des Schadens oft unterschiedliche Kriterien zugrunde legen.

Nur ein kleiner Teil der Unternehmen bringt Ausforschungsvorfälle zur Anzeige. Bei einem Verdacht auf Ausforschung sind häufig private Sicherheitsdienstleister die ersten Ansprechpartner und auch im Bereich der präventiven Abwehr von Ausforschung kooperieren die Unternehmen häufiger mit privaten Institutionen als mit staatlichen Behörden. Ihre Angebote und Dienstleistungen werden von vielen Unternehmen zudem besser bewertet als die Angebote von staatlichen Institutionen.

Viele Unternehmen sehen die Notwendigkeit von organisatorischen, personellen und IT-spezifischen Sicherheitsvorkehrungen für die Abwehr von Ausforschung, sind sich aber häufig nicht der schwerwiegenden Auswirkungen, die ein Ausforschungsvorfall für das Unternehmen haben kann, bewusst – somit werden vielfach nur Mindestvorkehrungen getroffen. Die Entwicklungen im Bereich der IKT führen zu neuen Risiken und erhöhen die Wahrscheinlichkeit, dass deutsche Unternehmen ausgeforscht werden.

Folgende Empfehlungen lassen sich aus der Fachliteratur und den empirischen Studien für die Sicherheitsbehörden ableiten:

Häufig wird den Unternehmen in der Fachliteratur empfohlen, sich im Verdachtsfall nicht sofort an die Strafverfolgungsbehörden zu wenden, da es ihnen nicht immer möglich sei, die Interessen der Unternehmen vollständig zu berücksichtigen. Gerät die Ausforschung eines Unternehmens an die Öffentlichkeit, führt dies möglicherweise zu Umsatzeinbußen und einem (hohen) Reputationsschaden für das betroffene Unternehmen. Bei einem Verdacht wenden sich Unternehmen somit häufiger an professionelle Sicherheitsunternehmen, da der Vorfall auf diese Weise nicht an die Öffentlichkeit gelangt und sie zudem selbst entscheiden können, wie mit den Ermittlungserkenntnissen verfahren werden soll (vgl. Schaaf

2009: 25). Gerade aber bei Vorfällen von Wirtschaftsspionage und Konkurrenzausspähung achten die Strafverfolgungsbehörden heutzutage auf eine besondere Sensibilität im Umgang mit betroffenen Unternehmen, da sie deren Sorgen vor einem Imageverlust und Wunsch nach Schadensbegrenzung kennen (vgl. Polizei Baden-Württemberg, ohne Jahresangabe, BKA 2014: 18 ff., Berliner Zeitung 2007). Gemäß dem Legalitätsprinzip sind die Strafverfolgungsbehörden verpflichtet, bei Kenntnis einer Straftat tätig zu werden. Für die Staatsanwaltschaft bestehen jedoch auch gesetzlich geregelte Ausnahmen vom Verfolgungszwang (vgl. Der Generalbundesanwalt beim Bundesgerichtshof, ohne Jahresangabe). Staatsanwaltschaft und Polizei ist es wichtig, den betroffenen Unternehmen den Handlungsspielraum aufzuzeigen und eine abgestimmte Vorgehensweise zu erarbeiten (vgl. BKA 2014: 19).

Auch unternehmensinterne Sanktionen im Rahmen von Compliance Management Systemen können ausschlaggebend dafür sein, dass Vorfälle den Strafverfolgungsbehörden nicht gemeldet werden. Es kann davon ausgegangen werden, dass sich auch weiterhin nur wenige Unternehmen im Verdachtsfall zeitnah an die Strafverfolgungsbehörden wenden werden.

Die Strafverfolgungsbehörden können über andere Wege wichtige Erkenntnisse zu der Phänomenentwicklung von Wirtschaftsspionage und Konkurrenzausspähung erhalten:

Eine Möglichkeit ist die Schaffung von Plattformen, die Unternehmen für einen vertrauensvollen Austausch mit den Strafverfolgungs- und Verfassungsschutzbehörden nutzen können (vgl. DIHK 2014). Denkbar ist auch eine Datenbank, in der die von Unternehmen anonym und freiwillig gemeldeten Ausforschungsvorfälle erfasst werden. Auf diese Weise stünde den Behörden eine bessere Basis für Lagebilder zur Verfügung, aus der Empfehlungen abgeleitet werden können.

Auch großangelegte repräsentative Opferbefragungen können den Sicherheitsbehörden relevante Informationen u. a. in Bezug auf die Betroffenheitsrate, das Anzeigeverhalten und die Schadenshöhe liefern. Der Bedarf an weiterer empirischer Forschung ist vorhanden. Die Sicherheitsbehörden sollten *eigene* repräsentative Dunkelfeld- und Opferbefragungen in Auftrag geben, um eine methodisch abgesicherte und transparente Vorgehensweise unter Berücksichtigung der eigenen Interessenslage gewährleisten zu können. Solch eine Befragung sollte speziell zu dem Thema WS/KA durchgeführt werden. Wichtig ist, dass die teilnehmenden Unternehmen eine genaue Anleitung für das Erhebungsinstrument (Fragebo-

gen) erhalten, in der u. a. vorgegeben wird, was unter Wirtschaftsspionage und unter Konkurrenzausspähung verstanden wird und wie der (finanzielle) Schaden berechnet werden soll. Im Rahmen so einer Unternehmensbefragung könnten die Sicherheitsbehörden darüber hinaus darauf achten, dass genauer zwischen den verschiedenen Akteursgruppen unterschieden wird (Strafverfolgungsbehörden, Verfassungsschutzbehörden, Netzwerke, private Unternehmen etc.), da solche Unterscheidungen in der Mehrzahl der ausgewerteten Befragungen fehlen. Zudem wäre es den Sicherheitsbehörden möglich, die Gründe der Unternehmen für eine unterbliebene Meldung eines Ausforschungsvorfalls sowie Empfehlungen und Vorschläge der Unternehmen zur Verbesserung des Schutzes vor Wirtschaftsspionage und Konkurrenzausspähung zu erheben – qualitative Aussagen, die bislang in den wenigsten Studien abgefragt wurden.

Häufig gaben Unternehmen an, dass ihnen die Arbeit der Sicherheitsbehörden sowie die zentralen Ansprechpartner im Bereich der Abwehr von Wirtschaftsspionage und Konkurrenzausspähung nicht bekannt sind. Auch wurden die Informations- und Beratungsangebote der Sicherheitsbehörden teilweise schlechter bewertet als die Angebote von privaten Sicherheitsunternehmen. Dies kann u. a. daran liegen, dass es mittlerweile eine große Anzahl an professionellen Beratungsunternehmen im Bereich Wirtschafts- und Informationsschutz gibt, für die es einfacher ist, die individuellen Interessen der Unternehmen zu wahren.

Es ist wichtig, dass die Sicherheitsbehörden ihre Angebote und Maßnahmen optimieren. So fordert der DIHK, dass die Bundesregierung die Sicherheitsbehörden personell und materiell dazu befähigt, wirksamer gegen Ausforschung vorgehen zu können (vgl. DIHK 2014). Optimierungsmöglichkeiten gibt es z. B. in Bezug auf die Handlungsfähigkeit und die Reaktionsgeschwindigkeit der Strafverfolgungsbehörden bei Straftaten im IT-Bereich, vor allem auch, wenn über Landesgrenzen hinweg agiert werden muss (vgl. Spiegel 2012 und IHK Nord 2013: 19).

Auch wünschen sich viele Unternehmen einen gemeinsamen Ansprechpartner im Bereich Wirtschafts- und Informationsschutz, der die verschiedenen Behörden wie BfV, BKA, BSI, BMWi etc. koordiniert (vgl. DIHK 2014). Es sollte für die Unternehmen leicht ersichtlich sein, wer bei einem Ausforschungsvorfall der richtige Ansprechpartner ist. Alle regionalen Ansprechpartner könnten z. B. auf einer zentralen Website zusammengefasst werden, auf der zudem die Ergebnisse relevanter Opferbefragungen präsentiert werden könnten.

Damit die Angebote und Maßnahmen der Sicherheitsbehörden im Bereich der Abwehr von Ausforschung sowie das konkrete Vorgehen der Behörden bei einem Fall von Ausforschung den Unternehmen besser bekannt werden, sollten die Behörden vermehrt in direkten Kontakt mit der Wirtschaft treten. Auf diese Weise können falsche Vorstellungen oder Befürchtungen aus dem Weg geräumt werden. Eine Kooperation mit Verbänden und Kammern ist zu empfehlen, da sie in dieser Hinsicht oft den engsten Kontakt zu Unternehmen pflegen und ihre wichtigsten Ansprechpartner sind (vgl. BMWi 2012: 10).

Die Europäische Agentur für Netz- und Informationssicherheit informiert die Behörden der Mitgliedsstaaten und die EU-Institutionen zur Netz- und Informationssicherheit in Europa. Darüber hinaus ist sie ein Forum, das die Kooperation und den Austausch zwischen europäischen Akteuren fördert und Kontakte zwischen EU-Institutionen, Behörden der Mitgliedsstaaten und europäischen Unternehmen, u. a. über öffentlich-private Partnerschaften in diesem Feld, erleichtert (vgl. European Union Agency for Network and Information Security, ohne Jahresangabe). Im Rahmen solcher (europäischer) Initiativen wäre es auch den deutschen Sicherheitsbehörden möglich, ihre Aufgaben, Belange und Interessen (vor allem bei den Unternehmen) bekannter zu machen und auf diese Weise mögliche Vorurteile ab- und Vertrauen aufzubauen. Erfolgreiche Beispiele für deutsche öffentlich-private Partnerschaften, in deren Rahmen sich Wirtschaft, Politik und Sicherheitsbehörden austauschen, sind z. B. die BSI-Initiative „Allianz für Cyber-Sicherheit“, die die Kooperation und den (Erfahrungs-) Austausch zwischen ihren Teilnehmern, Partnern und Multiplikatoren fördert (vgl. BSI 2013: 5 f.), das Sicherheitsforum Baden-Württemberg, die Sicherheitspartnerschaft gegen Wirtschaftskriminalität in Niedersachsen oder die Sicherheitspartnerschaft Nordrhein-Westfalen.

Anhang

Tabelle 9: Rahmendaten zu den ausgewerteten Studien

Auftraggebende Institution	Beteiligte Institutionen: an Datenerhebung, Auswertung etc.	Titel der Studie; Veröffentlichungsdatum	Erhebungszeitraum	Grundgesamtheit; Stichprobengröße	Anzahl befragter Unternehmen (Rücklauf)	Repräsentativität der Ergebnisse laut Studie
Sicherheitsforum Baden-Württemberg	Universität Lüneburg	Fall- und Schadensanalyse bezüglich Know-how-/ Informationsverlusten in Baden-Württemberg ab 1995; 10.06.2004	01.-03.2003	Unternehmen in Baden-Württemberg; 2.400	400 Unternehmen	ja, für Unternehmen in Baden-Württemberg und Deutschland
KPMG	TNS Emnid	Studie 2006 zur Wirtschaftskriminalität in Deutschland; 2006	k. A.	Unternehmen in Deutschland; k. A.	420 Unternehmen	ja, für Unternehmen in Deutschland
CORPORATE TRUST	Handelsblatt; Büro für Angewandte Kriminologie Hamburg	Studie: Industriespionage. Die Schäden durch Spionage in der deutschen Wirtschaft; 2007	08.-09.2007	Unternehmen in Deutschland; 7.486	741 Unternehmen	ja, für Unternehmen in Deutschland
Pricewaterhouse-Coopers; Martin-Luther-Universität Halle-Wittenberg	TNS Emnid	Wirtschaftskriminalität 2009 – Sicherheitslage in deutschen Großunternehmen; 09.2009	04.-05.2009	Großunternehmen in Deutschland; k. A.	500 Unternehmen	ja, für Großunternehmen in Deutschland
CORPORATE TRUST	Hochschule für Öffentliche Verwaltung Bremen	Studie: Gefahrenbarometer 2010 – Sicherheitsrisiken für den deutschen Mittelstand; 2009	01.-02.2009	Mittelständ. Unternehmen in D. (50–250 Beschäftigte, 10–50 Mio. Umsatz/Jahr) + größere Unternehmen, die sich zum Mittelstand zählen; 5.154	456 Unternehmen	k. A.

Auftraggebende Institution	Beteiligte Institutionen: an Datenerhebung, Auswertung etc.	Titel der Studie; Veröffentlichungsdatum	Erhebungszeitraum	Grundgesamtheit; Stichprobengröße	Anzahl befragter Unternehmen (Rücklauf)	Repräsentativität der Ergebnisse laut Studie
Bundesmin. für Inneres, Österreich/Bundesamt für Verfassungsschutz und Terrorismusbekämpfung	Fachhochschule Campus Wien	Gefahren durch Wirtschafts- und Industriespionage für die österreichische Wirtschaft; 18.11.2010	ab 09.2009	Unternehmen in Österreich; 9.200	220 Unternehmen	ja, für Unternehmen in Österreich
<kes> – Die Zeitschrift für Informations-Sicherheit; Microsoft	k. A.	<kes>/Microsoft-Sicherheitsstudie 2010 – Lagebericht zur Informations-Sicherheit; 2010	03.-05.2010	Unternehmen in Deutschland, Behörden, Wissenschaft/Forschung/ Schulen, Berater; k. A.	135 Befragte insgesamt/darunter ca. 94 Unternehmen	k. A.
KPMG	TNS Emnid, BKA, BMI	e-Crime-Studie 2010 Computerkriminalität in der deutschen Wirtschaft; 2010	04.-06.2010	Unternehmen in Deutschland; k. A.	500 Unternehmen	ja, für Unternehmen in Deutschland
KPMG	TNS Emnid	Wirtschaftskriminalität in Deutschland 2010 – Fokus Mittelstand; 2010	k. A.	Unternehmen in Deutschland; k. A.	300 Unternehmen	ja, für Unternehmen in Deutschland
Sicherheitsforum Baden-Württemberg	Ferdinand-Steinbeis-Institut; School of Governance, Risk & Compliance der Steinbeis-Hochschule Berlin	SiFo-Studie 2009/10 – Know-how-Schutz in Baden-Württemberg; 2010	07.-08.2009	Unternehmen in Baden-Württemberg; 4.000	239 Unternehmen	k. A.
Pricewaterhouse-Coopers; Universität Halle-Wittenberg	TNS Emnid Economy & Crime Research Center	Wirtschaftskriminalität 2011; 11.2011	05.-07.2011	Großunternehmen in Deutschland (> 500 Beschäftigte); k. A.	830 Unternehmen	ja, für Großunternehmen in Deutschland

Auftraggebende Institution	Beteiligte Institutionen: an Datenerhebung, Auswertung etc.	Titel der Studie; Veröffentlichungsdatum	Erhebungszeitraum	Grundgesamtheit; Stichprobengröße	Anzahl befragter Unternehmen (Rücklauf)	Repräsentativität der Ergebnisse laut Studie
Bundesministerium des Inneren	Bundesamt für Sicherheit in der Informationstechnik; secunet Security Networks	Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen. Grad der Sensibilisierung des Mittelstandes in Deutschland; 2011	k. A.	KMU in Deutschland; k. A.	30 Unternehmen	k. A.
Ernst & Young	VALID RESEARCH Marktforschung	Datenklau: Neue Herausforderungen für deutsche Unternehmen; 2011	04.2011	Unternehmen in Deutschland; k. A.	400 Unternehmen	ja, für Unternehmen in Deutschland
WIK – Zeitschrift für die Sicherheit der Wirtschaft	k. A.	WIK/ASW-Sicherheits-Enquête 2010/11; 2011	10.2010 – 01.2011	Sicherheitsberater und Unternehmen in Deutschland; keine Teilnahmebeschränkung	252 Befragte insgesamt/darunter 134 Unternehmen	nein
Bundesministerium für Wirtschaft und Technologie	INFO GmbH Markt- und Meinungsforschung	IT-Sicherheitsniveau in kleinen und mittleren Unternehmen; 09.2012	a) 08.-09.2011 b) 05.-06.2012	KMU in Deutschland (< 500 Beschäftigte, < 50 Mio. Umsatz/Jahr); a) 9.412, b) 5.056	a) 955 Unternehmen b) 922 Unternehmen	ja, für KMU in Deutschland
CORPORATE TRUST	Brainloop; TÜV SÜD	Industriespionage 2012 – Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar; 2012	01.-02.2012	Unternehmen in Deutschland; 6.924	597 Unternehmen	ja, für Unternehmen in Deutschland
Deutsche Telekom/T-Systems	Institut für Demoskopie Allensbach	Cyber Security Report 2012 – Ergebnisse einer repräsentativen Befragung von Entscheidungsträgern aus Wirtschaft und Politik; 2012	06.-07.2012	Großunternehmen in Deutschland (> 250 Beschäftigte, > 50 Mio. Umsatz/Jahr); k. A.	342 Befragte insgesamt/darunter 214 Unternehmen	ja, für Großunternehmen in Deutschland

Auftraggebende Institution	Beteiligte Institutionen: an Datenerhebung, Auswertung etc.	Titel der Studie; Veröffentlichungsdatum	Erhebungszeitraum	Grundgesamtheit; Stichprobengröße	Anzahl befragter Unternehmen (Rücklauf)	Repräsentativität der Ergebnisse laut Studie
<kes> – Die Zeitschrift für Informations-Sicherheit; Microsoft	k. A.	<kes>/Microsoft-Sicherheitsstudie 2012 – Lagebericht zur Informations-Sicherheit; 2012	03.-04.2012	Unternehmen in Deutschland, Behörden, Wissenschaft/Forschung/ Schulen, Berater; k. A.	133 Befragte insgesamt/darunter ca. 80 Unternehmen	k. A.
Europäische Kommission	Baker and McKenzie	Study on Trade Secrets and Confidential Business Information in the Internal Market; 04.2013	11.-12.2012	Unternehmen in Europa; k. A.	537 Unternehmen insgesamt/darunter 41 aus Deutschland	k. A.
Bundesverband der Deutschen Industrie	k. A.	BDI-Blitzumfrage: Aktuelles Stimmungsbild zur Betroffenheit deutscher Unternehmen von NSA-Abhörmaßnahmen; 28.08.2013	07.2013	Unternehmen in Deutschland; 300	ca. 60 Unternehmen	k. A.
Pricewaterhouse-Coopers; Universität Halle-Wittenberg	TNS Emnid; Economy & Crime Research Center der Martin Luther Universität Halle Wittenberg	Wirtschaftskriminalität und Unternehmenskultur 2013; 11.2013	a) 05.-07.2013 b) 09.2013	Großunternehmen in Deutschland (> 500 Beschäftigte); k. A.	a) 603 Unternehmen b) 250 Unternehmen	ja, für Großunternehmen in Deutschland
Arbeitsgemeinschaft Norddeutscher Industrie- und Handelskammern	Universität Hamburg, LKÄ MV, NI und SH, Polizeien Bremen und Hamburg	Unternehmensbefragung zur Betroffenheit der norddeutschen Wirtschaft von Cybercrime; 2013	01.-02.2013	Unternehmen in Norddeutschland; ca. 6.000	713 Unternehmen	k. A.

Auftraggebende Institution	Beteiligte Institutionen: an Datenerhebung, Auswertung etc.	Titel der Studie; Veröffentlichungsdatum	Erhebungszeitraum	Grundgesamtheit; Stichprobengröße	Anzahl befragter Unternehmen (Rücklauf)	Repräsentativität der Ergebnisse laut Studie
Ernst & Young	VALID RESEARCH Marktforschung	Datenklau: Neue Herausforderungen für deutsche Unternehmen; 2013	07.2013	Unternehmen in Deutschland; k. A.	400 Unternehmen	ja, für Unternehmen in Deutschland
KPMG	TNS Emnid	e-Crime Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz; 2013	06.-08.2012	Unternehmen in Deutschland, Österreich und der Schweiz; k. A.	700 Unternehmen insgesamt/darunter 500 aus Deutschland	ja, für Unternehmen in Deutschland, Österreich und der Schweiz
KPMG	School of Governance, Risk & Compliance der Steinbeis-Hochschule Berlin	Wirtschaftskriminalität Deutschland, Österreich, Schweiz im Vergleich; 2013	03.-07.2012	Unternehmen in Deutschland, Österreich und der Schweiz; k. A.	593 Unternehmen insgesamt/darunter 332 aus Deutschland	ja, für Unternehmen in Deutschland
Secusmart; Bundesverband IT-Sicherheit (TeleTrusT)	k. A.	Secure Mobile Computing 2013; 2013	09.-10.2013	Unternehmen in Deutschland; k. A.	106 Unternehmen	k. A.
WIK – Zeitschrift für die Sicherheit der Wirtschaft	k. A.	WIK/ASW-Sicherheits-Enquête 2012/13; 2013	10.2012 – 01.2013	Sicherheitsberater und Unternehmen in Deutschland; keine Teilnahmebeschränkung	279 Befragte insgesamt/darunter 126 Unternehmen	nein

Quelle: Eigene Darstellung

Literaturverzeichnis

Agentur "secure-it.nrw" (secure-it) 2008: *Wirtschaftsspionage und Konkurrenzausspähung: So schützen Firmenchefs ihr Unternehmen*. Bonn: IHK Bonn/Rhein-Sieg. URL: http://www.sicher-im-netz.de/sites/default/files/download-/sec1450_wirtschaftsspionage1.pdf, zugegriffen am 18.02.14.

Anderson, Ross/Barton, Chris/Böhme, Rainer/Clayton, Richard/van Eeten, Michel J.G./Levi, Michael/Moore, Tyler/Savage, Stefan 2012: *Measuring the Cost of Cybercrime*. Paper im Rahmen des Workshop on the Economics of Information Security, Berlin 25.-26. Juni 2012. URL: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf, zugegriffen am 18.02.14.

Arbeitsgemeinschaft Norddeutscher Industrie- und Handelskammern (IHK Nord) e. V. 2013: *Unternehmensbefragung zur Betroffenheit der norddeutschen Wirtschaft von Cybercrime*. Hamburg: IHK Nord e. V. URL: http://www.hannover.ihk.de/fileadmin/data/Dokumente-/Themen/Sicherheit/Studie_Cybercrime_Umfrageauswertung_10062013.pdf, zugegriffen am 18.02.14.

Arends, Holger/Kranawetter, Michael 2011: *Modell für ein unternehmensweites Security-Bewusstsein – Informationssicherheit ganzheitlich managen*. In: IT-SICHERHEIT 2011/2. Gelsenkirchen: Institut für Internet-Sicherheit, 52-55.

Balser, Markus 2014: *Wirtschaftsspionage. Angst vor Lauschangriff wächst*. In: Süddeutsche Zeitung, 01.02.2014. URL: http://www.sueddeutsche.de/wirtschaft/wirtschaftsspionage-angst-vor-lauschangriff-waechst-1.1877437, zugegriffen am 18.02.2014.

Bätz, Ralf/Claaßen, Uwe 2009: *Wirtschaftsspionage und Know-how-Verlust aus Sicht des niedersächsischen Verfassungsschutzes*. In: Bisanz, Stefan/Gerstenberg, Uwe (Hrsg.): Raubritter gegen den Mittelstand – Informationsschutz mittelständischer Unternehmen. Essen: Security Explorer, 37-50.

Berliner Zeitung 2007: Unternehmen stellen mehr Strafanzeigen. URL: http://www.berliner-zeitung.de/archiv/laut-einer-neuen-studie-zur-wirtschaftskriminalitaet-leiden-firmen-unter-vandalismus-und-diebstahl-unternehmen-stellen-mehr-strafanzeigen,10810590,10526158.html, zugegriffen am 18.02.2014.

Bernd-Striebeck, Uwe 2012: *Abwehr von Industriespionage*. In: kes 2012/2. Ingelheim: SecuMedia, 18-20.

Blass, Katrin 2011: *Kronjuwelen müssen geschützt werden. Interview mit Helmut Albert.* In: SR-online. URL: http://www.sr-online.de/sronline/nachrichten/panorama-/wirtschaftsspionage_interview_verfassungsschutz100~print.html, zugegriffen am 18.02.14.

Blume, Andreas 2008: *Überleben im globalen Wirtschaftskrieg*. In: Die neue Polizei 2008/02, 31-35.

Bundesamt für Sicherheit in der Informationstechnik (BSI) 2011: *Studie zur IT-Sicherheit in kleinen und* mittleren *Unternehmen. Grad der Sensibilisierung des Mittelstandes in Deutschland*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/-Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile, zugegriffen am 18.02.14.

Bundesamt für Sicherheit in der Informationstechnik (BSI) 2013: *Allianz für Cyber-Sicherheit*. Bonn: Bundesamt für Sicherheit in der Informationstechnik. URL: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/ACS_Flyer_PDF.pdf?__blob=publicationFile, zugegriffen am 18.02.14.

Bundesamt für Verfassungsschutz (BfV) 2008: *Spionage gegen Deutschland – Aktuelle Entwicklungen*. Köln: Bundesamt für Verfassungsschutz. URL: http://www.verfassungsschutz.brandenburg.de/media_fast/4055/Spinage%20gegen%20Deutschland.pdf, zugegriffen am 18.02.14.

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) 2010: *Gefahren durch Wirtschafts- und Industriespionage für die österreichische Wirtschaft. Studie 2010*. Wien: Bundesministerium für Inneres. URL: www.fh-campuswien.ac.at-/index.php?download=3067.pdf\u200e, zugegriffen am 18.02.14.

Bundeskriminalamt (BKA) 2014: *Cybercrime – Handlungsempfehlungen für die Wirtschaft in Fällen von* Cybercrime. URL: http://www.bka.de/DE/ThemenABisZ/Deliktsbereiche/-InternetKriminalitaet/HandlungsempfehlungenWirtschaft/handlungsempfehlungen__node.html?__nnn=true, zugegriffen am 18.02.2014.

Bundesministerium des Inneren (BMI) 2008: *Verfassungsschutzbericht 2008*. URL: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/vsb_2008.pdf?__blob=publicationFile, zugegriffen am 18.02.2014.

Bundesministerium des Innern (BMI) 2013b: *Verfassungsschutzbericht 2012*. URL: http://www.verfassungsschutz.de/de/download-manager/_vsbericht-2012.pdf, zugegriffen am 18.02.2014.

Bundesministerium des Inneren (BMI)/Bundesvereinigung der Deutschen Industrie/Deutscher Industrie- und Handelskammertag 2013a: *Wirtschaftsschutz in Deutschland 2015 – Vertrauen, Information, Prävention*. URL: http://www.dihk.de/ressourcen/downloads/erklaerung-wirtschaftsschutz-dihk-bdi-bmi.pdf/at_download/file?mdate=1377846315060, zugegriffen am 18.02.2014.

Bundesministerium für Wirtschaft und Technologie (BMWi) 2012: *IT-Sicherheitsniveau in kleinen und mittleren Unternehmen*. URL: http://www.bmwi.de/BMWi/Redaktion/PDF/S-T/studie-it-sicherheit,property%3Dpdf,bereich%3Dbmwi2012,sprache%3Dde,rwb%3Dtrue.pdf, zugegriffen am 18.02.14.

Bundesregierung 2013: *Deutschlands Zukunft gestalten. Koalitionsvertrag zwischen CDU, CSU und SPD. 18. Legislaturperiode*. URL: http://www.bundesregierung.de/Content/DE/_Anlagen/2013/2013-12-17-koalitionsvertrag.pdf;jsessionid=DB897A67B32484EA50530A3F6CF41352.s2t2?__blob=publicationFile&v=2, zugegriffen am 18.02.14.

Bundesverband der Deutschen Industrie e. V. (BDI) 2013: *BDI-Blitzumfrage: Aktuelles* Stimmungsbild *zur Betroffenheit deutscher Unternehmen von NSA-Abhörmaßnahmen*. URL: http://www.bdi.eu/images_content/SicherheitUndVerteidigung/BDI-Blitzumfrage_NSA_Webseite.pdf, zugegriffen am 18.02.14.

Corporate Trust Business Risk & Crisis Management GmbH 2007: *Studie: Industriespionage. Die Schäden durch Spionage in der deutschen Wirtschaft*. München: Verlagsgruppe Handelsblatt.

Corporate Trust Business Risk & Crisis Management GmbH 2010: *Studie: Gefahrenbarometer 2010. Sicherheitsrisiken für den deutschen Mittelstand*. München: Verlagsgruppe Handelsblatt. URL: http://www.corporate-trust.de/studie/Gefahrenbarometer2010.pdf, zugegriffen am 18.02.14.

Corporate Trust Business Risk & Crisis Management GmbH 2012: *Studie: Industriespionage 2012. Aktuelle Risiken für die deutsche Wirtschaft durch Cyberwar*. München: Verlagsgruppe Handelsblatt. URL: http://docs.dpaq.de/703-120423_-_studie_industriespionage_2012.pdf, zugegriffen am 18.02.14.

Cressey, Donald Ray 1973: *Other People's Money.* Montclair: Patterson Smith.

Der Generalbundesanwalt beim Bundesgerichtshof: Staatsanwaltschaftliche Ermittlungstätigkeit und Legalitätsprinzip. URL: http://www.generalbundesanwalt.de/de/legal.php, zugegriffen am 18.02.2014.

Detica 2011: *The Cost of Cyber Crime*. Surrey: Detica Limited. URL: https://www.gov.uk-/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf, zugegriffen am 18.02.2014.

Deutsche Telekom/T-Systems 2012: *Cyber Security Report 2012. Ergebnisse einer* repräsentativen *Befragung von Entscheidungsträgern aus Wirtschaft und Politik*. URL: http://www.t-systems.com/servlet/contentblob/ContentPool-Online2012/de/umn/uti-/988884_1/blobBinary/Sicherheitsreport-2012-teil2-ps.pdf?ts_layoutId=378, zugegriffen am 18.02.14.

Deutscher Industrie- und Handelskammertag (DIHK) 2014: *DIHK wünscht sich Beauftragten für* Wirtschaftsschutz. URL: http://www.dihk.de/presse/meldungen/2014-01-10-wernicke-wirtschaftsspionage, zugegriffen am 18.02.14.

Ernst & Young GmbH 2011: *Datenklau: Neue Herausforderungen für deutsche Unternehmen. Ergebnisse einer* Befragung *von 400 deutschen Unternehmen*. URL: http://www.netzwerk.de/de/pdf/E+Y%20Datenklau.pdf, zugegriffen am 18.02.14.

Ernst & Young GmbH 2013: *Datenklau: Neue Herausforderungen für deutsche Unternehmen – Ergebnisse einer* Befragung *von 400 deutschen Unternehmen*. URL: http://www.ey.com-/Publication/vwLUAssets/Praesentation_-_Datenklau_2013/$FILE/EY-Datenklau-2013.pdf, zugegriffen am 18.02.14.

Europäische Kommission 2013a: *Study on Trade Secrets and Confidential Business Information* in *the Internal Market*. URL: http://ec.europa.eu/internal_market-/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf, zugegriffen am 18.02.14.

Europäische Kommission 2013b: *Appendix 17 to Study on Trade Secrets and Confidential Business Information in the Internal Market*. URL: http://ec.europa.eu/internal_market-/iprenforcement/docs/trade-secrets/130711_appendix-17_en.pdf, zugegriffen am 18.02.14.

European Union Agency for Network and Information Security: What does ENISA do? URL: http://www.enisa.europa.eu/about-enisa/activities, zugegriffen am 18.02.14

Eurostat 2014: *Bruttoinlandsprodukt zu Marktpreisen*. URL: http://epp.eurostat.ec.europa.eu/tgm/table.do?tab=table&init=1&language=de&pcode=tec00001&plugin=0&tableSelection=2, zugegriffen am 18.02.14.

Even, Burkhard 2013: *Wirtschaftsspionage – vielfältige Risiken erfordern gemeinsames Handeln. Prävention durch Information*. In: IT-Sicherheit 2013/2, 36-39.

Even, Burkhard 2013b: *Begrüßung und Keynote des Abteilungsleiters Spionageabwehr im BfV*. In: Bundesamt für Verfassungsschutz: Proaktiver Wirtschaftsschutz: Prävention durch Information – Tagungsband der 7. Sicherheitstagung des BfV und der ASW. Köln: BfV, 5-11.

Focus Online 2014: *Schaden von 100 Milliarden Euro? Ingenieure warnen vor milliardenteurer Spionage*. In: Focus Online, 03.02.2014. URL: http://www.focus.de-/finanzen/news/ingenieursverband-schlaegt-alarm-wirtschaftsspionage-kostet-unternehmen-100-milliarden-euro_id_3586652.html, zugegriffen am 18.02.2014.

George, Michael 2013: *Cyberwar und Wirtschaftsspionage: Ein Strategiewechsel bei der Abwehr ist erforderlich*. In: der Kriminalist 2013/4, 23-25.

Glitza, Klaus-Henning 2012: *Der Spion von nebenan – Deutschlands jüngster Spionagefall*. In: CD Sicherheits-Management 2012/3-4, 114-121.

Gogolinski, Jim 2013: *Empfehlungen für den Kampf gegen zielgerichtete Angriffe.* In: Trend Micro Deutschland. URL: http://www.trendmicro.de/media/wp/suggestions-to-help-companies-with-the-fight-against-targeted-attacks-whitepaper-de.pdf, zugegriffen am 18.02.14.

Guldner, Jan 2014: *Trojanischer Ferrari – Bedingt abwehrbereit: Deutsche Unternehmen im Visier der* Wirtschaftsspionage. In: Internationale Politik 2014/1, 22-26.

Handelsblatt 2013: *Wirtschaftsspionage. 50-Milliarden-Schaden*. In: Handelsblatt, 28.08.2013. URL: http://www.handelsblatt.com/politik/deutschland/wirtschaftsspionage-50-milliarden-schaden/8705934.html, zugegriffen am 18.02.2014.

Heise 2011: *Innenministerium warnt vor zunehmender Wirtschaftsspionage*. In: heise Security, 07.04.2011. URL: http://www.heise.de/security/meldung/Innenministerium-warnt-vor-zunehmender-Wirtschaftsspionage-1223563.html, zugegriffen am 18.02.2014.

Höfer, Thomas 2009: *Kryptografie ist ein wichtiger Bestandteil des Informationsschutzes – Schlüssel zu mehr Sicherheit*. In: IT-Sicherheit 2009/3, 44-45.

Huber, Alexander 2009: *Spionageabwehr. Von ignorierter Pflicht zum Wettbewerbsvorteil*. In: Intelligenter Produzieren 2009/5, 40-41.

Huber, Alexander 2010: *Wirtschaftsspionage und Konkurrenzausspähung als Phänomene zunehmender Kooperationen und veränderter Loyalität*. In: Beschorner, Thomas/Schank, Christoph/Schmidt, Matthias/Vorbohle, Kristin (Hrsg.): Kooperation und Ethik. München: Rainer Hampp, 109-116.

Karden, Wilfried 2011: *Wirtschaftsspionage und IT – Weltkrieg um Informationen*. In: IT-Sicherheit 2011/4, 18-19.

kes – Die Zeitschrift für Informations-Sicherheit 2010: *<kes>/Microsoft-Sicherheitsstudie 2010 – Lagebericht zur Informations-Sicherheit*. In: kes 2010/4. Ingelheim: SecuMedia Verlags-GmbH.

kes – Die Zeitschrift für Informations-Sicherheit 2012*: <kes>/Microsoft-Sicherheitsstudie 2012 – Lagebericht zur Informations-Sicherheit*. In: kes 2012/4,5,6. Ingelheim: SecuMedia Verlags-GmbH.

Klingelhöller, Wolf 2008: *Wirtschaftsspionage via Internet*. In: Bundesamt für Verfassungsschutz (BfV): Braucht Ihr Sicherheitsbewusstsein ein Update? Tagungsband der 3. Sicherheitstagung des BfV und der ASW. Köln: BfV, 26-31.

KPMG AG 2010a: *e-Crime-Studie 2010. Computerkriminalität in der deutschen Wirtschaft*. URL: http://www.kpmg.de/docs/20100810_kpmg_e-crime.pdf, zugegriffen am 18.02.14.

KPMG AG 2010b: *Wirtschaftskriminalität in Deutschland 2010. Fokus Mittelstand*. URL: http://www.desa-berlin.de/documents/StudieKPMG-2009-20091220_Wirtschaftskriminalitaet.pdf, zugegriffen am 18.02.14.

KPMG AG 2013a: *e-Crime. Computerkriminalität in der deutschen Wirtschaft mit Kennzahlen für Österreich und Schweiz*. URL: http://www.tns-emnid.com-/politik_und_sozialforschung/pdf/Studie_e-Crime.pdf, zugegriffen am 18.02.14.

KPMG AG 2013b: *Wirtschaftskriminalität. Deutschland, Österreich, Schweiz im Vergleich*. URL: http://www.kpmg.com/CH/de/Library/Articles-Publications/Documents/Advisory-/pub-20130313-wirtschaftskriminalitaet-de.pdf, zugegriffen am 18.02.14.

Le Figaro 2011: *La France, as de l'espionnage industriel*. In: Le Figaro, 04.01.2011. URL: http://www.lefigaro.fr/flash-actu/2011/01/04/97001-20110104FILWWW00385-la-france-as-de-l-espionnage-industriel.php, zugegriffen am 18.02.14.

Leiner, Klaus-G. 2008: *Datendiebe und Spione – Möglichkeiten und Grenzen privater Ermittlungen in Betrieben*. In: Die neue Polizei 2008/02, 40-41.

Litzcke, Sven 2010: *Wirtschafts- und Industriespionage – Bedrohungen für Unternehmen*. In: Tagungsband der 2. Fachtagung der Hochschule der Polizei, 69-79.

Meissinger, Jan 2005: *Gefahren und Bedrohungen durch Wirtschafts- und Industriespionage in Deutschland*. Hamburg: Verlag Dr. Kovac.

Nathusius, Ingo 2001: *Wirtschaftsspionage: Gefahren, Strukturen und Bekämpfung*. Heidelberg: Kriminalistik Verlag.

Niemantsverdriet, Jelle 2011: *Basis-Best-Practices für IT-Sicherheit – Datenverletzungen und Industriespionage verhindern*. In: IT-Sicherheit 2011/4, 26-27.

Nuri, Midia 2009: *Wirtschaftsspionage. Mittelstand im Visier von Wirtschaftsspionen*. In: Handelsblatt, 04.03.2009. URL: http://www.handelsblatt.com/unternehmen-/mittelstand/wirtschaftsspionage-mittelstand-im-visier-von-wirtschaftsspionen-/3127338.html, zugegriffen am 18.02.2014.

Oelmaier, Florian 2012: *Mehr als Abwehr – Umfassende Sicherheitsstrategien brauchen auch eine gute Vorfallsbearbeitung und Vorsorge zur Forensik*. In: kes 2012/6, 24-27.

Peil, Florian 2013: *Wir müssen aufwachen – und wichtige Informationen besser schützen*. In: WIK 2013/6. Ingelheim: SecuMedia Verlags-GmbH, 14-17.

Polizei Baden-Württemberg: Landeskriminalamt Baden-Württemberg – Bekämpfung von Cybercrime. URL: http://www.polizei-bw.de/Dienststellen/LKA/Seiten/Cybercrime.aspx, zugegriffen am 18.02.2014.

PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft (PwC)/Martin-Luther-Universität Halle-Wittenberg 2009: *Wirtschaftskriminalität 2009. Sicherheitslage in deutschen Großunternehmen*. URL: http://www.pwc.de/de/risiko-management/assets-/Studie-Wirtschaftskriminal-09.pdf, zugegriffen am 18.02.14.

PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft (PwC)/Martin-Luther-Universität Halle-Wittenberg 2011: *Wirtschaftskriminalität 2011*. URL: http://www.pwc.de/de_DE/de/risiko-management/assets/wikri-studie-2011.pdf, zugegriffen am 18.02.14.

PricewaterhouseCoopers AG Wirtschaftsprüfungsgesellschaft (PwC)/Martin-Luther-Universität Halle-Wittenberg 2013: *Wirtschaftskriminalität und Unternehmenskultur 2013*. URL: http://files.vogel.de/vogelonline/vogelonline/files/5947.pdf, zugegriffen am 22.03.14.

Proschko, Rudolf 2010: *Schutz von Betriebsgeheimnissen. Phänomen Wirtschaftsspionage – unentdeckt und unterschätzt*. In: IT-Sicherheit 2010/4, 18-19.

Protector 2013: *Interview mit Michael George: Anlaufstelle für Opfer von Wirtschaftsspionage. Den Teufelskreis durchbrechen.* PROTECTOR 2013/10, 22-23.

Reuters 2013: *Verfassungsschutz – Cyber-Spionage kostet Firmen über 50 Mrd Euro*. In: Reuters Deutschland, 13.11.2013. URL: http://de.reuters.com/article/domesticNews-/idDEBEE9AC02G20131113, zugegriffen am 18.02.2014.

Röder, Nils 2011: *Industriespionage: Risikofaktor Mensch*. Masterarbeit, Fachhochschule Hannover. URL: http://serwiss.bib.hs-hannover.de/frontdoor/index/index/docId/298, zugegriffen am 18.02.2014.

RP Online 2014: Interview mit VDI-Chef Ralph Appel. „100 Milliarden Euro Spionage-Schaden“. In: Rheinische Post Online, 03.02.2014. URL: http://www.rp-online.de/wirtschaft/vdi-chef-ralph-appel-100-milliarden-euro-spionage-schaden-aid-1.4006616, zugegriffen am 18.02.2014.

Sack, Dieter K. 2008: *Gefährdungsaspekte und Lösungsansätze für Unternehmen – Das integrierte Informationsschutzkonzept I und II.* In: WIK 2008/1 und WIK 2008/2, Ingelheim: SecuMedia Verlags-GmbH, 19-21 und 19-23.

Sarin, André 2010: *Abhöraktionen, Industriespionage, Datenklau. IT-Sicherheit als Herausforderung für den Mittelstand*. In: Niederrhein Manager 2010/13, 72-73. URL: http://www.niederrhein-manager.de/sites/nrmdrupal.mmh.ag/files-/artikelpdfs/IT_Sicherheit.pdf, zugegriffen am 18.02.2014.

Schaaf, Christian 2009: *Industriespionage. Der große Angriff auf den Mittelstand*. Stuttgart: Richard Boorberg Verlag.

Schnaas, Dieter 2014: *Die Angst vor der Innovationsperipherie. Wirtschaftsspionage ganz neuer Qualität gefährdet den Vorsprung des Westens*. In: Internationale Politik 2014/1, 8-14. URL: https://zeitschrift-ip.dgap.org/de/archiv/ausgaben/jahrgang/2014/phish-chips, zugegriffen am 18.02.2014.

Schubert, Rolf 2010: *Wirtschafts- und Konkurrenzspionage sowie Proliferation – Auswertung öffentlich verfügbarer Quellen aus kriminalpolizeilicher Sicht.* In: Kriminalistisch-Kriminologische Schriften der hessischen Polizei im Intranet. Wiesbaden: Hessisches Landeskriminalamt.

Schwind, Hans-Dieter 2013: *Kriminologie: Eine praxisorientierte Einführung mit Beispielen, 22. Auflage*. Heidelberg: Kriminalistik.

Secusmart GmbH/TeleTrusT – Bundesverband IT-Sicherheit e. V. 2013: *Report. Secure Mobile Computing 2013*. URL: http://euromarcom.de/2013/12/wirtschaft-erwartet-verluste-von-uber-10-mrd-euro-durch-spionageattacken, zugegriffen am 11.12.13.

Sicherheitsforum Baden-Württemberg/Universität Lüneburg 2004: *Fall- und Schadensanalyse bezüglich Know-how-/Informationsverlusten in Baden-Württemberg ab 1995*. URL: http://www.connect-community.de/Events/rheinland2008/vortraege/Studie-Uni-Lueneburg.pdf, zugegriffen am 18.02.14.

Sicherheitsforum Baden-Württemberg 2010: *SiFo-Studie 2009/10. Know-how-Schutz in Baden-Württemberg*. Stuttgart: Steinbeis-Edition. URL: http://www.sicherheitsforum-bw.de/pb/site/sifo/get/documents/IV.Dachmandant/Sifo/PDF/SiFo-Studie%202009-10%20-%20Know-how-Schutz%20in%20Baden-W%C3%BCrttemberg.pdf, zugegriffen am 18.02.14.

Sicherheitsforum Baden-Württemberg 2010b: *SiFo-Studie 2009/10. Handlungsempfehlungen für Unternehmen*. Stuttgart: Steinbeis-Edition. URL: http://www.sicherheitsforum-bw.de/pb/site/sifo/get/documents/IV.Dachmandant/Sifo-/PDF/SiFo-Studie%202009-10%20-%20Handlungsempfehlungen%20f%C3%BCr%20Unternehmen.pdf, zugegriffen am 18.02.14.

Slovic, Paul 1999: *Trust, Emotion, Sex, Politics, and Science*: *Surveying the Risk-Assessment Battlefield*. In: Risk Analysis 19/4, S. 689-700.

Spiegel 2012: Industriespionage: Alles, nur keine Polizei! URL: http://www.spiegel.de-/wirtschaft/industriespionage-alles-nur-keine-polizei-a-814548.html, zugegriffen am 18.02.14.

Staron, Joachim/Tempel, Sylke 2014: *Die wirtschaftliche und gesellschaftliche Stabilität ist in Gefahr. Spionageexperte Alexander Huber über die Auswirkungen des Ausspähens*. In: Internationale Politik 2014/1, 16-21.

Statistisches Bundesamt 2014: *Volkswirtschaftliche Gesamtrechnung*. URL: https://www.destatis.de/DE/ZahlenFakten/Indikatoren/LangeReihen/Volkswirtschaftliche Gesamtrechnungen/lrvgr02.html, zugegriffen am 18.02.2014.

Többens, Hans W. 2000: *Wirtschaftsspionage und Konkurrenzausspähung in Deutschland*. In: NStZ 2000, 505-513.

Tsolkas, Alexander/Wimmer, Friedrich 2013: *Wirtschaftsspionage und Intelligence Gathering. Neue Trends der wirtschaftlichen Vorteilsbeschaffung*. Wiesbaden: Vieweg + Teubner.

Verizon 2011: *2011 Data Breach Investigations Report*. URL: http://www.verizon enterprise.com/DBIR/2011/download.xml, zugegriffen am 18.02.2014.

Verizon 2013: *2013 Data Breach Investigations Report*. URL: http://www.verizon enterprise.com/DBIR/2013/download.xml, zugegriffen am 18.02.14.

Warnecke, Gundula 2010: *Quellen illegalen Know-how-Abflusses aus Industrieunternehmen und Strategien gegen Industriespionage*. In: Fussan, Carsten (Hrsg.): Managementmaßnahmen gegen Produktpiraterie und Industriespionage, 249-333.

Wiedemann, Peter M./Mertens, Johannes 2005: *Sozialpsychologische Risikoforschung*. In: Technikfolgenabschätzung – Theorie und Praxis Nr. 3, 14 Jg. 38-45. URL: http://www.tatup-journal.de/downloads/2005/tatup053_wime05a.pdf, zugegriffen am 18.02.2014.

WIK Zeitschrift für die Sicherheit der Wirtschaft 2011: *WIK-Sicherheits-Enquête 2010/2011*. In: WIK 2011/1,2,3. Ingelheim: SecuMedia Verlags-GmbH.

WIK Zeitschrift für die Sicherheit der Wirtschaft 2013: *WIK-Sicherheits-Enquête 2012/2013*. In: WIK 2013/1,2. Ingelheim: SecuMedia Verlags-GmbH.

Ziercke, Jörg 2008: *Wirtschaftsspionage im Fadenkreuz des Bundeskriminalamtes*. In: Die neue Polizei 2008/02, 10-13.

Ziercke, Jörg 2012: *Die Gefährdungslage in Deutschland aus Sicht der Wirtschaft*. In: Handschuh, Andreas/Ring, Gerhard (Hrsg.): „Sicher forschen und entwickeln“ – 1. Freiberger Sicherheitskonferenz. Baden-Baden: Nomos, 97-113.