Industriespionage –
Risikofaktor Mensch

Nils Röder

Vorwort

Dieser Text ist eine überarbeitete Version der gleichnamigen Arbeit, die im Juni 2011 von der Hochschule Hannover, Fakultät IV – Abteilung Betriebswirtschaft als Masterarbeit angenommen wurde.

Mein erster Dank gilt dem niedersächsischen Landesamt für Verfassungsschutz und dem Arbeitskreis der Sicherheitsbevollmächtigten in Niedersachsen. Insbesondere möchte ich mich hier bei Herrn Claaßen, Herrn Bertram, Herrn Kohnert und Herrn Köster bedanken, ohne die eine Gewinnung derart renommierter Interviewpartner auf dem Gebiet des Informationsschutzes nicht möglich gewesen wäre. Ein gesonderter Dank gilt daher auch den acht Gesprächspartnern, die zur Geheimhaltung der Identität der Unternehmen, nicht genannt werden können. Des Weiteren möchte ich mich bei Herrn Prof. Dr. Litzcke und Herrn Prof. Dr. Dr. Jaspersen für die Betreuung seitens der Hochschule Hannover und die zahlreichen konstruktiven Anregungen zur Anfertigung der Masterarbeit bedanken. Nicht zuletzt danke ich auch meiner Familie und meinen Freunden für die vielfältige Unterstützung.

Hannover, im Juli 2011

Nils Röder

Inhaltsverzeichnis

Abkürzungsverzeichnis ..... **VI**

Abbildungsverzeichnis ..... **VIII**

Tabellenverzeichnis ..... **IX**

Kurzfassung ..... **X**

1 Einführung **1**

1.1 Problemstellung und Motivation 1

1.2 Zielsetzung 4

1.3 Vorgehensweise 4

2 Theoretischer Hintergrund **7**

2.1 Industriespionage 7

2.1.1 Begriffsklärung 7

2.1.2 Abgrenzung 9

2.1.3 Gefährdete Branchen und Unternehmen 12

2.1.4 Quantitative und qualitative Bewertung von Spionageschäden 14

2.1.5 Methoden der Informationsbeschaffung 16

2.1.5.1 Human Intelligence (HUMINT) 16

2.1.5.2 Technical Intelligence (TECHINT) 19

2.1.5.3 Open Source Intelligence (OSINT) 22

2.2 Information und Wissen als entscheidender Wettbewerbsfaktor 23

2.2.1 Unternehmerische Relevanz von Information und Wissen 23

2.2.2 Abgrenzung und Systematisierung von Wissen 24

2.2.3 Betriebliche Wissensträger 27

2.3 Gefahrenpotenziale eines Know-how-Abflusses 28

2.3.1 Mensch 28

2.3.2 Organisation 32

2.3.3 Technik ... 34
2.3.4 Recht ... 35
3 Methode ... 38
3.1 Stichprobe ... 38
3.2 Experteninterviews ... 40
3.3 Durchführung ... 41
3.4 Auswertung ... 43
4 Ergebnisse ... 45
4.1 Risikoanalyse ... 45
4.2 Risikobewertung ... 48
4.3 Präventive und repressive Spionageabwehrmaßnahmen ... 49
4.3.1 Personal ... 50
4.3.2 Organisation ... 56
4.3.3 Technik ... 60
4.3.4 Recht ... 63
5 Diskussion ... 68
5.1 Integration der Ergebnisse ... 68
5.2 Grenzen ... 74
5.3 Ausblick ... 75
Literatur ... 77
Anhang ... 85
A Leitfaden für die Experteninterviews ... 86
B Transkripte ... 90
B1 Transkript 1 ... 90
B2 Transkript 2 ... 103
B3 Transkript 3 ... 119

B4 Transkript 4 134
B5 Transkript 5 147
B6 Transkript 6 160
B7 Transkript 7 167
B8 Transkript 8 178

Abkürzungsverzeichnis

ASW	Arbeitsgemeinschaft für Sicherheit in der Wirtschaft
BDI	Bundesverband der Deutschen Industrie
BfV	Bundesamt für Verfassungsschutz
BVerfSchG	Bundesverfassungsschutzgesetz
BVW	Betriebliches Vorschlagswesen
CI	Competitive Intelligence
CIA	Central Intelligence Agency
DGSE	Direction Générale de la Sécurité
DIHT	Deutscher Industrie- und Handelstag
DIW	Deutsches Institut für Wirtschaftsforschung
DPMA	Deutsches Patent- und Markenamt
GM	General Motors
HUMINT	Human Intelligence
IfM	Institut für Mittelstandsforschung
IMINT	Imagery Intelligence
KMU	Klein- und mittelständische Unternehmen
LfV	Landesamt für Verfassungsschutz
MASINT	Measurement und Signature Intelligence
NSA	National Security Agency
OSINT	Open Source Intelligence
PWC	PriceWaterhouseCoopers
RlP	Rheinland-Pfalz
SiFo BW	Sicherheitsforum Baden-Württemberg
SIGINT	Signal Intelligence
TECHINT	Technical Intelligence

TRIPs	Trade-Related Aspects of Intellectual Property Rights
UWG	Gesetz gegen unlauteren Wettbewerb
VW	Volkswagen
ZEW	Zentrum für Europäische Wirtschaftsforschung

Abbildungsverzeichnis

Abbildung 1: Allgemeiner Prozess der Konkurrenzbeobachtung 11

Abbildung 2: Spionagegefährdete Branchen 13

Abbildung 3: Immaterielle Schäden in Unternehmen 15

Abbildung 4: Ablauf eines Social-Engineering-Angriffs 18

Abbildung 5: Fraud Triangle 31

Abbildung 6: Bewerberüberprüfung in Abhängigkeit zur hierarchischen Position der Stelle . 51

Abbildung 7: Katalog von Spionageabwehrmaßnahmen 73

Tabellenverzeichnis

Tabelle 1: Explizites vs. Implizites Wissen 26

Tabelle 2: Mögliche Spionageangriffe auf natürliche und unnatürliche Wissensträger 28

Tabelle 3: Unternehmensklassifikation 39

Tabelle 4: Spionageabwehrmaßnahmen der befragten Unternehmen 66

Kurzfassung

Durch die Globalisierung und den verschärften internationalen Wettbewerb sind innovative Unternehmen in zunehmendem Maße durch Industriespionage bedroht. Eine besondere Rolle kommt hierbei dem Faktor Mensch zu, der das größte Risiko für einen ungewollten Know-how-Abfluss darstellt. Hiervon ausgehend untersucht die vorliegende Arbeit, welche präventiven und repressiven Spionageabwehrmaßnahmen Unternehmen zur Verbesserung der personellen Sicherheit zur Verfügung stehen. Nach einer theoretischen Einführung in das Thema werden die Ergebnisse von acht Experteninterviews vorgestellt und in die bestehende Literatur integriert. Dabei zeigen die Ergebnisse, dass es keine Musterlösung gibt, sondern dass je nach Unternehmen, spezifischer Bedrohungslage und wirtschaftlichen Rahmenbedingungen ein individuelles und ganzheitliches Informationsschutzkonzept zu entwickeln ist.

Abstract

Due to globalization and increased international competition, innovative companies are increasingly threatened by industrial espionage. Regarding this, the human factor includes the highest risk of an unintentional knowledge outflow. Based on these facts, the present study investigates which preventive and repressive measures of counter-intelligence are available to improve the company's personnel security. After a theoretical introduction to the topic of industrial espionage, the results of eight interviews with experts are presented and integrated into the existing literature. In doing so, the results reveal that there is no sample solution, so that each company needs to develop its own and holistic system of information protection, depending on specific threats and economic environment.

1 Einführung

Die Einführung verdeutlicht die Problemstellung und die der Arbeit zugrunde liegende Motivation. Davon ausgehend werden anschließend die Zielsetzung sowie die Vorgehensweise der Arbeit vorgestellt.

1.1 Problemstellung und Motivation

Die zunehmende Globalisierung der Märkte und der damit einhergehende Eintritt von Entwicklungsländern in das weltwirtschaftliche Geschehen haben zu einem verschärften internationalen Wettbewerb geführt (Warnecke, 2010). Im Ringen um Marktanteile und Wettbewerbsvorteile unterstützen dabei ganze Staaten ihre einheimischen Unternehmen durch geheimdienstlich gelenkte Aktivitäten (Schaaf, 2009). Besonders aktiv in der staatlich gelenkten Wirtschaftsspionage gegenüber Deutschland sind derzeit China und Russland, aber auch von westlichen Ländern gehen Gefahren aus (Bundesamt für Verfassungsschutz (BfV), 2008a; Corporate Trust, 2007).

Spionage wird jedoch nicht nur durch Geheimdienste, sondern in erhöhtem Maße auch durch Konkurrenzunternehmen mit großem personellen und technischen Aufwand durchgeführt (Corporate Trust, 2007; Schaaf, 2009). In Folge des steigenden Kostendrucks werden kostenintensive Bereiche wie Forschungs- und Entwicklungsabteilungen zu Zielobjekten von Spionage. Aber auch Marketing-, Vertriebs- und weitere Unternehmensstrategien geraten vermehrt in den Fokus der Angreifer (Deutscher Industrie- und Handelstag (DIHT), 1997; Landesamt für Verfassungsschutz (LfV) Baden-Württemberg und Bayern, 2006). Aufgrund der zunehmend professionalisierten und vielfältigen Methoden der (illegalen) Informationsbeschaffung durch Unternehmen, sind die Grenzen zwischen Wirtschafts- und Industriespionage fließend geworden (Meissinger, 2005). Festzuhalten ist jedenfalls, dass Spionage eine verführerische Möglichkeit zur Einsparung von Kosten und Zeit bietet (DIHT, 1997).

Da Deutschland im Gegensatz zu anderen Ländern nicht über umfangreiche Rohstoffvorkommen und Bodenschätze verfügt, ist die Innovationsfähigkeit seiner Bürger und heimischen Unternehmen entscheidend für den Wohlstand des Landes (Corporate Trust, 2007). Trotz einiger Abstriche bezüglich der Innovationsbedingungen gehört Deutschland immer noch zu den führenden Innovationsnationen, was Begehrlichkeiten bei konkurrierenden Staaten und Unternehmen weckt (Deutsches Institut für Wirtschaftsforschung (DIW), 2009). An-

gesichts dieser Situation sind besonders innovative deutsche Unternehmen von Industriespionage betroffen. So wuchs die Zahl der registrierten Spionagefälle im Jahre 2006 auf 2990 Fälle an, was einem Anstieg um rund 25 Prozent zum Vorjahr entspricht (Corporate Trust, 2007). Dabei tritt das Phänomen der Spionage unabhängig von der Größe des Unternehmens auf. Vielmehr entscheidet die Innovationsfähigkeit eines Unternehmens darüber, ob es ein potenzielles Ziel von ausländischen Nachrichtendiensten oder konkurrierenden Wettbewerbern ist. Da jedoch gerade klein- und mittelständische Unternehmen (KMU) nicht über die finanziellen, personellen und technischen Ressourcen wie Großkonzerne verfügen, werden KMU vermehrt Opfer eines ungewollten Know-how-Abflusses (Sicherheitsforum Baden-Württemberg (SiFo BW), 2010a). Insgesamt wird die Gefährdung der deutschen Volkswirtschaft durch Wirtschafts- und Industriespionage dadurch erhöht, dass mittelständische Unternehmen mit ihrer internationalen Ausrichtung und ihren innovativen Produkten, Dienstleistungen sowie Verfahrenstechniken das Rückgrat der deutschen Wirtschaft bilden (LfV BW, 2004).

Oft fehlt es den Unternehmen an einer Grundsensibilisierung gegenüber den Gefahren der Wirtschafts- und Industriespionage, obwohl Spionage eine lange Tradition besitzt (LfV BW, 2004). Fälle wie die Entwendung des Geheimnisses der Seidenproduktion durch die Europäer aus China im 5. und 6. Jahrhundert nach Christus oder der Diebstahl von brasilianischen Kautschuksamen durch Großbritannien im 19. Jahrhundert, der die brasilianische Monopolstellung in der Kautschukindustrie brach, sind nur zwei Beispiele für die weitreichenden Folgen erfolgreicher Wirtschafts- und Industriespionage (Meissinger, 2005; Schaaf, 2009). Spionage nach wie vor eine reale Bedrohung, die deutlich unterschätzt wird (SiFo BW, 2010a).

Fast jedes fünfte deutsche Unternehmen wurde bereits Opfer von Industriespionage beziehungsweise ungewolltem Know-how-Abfluss (Corporate Trust, 2007). Dieses Hellfeld registrierter Straftaten bildet jedoch bei weitem nicht die gesamte Bedrohungslage ab. Spionage zeichnet sich gerade dadurch aus, dass sie nicht öffentlich, sondern im Verborgenen stattfindet (Schaaf, 2009). Spionierende, aber auch Spionageopfer, haben meist kein Interesse an einer öffentlichen Verfolgung von entdeckten Spionageaktivitäten (Meissinger, 2005). Die besonders hohe Dunkelziffer im Bereich der Industriespionage lässt sich unter anderem dadurch erklären, dass Spionagefälle von den Unternehmen aufgrund befürchteter Reputationsschäden oft vertuscht werden. Zusätzlich werden viele Vorfälle gar nicht erst aufgedeckt, sodass die Kriminalstatistik nur einen Teil der tatsächlichen Vorkommnisse und finanziellen Schäden erfasst (Corporate Trust, 2009).

Diese Situation, in der die verfügbaren Zahlen nur einen Bruchteil der Realität wiederspiegeln, führt dazu, dass das Thema der Industriespionage keine hohe Präsenz in den Medien besitzt und bisher relativ selten in der Literatur behandelt wurde (Meissinger, 2005). Folglich fehlt ein Bewusstsein für die tatsächlichen Gefahren und die Bedrohungen werden vernachlässigt oder erst gar nicht erkannt (Corporate Trust, 2009). Zusätzlich hierzu werden die Gefahren des komplexen Themas auch aufgrund des zunehmenden Kosten- und Zeitdrucks von Unternehmen verdrängt. Teilweise bestehen auch Ressentiments gegenüber dem Begriff der *Industriespionage* (Schaaf, 2009). Auch die gestiegenen Kommunikationsmöglichkeiten mittels neuer Technologien, der damit einhergehende sorglosere Umgang mit schützenswerten Informationen und die Fremdvergabe von Dienstleistungen an externe Firmen (Outsourcing) erschweren den Know-how-Schutz zunehmend (DIHT, 1997).

Ein besonderer Risikofaktor für Industriespionage ist der Mensch (Schaaf, 2009). Laut einer Studie des Sicherheitsforums Baden-Württemberg (2010a) kommen 70 Prozent der Täter aus dem eigenen Unternehmen. Diese Innentäterproblematik wird jedoch von vielen Unternehmen verkannt, indem Informationsschutz als isolierte Aufgabe der IT angesehen wird. Dabei wird oft vergessen, dass alleiniger technischer Schutz gegenüber Spionageangriffen nicht ausreicht. Denn selbst die beste Firewall kann Know-how nicht schützen, wenn ein Angreifer durch menschliche Ressourcen hinter der Firewall agiert (Sack, 2008). Folgerichtig ist der Mensch der entscheidende Faktor im Kampf gegen Industriespionage (Schaaf, 2009).

Ein solch umfassendes Sicherheitsverständnis, in dem Informationsschutz als Querschnittsaufgabe verstanden wird und alle relevanten Unternehmensbereiche mit einbezieht, ist jedoch oft bei mittelständischen Firmen nicht zu finden (Schaaf, 2009). Häufig ist der Bereich der Unternehmenssicherheit im Rahmen der Expansion unterproportional gewachsen, obwohl gerade durch den Eintritt in neue Märkte zusätzliche Risiken entstehen. Verdeutlicht wird die Relevanz des Themas Industriespionage auch durch die Schäden, die die deutsche Volkswirtschaft jährlich durch ungewollten Know-how-Abfluss erleidet. Experten der *Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW)* schätzen diesbezüglich Summen von bis zu 50 Milliarden Euro, wobei die Tendenz steigend ist (Creutz, 2007). Trotz der hohen Schäden, die deutsche Unternehmen jährlich zu verkraften haben, ist die Situation nicht ausweglos. Es gibt durchaus kostengünstige und umsetzbare Schutzmaßnahmen, die präventiven oder repressiven Charakter besitzen und so einen ungewollten Know-how-Abfluss vermeiden können (SiFo BW, 2010a). Die Gewährleistung der Informationssicherheit sollte jedoch keine von Un-

ternehmen allein zu bewältigende Aufgabe sein. Vielmehr bietet sich eine Kooperation von Wirtschaft und Staat an (DIHT, 1997).

1.2 Zielsetzung

Ausgehend von der Öffnung der Märkte, dem verschärften Wettbewerb, der veränderten Aufgabenstellungen ausländischer Geheimdienste, neuer Formen der inner- und zwischenbetrieblichen Kooperation, dem Einsatz neuer Kommunikationstechnologien und dem Risikofaktor Mensch, sind deutsche Unternehmen einer hohen Spionagegefahr ausgesetzt, die adäquate Schutzmaßnahmen erfordert (DIHT, 1997). Diese Bedrohungslage, die in erheblichem Maße durch die menschliche Komponente geprägt ist, ist der Grund dafür, im Rahmen dieser Arbeit die Spionagegefahr von firmeneigenem und -fremdem Personal zu untersuchen.

Im Zuge dieser Arbeit werden präventive und repressive Spionageabwehrmaßnahmen vorgestellt, wobei der Fokus, wie durch einschlägige Literatur belegt, auf der Prävention von Spionagetätigkeiten liegen sollte, da so kostenintensive Schäden im Vorhinein vermieden oder zumindest reduziert werden können (BfV, 2002; Corporate Trust, 2009/2007; Schaaf, 2009). Ein absoluter Schutz gegen Spionageangriffe ist jedoch nicht möglich. Vielmehr geht es darum, Schutzwälle vor Spionageangriffen so hoch aufzubauen, dass die Angriffskosten wie Zeit, Ressourcen, Fähigkeiten, Technologien und das Entdeckungsrisiko die Erlöse der Angreifer übersteigen (Huber, 2010a/2010b).

Die Arbeit setzt sich mit der Frage auseinander, welche präventiven und repressiven Spionageabwehrmaßnahmen Unternehmen zur Verbesserung der personellen Sicherheit zur Verfügung stehen. Dabei ist es das Ziel dieser Arbeit, einen Katalog von personellen, aber auch organisatorischen, technischen und rechtlichen Spionageabwehrmaßnahmen zu entwickeln, da Sicherheit immer ganzheitlich zu betrachten ist. Hierzu findet eine Verknüpfung von bestehender Literatur mit eigenen Untersuchungsergebnissen statt. Die Grundlage der eigenen Arbeit bilden acht Experteninterviews mit Sicherheitsverantwortlichen besonders gefährdeter Unternehmen.

1.3 Vorgehensweise

Die vorliegende Arbeit ist in mehrere Kapitel untergliedert, die nicht immer scharf voneinander abzugrenzen sind. Dies resultiert unter anderem aus Überschneidungen in der Industrie-

und Wirtschaftsspionage, aber auch durch die enge Verbindung zwischen den Gefahren und den zu ergreifenden Abwehrmaßnahmen gegenüber Spionage.

Zu Beginn der Arbeit wird in das Thema eingeführt. Neben der Definition von *Industriespionage*, findet eine Abgrenzung zu den verwandten Begriffen der *Wirtschaftsspionage* und *Competitive Intelligence* (CI) statt, da erst durch die Klarheit der Begriffe eine spätere fachliche Diskussion möglich ist. Im Folgenden wird auf besonders spionagegefährdete Branchen und Unternehmen eingegangen sowie eine quantitative und qualitative Bewertung der Spionageschäden deutscher Unternehmen vorgenommen. In einem nächsten Schritt werden unterschiedliche Methoden der Informationsbeschaffung erläutert, wobei der Schwerpunkt auf personenbezogenen Methoden liegen wird. Anschließend wird die unternehmerische Relevanz von Informationen und Wissen dargelegt. Es findet sowohl eine Abgrenzung und Systematisierung von Wissen als auch eine Zuordnung zu betrieblichen Wissensträgern statt. Abgeschlossen wird der theoretische Teil durch das Aufzeigen von menschlichen, organisatorischen, technischen und rechtlichen Gefahrenpotenzialen des Know-how-Abflusses, wobei auch hier der Fokus auf der menschlichen Komponente liegt.

Im dritten Kapitel wird das methodische Vorgehen der Arbeit veranschaulicht. Durch Experteninterviews mit Sicherheitsverantwortlichen besonders gefährdeter Unternehmen, die mit Unterstützung der niedersächsischen Verfassungsschutzbehörde und des Arbeitskreises der Sicherheitsbevollmächtigten in Niedersachsen gewonnen wurden, konnten Erkenntnisse über angewandte Spionageabwehrmaßnahmen generiert werden.

Die Resultate der Interviews werden im vierten Kapitelvorgestellt. Hierbei wird zunächst auf die vorangehenden Maßnahmen der Analyse und Bewertung von Spionagerisiken eingegangen. Die vorliegenden Spionageabwehrmaßnahmen sind, wie in der gängigen Literatur üblich, in personelle, organisatorische, technische und rechtliche Maßnahmen differenziert, die sowohl präventiven als auch repressiven Charakter haben können (DIHT, 1997; LfV BW, 2004; Meissinger, 2005; Schaaf, 2009; SiFo BW, 2010b; Warnecke, 2010).

In einer abschließenden Diskussion werden die empirisch erhobenen Ergebnisse in die bestehende Literatur integriert. Dabei werden auch methodische Grenzen der Arbeit und die Grenzen der Umsetzbarkeit möglicher Schutzmaßnahmen erörtert sowie Ausblicke auf zukünftige Spionagegefahren gegeben.

Um die Bedrohungen und möglichen Schäden von Industriespionage zu verdeutlichen, sind im Laufe der Arbeit zahlreiche Fallbeispiele aufgeführt. Neben der klassischen Literaturana-

lyse wurden auch zahlreiche weitere Quellen wie das Internet oder Gespräche mit Vertretern von Unternehmen und Behörden geführt. Aufgrund der Sensibilität des Themas der Industriespionage wurden die im Anhang befindlichen Transkripte der Experteninterviews anonymisiert.

2 Theoretischer Hintergrund

Zunächst wird in das Thema Industriespionage eingeführt. Aufbauend wird näher auf die Begriffe *Information* und *Wissen* sowie deren betriebliche Relevanz eingegangen. Das Kapitel schließt mit einer Darstellung der Gefahrenpotenziale des Know-how-Abflusses.

2.1 Industriespionage

Im Rahmen der Einführung in die Industriespionage werden in den folgenden Unterkapiteln die Begriffe Industrie- und Wirtschaftsspionage sowie Competitive Intelligence (CI) vorgestellt bzw. voneinander abgegrenzt. Anknüpfend wird auf besonders spionagegefährdete Branchen und Unternehmen eingegangen und eine quantitative sowie qualitative Bewertung der Spionageschäden für deutsche Unternehmen vorgenommen.

2.1.1 Begriffsklärung

Das Bundesamt für Verfassungsschutz definiert den Begriff der *Industriespionage* als „Ausforschung eines Unternehmens durch einen Wettbewerber“ (BfV, 2008a, S. 2). Industriespionage findet jedoch nicht nur zwischen Wettbewerbern statt, sondern bezieht sich auf das gesamte Wettbewerbsumfeld eines Unternehmens. Hierzu gehören unter anderem Lieferanten, Abnehmer oder Hersteller von Ersatzprodukten, sodass alle wirtschaftlichen Beziehungen eines Unternehmens ein gewisses Spionagerisiko enthalten. Dies schließt ebenfalls zukünftige Geschäftsbeziehungen ein (Lux/Peske, 2002a).

Industriespionage, die oft auch als Konkurrenzausspähung, Wettbewerbsspionage oder Konkurrenzspionage bezeichnet wird, zeichnet sich im Speziellen durch die illegale Informationsbeschaffung von Geschäftsgeheimnissen und Betriebsinterna aus, wobei die Grenzen zur CI und Wirtschaftsspionage fließend sind (LfV BW und Bayern, 2006; SiFo BW, 2010a; Warnecke, 2010). Insbesondere Informationen über Wettbewerber, Märkte, Technologien und Kunden, Know-how zu Produktentwicklungen und Verfahrenstechniken, Preisinformationen, Kalkulationen und Designstudien liegen im Interesse der spionierenden Unternehmen (BfV, 2008a; SiFo BW, 2010a). Diese Auflistung zeigt, dass Industriespionage in ihrer Zielsetzung enger als die in Kapitel 2.1.2 angesprochene Wirtschaftsspionage definiert ist (Meissinger, 2005). Ein weiteres Charakteristikum von Konkurrenzausspähung liegt in der Kurzfristigkeit

der Spionageaktivitäten und der hohen Informationsasymmetrie der Akteure (BfV, 2008a; Fussan, 2010).

Das generelle Ziel von Industriespionage liegt in der Steigerung der eigenen Wettbewerbsfähigkeit. Die spezifischen Spionageziele hängen jedoch vom Entwicklungsstand des spionierenden Unternehmens ab (SiFo BW, 2010a). Hochentwickelte Unternehmen spionieren Wettbewerber aus, um auf einem gleichen Wissensniveau zu bleiben, wohingegen technologisch weniger entwickelte Unternehmen eher an Basistechnologien und Wissen zum Nachbau, zum Beispiel für Plagiate, interessiert sind (Lux/Peske, 2002a). Ein weiteres Differenzierungskriterium bezüglich der Spionageziele stellt die Unternehmensgröße dar. KMU verfolgen eher kurzfristige Ziele wie Fertigungsverfahren und Produkteigenschaften. Aufbauend hierzu interessieren Konzerne sich auch für langfristig wirksame Aspekte wie die Strategie und Kultur ihrer Konkurrenten (Meissinger, 2005).

Industriespionage findet im Verborgenen statt, bleibt daher oft unbemerkt und ist meist nur schwer nachzuweisen. Im Gegensatz zu früher ist Industriespionage heute aufgrund der umfassenden Kommunikationsmöglichkeiten stark durch technische Angriffe geprägt, die meist über das Internet erfolgen (Havranek, 2010; Schaaf, 2009). Ein Beispiel für einen solchen technischen Angriff stellt der Informationsabfluss beim Windkraftanlagenhersteller *ENERCON* dar, der mittels des Echelon-Spionagesystems erfolgte. Auf diese Weise konnte der amerikanische Konkurrent *Kenetech Windpower* mithilfe der *National Security Agency (NSA)* und des Abhörsystems Echelon vertrauliche Informationen über die Kerntechnologie des Weltmarktführers *ENERCON* erhalten und Wettbewerbsnachteile egalisieren (Schaaf, 2009).

Neben den vielfältigen und ständig anwachsenden technischen Möglichkeiten spielt der menschliche Faktor im Rahmen der Industriespionage jedoch eine entscheidende Rolle (Corporate Trust, 2007). Oft nehmen ausscheidende Mitarbeiter vertrauliche Unterlagen mit zu ihrem neuen Arbeitgeber und schädigen ihren ehemaligen Arbeitgeber damit erheblich. Ein bekanntes Beispiel ist der Verrat und die Mitnahme von Betriebs- und Geschäftsgeheimnissen des Chef-Einkäufers José Ignacio López, der im März 1993 von *General Motors (GM)* zu *Volkswagen (VW)* wechselte (Schaaf, 2009). Ein ähnlicher Fall ereignete sich in der Formel 1 als zwei ehemalige *Ferrari*-Rennstall-Mitarbeiter Betriebsgeheimnisse und vertrauliche Daten an ihren neuen Rennstall *Toyota* verrieten (Havranek, 2010).

Rechtlich ist die Thematik der Industriespionage insbesondere im Gesetz gegen unlauteren Wettbewerb (UWG) verankert. In § 17 UWG wird der Verrat von Geschäfts- der Betriebsge-

heimnissen, wie zum Beispiel Kostenkalkulationen und Angebote an Kunden, mit einer Geldstrafe oder einer Freiheitsstrafe von bis zu 3 Jahren belegt. Auch die Verwertung von Vorlagen, wie Rezepten und technischen Zeichnungen, nach § 18 UWG und das Verleiten zum Verrat durch Dritte nach § 20 UWG, kann zu Geld- oder Freiheitsstrafen führen. Die Bekämpfung von Industriespionage fällt nicht in den Kompetenzbereich der Verfassungsschutzbehörden. Ihnen kommt eher eine beratende und sensibilisierende Funktion zu. Zur Verfolgung von Industriespionage sind vielmehr Polizei und Staatsanwaltschaft einzuschalten, die dem Legalitätsprinzip unterliegen. Oft scheuen Unternehmen jedoch diesen Weg, da sie in Folge der Veröffentlichung von Spionagefällen Reputationsschäden befürchten und beauftragen daher private Sicherheitsunternehmen mit der Ermittlung bei Verdachtsfällen (Schaaf, 2009).

Grundsätzlich lässt sich festhalten, dass Industriespionage sich als ein gebräuchliches Mittel der Informationsbeschaffung etabliert hat, was eine ernsthafte Bedrohung deutscher Unternehmen zur Folge hat (Schaaf, 2009).

2.1.2 Abgrenzung

Laut Bundesamt für Verfassungsschutz (2008a, S. 2) bezeichnet der Begriff der *Wirtschaftsspionage* die „staatlich gelenkte oder gestützte von Nachrichtendiensten fremder Staaten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben“. Im Vergleich zur Industriespionage, die von privatwirtschaftlichen Organisationen betrieben wird, ist im Rahmen der Wirtschaftsspionage der Staat Urheber/Durchführender der Spionagetätigkeit. Der Unterschied liegt daher im Akteur der Spionage (BfV, 2008a).Staatliche Akteure von Spionagetätigkeiten gegen die Bundesrepublik Deutschland sind insbesondere Russland und China, deren Geheimdienste sowohl über umfangreiche personelle als auch technische Ressourcen zur illegalen Informationsbeschaffung verfügen und sogar gesetzlich zur Wirtschaftsspionage verpflichtet sind (BfV, 2009; BfV, 2008a).

Die Informationsbeschaffung über Nachrichtendienste wird dabei mithilfe unterschiedlicher Methoden durchgeführt und kann sowohl über die Auswertung öffentlicher Quellen als auch durch geheimtechnische Angriffe oder Agententätigkeiten erfolgen (BfV, 2008a; Meissinger, 2005). Allerdings wird Industriespionage häufig mit ähnlichen Mitteln wie Wirtschaftsspionage betrieben, was die Suche nach dem Akteur der Spionagetätigkeit, Wettbewerber oder Staat, nicht leicht macht (Schaaf, 2009). Die Grenzen zwischen Industrie- und Wirtschafts-

spionage sind auch dahingehend fließend, dass viele staatliche Geheimdienste eng mit ihren einheimischen Unternehmen in der Beschaffung von Informationen ausländischer Unternehmen kooperieren. Daher ist eine Abgrenzung zwischen Industrie- und Wirtschaftsspionage nicht immer praxistauglich (Huber, 2010a).

Wie die Konkurrenzausspähung besitzt auch die Wirtschaftsspionage eine lange Tradition. So ist die Verfolgung nationalstaatlicher Interessen im Rahmen von Spionagetätigkeiten bis circa 500 nach Christus rückverfolgbar (Meissinger, 2005). Die Ziele der Wirtschaftsspionage sind abhängig von dem wirtschaftlichen und technologischen Entwicklungsstand sowie den spezifischen Bedürfnissen und volkswirtschaftlichen Prioritäten des spionierenden Landes (BfV, 2008a/2008b/2002; SiFo, 2010a). Technisch und wirtschaftlich entwickelte Staaten sind insbesondere an wirtschaftspolitischen Strategien, sozioökonomischen Trends, Marketing-, Absatz- und sonstigen Unternehmensstrategien sowie an Kooperationen und Absprachen zwischen Unternehmen interessiert (BfV, 2008a; LfV Rheinland-Pfalz (RlP), 2008). Ein Beispiel für Wirtschaftsspionage eines hochentwickelten Landes ist der Bieterstreit zwischen *Siemens* und *Alsthom* im Zuge der Ausschreibung für den Bau eines Hochgeschwindigkeitszuges in Südkorea. Zielsicher wurden die Angebote von *Siemens* vom französischen Konkurrenten unterboten. Dabei gab es Hinweise darauf, dass der französische Geheimdienst *Direction Générale de la Sécurité (DGSE)* den *Alsthom*-Konzern unterstützte, indem er die Angebote von Siemens ausspionierte. Eindeutige Beweise konnten jedoch nicht gefunden werden, was ein typisches Merkmal von Spionagetätigkeiten ist(Nathusius, 2001; Schaaf, 2009). Staaten mit Technologierückstand sind eher auf die Beschaffung von technischem Know-how und Informationen über Fertigungstechniken fokussiert, um Entwicklungszeiten einzusparen und kostengünstiger produzieren zu können (BfV, 2008a).

Die Bekämpfung von Wirtschaftsspionage ist laut Bundesverfassungsschutzgesetz (BVerfSchG) Aufgabe der Verfassungsschutzbehörden, die nicht dem Legalitätsprinzip unterliegen (BfV, 2002; SiFo, 2010a). Zum Wirtschaftsschutz und der Beobachtung fremder Nachrichtendienste stehen den Verfassungsschutzbehörden unter anderem Observationen, verdeckte Ermittlungen sowie Überwachungsmöglichkeiten des Fernmelde- und Postverkehrs zur Verfügung (Schaaf, 2009).

Das Konzept der *Competitive Intelligence (CI)* entstand um 1970 als Teil der Marktforschung und kann als systematisch strukturierter Prozess der Informationsbeschaffung bezeichnet werden, wobei das gesamte Wettbewerbsumfeld bezüglich frei zugänglicher Informationen untersucht wird (Lux/Peske, 2002a). Ziel der CI ist es, Veränderungen der Marktteilnehmer

und des Marktes insgesamt möglichst frühzeitig zu erkennen, Lehren aus diesen Entwicklungen zu ziehen und proaktiv Strategie, Prozesse und Leistungsangebot des eigenen Unternehmens weiterzuentwickeln (Brellochs, 2000). Intelligence steht hierbei nicht für Intelligenz, sondern für das Sammeln und Aufbereiten von Informationen, um Erkenntnisse zu generieren (Havranek, 2010). Der idealtypische Ablauf der legalen Informationsgewinnung lässt sich am *Intelligence Cycle* verdeutlichen, der seinen Ursprung in den 1960-er Jahren hat und durch Nachrichtendienste wie die CIA geprägt wurde (Lux/Peske, 2002a).

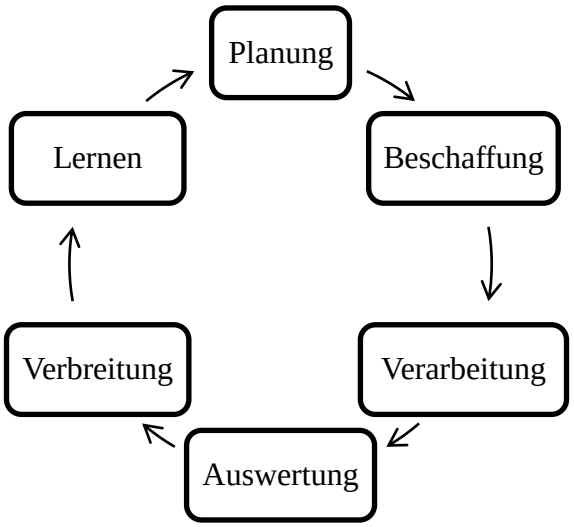

Abbildung 1: Allgemeiner Prozess der Konkurrenzbeobachtung
Quelle: www.ci-handbuch.de

Im ersten Schritt werden die späteren Phasen geplant und der notwendige Informationsbedarf identifiziert. Aufbauend werden in der zweiten Phase der Beschaffung Rohinformationen gesammelt. Durch die Verarbeitung, zum Beispiel durch Übersetzung und Kategorisierung, können die Informationen im nächsten Schritt der Auswertung analysiert, bewertet und verglichen werden. Die Ergebnisse stehen dann den Nutzern zur Verfügung. Abschließend erfolgt eine Reflexion des Prozesses (Kondruß, 2010).

Im Gegensatz zur Spionage werden bei Maßnahmen der Competitive Intelligence (CI) ausschließlich legale Mittel der Informationsbeschaffung eingesetzt (Lux/Peske, 2002b). Informationsgewinnung muss somit nicht unbedingt durch illegales Vorgehen erfolgen. Die Grenzen sind jedoch fließend.

2.1.3 Gefährdete Branchen und Unternehmen

Industrie- und Wirtschaftsspionage sind als ernst zu nehmende Bedrohungen der deutschen Wirtschaft einzustufen (Schaaf, 2009). Gerade forschungsintensive Unternehmen der Technologiebranche sind oft von ungewolltem Know-how-Abfluss betroffen. Laut einer Studie der Unternehmensberatung Corporate Trust (2007) sind insbesondere Unternehmen des Automobil-, Luftfahrzeug-, Schiffs- und Maschinenbaus Ziel von Spionageaktivitäten konkurrierender Unternehmen und ausländischer Staaten (27 Prozent). Beispielhaft kann hier der Abfluss von vertraulichen Informationen beim französischen Automobilzulieferer *Valeo* durch die chinesische Praktikantin Li-Li W. angeführt werden, die trotz ihrer niedrigen hierarchischen Stellung volle Zugriffsrechte innerhalb der IT besaß (Schaaf, 2009). Weitere hochgefährdete Bereiche sind die Eisen-und Stahlindustrie sowie die Metall- und Grundstoffverarbeitung. Etwa jedes fünfte Unternehmen (22 Prozent), das einen (vermuteten) Spionagevorfall aufwies, stammt aus dieser Branche. Weniger forschungsintensive Bereiche wie der Handel oder die Lebensmittelindustrie zeigen hingegen eine geringere Gefährdungslage auf (Abbildung 2). Bei der Betrachtung der Ergebnisse der Studie fällt auf, dass trotz branchenübergreifender Befragung Unternehmen der Chemie- und Pharmaindustrie als auch des Banken- und Versicherungssektors nach eigenen Angaben nicht von Spionageangriffen betroffen sind. Diese Ergebnisse sind durchaus in Frage zu stellen, da gerade forschungsintensive Bereiche wie die Chemie- und Pharmabranche von ungewolltem Know-how-Abfluss betroffen sein dürften. Ebenfalls ist es schwer vorstellbar, dass Banken und Versicherungen noch in keinem Fall Opfer von Industriespionage geworden sind. Vielmehr könnten diese Nullergebnisse auch auf die Angst vor Reputationsschäden seitens der Unternehmen zurückzuführen sein, sodass Untersuchungen zum sensiblen Thema der Industriespionage immer kritisch zu hinterfragen sind (Corporate Trust, 2007). In der folgenden Abbildung werden die diskutierten Ergebnisse noch einmal graphisch dargestellt.

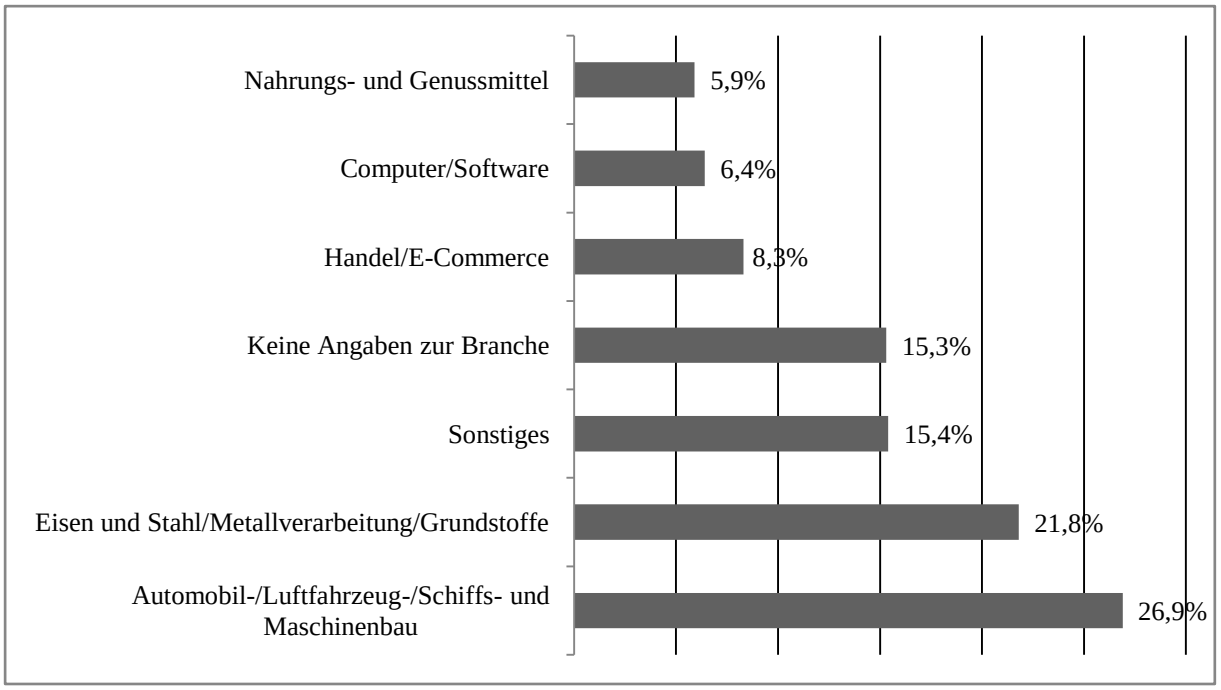

Abbildung 2: Spionagegefährdete Branchen
Quelle: Eigene Darstellung in Anlehnung an Corporate Trust, 2007, S. 15

Betrachtet man die Resultate in einem internationalen Kontext, so wird deutlich, dass auch andere Länder wie die USA ähnliche Schwerpunkte bezüglich gefährdeter Branchen setzen (Pittori, 1998).

Wie bereits gezeigt, sind forschungs- und technologieintensive Unternehmen deutlich häufiger Opfer von Industriespionage (Corporate Trust, 2007; LfV RlP, 2008; SiFo, 2010a). Besonders das zum Teil weltweit einzigartige Know-how deutscher KMU weckt Begehrlichkeiten bei Konkurrenten oder ausländischen Staaten (Hummelt, 1997). Zwar operieren viele KMU heute weltweit, jedoch verfügen sie bei weitem nicht über die erforderlichen Sicherheitsstrukturen wie Großunternehmen (Corporate Trust, 2009).

Innerhalb forschungsintensiver Unternehmen sind vor allem die Bereiche Produktion und Fertigung sowie Forschung und Entwicklung Ziel von Spionageaktivitäten (SiFo, 2010a). So gaben in der Studie des Sicherheitsforums Baden-Württemberg (2010a) 19 Prozent der befragten forschungsintensiven Unternehmen Informationsabflüsse in der Produktion und Fertigung an. Bei 14 Prozent der Unternehmen wurden Geschäfts-und Betriebsgeheimnisse im Forschungs- und Entwicklungsbereich verraten. Die Bereiche Personalmanagement, Einkauf und Vertrieb sowie Marketing und Werbung wiesen geringere Spionageangriffe auf (jeweils 5 Prozent). Im Vergleich zur Studie des SiFo BW konnten die Unternehmensberatungen KPMG (2010) und Corporate Trust (2007) in ihren Untersuchungen weitaus höhere wirtschaftskrimi-

nelle Aktivitäten in den Unternehmensbereichen Vertrieb und Personal feststellen, sodass sich kein abschließendes und einheitliches Bild über gefährdete Unternehmensbereiche ergibt.

2.1.4 Quantitative und qualitative Bewertung von Spionageschäden

Die deutsche Wirtschaft erleidet jährlich Milliardenverluste durch Industrie- und Wirtschaftsspionage. Dabei gefährdet der ungewollte Know-how-Abfluss nicht nur die Wirtschaftskraft, sondern auch die Reputation deutscher Unternehmen, sodass neben den quantitativen auch die qualitativen Auswirkungen von Spionageaktivitäten zu bewerten sind (LfV RlP, 2008).

Laut der Unternehmensberatung Corporate Trust (2007) liegen die jährlichen finanziellen Schäden aus Industriespionage für deutsche Unternehmen bei rund 2,8 Milliarden Euro. Andere Institutionen wie die Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW) oder das Sicherheitsforum Baden-Württemberg (SiFo BW) setzen Schadenssummen von 30 beziehungsweise 50 Milliarden Euro an (Pressetext, 2008; SiFo BW, 2004). Die Spannweite der Schätzungen zeigt, dass eine exakte Quantifizierung der Schäden von ungewolltem Know-how-Abfluss schwierig ist (PriceWaterhouseCoopers (PWC), 2009). Gerade die hohe Dunkelziffer von Spionageaktivitäten, die geringe Meldebereitschaft seitens der betroffenen Unternehmen und die problematische Quantifizierbarkeit eines konkreten Spionagevorfalls lassen verlässliche Zahlen zu Spionageschäden nicht zu (Huber, 2010a/2010c/2010d/2009). Erschwerend kommt hinzu, dass wenig unabhängige Forschung zur Schadenshöhe vorliegt. Rund 80 Prozent der Veröffentlichungen stammen von Beratungsunternehmen, die mit den Zahlen ihre Berechtigung verstärken wollen und ihr Geld mit zunehmend verunsicherten Unternehmen verdienen (Huber, 2010a; Meissinger, 2005). Des Weiteren führt die mangelnde Abgrenzbarkeit der Begriffe Industrie- und Wirtschaftsspionage zu einer erhöhten Komplexität in der Schadensquantifizierung (Lux/Peske, 2002a). Dies zeigt, dass Zahlen zu den finanziellen Auswirkungen von Industriespionage aufgrund der Vielzahl von Einflussfaktoren mit Vorsicht zu genießen sind (Huber, 2010a). Vielmehr sind sie als Größenorientierung zu verstehen. Allerdings ist durch die anhaltende Globalisierung und den international steigenden Wettbewerbsdruck davon auszugehen, dass die Schäden weiter ansteigen werden (Huber, 2009; Meissinger, 2005).

Neben den quantitativen Auswirkungen führt Industriespionage auch zu qualitativen Schäden. Diese können durchaus schwerwiegendere Konsequenzen als finanzielle Aspekte haben (SiFo, 2010a). Reputationsverluste bei Kunden und Geschäftspartnern sowie sinkende Attrakti-

vität als Arbeitgeber sind nur einige mögliche Folgen (Corporate Trust, 2007). In der Studie der Unternehmensberatung Corporate Trust (2007) gaben Unternehmen, nach den immateriellen Schäden befragt, am häufigsten den eigentlichen Informationsabfluss als Problem an (54 Prozent). Weitere 28 Prozent der befragten Unternehmen schilderten Mitarbeiterabwanderung und weitere 15 Prozent Imageschäden als negative Konsequenzen (Abbildung 3). Die folgende Abbildung verdeutlicht noch einmal die Probleme im Zusammenhang mit immateriellen Spionageschäden.

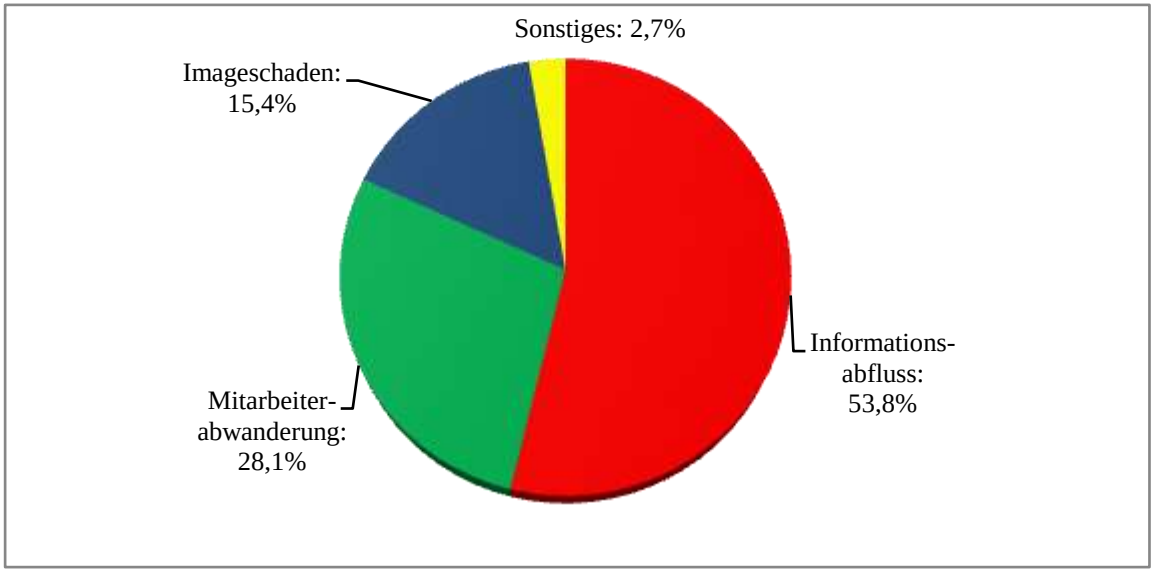

Abbildung 3: Immaterielle Schäden in Unternehmen
Quelle: Eigene Darstellung in Anlehnung an Corporate Trust, 2007, S. 22

Die negativen Auswirkungen des Informationsabflusses liegen darin, dass Konkurrenten Wettbewerbsnachteile egalisieren können und somit den Wettbewerbsdruck auf das betroffene Unternehmen erhöhen. Zusätzlich kann durch qualitativ minderwertige Kopien eines Wettbewerbers das Vertrauen in das Unternehmen und dessen Produkte sinken (Corporate Trust, 2007). Die Folge können Mitarbeiterabwanderungen sein, welche insbesondere forschungsintensive Unternehmen, die auf ihre innovative Belegschaft angewiesen sind, schwer schädigen können(Corporate Trust, 2007).

Bei der Lokalisierung der Spionageschäden deutscher Unternehmen ist festzustellen, dass sich der überwiegende Teil der Schäden in Deutschland ereignet (Corporate Trust, 2007). Diese Häufung der Angriffe ist jedoch dadurch zu erklären, dass zum einen die besonders spionagegefährdeten Forschungs- und Entwicklungsabteilungen deutscher Unternehmen im Gegensatz

zu anderen Unternehmensbereichen immer noch eher in Deutschland beheimatet sind und zum anderen Spionagevorfälle aufgrund der hiesigen umfangreicheren Sicherheitsstrukturen in Deutschland eher registriert werden (Corporate Trust, 2007).

2.1.5 Methoden der Informationsbeschaffung

In den folgenden drei Unterkapiteln werden die unterschiedlichen Methoden der Informationsbeschaffung vorgestellt. Dabei findet eine begriffliche Anlehnung an die Vorgehensweise staatlich gelenkter Wirtschaftsspionage statt, die jedoch in vielen Punkten dem Vorgehen in der Industriespionage gleicht (Lux/Peske, 2002a).

2.1.5.1 Human Intelligence (HUMINT)

Trotz der zunehmenden Technisierung der heutigen Zeit ist der Mensch noch immer der wichtigste Faktor in der Gewinnung von Informationen (Meissinger, 2005). Zwar gibt es eine große Bandbreite an technischen Spionagemethoden, doch liegt der Schlüssel weiterhin in der klassischen menschlichen Quelle (Lux/Peske, 2002a; Jakob, 1999). Genau diesen Sachverhalt greift die Human Intelligence (HUMINT) auf.

Unter HUMINT kann die Nutzung von Personen zur Beschaffung von Informationen verstanden werden (Lux/Peske, 2002a). Kennzeichnend für diese Form der Informationsbeschaffung ist, dass der Know-how-Abfluss mithilfe menschlicher Akteure erfolgt und die bespitzelten Opfer häufig nicht einmal merken, dass sie für die Informationsgewinnung konkurrierender Unternehmen oder fremder Staaten missbraucht werden(BfV, 2006; LfV BW und Bayern, 2006;Warnecke, 2010). Die Wege der Informationsbeschaffung sind dabei vielfältig. So kann es im Rahmen von Messen oder Veranstaltungen zur Gesprächsabschöpfung durch Wettbewerber kommen, was schwerwiegende wirtschaftliche Folgen für das betroffene Unternehmen haben kann (LfV BW und Bayern, 2006; Warnecke, 2010). Neben der Gesprächsabschöpfung auf solchen Veranstaltungen können Mitarbeiter aber auch in ihrer Freizeit gezielt zu ihrem zum Teil einzigartigen Expertenwissen befragt werden (Lux/Peske, 2002a). Gerade die Gutgläubigkeit vieler Mitarbeiter und die Offenheit von Experten und Wissenschaftlern in der Wissensteilung stellen eine große Gefahr dar (Warnecke, 2010).

Eine weitere Möglichkeit der Informationsgewinnung für fremde Firmen betrifft das Abwerben von Mitarbeitern. Konkurrenzunternehmen können dabei mittels Headhunter zum Bei-

spiel auf die aktuelle Unzufriedenheit eines Mitarbeiters eingehen, indem sie ihrem Opfer interessante Arbeitsinhalte in einem sozialen Arbeitsumfeld versprechen oder finanzielle Anreize für einen Firmenwechsel bieten (Schaaf, 2009). Der grundsätzliche Vorteil einer Abwerbung von Mitarbeitern besteht darin, dass der Wettbewerber mit einem Schlag umfangreiches Know-how erwerben kann. Dieser Effekt wird bei einem kollektiven Wechsel von Mitarbeitern noch verstärkt, wenn beispielsweise ganze Teams zu einem Mitbewerber wechseln (Schaaf, 2009).

Informationsgewinnung mit Menschen kann des Weiteren auch durch die Einschleusung von externen Spionen erfolgen (Lux/Peske, 2002a). Hierbei infiltrieren Mitarbeiter eines Konkurrenzunternehmens das Zielunternehmen, um an vertrauliche Informationen zu gelangen. Jedoch besteht eine erhebliche Schwierigkeit dieses Vorgehens darin, dass sich die externen Spione erst eine gewisse Position im Unternehmen erarbeiten müssen, um an entsprechende Informationen zu gelangen (Harbich, 2006). Eine verwandte Methode stellt die Annäherung durch die Gründung einer neuen Firma dar, die im Laufe der Zeit in Geschäftsbeziehungen zum betroffenen Unternehmen tritt (Lux/Peske, 2002a). Da diese Vorgänge jedoch sehr zeitaufwendig sind, kollidieren sie oftmals mit den kurzfristig ausgelegten Zielen der Industriespionage und finden daher eher seltener statt (LfV BW und Bayern, 2006). Am Rande sei auch die Möglichkeit des Einbruchs und des Diebstahls von Geschäfts- und Betriebsgeheimnissen erwähnt. Diese Methode birgt jedoch ein hohes Entdeckungsrisiko und ermöglicht keinen langfristigen Know-how-Abfluss, sodass sie verhältnismäßig gering auftritt (Lux/Peske, 2002a; Meissinger, 2005). Die Informationsbeschaffung mit Menschen muss jedoch nicht zwangsläufig illegal erfolgen. Im Rahmen von Werksführungen oder Tagen der offenen Tür können Mitarbeiter von Wettbewerbern legal in das betroffene Unternehmen eingeschleust werden (Meissinger, 2005).

Eine gefährliche Form der HUMINT stellt das Social Engineering, auch soziale Manipulation genannt, dar. Dieser Vorgang kann als eine zwischenmenschliche Beeinflussung von Menschen bezeichnet werden, die das Ziel verfolgt, unberechtigt an vertrauliche Informationen, Dienstleistungen oder sonstige Gegenstände zu gelangen (Schaaf, 2009). Meist wird im Vorfeld des Angriffs das persönliche Umfeld des Opfers durch den Angreifer (Social Engineer) ausgeforscht, um präzise Informationen über hierarchische Stellung im Unternehmen, familiäre Zusammenhänge und persönliche Vorlieben zu erhalten. Im Rahmen einer solchen Recherche nehmen soziale Netzwerke, wie Facebook oder Xing, eine immer wichtigere Rolle ein, da potenzielle Opfer auf diesen Plattformen wertvolle Informationen über sich preisgeben (BfV,

2010c; Grund/Fischer, 2009). Im Zuge eines Angriffs spiegelt der Social Engineer bei der Kontaktaufnahme mit dem Opfer falsche Identität sowie Tatsachen vor und nutzt menschliche Eigenschaften, wie Hilfsbereitschaft oder Autoritätshörigkeit, zur Informationsbeschaffung aus (Schaaf, 2009; Schaumann, 2009; Warnecke, 2010).

Laut Sidler (2008) gliedert sich der typische Social-Engineering-Angriff in die folgenden sechs Schritte (Abbildung 4).

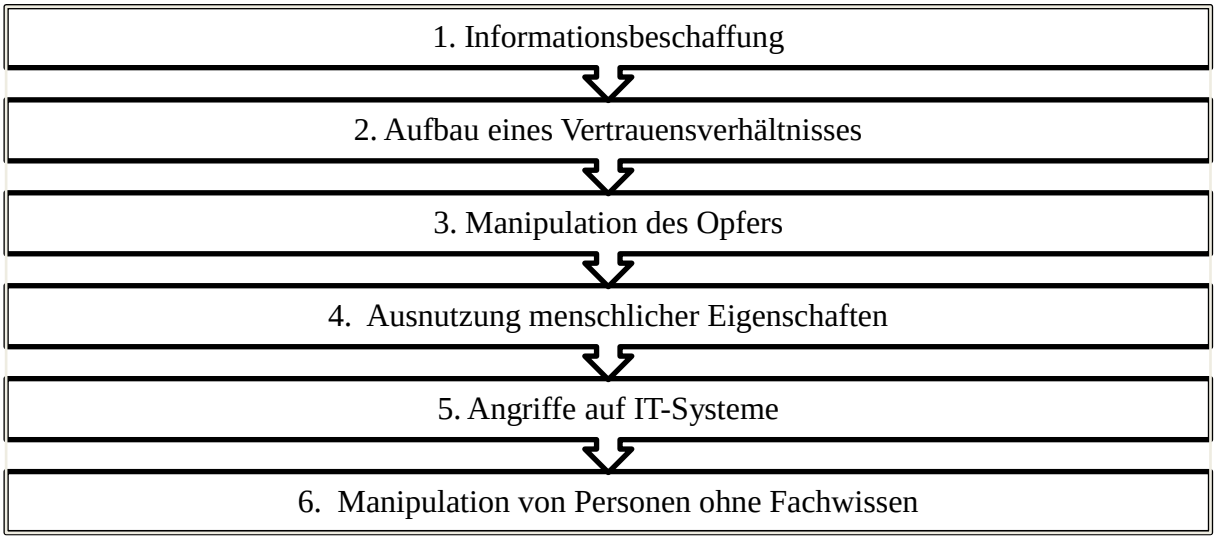

Abbildung 4: Ablauf eines Social-Engineering-Angriffs
Quelle: Eigene Darstellung in Anlehnung an Sidler, 2008, S. 2

In der ersten Phase findet zunächst eine Informationsbeschaffung über das Opfer der Attacke statt. Diese kann zum Beispiel durch eine Internetrecherche oder das Studieren von Adressverzeichnissen erfolgen. Nach der anfänglichen und intensiven Informationsgewinnung wird unter Vorspiegelung falscher Tatsachen der Aufbau von Vertrauen zum Opfer initiiert, indem sich der Angreifer zum Beispiel als Mitarbeiter eines Partnerunternehmens ausgibt, der noch ganz schnell die aktuelle Preisliste benötigt. Eine weitere der vielfältigen Möglichkeiten könnte die Ausgabe als Journalist oder Mitarbeiter eines Umfrageinstituts sein (Schaumann, 2009). In der dritten Phase findet die eigentliche Manipulation des Opfers statt, indem der Täter durch geschicktes Vorgehen und auf den ersten Blick zusammenhangslose Fragen zu den gewünschten Informationen gelangt. Dabei macht sich der Angreifer im vierten Schritt menschliche Eigenschaften, wie Hilfsbereitschaft, Kundenfreundlichkeit oder die Suche nach Anerkennung, zu Nutze und verleitet das Opfer so zu brisanten Aussagen. Mithilfe der gewonnen Informationen können dann in einem fünften Schritt weitere Angriffe auf IT-Systeme

gefahren werden, da die Opfer beispielsweise in Gesprächen ihre Passwörter oder zumindest Hinweise auf ihre Zugangsdaten hinterlassen haben. Abschließend können auch Personen ohne Fachwissen zu sicherheitsgefährdeten Aktionen bewegt werden.

Als konkretes Beispiel für die Methode des Social Engineering kann das folgende Überfalltelefonat angeführt werden: „Guten Tag Frau X, hier ist Herr Y von der IT. Wir haben gerade ein riesiges Systemproblem und brauchen unbedingt Ihre Hilfe. Wie lautet denn Ihr Passwort?“(Sidler, 2008). Zahlreiche Untersuchungen zeigen, dass solche und auch andere Angriffsversuche sehr erfolgreich sind, da Mitarbeiter oft nicht ausreichend über die Gefahren des Social Engineering aufgeklärt sind (Hirschmann, 2009). Insbesondere die Tatsache, dass Social Engineering Mitarbeiter nicht nur im Büro und auf Veranstaltungen, sondern auch im privaten Umfeld, wie in Sportvereinen oder Gaststätten, ereilen kann, macht diese Methode der HUMINT so attraktiv für Angreifer (Schaaf, 2009).

Insgesamt lässt sich festhalten, dass HUMINT eine wichtige Informationsbeschaffungsmethode ist, da Mitarbeitern ein Großteil des interessierenden Wissens besitzen (Schildbauer et al., 2003). Anhand der aufgezeigten Aktivitäten wird jedoch auch deutlich, dass die HUMINT legalen als auch illegalen Charakter besitzt, was verdeutlicht wie fließendend die Grenzen zwischen Spionage und CI sind (Meissinger, 2005).

2.1.5.2 Technical Intelligence (TECHINT)

Der Begriff der Technical Intelligence (TECHINT) umfasst sämtliche Spionagetätigkeiten, die durch den Einsatz technischer Hilfsmittel erfolgen (Meissinger, 2005). Im Zuge des technischen Fortschrittes findet eine immer stärker wachsende inter- und intraorganisationale Vernetzung von Unternehmen statt, die technische Spionageangriffe begünstigt (LfV BW und Bayern, 2006). Unternehmen sind daher gezwungen, in einem ständigen Prozess ihre technischen Sicherheitsstrukturen den neuen Möglichkeiten anzupassen. Dieser Anpassungsprozess ist jedoch oftmals für KMU aufgrund limitierter finanzieller Ressourcen nicht möglich (Warnecke, 2010).

Die technischen Möglichkeiten der Informationsgewinnung sind vielfältig und stehen nicht nur Nachrichtendiensten, sondern in zunehmendem Maße auch Konkurrenzunternehmen zu relativ geringen Preisen zur Verfügung (Meissinger, 2005; SiFo BW, 2010a). Allerdings erfordert die Benutzung von technischen Methoden der Informationsgewinnung auch immer menschliche Beihilfe, was die enge Verbundenheit von TECHINT und HUMINT verdeutlicht

(Lux/Peske, 2002a). So sind beispielsweise Wanzen für Abhörangriffe oder Kameras zur Beobachtung von Produktionsprozessen zunächst durch interne oder externe Täter anzubringen. Da der Fokus dieser Arbeit auf der menschlichen Komponente liegt, werden die zahlreichen technischen Spionagemöglichkeiten im Folgenden nur kurz angerissen und in Beziehung zu den menschlichen Akteuren behandelt.

Das Abfangen von elektromagnetischen Signalen, auch Signal Intelligence (SIGINT) genannt, stellt einen Teil der TECHINT dar. Hierbei kann die Informationsgewinnung zum Beispiel über das Abfangen von Telefonaten, Faxmitteilungen oder Videoübertragungen erfolgen (Meissinger, 2005). Die Schwierigkeit dieser Methode liegt darin, dass vor dem eigentlichen Informationsabfluss zunächst Überwachungsgeräte wie Wanzen an Kommunikationseinrichtungen zu platzieren sind. Möglich hierbei wäre, dass relativ niedrig entlohnte Sicherheits- und Reinigungskräfte für diese Arbeit mittels finanzieller Anreize angeworben werden, da diese Personen insbesondere außerhalb der Geschäftszeiten unbemerkt genannte Apparaturen anbringen können (Meissinger, 2005).

Die Informationsgewinnung im Rahmen der SIGINT kann jedoch auch extern über das Internet erfolgen. Nach einer Studie des *Zentrums für Europäische Wirtschaftsforschung (ZEW)* von 2007 verfügen fast alle der befragten Unternehmen (98 Prozent) über einen Internetanschluss. Des Weiteren besaßen mehr als die Hälfte aller Mitarbeiter (54 Prozent) von ihrem Arbeitsplatz direkten Zugriff auf das Internet, was das Gefahrenpotenzial des Internets verdeutlicht. Häufig erfolgt der Angriff aus dem Internet über Emails mit manipuliertem Anhang, bei deren Öffnung sich signaturarme Schadsoftware installiert, die von kommerziellen Virenscannern oft nicht entdeckt wird (LfV RlP, 2008). Nach der Installation der Schadsoftware wird dann eine Verbindung zu einem vorgegebenen Computer im Internet hergestellt, sodass eine Übertragung vertraulicher Firmeninformationen erfolgen kann. Neben Emails mit Anhang können auch Emails mit einer Verlinkung auf infizierten Seiten verschickt werden. Bei Aufruf solcher Links entstehen ähnlich schwerwiegende Folgen (SiFo BW, 2010a). Kennzeichnend für derartige Angriffe ist, dass ihnen ein Social Engineering vorausgeht, um mit den Themen der Emails die Interessen der Opfer zu adressieren (LfV RlP, 2008; SiFo BW, 2010a). Aus Sicht der Täter bietet der Angriff aus dem Internet den Vorteil, dass die Attacken von nahezu jedem Ort der Welt gestartet werden können und mit einem geringen Entdeckungsrisiko verbunden sind. Aufgrund dieses Gefahrenpotenzials kann eine physikalische Trennung des Firmen-IT-Netzes in einen internen und einen öffentlich zugänglichen Bereich durchaus sinnvoll sein (LfV RlP, 2008).

Neben den unzureichend gesicherten Unternehmensnetzwerken mit Internetanschluss bieten auch neue Formen der Datenübertragung, wie WLAN oder Bluetooth, technische Angriffsmöglichkeiten (Meissinger, 2005). So können in kürzester Zeit vertrauliche Informationen wie Kundenlisten oder Termine mit Geschäftspartnern, von mobilen Endgeräten heruntergeladen werden, sodass derartige drahtlose Verbindungen neuesten Sicherheitsstandards genügen und nur bei Notwendigkeit durch die sensibilisierten Mitarbeiter eingeschaltet werden sollten (Meissinger, 2005).

Technische Innovationen wie Laptops oder Handys können jedoch nicht nur Mittel zum Zweck, sondern auch Ziel von Spionagetätigkeiten konkurrierender Unternehmen sein (SiFo BW, 2010a). Zum Teil wird die gesamte Hardware gestohlen. Dabei liegt der eigentliche Verlust jedoch nicht im Diebstahl der Hardware, sondern in den auf ihr gespeicherten Informationen (LfV BW und Bayern, 2006). Auch hier zeigt sich die besondere Rolle des menschlichen Faktors, da auf der einen Seite kriminelle Energie der Täter und auf der anderen Seite Unachtsamkeit der Mitarbeiter bezüglich der mitgeführten Hardware notwendig ist, um einen erfolgreichen Angriff durchzuführen.

Einen weiteren Teil der TECHINT bildet die Auswertung von Bildinformationen, auch Imagery Intelligence (IMINT) genannt. Diese kann die Auswertung von Fotoaufnahmen bis hin zu Satellitenaufnahmen umfassen (Meissinger, 2005). So können mittels Fotoaufnahmen, wie bei *VW* passiert, Details zu neuen Produkten von Konkurrenten erspäht werden (Schmid, 2004). Satellitenaufnahmen dienen eher dazu, großflächige Veränderungen, wie beispielsweise Baumaßnahmen, zu entdecken, die Konkurrenten Aufschlüsse über Investitionsvolumina des betroffenen Unternehmens geben können. Diese Methode ist nicht nur in der Wirtschafts-, sondern auch in der Industriespionage zu finden. So vermieten mittlerweile private Anbieter Satellitenkapazitäten (Lux/Peske, 2002a). Der dritte Teilbereich der TECHINT ist die Measurement und Signature Intelligence (MASINT). Mithilfe dieser Methode können sekundäre Eigenschaften eines Spionageziels ermittelt werden, die Rückschlüsse auf Eigenschaften des Spionageziels geben (Lux/Peske, 2002a). Beispielhaft kann die thermische Signatur eines Motors Rückschlüsse auf das Leistungsprofil ermöglichen (Meissinger, 2005).

Aufgrund dieser Sachlage kann davon ausgegangen werden, dass technisch basierte Angriffe in Zukunft weiter ansteigen werden. Dabei sind die technischen Informationsbeschaffungsmethoden nicht eindeutig von menschlichen Akteuren trennbar.

2.1.5.3 Open Source Intelligence (OSINT)

Neben den konspirativen Methoden der HUMINT und TECHINT steht Unternehmen auch die Möglichkeit der offenen Informationsbeschaffung zur Verfügung (Warnecke, 2010). Genau diesen Aspekt berücksichtigt die Methode der Open Source Intelligence (OSINT), bei der eine offene Beschaffung und Auswertung von frei zugänglichen Quellen durchgeführt wird (Meissinger, 2005).

Wie bei der HUMINT und TECHINT stehen Unternehmen bei der OSINT zahlreiche Möglichkeiten der Informationsbeschaffung zur Verfügung. Beispielsweise stellen Veröffentlichungen in Zeitungen und Fachzeitschriften, Dissertationen, Produktbeschreibungen oder der Besuch von öffentlichen Veranstaltungen, wie Messen, Kongressen und Symposien, eine Informationsquelle dar (BfV, 2008a; SiFo, 2010a). Das ergiebigste Medium innerhalb der OSINT ist jedoch das Internet, welches eine große Fülle an Informationen bietet (Warnecke, 2010). So geben Unternehmen aufgrund des verschärften Wettbewerbs in immer umfangreicherem Maße auf ihren Websites Auskunft über ihre Produkte und Dienstleistungen. Diese Informationsbereitstellung wird nicht nur von Kunden, sondern auch von Konkurrenzunternehmen in Anspruch genommen (Harbich, 2006). Auch die im Internet frei zugänglichen Jobbörsen von Unternehmen geben Hinweise über zukünftige Geschäftsaktivitäten (Warnecke, 2010).

Da das Internet jedoch auch immer kritisch bezüglich der Zuverlässigkeit der bereitgestellten Informationen zu betrachten ist, bieten kommerzielle Wirtschaftsdatenbanken eine Alternative. Solche, meist kostenpflichtige, Datenbanken können umfangreiche Informationen über bestimmte Unternehmen oder Personen bereitstellen, sodass Unternehmen zum Beispiel frühzeitig neue Wettbewerber identifizieren und infolgedessen geeignete Gegenmaßnahmen ergreifen können (Goemann-Singer et al., 2004; Meissinger, 2005). Eine weitere Möglichkeit besteht in der Auswertung von Patentdatenbanken nationaler oder internationaler Patentorganisationen. Hierdurch können Unternehmen Informationen über eingereichte Patente und die technischen Eigenschaften der Konkurrenzprodukte erhalten. Zusätzlich sind vorgetäuschte Kaufanfragen oder der Kauf des Konkurrenzprodukts denkbar (Goemann-Singer et al., 2004). Auf Basis dieser fragmentierten Einzelinformationen können dann detaillierte Unternehmensprofile erstellt und Rückschlüsse auf das zukünftige Verhalten des Wettbewerbers gewonnen werden (LfV BW und Bayern, 2006; Meissinger, 2005). Der Vorteil der OSINT liegt zum einen darin, dass im Gegensatz zur TECHINT keine teuren technischen Hilfsmittel zur Informationsgewinnung benötigt werden. Zum anderen ist die Sammlung und Auswertung von frei

zugänglichen Informationen keine Straftat (Harbich, 2006). Diese Legalität der OSINT bildet das Hauptunterscheidungsmerkmal zu den anderen Methoden der Informationsbeschaffung, sodass die Methode der OSINT der CI zuzuordnen ist (Meissinger, 2005). Findet eine offene Informationsbeschaffung jedoch in Kombination mit Gesprächsabschöpfung oder Vortäuschung falscher Identitäten statt, sind die Grenzen zur Illegalität nicht fern (LfV BW und Bayern, 2006; Lux/Peske, 2002a).

Abschließend lässt sich festhalten, dass mithilfe der OSINT große Teile der unternehmensspezifischen Informationsbedürfnisse befriedigt werden. Auf Grundlage solcher Basisinformationen können dann weitere menschliche und technische Informationsbeschaffungsmethoden angewandt werden (Lux/Peske, 2002a). Im Zuge des Wandels hin zu einer Informationsgesellschaft ist davon auszugehen, dass die Methode der OSINT weiter an Relevanz gewinnen wird (Meissinger, 2005).

2.2 Information und Wissen als entscheidender Wettbewerbsfaktor

Im Rahmen der folgenden drei Unterkapitel wird zunächst die Bedeutung von *Informationen* und *Wissen* für heutige Unternehmen vorgestellt. Aufbauend findet eine Abgrenzung und Systematisierung des Wissensbegriffs als auch eine Zuordnung auf betriebliche Wissensträger statt.

2.2.1 Unternehmerische Relevanz von Information und Wissen

Infolge der zunehmenden Grenzaufhebung auf den Waren-, Dienstleistungs-, Finanz- und Personenmärkten sowie der immer stärker anwachsenden weltweiten inter- und intraorganisationalen Vernetzung, bilden *Informationen,* als interpretierbare Daten, und *Wissen,* als Prozess der Verknüpfung von Informationen, für heutige Unternehmen einen kritischen Erfolgsfaktor (Meissinger, 2005). Gerade Deutschland, das nicht über umfangreiche Rohstoffvorkommen oder Bodenschätze verfügt, ist auf die Innovationsfähigkeit seiner Bürger und heimischen Unternehmen angewiesen, um sich im internationalen Wettbewerb behaupten zu können (Bundesverband der Deutschen Industrie (BDI), 2006; Corporate Trust, 2007).

So können Unternehmen mit innovativen Mitarbeitern Wissensvorsprünge gegenüber Konkurrenten generieren und diese in Wettbewerbsvorteile ummünzen (Marwehe/Weißbach, 2000; North, 2005). Diese Ungleichverteilung von Informationen und Wissen zugunsten in-

novativer Unternehmen weckt jedoch auch Begehrlichkeiten bei Wettbewerbern, die durch den heftigen Konkurrenzkampf auf den internationalen Märkten zu immer radikaleren Mitteln der Informationsbeschaffung greifen (Sobbek/Bühler, 2009). Daher ist es für innovative Unternehmen zunächst wichtig, in welchen Bereichen Wissensvorsprünge zur Konkurrenz bestehen, um dieses wettbewerbsrelevante Wissen auch vor entsprechenden Spionageangriffen zu schützen (Best/Weth, 2007).

Die Gefahr eines ungewollten Informations- und Wissensabflusses wird dadurch verdeutlicht, dass nicht nur das spionierende Konkurrenzunternehmen Wettbewerbsnachteile egalisieren und aufwendige Kosten der Wissensgenerierung sparen kann, sondern gleichzeitig das betroffene Unternehmen erhebliche materielle und immaterielle Schäden erleidet, die bis zur Schließung des Betriebs führen können (Corporate Trust, 2007; LfV BW und Bayern, 2006; Sobbek/Bühler, 2009).

Hieraus ergibt sich, dass *Informationen* und *Wissen* für Unternehmen der heutigen Informationsgesellschaft zu einem strategischen Wettbewerbsfaktor und begehrten Spionageziel gereift sind. Ein adäquates Informationsschutzkonzept bildet daher die Grundlage für den unternehmerischen Erfolg (Sobbek/Bühler, 2009; Warnecke, 2010).

2.2.2 Abgrenzung und Systematisierung von Wissen

Nach der Schaffung eines Bewusstseins für die unternehmerische Relevanz von Informationen und Wissen, ist es in einem nächsten Schritt sinnvoll, den Wissensbegriff inhaltlich zu verwandten Begriffen abzugrenzen und zu systematisieren, da nur so auch Rückschlüsse auf Vorgehensweisen der (illegalen) Informationsbeschaffung möglich sind und letztendlich ein effektiver Informationsschutz zu gewährleisten ist (Warnecke, 2010).

Ausgangpunkt der Betrachtung sind Zeichen, die unter anderem aus Buchstaben, Ziffern oder Sonderzeichen bestehen können und, mittels einer Syntax verbunden, zu Daten werden (Lux/Peske, 2002a; Rehäuser/Krcmar, 1996). Mit den entstandenen Daten, zum Beispiel „1,70“, ist jedoch noch keine Aussage über den Verwendungszweck getroffen. So könnte die Zahl „1,70“ einen Preis, aber auch eine Körpergröße angeben (Rehäuser/Krcmar, 1996). Erst wenn Daten in den Kontext eines Problemzusammenhangs gestellt werden und interpretierbar sind, entstehen aus diesen Daten *Informationen* (Rehäuser/Krcmar, 1996). Diese Beziehung lässt sich zum Beispiel dadurch verdeutlichen, dass Daten zur Herstellung von bestimmten Nahrungsmitteln in einem Softwareentwicklungsunternehmen keine Informationen darstellen,

da diese Daten irrelevant für die Entwicklung von Software sind. Erst durch den entsprechenden Kontext, hier Nahrungsmittelindustrie, werden die Daten zu Informationen (Probst et al., 1999). *Wissen* hingegen kann als Prozess der zweckorientierten Vernetzung, Verarbeitung und Speicherung von Informationen im menschlichen Gehirn verstanden werden (North, 2005; Rehäuser/Krcmar, 1996). Somit sind *Informationen* eine notwendige Voraussetzung zur Generierung von *Wissen*, da der Prozess der Wissensgenerierung durch die Verknüpfung von neuen Informationen mit bestehendem Wissen erfolgt (Osterloh/Frost, 2006). Weil der Entstehungsort des Wissens im menschlichen Gehirn liegt, ist Wissen personengebunden und kann streng genommen nicht auf Speichermedien wie Festplatten oder USB-Sticks transferiert werden (Fick et al., 2002). Da jedoch die Informationen im Unternehmen in hochverdichteter Form auf Datenträgern vorliegen, besteht eine hohe Ähnlichkeit zum Wissensbegriff (Warnecke, 2010). In diesem Zusammenhang sei auch der Begriff des *Know-how* kurz vorgestellt. Hierbei handelt es sich um Spezialwissen, das aus betrieblichen oder technischen Erfahrungen resultiert (Gabler Wirtschaftslexikon, 2010). Im Unternehmensalltag wird allerdings oftmals auf die Differenzierung der vorgestellten Begriffe verzichtet. Vielmehr geht es um den eigentlichen Schutz vor Abflüssen, um materielle und immaterielle Schäden zu verhindern (Rehäuser/Krcmar, 1996; Schaaf, 2009).

Durch eine klare Systematisierung des im Unternehmen vorhandenen Wissens kann der Schutz vor Spionageangriffen deutlich verbessert werden. Die wohl bekannteste Wissenssystematisierung geht auf Polanyi (1966) zurück, der zwischen explizitem und implizitem Wissen differenziert. Demnach ist explizites Wissen schriftlich, mündlich oder in einer beliebig anderen Form fassbar und damit in materieller Form transportierbar (Best/Weth, 2007; North, 2005; Schildbauer et al., 2003). Dieses Wissen liegt im Unternehmen unter anderem in Datenbanken, Handbüchern, Zeichnungen sowie Emails vor und wird durch den zunehmenden Einsatz moderner Informations- und Kommunikationstechnologien immer schneller abgerufen, verarbeitet, transferiert und gespeichert (Frey/Osterloh, 2002; Picot et al., 2003). Explizites Wissen, wie Produktionsunterlagen und Verfahrensvorschriften, macht jedoch nur einen kleinen Teil des Wissensbestandes eines Unternehmens aus (Meissinger, 2005). Eine größere Bedeutung hat oft implizites Wissen (Frey/Osterloh, 2002). Hierbei handelt es sich um unbewusste, personengebundene Kenntnisse, die nicht auf Datenträgern speicherbar sind, und durch das Zusammentreffen von Wissensstand und subjektiver Erfahrungen der Mitarbeiter entstehen (Best/Weth, 2007; Frey/Osterloh, 2002). Da sich implizites Wissen in den „Köpfen“ der Mitarbeiter befindet, ist eine Wissensverbreitung nur durch den persönlichen Austausch

möglich (Best/Weth, 2007; Picot et al., 2003). Dabei erstreckt sich das implizite Wissen von intellektuellen Kenntnissen der Problemerkennung und -lösung bis hin zu körperlichen Fertigkeiten wie der komplexen Bedienung einer Maschine (Frey/Osterloh, 2002; Frost, 2005).

Aus der Unterscheidung zwischen explizitem und implizitem Wissen lassen sich Schlüsse für die illegale Informationsbeschaffung ableiten. So kann explizites Wissen aufgrund seiner Speicherbarkeit zum Beispiel relativ unbemerkt auf firmenexterne Datenträger kopiert werden. Ebenfalls ist der komplette Diebstahl firmeneigener Datenträger und dem darauf befindlichen expliziten Wissen denkbar (Meissinger, 2005). Gerade die Mobilität und hohe Speicherkapazität moderner Datenträger macht es Dieben leicht, innerhalb kürzester Zeit große Mengen an explizitem Unternehmenswissen zu entwenden (Meissinger, 2005). Implizites Wissen ist hingegen schwieriger zu beschaffen. Da es nur personengebunden auftritt und zwischenmenschlich ausgetauscht werden kann, ist die Anwendung der HUMINT unumgänglich (Best/Weth, 2007; Warnecke, 2010). Beispielsweise könnten Konkurrenten an das sensible implizite Wissen eines Unternehmens gelangen, indem sie eigene Mitarbeiter in das betroffene Unternehmen einschleusen oder Mitarbeiter des betroffenen Unternehmens, bemerkt oder unbemerkt, für die illegale Informationsbeschaffung gewinnen (Warnecke, 2010). Des Weiteren wäre ein Informationsabfluss auch durch die Abwerbung von Mitarbeitern möglich (Meissinger, 2005). Die folgende Tabelle 1 fasst die vorgestellten Ausführungen zusammen.

	Explizites Wissen	**Implizites Wissen**
Eigenschaften	▪ schriftlich und mündlich fassbar	▪ nicht direkt fassbar
	▪ personenungebunden	▪ personengebunden
	▪ Speicherung durch verschiedenste Medien möglich	▪ personengebunde Speicherung
Anwendbare Methoden der Informationsbeschaffung	▪ Methoden der HUMINT als auch der TECHINT	▪ großteils Methoden der HUMINT

Tabelle 1: Explizites vs. Implizites Wissen
Quelle: Eigene Darstellung in Anlehnung an Warnecke, 2010, S. 268

Somit lässt sich festhalten, dass Wissen mit seinen Bestandteilen, den Informationen, in zahlreichen Facetten im Unternehmen auftreten kann. Angesichts der Tatsache, dass rund 70 Prozent aller Informationsabflüsse auf das eigene Personal zurückzuführen sind, sollten gerade die eigenen Mitarbeiter adäquat im Umgang mit Informationen geschult und sensibilisiert werden (Schaaf, 2009; SiFo BW, 2010a).

2.2.3 Betriebliche Wissensträger

Wissensträger sind „Objekte, Personen oder Systeme, die in der Lage sind, Wissen zu speichern und zu repräsentieren“ (Rehäuser/Krcmar, 1996, S. 16). Grundsätzlich kann zwischen natürlichen und unnatürlichen Wissensträgern differenziert werden (Warnecke, 2010). Hierbei kann der Mensch als alleiniger natürlicher Wissensträger angesehen werden, da er als einziges Trägermedium in der Lage ist, Informationen zu transformieren und Wissen aktiv weiterzuentwickeln (North, 2005; Rehäuser/Krcmar, 1996). Im betrieblichen Kontext bilden somit einzelne Mitarbeiter, Gruppen von Mitarbeitern oder aber die gesamte Belegschaft natürliche Wissensträger (Warnecke, 2010). Die Besonderheit natürlicher Wissensträger liegt darin begründet, dass sie explizites als auch implizites Wissen speichern können. Unnatürliche Wissensträger hingegen können lediglich explizites Wissen wie Produktionsunterlagen und Verfahrensvorschriften speichern, da sie nicht selbstständig Informationen mit bestehendem Wissen zu neuem Wissen verknüpfen können (Osterloh/Frost, 2006). Daher werden sie in der Literatur auch als reine (Zwischen-)Speicher verstanden (Werner, 2004). Künstliche Wissensträger sind heutzutage vor allem elektronische Speichermedien, wie Datenbanken, Festplatten, CDs oder USB-Sticks, aber auch Printmedien, wie Bücher und Zeitschriften, können explizites Wissen beinhalten (Boyens, 1998; Warnecke, 2010).

Anknüpfend an die Differenzierung in natürliche sowie unnatürliche Wissensträger und ihre Möglichkeiten der Wissensspeicherung lässt sich feststellen, dass gerade Menschen durch ihre Fähigkeit zur Speicherung von explizitem und implizitem Wissen, Gefahren der Industriespionage ausgesetzt sind. So befindet sich laut einer Studie der Delphigroup ein Großteil des Unternehmenswissens in den „Köpfen“ der Mitarbeiter (Schildbauer et al., 2003). Insbesondere Experten eines Unternehmens, die über zum Teil einzigartiges Spezialwissen und über besondere Fähigkeiten und Erfahrungen verfügen, geraten in den Fokus von Konkurrenzunternehmen (Macharzina, 2008; Rehäuser/Krcmar, 1996). Die herausragende Bedeutung von natürlichen Wissensträgern für ein Unternehmen und die besondere Spionagegefahr im Personalbereich kann am López-Fall verdeutlicht werden. Durch die Abwerbung des Chefeinkäufers José Ignacio López von *GM* durch *VW*, konnte *VW* mit dem Wissen von López die Kosten im Einkauf drastisch reduzieren und in Kombination mit weiteren Umstrukturierungs- und Rationalisierungsmaßnahmen Wettbewerbsnachteile gegenüber der Konkurrenz egalisieren (Schaaf, 2009; Spiegel Online, 2000).

So lässt sich festhalten, dass zur (illegalen) Informationsbeschaffung immer ein anzugreifender Wissensträger benötigt wird. Neben der Form dieses Wissensträgers, natürlich oder unna-

türlich, spielt auch die Wissensform, explizit oder implizit, eine Rolle welche Spionagemaßnahmen von Wettbewerbern ergriffen werden (Schindler, 2011; Warnecke, 2010). Unterschiedliche Angriffsszenarien sind dementsprechend aus der folgenden Tabelle 2 ersichtlich.

		Spionagemaßnahmen		
		HUMINT	**TECHINT**	**OSINT**
Spionageziel	**Natürliche Wissensträger**	▪ Social Engineering ▪ An- bzw. Abwerbung von Mitarbeitern ▪ Gesprächsabschöpfung ▪ Einschleusung von Spionen	▪ Social Engineering ▪ Lauschangriffe	▪ Recherche öffentlicher Quellen: zum Beispiel Befragung von Firmenvertretern auf Veranstaltungen für weitere menschliche und technische Spionagemaßnahmen
	Unnatürliche Wissensträger	▪ Entwendung von Wissensspeichern ▪ Einschleusung von Spionen	▪ Einsatz technischer Hilfsmittel: zum Beispiel Hacking und Phishing	▪ Recherche öffentlicher Quellen: zum Beispiel von Websites, Dissertationen oder Fachzeitschriften für weitere menschliche und technische Spionagemaßnahmen

Tabelle 2: Mögliche Spionageangriffe auf natürliche und unnatürliche Wissensträger
Quelle: Eigene Darstellung in Anlehnung an Warnecke, 2010, S. 270

2.3 Gefahrenpotenziale eines Know-how-Abflusses

Industriespionage ist eine reale und ernsthafte Bedrohung für deutsche Unternehmen. Um einen Überblick über die vielfältigen Risiken des Informationsabflusses zu erhalten, werden in den nächsten vier Unterkapiteln die wesentlichen Gefahrenbereiche Mensch, Organisation, Technik und Recht vorgestellt, wobei der Schwerpunkt auf dem Risikofaktor Mensch liegen wird.

2.3.1 Mensch

Untersuchungen und Statistiken zum Thema Industriespionage belegen, dass das größte Risiko eines ungewollten Informationsabflusses im Faktor Mensch liegt (unter anderem SiFo BW, 2010a; PWC, 2009; BfV, 2008a; Corporate Trust, 2007; Baeck/Weber, 2007). Zu oft konzentrieren sich Unternehmen im Rahmen ihrer Sicherheitskonzepte jedoch einseitig auf technische Aspekte des Informationsschutzes und vergessen dabei, dass selbst die beste Abschir-

mung nach außen keinen Schutz bietet, wenn der Täter bereits hinter dem Schutzwall agiert (Hirschmann, 2009; Huber, 2010b; Schaaf, 2009; Sidler, 2008). So besitzen viele der eigenen Mitarbeiter unnötigerweise sämtliche Zugriffsrechte innerhalb der EDV und genießen aufgrund langer Betriebszugehörigkeit uneingeschränktes Vertrauen seitens der Unternehmensleitung, wodurch große Mengen an vertraulichen Informationen und Know-how abfließen können (Corporate Trust, 2007; Kaufmann, 2007; Schaaf, 2009; SiFo BW, 2010a). Grundsätzlich bestehen beim Risikofaktor Mensch zwei Hauptprobleme (Schaaf, 2009):

- Illoyalität und
- Leichtfertigkeit

Bezugnehmend auf illoyale Mitarbeiter ist zunächst der Begriff des *Innentäters* einzuführen. Innentäter sind nicht nur fest angestellte Mitarbeiter, sondern auch Praktikanten, Doktoranden und Mitarbeiter externer Firmen, die oftmals die gleichen Zugangsrechte wie eigene Mitarbeiter besitzen (Schaaf, 2009). So gehen neben den eigenen Mitarbeitern auch von Praktikanten erheblichen Gefahren aus, wie der Vorfall beim französischen Automobilzulieferer *Valeo* und der Datenklau eines chinesischen Praktikanten in einem metallverarbeitenden Betrieb in Baden-Württemberg zeigen (Schaaf, 2009; SiFo BW, 2005). Ferner bestehen hohe Risiken bei Mitarbeitern externer Dienstleister. Hierzu gehören unter anderem Berater, speziell Wirtschaftsprüfer, IT-Dienstleister, Handwerker sowie Reinigungs- und Sicherheitskräfte. Gerade Arbeitnehmer der beiden letztgenannten Berufsgruppen werden relativ niedrig entlohnt und sind außerhalb der normalen Arbeitszeiten beschäftigt, sodass sensible Informationen relativ unbemerkt illegal beschafft werden können (KPMG, 2010). Ein Beispiel für einen Angriff wären sogenannte Keylogger, die innerhalb weniger Sekunden unscheinbar zwischen Tastatur und PC anzubringen sind und Passwörter von Mitarbeitern aufzeichnen (Baumgartner, 2005). Eine weitere Gefahr liegt in wechselbereiten Mitarbeitern, die zum Teil bereits eine innerliche Kündigung vollzogen haben. Diese Personen werden oft diskret durch Headhunter für konkurrierende Unternehmen abgeworben, indem ihnen ein materiell und immateriell attraktives Jobangebot unterbreitet wird (Schaaf, 2009). So ist es im Zuge des Weggangs keine Seltenheit, dass sensible Informationen über Kunden, Produkte sowie Preise abfließen und teilweise sogar ganze Maschinen oder Prototypen mitgenommen werden (Galdy, 2008; Schaaf, 2009).

Innentäter können entweder von sich aus vertrauliche Informationen anbieten oder aber diskret durch ein Konkurrenzunternehmen abgeworben sein (Hirschmann, 2009; Schaaf, 2009; Meissinger, 2005). Grundsätzlich lassen sich nach Lux und Peske (2002a) vier Motivgruppen des Verrats von Geschäfts- und Betriebsgeheimnissen feststellen. Das klassische und immer

noch dominante Motiv besteht in der finanziellen Komponente. Mehr als die Hälfte aller Spionagefälle, in denen Mitarbeiter involviert waren, gehen hierauf zurück (Lux/Peske, 2002a; PWC, 2009;). So ist es möglich, dass betroffene Mitarbeiter ihre Entlohnung als unangemessen ansehen oder Süchte zu einem erhöhten finanziellen Bedarf führen (Schaaf, 2009). Das zweite Hauptmotiv liegt in der Unzufriedenheit und Verlust der inneren Bindung aufgrund monotoner Arbeitsinhalte, unzureichenden organisatorischen Rahmenbedingungen, mangelhaftem sozialen Umfeld und geringer Wertschätzung der Arbeit durch Vorgesetzte und Kollegen (Meissinger, 2005; Warnecke, 2010). Gerade durch das heutige Streben nach Selbstverwirklichung in westlichen Gesellschaften nimmt dieses Motiv erheblich zu (Lux/Peske, 2002a). Hierbei kann sich die Unzufriedenheit bis zum Hass auf das eigene Unternehmen steigern, was mit Racheakten verbunden sein kann (Schaaf, 2009). Weitere Gründe sind ideologische Motive und persönliche Bindungen, die insgesamt eine eher untergeordnete Rolle spielen (Lux/Peske, 2002a).

Neben den vier vorgestellten Motiven liegt ein weiterer Erklärungsansatz für Spionagehandlungen im Kriminalitätsrisikomodell, dem sogenannten Fraud Triangle, von Cressey (Hirschmann, 2009). Danach muss für einen Täter zunächst eine Gelegenheit zur Tat bestehen, ohne dabei entdeckt zu werden. Diese Voraussetzung ist gegeben, wenn in einem Unternehmen die Kontrollen sowohl quantitativ als auch qualitativ unzureichend sind. Die zweite Bedingung liegt in der Motivation des Täters, die zum Beispiel durch finanzielle oder persönliche Gründe genährt sein kann. Das dritte Element des Dreiecks liegt in der Rechtfertigung des Täters, indem er zum Beispiel sein Verhalten als Normalität in dem betroffenen Unternehmen ansieht. Im Gegensatz zum persönlichen Wertesystem, das kaum beeinflussbar ist, kann jedoch auf das Verhalten eines Mitarbeiters innerhalb des Betriebs mittels der Unternehmenskultur, die ein solches Verhalten missbilligt, positiv eingewirkt werden. Zur Verdeutlichung der Ausführungen dient die folgende Abbildung 4.

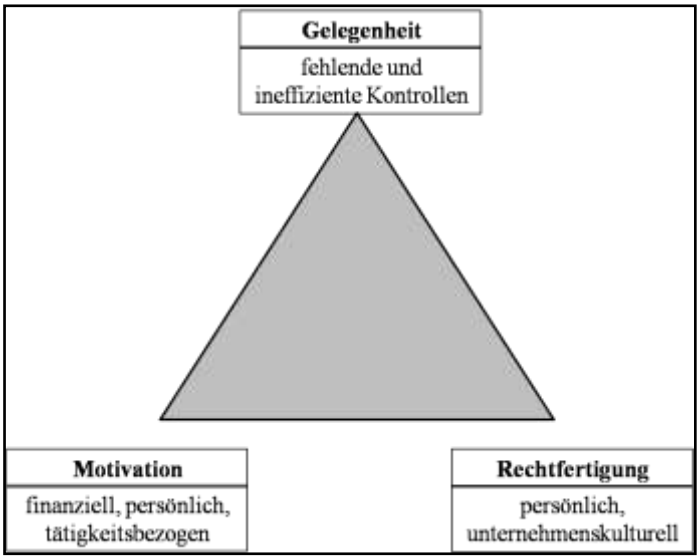

Abbildung 5: Fraud Triangle
Quelle: Eigene Darstellung in Anlehnung an KPMG, 2010, S. 17

Das von Mitarbeitern ausgehende Gefahrenpotenzial ist nicht an die hierarchische Stellung im Unternehmen gekoppelt und reicht von externen Dienstleister sowie Sachbearbeitern, über das mittlere Management, bis hin zur Geschäftsführung (Lux/Peske, 2002a). So erstrecken sich Spionagetätigkeiten über die Mitnahme von Geschäftskonzepten durch Mitglieder des Vorstands, wie im *Hilton*-Fall passiert, bis hin zum Abfluss von vertraulichen Informationen durch Praktikanten (Havranek, 2010; Schaaf, 2009). Gemessen an der Personalstärke wird jedoch ein relativ hoher Anteil von Wirtschaftskriminalität auf der Führungsebene verübt (PWC, 2009; SiFo, 2010a). Zusammenfassend wird die vorgestellte Innentäterproblematik noch einmal durch die folgende Abbildung verdeutlicht.

Das zweite Hauptproblem beim Risikofaktor Mensch ist die Leichtfertigkeit (Schaaf, 2009). Allzu oft werden sensible Informationen an öffentlichen Plätzen von firmeneigenen Mitarbeitern leichtfertig und lautstark mitgeteilt, sodass es für Fremde ein Leichtes ist diese Informationen abzuschöpfen (Meissinger, 2005; Schaaf, 2009). Auch das fehlende Bewusstsein im Umgang mit mobilen Endgeräten, wie Handys und Laptops, eröffnet Angreifern Möglichkeiten, indem zum Beispiel der W-LAN- oder Bluetooth-Zugang nicht ausreichend gesichert sind oder die Endgeräte unbeaufsichtigt an frei zugänglichen Plätzen liegen gelassen werden, sodass die Endgeräte innerhalb kürzester Zeit mit Spionagesoftware infiziert werden können (Schaaf, 2009). Fahrlässiges Verhalten seitens einiger Mitarbeiter ist auch im Umgang mit dem Internet zu beobachten, was durch die zunehmende Anbindung aller Mitarbeiterdie Gefahrenlage verschärft (LfV RlP, 2008; ZEW, 2007). Leichtfertigkeit und Gutgläubigkeit als

menschliche Eigenschaften werden auch in der bereits geschilderten und besonders effektiven Methode des Social Engineering ausgenutzt (Meissinger, 2005; Rogge/Ziegler, 2007). So besteht gerade bei Geschäftsreisen ins Ausland ein erhöhtes Risiko solcher Angriffe (Schaaf, 2009).

Relativierend lässt sich aber auch festhalten, dass die meisten Mitarbeiter loyal gegenüber ihrem Unternehmen sind und keine akute kriminelle Gefahr von ihnen ausgeht. Allerdings fehlt es oft an einem Bewusstsein für die Gefahren eines Informationsabflusses, sodass verhältnismäßig günstige Schulungs- und Sensibilisierungsmaßnahmen die Sicherheit bereits wirksam erhöhen können (Schaaf, 2009).

2.3.2 Organisation

Organisatorische Aspekte gehören zum zweiten wesentlichen Gefahrenbereich im Rahmen von Industriespionage und sind eng mit dem Risikofaktor Mensch verbunden. Diese enge Verbundenheit zwischen den Gefahrenbereichen Mensch und Organisation wird dadurch deutlich, dass jede betriebliche Organisation als System von Regeln durch Menschenhand geschaffen wird und sich gleichzeitig mit Regeln an die Mitarbeiter wendet, um Betriebsziele, wie Gewinn und Umsatz, bestmöglich zu erreichen.

Gerade zur Verhinderung eines ungewollten Know-how-Abflusses sind organisatorische Regelungen innerhalb eines Unternehmens unverzichtbar. Eine Vielzahl von Studien zeigt jedoch, dass solche Sicherheitsstandards in Unternehmen oft nur in unzureichendem Maße vorhanden sind oder die vereinbarten Regeln missachtet werden (Corporate Trust, 2009/2007; SiFo BW, 2010a). Die Gründe für fehlende organisatorische Sicherheitsvorkehrungen sind vielfältig und reichen von mangelndem Risikobewusstsein bis hin zu vorgeschobenen oder tatsächlichen finanziellen Restriktionen, die besonders bei KMU anzutreffen sind (Schaaf, 2009). Dabei sind gerade organisatorische Spionageabwehrmaßnahmen relativ kostengünstig im Vergleich zu aufwendigen technischen Sicherheitsanlagen. Sind die Regeln im Umgang mit sensiblen Informationen erst einmal durch das Personal verinnerlicht worden, bilden sie ein wichtiges Element in einem ganzheitlichen Informationsschutzkonzept (Schaaf, 2009). Das Gefahrenpotenzial, das von mangelnden organisatorischen Sicherheitsvorkehrungen und deren Missachtung ausgeht, wird nachfolgend anhand einiger Beispiele verdeutlicht.

Der Schutz von kritischem Erfolgswissen beginnt mit der Objektsicherheit. Zwar sind die meisten Unternehmen nach außen durch bauliche Sicherheitsmaßnahmen wie Zäune und

Mauern geschützt, doch fehlt es oft an einem Schutz einzelner unternehmenssensibler Bereiche auf dem Betriebsgelände (Corporate Trust, 2009; Schaaf, 2009). Handelt es sich um ein Unternehmen, das über eine einzigartige Vertriebsstrategie verfügt, so sind besonders in diesem Bereich erhöhte baulich-organisatorische Sicherheitsvorkehrungen zu treffen, indem zum Beispiel Identifikationssysteme den Zugang zu einem solchen Bereich regeln (SiFo BW, 2010a). Die mangelnden Regelungen im räumlichen Zugang zu unternehmenssensiblen Bereichen setzen sich in vielen Unternehmen auch in den Zugriffsrechten innerhalb der EDV fort. So besitzen viele der eigenen Mitarbeiter unnötigerweise sämtliche Zugriffsrechte und genießen aufgrund langer Betriebszugehörigkeit ungeprüftes Vertrauen seitens der Geschäftsführung, was die Gefahr eines ungewollten Know-how-Abflusses erhöht (Corporate Trust, 2007; Kaufmann, 2007; Schaaf, 2009; SiFo BW, 2010a).

Ein weiterer Problembereich besteht im Umgang mit schützenswerten Informationen. Laut Studien der Unternehmensberatung Corporate Trust (2009/2007) machen weniger als die Hälfte aller befragten Unternehmen ihren Mitarbeitern klare Vorgaben für den Umgang mit vertraulichen Informationen, Daten oder Dokumenten. So fällt bei Betrachtung der Studienergebnisse auf, dass nur jedes fünfte Unternehmen eine eindeutige Kennzeichnung und Klassifizierung von Geschäfts- und Betriebsgeheimnissen in Vertraulichkeitsstufen, beispielsweise- *offen zugänglich*, *vertraulich* und *geheim*, vornimmt. Eine solche Kategorisierung des Firmenwissens und eine entsprechende Kommunikation an die Mitarbeiter ist jedoch zwingend notwendig, um einen adäquaten Informationsschutz zu gewährleisten (Corporate Trust, 2007; Schaaf, 2009).Aufgrund eines mangelnden Risikobewusstseins und zur Vermeidung von Personalkosten, verzichten auch noch immer viele Unternehmen auf die Einstellung eines Sicherheitsverantwortlichen (Baeck, 2006). Gemäß Corporate Trust (2007) gaben nur circa 40 Prozent der befragten Unternehmen an, über eine solche Stelle zu verfügen, wobei davon auszugehen ist, dass die meisten Stelleninhaber einen IT-Schwerpunkt besitzen und daher die von Mitarbeitern ausgehenden Risiken vernachlässigen.

Selbst wenn seitens der Unternehmensleitung adäquate organisatorische Sicherheitsvorkehrungen getroffen worden sind, hängt der Grad des Informationsschutzes entscheidend von der Umsetzung der Regelungen im betrieblichen Alltag ab. So werden festgelegte Sicherheitsstandards oft aufgrund von Bequemlichkeit missachtet, indem zum Beispiel abzuschließende Türen offen gelassen werden oder sensible Unterlagen, trotz geltender Clean-Desk-Policy, unbeaufsichtigt auf den Schreibtischen der Mitarbeiter liegen bleiben (Schaaf, 2009). Daher sind regelmäßige Kontrollen der bestehenden Sicherheitsmaßnahmen unumgänglich. In der

Praxis finden solche Prüfungen jedoch nur bei jedem fünften Unternehmen statt (Corporate Trust, 2007).

2.3.3 Technik

Die moderne Technik bietet eine Vielzahl an Möglichkeiten für einen Angriff auf vertrauliche Unternehmensdaten und ist nach dem Informationsabfluss durch Mitarbeiter die zweithäufigste Angriffsform (Corporate Trust, 2007; Schaaf, 2009). Im Rahmen der folgenden Ausführungen sollen die Gefahrenpotenziale dieses Bereichs verdeutlicht werden.

Häufiges Einfallstor technischer Spionageaktivitäten sind EDV- und Telekommunikationsanlagen eines Unternehmens. Diese Anlagen sind, wie die Studie des *ZEW* (2007) belegt, fast immer mittels Internet an die Außenwelt angebunden, was ein grundsätzliches Bedrohungspotenzial mit sich bringt. Zudem werden diese technischen Einrichtungen meist nur unzureichend verschlüsselt, sodass sich Angreifer in relativ kurzer Zeiteinen digitalen Zugang zum Firmennetzwerk verschaffen können und Telefongespräche ohne die Installation von Wanzen abhörbar sind (BfV, 2008a; Schaaf, 2009). Eine weitere Form eines internetbasierten Angriffs auf sensibles Firmenwissen stellen Emails mit manipuliertem Anhang dar. Diese sind oft inhaltlich auf die adressierten Opfer zugeschnitten, sodass viele Mitarbeiter entsprechende Anhänge leichtfertig öffnen (LfV RlP, 2008). Dabei installiert sich im Hintergrund unbemerkt Schadsoftware, die vorher festgelegten Computern via Internet Zugriff auf das Firmennetzwerk verschafft (BfV, 2010b; Faber, 2009). Dass diese Angriffsform durchaus effektiv ist, zeigt eine Studie der University of California (2008), in der der wirtschaftliche Erfolg von Spam analysiert wurde. Demnach ist eine von circa 12,5 Millionen Spam-Mails erfolgreich. Das scheint auf den ersten Blick eine verschwindend geringe Trefferquote zu sein. Wird jedoch berücksichtigt, dass alleine minütlich mehrere Millionen Spam-Mails von Computern rund um die Welt ausgehen, wird die tatsächlich von Spam-Mails ausgehende Gefahr deutlich.

Neben dem klassischen kabelgebundenen Zugang ins Internet sind auch neue Formen der Datenübertragung, wie WLAN und Bluetooth, durch technische Angriffe bedroht (Faber, 2009; Meissinger, 2005). Sind diese Zugangsformen nicht ausreichend gesichert, können die jeweiligen mobilen Endgeräte, wie Handys und Laptops, ausspioniert werden und damit sensible Firmeninformationen an Wettbewerber abfließen (Schaaf, 2009). Gerade im Ausland besteht ein erhöhtes Risiko, dass der Datenverkehr mobiler Endgeräte abgefangen wird. Trotz

dieser Tatsache verfügen jedoch nur die wenigsten der mittelständischen Unternehmen über eine angemessene Verschlüsselung ihrer Kommunikationsmittel (BfV, 2008a; Corporate Trust, 2009).

Zusätzlich zu den Angriffsmöglichkeiten von außen treten technische Angriffe auch von innen auf, indem zum Beispiel Keylogger innerhalb weniger Sekunden von internem oder externem Personal angebracht werden können und jeden Tastenanschlag von Mitarbeitern aufzeichnen (Schaaf, 2009). Wie bei vielen weiteren technischen Angriffsszenarien ist jedoch menschliche Beihilfe notwendig, was die enge Beziehung zwischen der technischen und menschlichen Komponente aufzeigt (Meissinger, 2005; Schaaf, 2009).

Abschließend lässt sich festhalten, dass Unternehmen sich mit geeigneten Maßnahmen durchaus gegen die geschilderten Gefahren schützen können. Grundlage ist jedoch, dass die Bedrohungslage zunächst seitens des Unternehmens erkannt wird (Faber, 2009).

2.3.4 Recht

Rechtliche Aspekte bilden den vierten und letzten Gefahrenbereich im Rahmen von Industriespionage und werden seitens der Unternehmensleitung oft unterschätzt (Warnecke, 2010). Dabei gehen erhebliche Bedrohungen von unzureichenden oder falsch getroffenen rechtlichen Sicherheitsvorkehrungen aus, wie die folgenden Szenarien veranschaulichen.

Eine Problematik besteht in der Anmeldung von gewerblichen Schutzrechten wie Patenten, Marken, Geschmacks- und Gebrauchsmustern (SiFo, 2010a). So dient das Patent grundsätzlich zum Schutz technischer Erfindungen und verleiht seinem Inhaber das räumlich und zeitlich befristete Privileg, allein über die Erfindung zu verfügen (Deutsches Patent- und Markenamt (DPMA), 2010). Diesbezüglich steht dem Erfinder somit ein Exklusivrecht in der Verwertung seiner Erfindung zu, was jedoch oft durch Plagiatoren ebenfalls in Anspruch genommen wird. Neben der originären Schutzfunktion geben Erfinder durch die Anmeldung des Patents auch detaillierte Informationen zu ihrer Erfindung offen preis, die Konkurrenten aufmerksam machen und Informationsabfluss sowie Produktpiraterie eher noch unterstützen (LfV BW, 2004; Schaaf, 2009). Des Weiteren reicht es für ein deutsches Unternehmen in einer globalisierten Welt nicht aus, sein Patent nur in Deutschland anzumelden. Auf der anderen Seite existieren gerade im Ausland besondere Gefahren des Know-how-Abflusses. Zum Teil liegen enge Beziehungen zwischen Patentämtern, Geheimdiensten und ausländischen Unternehmen vor, sodass Unternehmenswissen ungewollt in fremde Hände gelangt (Schaaf,

2009). Speziell im asiatischen Raum gilt das Kopieren von Erfindungen als Anerkennung, die dem Erfinder zu Teil wird, sodass hier die Durchsetzung eines exklusiven Patentrechts als schwierig zu betrachten ist (Schaaf, 2009; SiFo BW, 2010a). Umso wichtiger sind Fortschritte auf dem Weg zu einem international einheitlichen Urheberrechtsschutz, wie das seit 1994 geltende TRIPs-Abkommen (SiFo BW, 2010a). Generell sollten Patentanmeldungen daher nur durchgeführt werden, wenn auch die rechtliche Durchsetzung mit einem adäquaten zeitlichen und finanziellen Aufwand gesichert ist (Schaaf, 2009). Andernfalls bietet es sich an, auf Patente zu verzichten und vielmehr mit einer Strategie kurzer Produktlebenszyklen und ständiger Innovationen dem Wettbewerb stets einen Schritt voraus zu sein (Meissinger, 2005). Die Gefahren durch Verletzungen des Patent- und Markenrechts werden von deutschen Unternehmen immer noch unterschätzt (PWC, 2009).

Eine weitere rechtliche Gefahr existiert bei Zertifikaten, wie der Qualitätsmanagementnorm DIN EN ISO 9000 (Meissinger, 2005). Auf der einen Seite können sich Unternehmen mit derartigen Zertifikaten in ihrer Leistungsfähigkeit gegenüber der Konkurrenz abheben. Auf der anderen Seite werden durch solche Vorgänge detaillierte firmeninterne Strukturen und Prozesse für Wettbewerber sichtbar (Nathusius, 2001). Zwar sind Zertifizierungsgesellschaften zur Geheimhaltung verpflichtet, doch kann sich auch hier, wie in jedem anderen Unternehmen, ein Informationsabfluss stattfinden (Meissinger, 2005).

Viele deutsche Unternehmen sind im Ausland über Niederlassungen, Tochterunternehmen, Joint-Ventures oder Handels- und Vertriebsvertretungen tätig (Corporate Trust, 2009). Gerade Joint-Ventures sind eine beliebte Rechtsform des Markteintritts, da durch die Zusammenarbeit mit einem ausländischen Unternehmen unter anderem Markt- und Landeskenntnisse sowie bestehende Kontakte zu lokalen Behörden genutzt werden können. Allerdings bestehen neben Abstimmungsschwierigkeiten aufgrund kultureller Distanzen auch Gefahren des Know-how-Abflusses, sodass, unter Berücksichtigung der Risiken, solche Kooperationen nicht mit direkten Konkurrenten durchgeführt werden sollten (Berndt et al., 2010; Meissinger, 2005).

Mit der Expansion ins Ausland kommt es zwangsläufig auch zu Kontakten mit Behörden. So sind beispielsweise Baugenehmigungen einzuholen sowie Vorgaben und Vorschriften zum Arbeits- und Umweltschutz vom Unternehmen einzuhalten. Im Rahmen solcher Kontaktekönnen ebenfalls Informationen abfließen. Wenn beispielsweise die Baupläne einer Maschine an die zuständigen Behörden weitergereicht werden, reicht ein korrupter Beamter aus und der Informationsabfluss ist erfolgt. Selbst wenn ein Unternehmen über gute Beziehungen zu staat-

lichen Institutionen verfügt, sind diese Kontakte stets kritisch zu hinterfragen, da viele Staaten systematisch ihre heimische Wirtschaft durch Wirtschaftsspionage unterstützen (BfV, 2008a; Schaaf, 2009).

3 Methode

In diesem Kapitel wird zunächst auf die zu untersuchende Stichprobe und das Experteninterview eingegangen. Anschließend folgt eine Erläuterung zur Durchführung und Auswertung der Experteninterviews.

3.1 Stichprobe

Im Rahmen dieser Masterarbeit wurden im Zeitraum vom 29. März bis zum 27. April 2011 acht Experteninterviews zum Thema Industriespionage und ungewolltem Know-how-Abfluss geführt. Ziel dieser Untersuchung war es, die Spionagerisiken, denen Unternehmen ausgesetzt sind, herauszuarbeiten und verwendete personelle, organisatorische, technische sowie rechtliche Spionageabwehrmaßnahmen zu identifizieren, um durch Integration in den bestehenden theoretischen Erkenntnisstand, einen Katalog an Handlungsmaßnahmen zu entwickeln, mit dem sich Unternehmen adäquat vor ungewolltem Know-how-Abfluss schützen können. Hierfür wurden acht Sicherheitsverantwortliche beziehungsweise Geschäftsführer besonders spionagegefährdeter Unternehmen befragt.

Ausgehend von der Forschungsfrage, welche präventiven und repressiven Spionageabwehrmaßnahmen Unternehmen zur Verbesserung der personellen Sicherheit zur Verfügung stehen, erfolgte die Gewinnung der Interviewpartner und die damit zusammenhängende Festlegung der Stichprobe in Zusammenarbeit mit dem *niedersächsischen Landesamt für Verfassungsschutz* und dem *Arbeitskreis der Sicherheitsbevollmächtigten in Niedersachsen*. Bereits bei der ersten Betrachtung wird deutlich, dass es sich bei der vorliegenden Auswahl um eine relativ kleine Stichprobe handelt. Dieser geringe Umfang der Stichprobe ist jedoch im Rahmen von qualitativer Forschung beziehungsweise Experteninterviews nicht unüblich (Pfaff, 2005). Im Gegensatz zur quantitativen Forschung, bei der die Stichprobe insbesondere dem Kriterium der statistischen Repräsentativität genügen muss, hat sich die Stichprobenbildung in der qualitativen Forschung primär an der inhaltlichen Repräsentation zu orientieren, wobei auch die Ergebnisse der qualitativen Forschung generalisierbar sein sollten (Flick, 2005; Merkens, 1997; Friebertshäuser, 1997). Eine größere Stichprobe war unter anderem auch aufgrund limitierter zeitlicher und finanzieller Ressourcen im Rahmen einer Masterarbeit nicht möglich, sodass ein Kompromiss aus Ökonomie und Vollständigkeit gewählt wurde.

Bei der Auswahl der Unternehmen wurde darauf geachtet, dass besonders innovative und damit spionagegefährdete Unternehmen in der Untersuchung berücksichtigt werden. Je nach organisatorischer Ansiedlung des Informationsschutzes konnten so Sicherheitsverantwortliche beziehungsweise Geschäftsführer der jeweiligen Unternehmen befragt werden. Diese Personen konnten im Vorfeld der Untersuchung als firmeninterne Experten auf dem Gebiet des Informationsschutzes identifiziert werden.

Nach der Definition des *Instituts für Mittelstandsforschung (IfM)* in Bonn gelten Unternehmen als mittelständisch, wenn sie über mehr als zehn und weniger als 500 Mitarbeiter verfügen und gleichzeitig einen Jahresumsatz von mehr als einer Million Euro bis hin zu 50 Millionen Euro erwirtschaften. Die folgende Tabelle 3 gibt diesbezüglich einen Überblick über die Differenzierung zwischen Klein-, Mittel- und Großunternehmen anhand der Kriterien Mitarbeiteranzahl und Jahresumsatz.

	Mitarbeiteranzahl	**Jahresumsatz (in Millionen Euro)**
Kleine Unternehmen	< 10	≤ 1
Mittlere Unternehmen	< 500	≤ 50
Große Unternehmen	≥ 500	> 50

Tabelle 3: Unternehmensklassifikation
Quelle: Eigene Darstellung in Anlehnung an IfM, 2007, S. 4

Demnach wurden Vertreter von fünf Großunternehmen und drei mittelständischen Unternehmen zu ihren spezifischen Spionagerisiken und vorhandenen Abwehrmaßnahmen befragt. Die Akquisition von mittelständischen Firmen und Großunternehmen wurde dabei bewusst durchgeführt, um auch mögliche Unterschiede im Gefährdungspotenzial und bestehenden Abwehrmaßnahmen zu identifizieren. Die Stichprobe deckt unter anderem besonders spionagegefährdete Branchen, wie den Maschinen- und Automobilbau, die forschungsintensive Chemiebranche und Unternehmen der IT-Branche, ab. Bei der Auswahl der Sichtprobe wurde darauf geachtet, Unternehmen aus unterschiedlichen spionagegefährdeten Branchen zu berücksichtigen, um generalisierende Aussagen zu ermöglichen. Dennoch sind diese Aussagen aufgrund der begrenzten Größe der Stichprobe mit Einschränkungen behaftet und müssen immer vor dem spezifischen Unternehmenskontext betrachtet werden.

3.2 Experteninterviews

In dieser Masterarbeit wurde das Experteninterview als Instrument der Datenerhebung ausgewählt. Experteninterviews sind eine besondere Form der verbalen Befragung, bei der eine Person zu ihrem Spezialwissen befragt wird (Mayer, 2009). Das Ziel dieser Erhebungsmethode liegt in der Rekonstruktion des Wissens von Experten und deren Perspektiven auf bestimmte Sachverhalte (Pfadenhauer, 2009). Der Interviewte ist hier weniger als Person, sondern vielmehr in seiner Funktion als Experte auf einem abgegrenzten Teilgebiet von Interesse (Mayer, 2009). Diese klare Begrenzung zeigte sich im Rahmen dieser Untersuchung durch die bewusste Auswahl und Befragung von zuvor identifizierten Experten auf dem Gebiet des Informationsschutzes.

Hierbei kann unter dem Begriff des Experten eine Person verstanden werden, die auf einem begrenzten Gebiet über spezifisches und abrufbares Wissen verfügt, in einer verantwortungsvollen Position eines Problemlösungsprozesses steht und über einen privilegierten Zugang zu Informationen, Personengruppen oder Entscheidungsprozessen verfügt (Hitzler, 1994; Mayer, 2009; Meuser/Nagel, 1991). Diese Definition zeigt, dass dem Experten neben seinem Wissensvorteil jedoch auch eine hohe Verantwortlichkeit in Bezug auf die Problemlösung zukommt (Pfadenhauer, 2009). Ob jemand Experte ist, hängt zudem vom jeweiligen Untersuchungsgebiet ab (Mayer, 2009).

Das Experteninterview ist eine besondere Form des Leitfadeninterviews (Mayer, 2009). Dabei dient der Interviewleitfaden zur Orientierung. Mit offen formulierten Fragen können Experten relativ frei antworten, um ihr Spezialwissen möglichst vollständig zur Entfaltung kommen zu lassen. Durch den Leitfaden kann der Interviewer gezielt auf das relevante Wissen eines Experten eingehen und dem Befragten gleichzeitig verdeutlichen, dass er mit der zu untersuchenden Thematik vertraut ist (Mayer, 2009; Meuser/Nagel, 1991). Die Interviews müssen, trotz des Leitfadens, nicht einem vorher festgelegten Ablauf folgen. Vielmehr entscheidet der Interviewer selber, ob und wann er detailliert nachfragt (Mayer, 2009). Diese Freiheiten ermöglichen es dem Interviewer gleichzeitig auch bei ausschweifenden Ausführungen den Befragten wieder auf das Thema zurückzuführen (Flick, 2005). Der Interviewer sollte sich daher nicht zu starr am Leitfaden orientieren, aber wenn nötig, themenferne Ausschweifungen des Befragten, auch schon unter Berücksichtigung der limitierten Zeit, unterbrechen (Mayer, 2009). Somit wird dem Interviewer während der Befragung ein hohes Maß an Sensibilität in der Steuerung des Interviews abverlangt. Dabei ist bereits Gesagtes mit den Fragestellungen abzugleichen, um gezielt alle notwendigen Informationen zur Beantwortung der Forschungs-

frage zu erlangen (Mayer, 2009). Zusätzlich ist seitens des Interviewers darauf zu achten, dass die Befragung nicht zu einem Frage-Antwort-Dialog verkürzt wird und damit wichtige Ausführungen des Experten verloren gehen (Friebertshäuser, 1997).

Somit hängt der Erfolg eines Experteninterviews maßgeblich vom situationsflexiblen Einsatz des Interviewleitfadens ab (Pfadenhauer, 2009). Interviewtrainings vor den eigentlichen Befragungen gelten daher als sinnvolle Maßnahme (Flick, 2005). Als notwendige Voraussetzung für das Gelingen eines Experteninterviews gilt ferner eine angemessene thematische Kompetenz des Interviewers, damit das Gespräch auf annähernd gleicher Augenhöhe stattfinden kann (Pfadenhauer, 2009; Trinczek, 1995). Nicht zuletzt wird das Experteninterview, mit seiner Fokussierung auf Personen mit besonderem Wissensstand, im Rahmen der zunehmenden Arbeitsteilung ein immer wichtigeres Instrument der qualitativen Forschung (Pfadenhauer, 2009).

3.3 Durchführung

Da Experteninterviews eine besondere Form von Leitfadeninterviews sind, wurde vor der eigentlichen Durchführung der acht Experteninterviews zunächst ein Interviewleitfaden (Anhang A) erstellt. Hierbei fand im Rahmen der Konstruktion des Leitfadens eine konsequente Orientierung an der Forschungsfrage statt. So wurde bei der Strukturierung des Leitfadens bewusst mit Fragen zur Analyse und Bewertung von möglichen Spionagerisiken und -schäden begonnen, um das grundsätzliche Gefährdungspotenzial des jeweiligen befragten Unternehmens vorab herauszustellen. Anknüpfend erfolgte eine Konzentration auf bestehende und geplante Spionageabwehrmaßnahmen des Unternehmens, wobei personelle, organisatorische, technische und rechtliche Maßnahmen nacheinander behandelt wurden. Des Weiteren enthielt der Leitfaden überwiegend offene Fragen, um das einzigartige Wissen und die besonderen Sichtweisen der Experten zur Geltung zu bringen, was durch eine standardisierte Form des Interviewleitfadens nicht möglich gewesen wäre. Neben der leitfragenorientierten Erstellung des Leitfadens bildete die dreimonatige Einarbeitung in das Thema der Industriespionage eine notwendige Voraussetzung für das Gelingen der Interviews. Hierzu wurden zahlreiche Lehrbücher und Fachbeiträge studiert sowie diverse Gespräche im Vorfeld der Untersuchung geführt, um Interviews auf annähernd gleicher Augenhöhe zu gewährleisten.

Der ausgewählte Expertenkreis wurde im Vorfeld der Interviews über Dauer und groben Inhalt der Befragung informiert. Auch deshalb kam es zu einer sehr hohen Kooperationsbereit-

schaft seitens Gesprächspartner, was eine zeitnahe Durchführung der Interviews ermöglichte. So wurden im Zeitraum vom 29. März bis zum 27. April 2011 acht Interviews geführt. Im Zuge der Durchführung der Interviews gestaltete sich jedes Gespräch unterschiedlich, indem sich, je nach Gesprächspartner, andere inhaltliche Schwerpunkte ergaben (Anhang B). Diese gewährten Freiheiten der Gesprächspartner dienten in erster Linie zur Erfassung des wertvollen Expertenwissens. Um dennoch eine vergleichbare Erhebung sicher zu stellen, wurde in allen acht Interviews der gleiche Leitfaden verwendet. Die besondere Schwierigkeit des Interviewers bestand somit im situationsflexiblen Einsatz des Leitfadens. Aussagen des Gesprächspartners mussten ständig mit den bestehenden Fragestellungen abgeglichen werden, um zu einer möglichst vollständigen Beantwortung der Forschungsfrage zu gelangen. Damit diese herausfordernde Aufgabe bewältigt werden konnte, fanden im Vorfeld Gespräche mit dem Erstprüfer und dem niedersächsischen Verfassungsschutz statt, in denen das spätere Vorgehen in den Interviews diskutiert und der Umfang des Leitfadens abgestimmt wurden, um der Interviewdauer von einer Stunde gerecht zu werden. Explizite Interviewtrainings, wie sie in der Literatur angeführt werden, fanden in der vorliegenden Untersuchung nicht statt (Flick, 2002).

Hinsichtlich einer flexiblen Handhabung des Leitfadens wurden die Interviews, mit Einverständnis der Befragten, digital aufgezeichnet. Im Anschluss an die Aufzeichnung erfolgte eine anonymisierte Transkription der Interviews, um keine Rückschlüsse auf die befragten Unternehmen und ihr Vorgehen im Informationsschutz zu ermöglichen. Die Anonymisierung diente ferner der Herstellung einer möglichst vertrauten Kommunikationssituation, was sich positiv auf die Ergebnisse auswirkte. Bezüglich des Vorgehens in der Transkription wurde ein ökonomischer Ansatz gewählt, der primär auf die Wiedergabe des Inhalts abzielte. Da keine sprachwissenschaftlichen Aspekte, sondern das Thema der Industriespionage im Vordergrund stand, kann dieses Vorgehen als vertretbar angesehen werden. Dementsprechend wurden die Transkriptionsregeln nach Kuckartz (1999) verwendet. Nach Kontrolle der Transkripte durch den Erstprüfer wurden die Digitalaufnahmen gelöscht, um eine missbräuchliche Verwendung zu verhindern.

Die Ergebnisse der Befragung sind im vierten Kapitel, gemäß der Strukturierung des Interviewleitfadens, ersichtlich. Der Leitfaden für die Experteninterviews befindet sich im Anhang A. Die dazugehörigen Transkripte liegen im Anhang B vor.

3.4 Auswertung

Das Ziel der Interviewauswertung war es, die spezifischen Risiken eines ungewollten Know-how-Abflusses sowie bestehende und geplante Sicherheitsmaßnahmen zur Spionageabwehr bei den befragten Unternehmen zu identifizieren, um letztendlich generalisierende Aussagen über die von Industriespionage ausgehenden Gefahren und resultierende Sicherheitsmaßnahmen machen zu können.

Die Grundlage der Auswertung bildeten die Transkripte der acht Interviews. Bei der Auswertung der Experteninterviews erfolgte eine Orientierung am sechsstufigen Verfahren von Mühlfeld et al. (1981). Hierbei handelt es sich um eine pragmatische und ökonomische Vorgehensweise, bei der Pausen, Stimmlagen sowie weitere parasprachliche Elemente nicht Gegenstand der Interpretation sind, sondern vielmehr der reine Inhalt des Gesprächs im Vordergrund steht (Mayer, 2009). Anstatt die geführten Interviews bis ins letzte Detail zu interpretieren, liegt der Fokus auf der Identifikation von Problembereichen anhand der Fragen im Leitfaden (Lamnek, 1995). Somit wurde auch in der Transkription der Interviews auf entsprechende Anmerkungen verzichtet. Im Rahmen der Auswertung schlagen Mühlfeld et al. (1981) die folgenden sechs Schritte vor:

1. Markierung der Antworten
2. Einordnung des Textes in ein Kategorieschema
3. Herstellung einer inneren Logik
4. Erstellung eines Textes zur inneren Logik
5. Erstellung der Auswertung
6. Präsentation der Auswertung

In der vorliegenden Untersuchung wurden die Transkripte ebenfalls zunächst gelesen und Antworten auf entsprechende Fragen des Leitfadens markiert. In einem zweiten Schritt erfolgten ein erneutes Durchlesen und die Einordnung der Textpassagen in ein Kategorieschema. Dieses Kategorieschema setzte sich gemäß der Gliederung des vierten Kapitels aus den Elementen *Risikoanalyse*, *Risikobewertung* sowie *personellen*, *organisatorischen*, *technischen* und *rechtlichen Spionageabwehrmaßnahmen* zusammen. Anknüpfend an die Kategorieschemabildung wurde für jedes Interview eine innere Logik erstellt, indem sowohl bedeutungsgleiche als auch widersprüchliche Aussagen des Interviewten berücksichtigt wurden. Nach der Erstellung einer inneren Logik erfolgte die eigentliche Auswertung, wo bezogen auf eine Frage des Leitfadens alle hierzu passenden Antworten aus den acht Interviews eingefügt und

kommentiert wurden. Die Präsentation der Auswertung wird im folgenden vierten Kapitel dargestellt.

4 Ergebnisse

In diesem Kapitel werden die Ergebnisse der acht Experteninterviews vorgestellt. Dabei liegt der Fokus in den ersten beiden Unterkapiteln auf den unternehmensspezifischen Risiken eines ungewollten Know-how-Abflusses sowie der Analyse und Bewertung solcher Risiken. Im weiteren Verlauf werden die personellen, organisatorischen, technischen und rechtlichen Spionageabwehrmaßnahmen aus der Unternehmenspraxis präsentiert, wobei der Schwerpunkt im Bereich Personal liegt. Die Grundlage zur Strukturierung der Ergebnisse bildet der Leitfaden der Experteninterviews.

4.1 Risikoanalyse

Das Risiko eines ungewollten Know-how-Abflusses ist besonders für innovative Unternehmen eine allgegenwärtige Gefahr. Um Industriespionage dementsprechend adäquat begegnen zu können, ist es daher für Unternehmen wichtig und notwendig solche Risiken im Vorfeld zu analysieren.

Im Rahmen der geführten Interviews wird deutlich, dass zwar in allen befragten Unternehmen Risikoanalysen durchgeführt werden, der Umfang, die Häufigkeit und die Systematik solcher Analysen sich jedoch erheblich unterscheiden. Dieses Gefälle ist insbesondere beim Vergleich von Großunternehmen zu mittelständischen Unternehmen sichtbar, sodass im Folgenden eine differenzierte Betrachtung der Risikoanalysesysteme nach Unternehmensgröße stattfindet.

Großunternehmen, die nach der Definition des IfM über mindestens 500 Mitarbeiter und mehr als 50 Millionen Euro Jahresumsatz verfügen, zeigen in der vorliegenden Untersuchung erheblich umfassendere Risikoanalysesysteme als mittelständische Unternehmen. Solche Risikoanalysesysteme sind für einen Teil der befragten Großunternehmen, die nach der ISO 27001 – Informationssicherheit zertifiziert sind, sogar Pflicht. Hierbei werden in obligatorischen Risikoanalysen alle Abteilungen eines Unternehmens einer jährlichen Prüfung unterzogen, ohne die das jeweilige Unternehmen keine Zertifizierung erhalten würde (Transkript 3, 10 ff.). So werden in einem Unternehmen aus der IT-Branche die einzelnen Abteilungen im Rahmen der Risikoanalysen von den Landesverantwortlichen für Informationssicherheit dazu aufgefordert in ihren Bereichen Risiken eines ungewollten Know-how-Abflusses zu identifizieren und zu lokalisieren. Die Landesverantwortlichen begutachten wiederum die Risikoana-

lysen und berichten direkt an den Manager für Informationssicherheit in der Unternehmenszentrale. Dieser Vorgang bildet die Grundlage für die Definition von Maßnahmen (Transkript 3, 17 ff).

Ein weiteres Instrument des systematischen Vorgehens in der Risikoanalyse bei Großunternehmen bilden Umfragen zum Thema Informationsschutz. Durch den Einsatz solcher Umfragen, die in einem der befragten Großunternehmen webbasiert erfolgten, konnten dort relativ schnell Wissenslücken bei Mitarbeitern und Führungskräften aufgedeckt und entsprechende Gegenmaßnahmen eingeleitet werden (Transkript 8, 7 ff.). Des Weiteren fließen auch die Erfahrungen aus laufenden Ermittlungsvorgängen in die Risikoanalysen zum Informationsschutz ein, da auch auf Basis solcher Vorfälle Defizite deutlich werden (Transkript 8, 13 ff.). Die Risikoanalysen zur Informationssicherheit in Großunternehmen sind dabei in ein gesamtes System von Risikoanalysen integriert, die in unterschiedlichen Bereichen und Ebenen erfolgen und dann zentral zusammengeführt werden (Transkript 5, 9 ff.).

Mit sinkender Unternehmensgröße nimmt auch der Umfang der Risikoanalysesysteme von Unternehmen ab, wobei zwei der befragten mittelständischen Unternehmen durchaus über angemessene Systeme zur Risikoanalyse verfügen. So finden in einem Unternehmen der IT-Branche vierteljährliche Aktualisierungen statt, die in einem Risikokatalog festgehalten werden (Transkript 1, 7 ff.). Ähnliches erfolgt bei einem mittelständischen Maschinenbauunternehmen, in dem jährliche Risikoinventuren durchgeführt werden (Transkript 6, 8 ff.). Im Gegensatz zu Großunternehmen erhalten Risiken des ungewollten Informationsabflusses in den Analysen mittelständischer Unternehmen allerdings einen geringeren Stellenwert. Dieser dargestellte Trend konnte auch durch ein kleineres mittelständisches Unternehmen bestätigt werden. Systematische Risikoanalysen sind hier nicht anzutreffen, was das Unternehmen angreifbarer als Großunternehmen macht. Ursache hierfür sind limitierte finanzielle Ressourcen (Transkript 4, 9 ff.).

Auf Basis der durchgeführten Risikoanalyse wurden die Unternehmen anschließend befragt, welche der Bereiche Personal, Organisation, Technik und Recht die höchsten Risiken in Bezug auf ungewollten Know-how-Abfluss aufweisen. Hierbei zeigt sich ein einheitliches Bild, nach dem das größte Risiko im Faktor Menschliegt (Transkript 1, 30 f.; Transkript 2, 20 ff.; Transkript 3, 71 ff.; Transkript 4, 19 ff.; Transkript 5, 18 ff.; Transkript 7, 20 ff.; Transkript 8, 28 ff.). Dabei geht das menschliche Risiko weniger von besonders kriminellen Energien der Mitarbeiter aus, sondern ist vielmehr auf ein mangelndes Risikobewusstsein und den laxen Umgang mit Sicherheitsrichtlinien zurückzuführen (Transkript 1, 31 ff.; Transkript 5, 20 ff.;

Transkript 8, 28 f.). So sperren Mitarbeiter ihr Handy nicht mit einem PIN-Code ab, verschlüsseln Festplatten oder Emails nicht oder lassen auf Zug- oder Flugreisen ihr Laptop unbeaufsichtigt liegen (Transkript 1, 34 ff.; Transkript 8, 26 f.). Dieses mangelnde Risikobewusstsein der Mitarbeiter liegt unter anderem an der nicht ausreichenden Sensibilisierung der Mitarbeiter, welche Folgen eine Entwendung der von ihnen verwendeten Daten hätte. So schildert ein Befragter, dass sich Mitarbeiter in der Entwicklungsabteilung seines Unternehmens zum Teil gar nicht über die Gefahren eines Informationsabflusses bewusst sind und dementsprechend fortlaufend sensibilisiert werden müssen, damit wichtige Informationen nicht an den Wettbewerb abfließen (Transkript 3, 53 ff.). Ein anderer Interviewpartner erwähnt, dass trotz eines vorhandenen Klassifizierungssystem für Informationen, die Mitarbeiter nicht genau wissen, wie Informationen einzuordnen sind oder den Mitarbeitern dieses System nicht einmal bekannt ist (Transkript 8, 27 ff.). Besondere Gefahren des ungewollten Know-how-Abflusses bestehen dann, wenn selbst in der Leitung des Unternehmens kein Risikobewusstsein vorherrscht (Transkript 3, 60 f.). Daher sind Schulungs- und Sensibilisierungsmaßnahmen neben der Vorbildwirkung durch die Unternehmensspitze entscheidende Faktoren für den Informationsschutz in den Unternehmen.

Neben dem mangelnden Risikobewusstsein der Belegschaft, das zum Teil auch der hohen Arbeitslast in den Unternehmen geschuldet ist, liegen die Risiken eines Informationsabflusses auch im Weggang von Mitarbeitern mit sensiblem Firmenwissen. Gerade dann, wenn Mitarbeiter bereits innerlich gekündigt haben, aber noch für das Unternehmen tätig sind, ist die Gefahr eines Know-how-Abflusses besonders hoch (Transkript 3, 73 f.; Transkript 4, 19 ff.; Transkript 8, 29 ff.). Um dieser Bedrohung adäquat begegnen zu können, werden zum Teil Know-how-Träger identifiziert, um sie durch aufwendige Programme langfristig an das Unternehmen zu binden (Transkript 5, 23 f.).

Zu den Risiken im Kontext von Industriespionage zählen die Befragten auch Berater und Unternehmenskooperationen. So erhalten Berater Einblick in sensible Unterlagen eines Unternehmens und arbeiten zeitgleich vielleicht sogar für den Wettbewerb (Transkript 5, 24 ff.). Auch Unternehmenskooperationen, wie Joint-Ventures, stellen die Unternehmen vor das Problem eines ungewollten Know-how-Abflusses (Transkript 4, 46 ff.; Transkript 5, 28 f.).

Aus Sicht der Interviewpartner bildet der Bereich Technik ebenfalls einen besonderen Risikobereich, in dem Sicherheitsmaßnahmen ständig überarbeitet und erweitert werden müssen (Transkript 3, 27 ff.; Transkript 4, 34 ff.; Transkript 6, 17 ff.). Großteils geben die Unternehmen jedoch an, dass sich ihre IT-Sicherheitstechnik auf dem neuesten Stand befindet (Trans-

kript 3, 352 ff.; Transkript 5, 318 ff.; Transkript 8, 22 f.). Organisatorische Risiken, wie zum Beispiel im Wissensmanagement, und rechtliche Risiken, wie zum Beispiel bei der Patentierung, wurden ebenfalls genannt, waren aber nicht Schwerpunkt der Ausführungen (Transkript 4, 34 ff.; Transkript 8, 35 ff.).

4.2 Risikobewertung

Um Klarheit über die wirtschaftlichen Folgen von Industriespionage zu gewinnen, ist eine Risikobewertung unabdingbar. Ähnlich wie bei der Risikoanalyse nehmen auch Umfang, Häufigkeit und Systematik der Risikobewertungen mit der Größe der Unternehmen zu. Dennoch lassen sich auch Gemeinsamkeiten zwischen mittelständischen und großen Unternehmen festhalten.

So werden die Parameter *Schadeneintrittswahrscheinlichkeit* und *Schadenshöhe* von allen befragten Unternehmen als maßgebliche Größen zur Risikobewertung angegeben (Transkript 1, 12 ff.; Transkript 2, 53 ff.; Transkript 3, 49 ff.; Transkript 4, 57 ff.; Transkript 5, 44 ff.; Transkript 6, 23 ff.; Transkript 7, 33 ff.; Transkript 8, 41 ff.). Neben diesen klassischen Parametern spielt in Großunternehmen jedoch auch die Beschaffenheit der Vermögenswerte eine Rolle. In einem der befragten Unternehmen wird zum Beispiel zwischen physischen, humanen und softwarebezogenen Assets differenziert, die Unterschiede im Kontext von Industriespionage aufweisen (Transkript 3, 51 ff.). So bilden Mitarbeiter des Vertriebs einen humanen Vermögenswert eines Unternehmens. Gerade weil diese Mitarbeiter jedoch viel mit externen Personen zu tun haben, bestehen hier erhöhte Risiken eines Informationsabflusses (Transkript 7, 33 f.).

Parallel zur Bewertung der finanziellen Risiken mithilfe der möglichen Schadenshöhe und Schadenseintrittswahrscheinlichkeit bilden imageschädigende Risiken eine weitere Komponente in der Risikobewertung. Diese schwer quantifizierbaren Risiken wurden nicht von allen befragten Unternehmen berücksichtigt, obwohl gerade Imageschäden zum Teil schwerwiegendere Auswirkungen als die eigentlich verlorenen Daten haben können. So kann zum Beispiel der Ruf eines Unternehmens durch ein bekanntgemachtes Informationsleck beschädigt werden, was indirekt die Personalrekrutierung erschweren könnte (Transkript 6, 25 ff.). Somit hat der Abfluss von Informationen nicht nur monetäre Auswirkungen für das betroffene Unternehmen, sondern auch immer Konsequenzen für dessen Potenziale (Transkript 8, 48 ff.).

Ein weiteres Element systematischer Risikobewertungen in Großunternehmen ist der Einbezug von Trends (Transkript 5, 47 ff.).

Auf die Frage, inwieweit auf Basis der Analyse und Bewertung von potenziellen Risiken des Know-how-Abflusses Prioritätenlisten für notwendige Sicherheitsmaßnahmen entwickelt wurden, zeigt sich ein überwiegend positives Bild. So liegen bei sechs der acht befragten Unternehmen Prioritätenlisten vor, die zwar unternehmensspezifisch ausgestaltet sind und in unterschiedlichen Abständen aktualisiert werden, doch grundsätzlich sind die zuvor analysierten und bewerteten Risiken eines Know-how-Abflusses nach Dringlichkeit des Handlungsbedarfs klassifiziert (Transkript 1, 23 ff.; Transkript 2, 69 ff.; Transkript 3, 85 ff.; Transkript 5, 55 ff.; Transkript 6, 34 ff.; Transkript 8, 53 ff.).

So findet in einem der befragten Unternehmen eine fünfstufige Klassifizierung der Risiken statt. Geringe Risiken der Stufen eins und zwei erfordern zwar Maßnahmen zur Reduzierung oder Eliminierung, haben jedoch nicht die höchste Priorität. Risiken der Stufen drei bis fünf müssen in eine zentrale Datenbank eingetragen werden, erfordern eine sofortige Stellungnahme der betroffenen Abteilung und werden durch eine gesonderte Risiko-Abteilung, die direkt am Vorstand angesiedelt ist, verfolgt (Transkript 3, 84 ff.). Ein weiteres Beispiel zur Klassifizierung bildet das klassische Ampelsystem. Solange Themen mit „grün“ bewertet werden, besteht kein Handlungsbedarf. Erhöhte Risiken werden mit „gelb“ markiert. In der „roten“ Phase besteht akuter Handlungsbedarf (Transkript 5, 70 ff.).

Lediglich bei einem großen und einem mittelständischen Unternehmen liegen laut Aussage der Interviewpartner keine expliziten Prioritätenlisten vor (Transkript 4, 69 ff; Transkript 7, 40 ff.). Dieses Defizit wird im Fall des mittelständischen Unternehmens mit limitierten finanziellen und personellen Ressourcen erklärt. Vorrangig werden hier die Vorteile des flexiblen Handelns betrachtet, sodass Risiken eines potenziellen Informationsabflusses weniger Berücksichtigung finden (Transkript 4, 69 f.). Im Fall des Großunternehmens besteht zumindest die Einsicht, dass in diesem Bereich Verbesserungspotenziale erzielbar sind (Transkript 7, 40 ff.).

4.3 Präventive und repressive Spionageabwehrmaßnahmen

In den folgenden vier Unterkapiteln werden die personellen, organisatorischen, technischen und rechtlichen Know-how-Schutzmaßnahmen der acht befragten Unternehmen vorgestellt. Gemäß der Forschungsfrage, welche präventiven und repressiven Spionageabwehrmaßnah-

men Unternehmen zur Verbesserung der personellen Sicherheit zur Verfügung stehen, liegt der Schwerpunkt der Ergebnisauswertung im Bereich Personal.

4.3.1 Personal

Der überwältigende Anteil der Untersuchungen und Statistiken zum Thema Industriespionage zeigt, dass das größte Risiko eines ungewollten Informationsabflusses im Faktor Mensch zu sehen ist und somit innerhalb des Unternehmens lauert (BfV, 2008a; Baeck/Weber, 2007; Corporate Trust, 2007; PWC, 2009; SiFo BW, 2010a). Auf Grundlage der Analyse und Bewertung der betriebsspezifischen Spionagerisiken sind daher besonders adäquate personelle Sicherheitsmaßnahmen zu ergreifen, um sensibles Firmen-Know-how zu schützen.

Personelle Spionageabwehrmaßnahmen beginnen mit der Personalakquisition. Folgerichtig wurden die Repräsentanten der acht Unternehmen zunächst dazu befragt, inwieweit sicherheitsrelevante Firmeninterna im Rahmen von Stellenausschreibungen veröffentlicht werden. Hierbei weisen die Aussagen darauf hin, dass die Unternehmen für diesen Teilbereich stark sensibilisiert sind. So gab keines der befragten Unternehmen an, dass in seinen Stellenausschreibungen sicherheitsrelevante Informationen enthalten sind (unter anderem Transkript 1, 48 ff.; Transkript 2, 98; Transkript 3, 118 ff.; Transkript 4, 87 ff.; Transkript 5, 82 ff.; Transkript 6, 42 ff.; Transkript 7, 51; Transkript 8, 61 ff.). Zwar werden in den Stellenausschreibungen Angaben zu den Aufgaben und später verwendeten Programmen gemacht, doch sind diese Angaben so allgemein gehalten, dass keine Rückschlüsse auf sensible Tätigkeiten des Unternehmens möglich sind (Transkript 1, 55 ff.; Transkript 8, 61 ff.). In einem Unternehmen werden darüber hinaus sogar Eintrittsdatum und Einsatzort des potenziellen Mitarbeiters verschwiegen (Transkript 2, 80 ff.). Neben den tätigkeitsbezogenen Informationen werden auch keine finanziellen Informationen veröffentlicht, die nicht auch auf der Homepage oder in den Geschäftsberichten nachlesbar sind (Transkript 7, 46 ff.). Aufgrund dieser Sicherheitsvorkehrungen kann davon ausgegangen werden, dass sich die befragten Unternehmen über die Möglichkeiten eines Informationsabflusses durch Stellenausschreibungen bewusst sind.

Den nächsten Schritt einer sicherheitsbewussten Personalrekrutierung bildet eine intensive Überprüfung der Bewerber im Rahmen des Personalauswahlverfahrens. In diesem Teilbereich zeigen die Aussagen der Interviewpartner ein differenziertes Bild auf, was unter anderem mit der unternehmensspezifischen Gefahrenlage und Unsicherheiten in der Rechtskonformität von Sicherheitsmaßnahmen in diesem Teilbereich zu erklären ist. Die Verifizierung der Bewer-

bungsunterlagen bezüglich früherer Ausbildungsstätten und Arbeitgeber ist eine der grundlegenden Sicherheitsmaßnahmen in der Personalauswahl. Eine solche Überprüfung findet fallbezogen in fast allen der befragten Unternehmen statt, zum Beispiel durch Kontrollanrufe (Transkript 2, 112; Transkript 3, 125 ff.; Transkript 8, 68 ff.). Die Berücksichtigung individueller Risikofaktoren, wie Kontakte der Bewerber zu Risikostaaten, erfolgt hingegen nur durch wenige Unternehmen der Stichprobe (Transkript 3, 123 ff.; Transkript 8, 75 ff.). Folgerichtig geben auch nur einige Unternehmen an, im Zuge des Personalauswahlverfahrens Kontakte zu polizeilichen und nachrichtendienstlichen Behörden zu haben, die über die Regelungen der Anti-Terror-Gesetzgebung hinausgehen (Transkript 1, 61 ff.; Transkript 3, 123 ff.; Transkript 8, 78 ff.). Unsicherheit besteht auch darin, inwieweit die Prüfung von sozialen Netzwerken in der Personalauswahlrechtskonform ist (Transkript 3, 105 ff.; Transkript 5, 98 ff.). Somit lässt sich trotz dieses differenzierten Lagebildes festhalten, dass zumindest teilweise intensive sicherheitsbezogene Überprüfungen der Bewerber stattfinden, wobei die Prüfung, laut Aussagen einiger Interviewpartner, auch von der hierarchischen Position und der damit verbundenen Verantwortung der Stelle abhängt (Transkript 2, 95 ff.; Transkript 8, 75 ff.). Dieser vermutete Zusammenhang wird in der folgenden Abbildung noch einmal veranschaulicht.

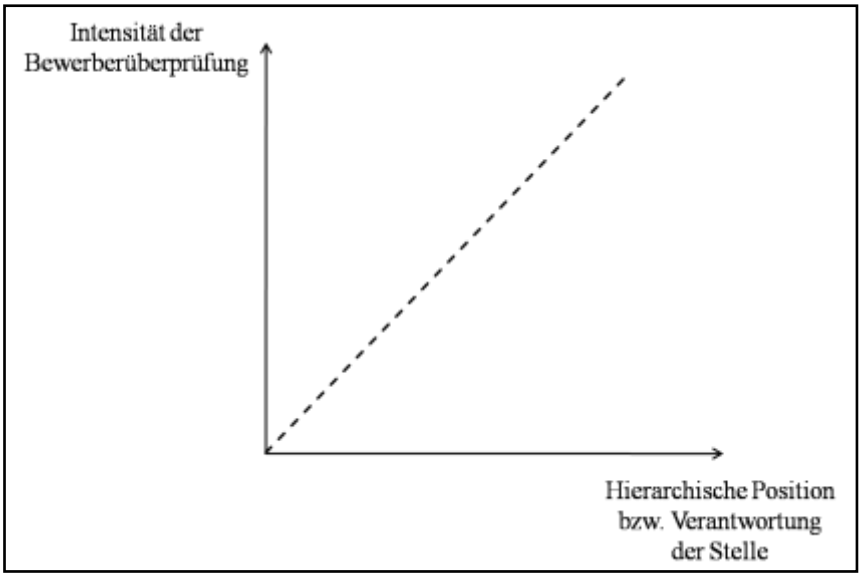

Abbildung 6: Bewerberüberprüfung in Abhängigkeit zur hierarchischen Position der Stelle
Quelle: Eigene Darstellung

Durchläuft der Bewerber das Personalauswahlverfahren mit Erfolg, kommt es zum Schritt der Personaleinstellung. Auch hier sind adäquate Know-how-Schutzmaßnahmen, wie Sicherheitsbelehrungen, Datenschutz- und Geheimhaltungsverpflichtungen oder nachvertragliche Wettbewerbsverbote, durch das spionagegefährdete Unternehmen zu ergreifen. Auf die Frage, ob es im Zuge zu Sicherheitsmaßnahmen kommt, zeigt sich ein durchweg positives Bild. So bestehen in jedem der befragten Unternehmen Datenschutz- und Geheimhaltungsvereinbarungen, die entweder in den Arbeitsvertrag integriert sind oder gesondert durch den Mitarbeiter gelesen und unterschrieben werden müssen (Transkript 1, 72 ff.; Transkript 2, 128 f.; Transkript 3, 135 ff.; Transkript 4, 116 ff.; Transkript 5, 108 ff.; Transkript 6, 54 ff.; Transkript 7, 72 ff.; Transkript 8, 84 ff.). In einigen Unternehmen sind Datenschutz- und Geheimhaltungsvereinbarungen auch durch Besucher zu unterschreiben (Transkript 6, 57). Zusätzlich zu diesen Vereinbarungen finden in vielen Unternehmen der Stichprobe auch Arbeitssicherheitsbelehrungen statt, in denen zum Beispiel der Betrieb von Servern und Software sowie das ordnungsgemäße Verhalten auf Dienstreisen geregelt ist (Transkript 3, 138 ff.). Im Bereich der Konkurrenzklauseln und nachvertraglichen Wettbewerbsverbote ergibt sich ein anderes Bild. Lediglich ein Unternehmen gab explizit an, das rechtliche Instrument eines nachvertraglichen Wettbewerbsverbots zu verwenden, um sich nach einem Ausscheiden des Mitarbeiters abzusichern (Transkript 6, 55 ff.). Dabei wird das Fehlen eines nachvertraglichen Wettbewerbsverbots zum einen durch die bereits bestehenden Datenschutz- und Geheimhaltungsvereinbarungen und zum anderen durch Unsicherheiten in der rechtlichen Umsetzung begründet (Transkript 2, 129; Transkript 3, 148 ff.). Werden solche Wettbewerbsverbote zu weit gefasst, ist der Mitarbeiter nach seiner Tätigkeit im Unternehmen zu stark in seiner Berufswahl eingeschränkt. Werden die Wettbewerbsverbote zu eng gefasst, kann der Mitarbeiter in der gleichen Funktion bei einem Konkurrenzunternehmen arbeiten (Transkript 5, 176 ff.).

Mit dem Eintritt des Bewerbers in das Unternehmen ist auch ein sicherheitsbewusstes Personalmanagement notwendig, das schwerpunktmäßig präventiven Charakter besitzen sollte. Gerade Führungskräften eines Unternehmens kommt hierbei im Know-how-Schutz eine Vorbildfunktion zu. Die Frage, ob Informationsschutz als Chefsache betrachtet wird und das Management mit gutem Beispiel voran geht, wird grundsätzlich durch die Unternehmen der Stichprobe bejaht (Transkript 1, 86 ff.; Transkript 3, 101; Transkript 5, 120 f.; Transkript 8, 97 ff.). Dieses Ergebnis lässt sich auch dadurch stützen, dass in vielen der befragten Unternehmen der Informationsschutz organisatorisch direkt an die Geschäftsleitung oder den Vorstand angebunden ist und Sicherheitsprojekte zum Teil durch den Vorstand gefördert werden

(Transkript 5, 236; Transkript 8, 97 ff.). Trotz dieses positiven Tatbestands gibt es jedoch auch individuelle Unterschiede in der Führungsebene (Transkript 6, 64 f.). So wurde in einem Fall seitens der Führungskraft einer privaten Nutzung der Firmenlaptops zugestimmt, was die spätere Auswertung der Laptops bei Abwanderung einer kompletten Vertriebsabteilung verhinderte (Transkript 2, 129 ff.).

Im Bereich der Sensibilisierung und Schulung der Mitarbeiter gegen Industriespionage zeigt sich ein deutliches Gefälle zwischen den großen und mittelständischen Unternehmen des Samples. In vier der fünf befragten Großunternehmen bestehen umfangreiche und systematisch geplante Sensibilisierungs- und Schulungsmaßnahmen, die zum Teil durch die ISO 27001 – Informationssicherheit vorgegeben sind (Transkript 3, 156 ff.; Transkript 5, 275 ff.; Transkript 7, 88 ff.; Transkript 8, 110 ff.). Hierbei werden die Mitarbeiter in jährlichen Trainings entweder persönlich in Präsenzveranstaltungen oder durch webbasierte Trainings sensibilisiert und geschult (Transkript 3, 156 ff.; Transkript 8, 110 ff.). Die Inhalte der Präsenzveranstaltungen und Trainings reichen von der ordnungsgemäßen Klassifizierung und Verschlüsselung von Daten bis hin zu den Gefahren des Social Engineering. Ein besonders erfolgreiches Instrument in der Vermittlung solcher Inhalte scheinen Comics zu sein, die die abstrakten Gefahren von Industriespionage veranschaulichen und dabei den Top-Manager aber auch die Mitarbeiter an der Basis ansprechen. So wird in einem Comic auf einfache Weise die Umsetzung einer Clean-Desk-Policy dargestellt. Informationsflyer in Gehaltsabrechnungen oder Plakate in Aufenthaltsräumen bilden weitere Möglichkeiten der Prävention (Transkript 8, 110 ff.). Auch dem Punkt der Reisesicherheit wird in den Schulungsmaßnahmen besondere Aufmerksamkeit geschenkt. Hier wird den Mitarbeitern ein sicherheitsadäquates Verhalten auf Dienstreisen vermittelt. So sollen beispielsweise sensible Telefonate nicht an öffentlichen Plätzen geführt werden oder Laptops mit einem Sichtschutzfilter ausgestattet sein (Transkript 3, 163 ff.). Je nach Position und Reiseziel des Mitarbeiters finden auch spezifische Schulungen zur Reisesicherheit in Einzelgesprächen statt (Transkript 5, 275 ff.; Transkript 8, 137 ff.). Des Weiteren werden Mitarbeiter auch über das Vorgehen von Geheimdiensten informiert. Dies beinhaltet zum Beispiel, wie Geheimdienste durch finanzielle Anreize Mitarbeiter gewinnen oder Personen durch kompromittierende Daten zur Kooperation zwingen (Transkript 3, 174 ff.; Transkript 7, 20 ff.). Bei den befragten mittelständischen Unternehmen bestehen noch erhebliche Verbesserungspotenziale in der Sensibilisierung und Schulung von Mitarbeitern zum Thema Industriespionage. Großteils bestehen hier keine regelmäßigen Trainings für Mitarbeiter (Transkript 1, 104ff.; Transkript 6, 68 ff.). Dies ist zum Teil den limitierten finan-

ziellen Ressourcen und der hohen Arbeitslast geschuldet, ist aber auch auf das noch immer nicht ausreichende Risikobewusstsein zurückzuführen (Transkript 4, 116 ff.; Transkript 6, 68 ff.). Zumindest besteht in einem Fall die Absicht, zukünftig Sensibilisierungs- und Schulungsmaßnahmen durchzuführen (Transkript 6, 68 ff.).

Anknüpfend an Fragestellungen zur Sensibilisierung und Schulung der Mitarbeiter wurden die Unternehmen gefragt, inwieweit eine Einbindung der Mitarbeiter bei der Entwicklung von Spionageabwehrmaßnahmen stattfindet. Dabei geben die Interviewpartner an, dass eine direkte Einbindung der Mitarbeiter nicht zielführend sei, da Sicherheitsmaßnahmen immer mit zusätzlichem Aufwand für das Personal verbunden seien und daher eher top-down erfolgen (Transkript 6, 79 ff.; Transkript 7, 96; Transkript 8, 145 ff.). Dennoch kann das Wissen der Mitarbeiter indirekt durch Umfragen genutzt werden, die die Basis für spätere Maßnahmen bilden (Transkript 8, 145 ff.). Die Implementierung der Maßnahmen in die betriebliche Praxis kann dann durch Schlüsselmitarbeiter vollzogen werden (Transkript 6, 79 ff.). Wie bereits mehrfach gezeigt, lässt sich auch im Punkt der Entwicklung von Spionageabwehrmaßnahmen festhalten, dass die befragten Großunternehmen systematischere Prozesse als die mittelständischen Unternehmen aufweisen (Transkript 1, 126 ff.; Transkript 3, 203 ff.).

Loyale und zufriedene Mitarbeiter tragen zur inneren und äußeren Sicherheit vor ungewollten Informationsabflüssen bei. Dementsprechend wurden die acht Unternehmen der Stichprobe auch zur Ausgestaltung ihrer Entgelt- und Anreizsysteme befragt. Bei der Betrachtung der Aussagen zeigt sich, dass alle Unternehmen die hauseigene Entlohnung als marktkonform oder marktüberdurchschnittlich ansehen (Transkript 2, 158 ff.; Transkript 3, 214 ff.; Transkript 5, 132 ff.; Transkript 7, 103 ff.). Dabei werden zusätzlich zum Gehalt in vielen Unternehmen umsatzabhängige Prämien und materielle Werte, wie Gutscheine oder hauseigene Produkte, an die Mitarbeiter ausgeschüttet (Transkript 3, 220 ff.; Transkript 4, 167 ff.). Auch über den Tarifvertrag hinausgehende Sozialleistungen liegen teilweise vor (Transkript 2, 171 ff.; Transkript 5, 137 ff.). Neben der finanziellen Komponente findet auch eine umfangreiche unentgeltliche Anerkennung beruflicher Leistungen statt. So wird besonderer beruflicher Einsatz durch Vorgesetzte gelobt und in Mitarbeiterzeitungen oder im Intranet publiziert (Transkript 2, 325 ff.; Transkript 3, 220 ff.). Somit lässt sich festhalten, dass die befragten Unternehmen Mitarbeitermotivation nicht nur unter dem Aspekt der Leistungssteigerung, sondern auch unter den Gefahren eines möglichen Know-how-Abflusses betrachten. Allerdings bestehen unternehmensspezifische Unterschiede in der Ausprägung dieses Bewusstseins.

Um die Zufriedenheit und Loyalität der Mitarbeiter nachhaltig zu verbessern und Know-how-Abfluss zu verhindern, müssen diese Parameter zunächst durch passende Instrumente gemessen werden. Dabei zeigen die Aussagen der Interviewpartner, dass lediglich in Großunternehmen systematisch Instrumente zur Messung der Mitarbeiterzufriedenheit eingesetzt werden (Transkript 2, 185 ff.; Transkript 3, 227 ff.: Transkript 5, 153 ff.; Transkript 8, 157 ff.). In diesen Unternehmen finden jährliche Umfragen zur Mitarbeiterzufriedenheit statt, die zum Teil verpflichtend sind und Auswirkungen auf die betriebliche Praxis beinhalten. Ein weiteres Instrument bilden Mitarbeitergespräche, in denen neben der Bewertung der Leistung des Mitarbeiters auch seine Identifikation mit dem Unternehmen festgestellt werden kann. Die befragten mittelständischen Firmen weisen keine solche Systematik auf. Vereinzelt werden Fluktuationsraten und Krankenstände als Indikatoren der Mitarbeiterzufriedenheit angegeben (Transkript 6, 90 ff.).

Jedes Arbeitsverhältnis ist zeitlich gesehen befristet. Daher bilden Spionageabwehrmaßnahmen bei der Beendigung eines Arbeitsverhältnisses einen unverzichtbaren Baustein im Bereich Personal. So zeigen die Ausführungen der Gesprächspartner, dass sich alle Unternehmen der Stichprobe über die Relevanz einer ordnungsgemäßen Beendigung des Arbeitsverhältnisses im Kontext von Industriespionage bewusst sind. Grundsätzlich kann hierbei festgehalten werden, dass die befragten Unternehmen beim Einsatz von Sicherheitsmaßnahmen deutlich zwischen einem regulären und einem nicht einvernehmlichen Ausscheiden differenzieren (Transkript 2, 195 ff.; Transkript 5, 187 ff.; Transkript 6, 99 ff.). Im Falle eines regulären Ausscheidens werden über die Personalabteilungen Prozesse zur Rückgabe der firmeneigenen Materialien und Unterlagen initiiert. Dabei stehen die Personalabteilungen in engem Kontakt mit den IT-Abteilungen, sodass die Deaktivierung aller Zugriffsrechte des Mitarbeiters innerhalb der EDV zum Austrittstermin erfolgt (Transkript 1, 176 ff.; Transkript 5, 187 ff.; Transkript 8, 164 ff.). Im Falle einer nicht einvernehmlichen oder anlassbezogenen Beendigung eines Arbeitsverhältnisses findet in nahezu allen Unternehmen ein rigoroses und fallbezogenes Vorgehen statt. Beispielsweise werden sofortsämtliche Zutritts- und Zugriffsrechte entzogen und die betreffenden Mitarbeiter von ihren Arbeitsplätzen entfernt (Transkript 2, 195 ff.; Transkript 5, 187 ff.). Eine intensive Beobachtung ehemaliger Mitarbeiter findet allerdings mit Verweis auf die gesetzlichen Bestimmungen in keinem der befragten Unternehmen statt (Transkript 3, 249 ff.; Transkript 5, 194; Transkript 8, 180 ff.).

Um einen effektiven Know-how-Schutz zu gewährleisten, sind die personellen Spionageabwehrmaßnahmen nicht nur auf das firmeneigene, sondern auch auf das firmenfremde Perso-

nal, wie Leiharbeiter, Geschäftspartner, Berater, Handwerker oder Sicherheits- und Reinigungspersonal, anzuwenden. Bei der Betrachtung der Interviews wird deutlich, dass in den befragten Unternehmen Fremdpersonal ähnlichen oder noch strengeren Sicherheitsauflagen unterliegt als eigenes Personal (Transkript 2, 222 ff.; Transkript 5, 197; Transkript 8, 187 ff.). Dieser Sachverhalt ist unter anderem auch früheren Informationsabflüssen durch Fremdpersonal geschuldet (Transkript 5, 199 f.). So ereignete sich in einem Unternehmen ein Vorfall, bei dem das Reinigungspersonal außerhalb der Geschäftszeiten Zugriff auf offenliegende Dokumente einer Führungskraft hatte (Transkript 3, 261 ff.). Aufgrund solcher Geschehnisse erfolgen in den meisten der befragten Unternehmen die Reinigungsarbeiten während der Geschäftszeit (Transkript 3, 261 ff.; Transkript 6, 111 ff.; Transkript 7, 133 ff.). Des Weiteren sind die Sicherheitsmaßnahmen für firmenfremdes Personal auch vom Einsatzgebiet abhängig (Transkript 5, 197). Sind beispielsweise Fremdfirmen in die Entwicklung von Prototypen involviert, erhalten diese Unternehmen besondere Geheimhaltungsvereinbarungen und werden auch Sicherheits-Audits unterzogen (Transkript 8, 187 ff.).

4.3.2 Organisation

Organisatorische Spionageabwehrmaßnahmen bilden die zweite Säule eines ganzheitlichen Informationsschutzkonzepts und sind eng mit den personellen Maßnahmen verbunden. Die enge Verbundenheit zwischen diesen beiden Bereichen wird schon dadurch deutlich, dass der Aufbau eines Systems organisatorischer Regelungen zum Informationsschutz nur durch Menschen erfolgen kann und dieses System gleichzeitig auf das sicherheitsbewusste Handeln der Mitarbeiter abzielt.

Eine zentrale Rolle spielen hierbei Sicherheitsverantwortliche oder Unternehmenssicherheitsabteilungen, die für Aufbau, Umsetzung und Kontrolle von Sicherheitsmaßnahmen zuständig sind. Grundsätzlich wird die Frage, ob es einen Sicherheitsverantwortlichen oder eine entsprechende Abteilung im Unternehmen gebe, von allen Unternehmen der Stichprobe bejaht (Transkript 2, 270 ff.; Transkript 5, 237 ff.; Transkript 6, 128 f.; Transkript 8, 235 ff.). Die genauere Betrachtung der Aufgaben der Sicherheitsverantwortlichen zeigt jedoch, dass sich nur in den befragten Großunternehmen Mitarbeiter mit dem Thema Informationsschutz hauptberuflich beschäftigen (Transkript 3, 299 ff.; Transkript 5, 234 ff.; Transkript 8, 235 ff.). Die Aufgaben solcher Informationsschutzbeauftragten sind vielfältig und beginnen bei der Erstellung von Regelwerken zur Informationssicherheit im Unternehmen. Neben der Konzep-

tion von Sicherheitsstandards sind die Informationsschutzbeauftragten auch für die Koordination dezentral durchgeführter Risikoanalysen zuständig und führen in den jeweiligen Standorten regelmäßige geplante aber auch unangekündigte Audits zur Informationssicherheit durch (Transkript 3, 302 ff.). Im Gegensatz zu den Großunternehmen besitzt der Informationsschutz in den befragten mittelständischen Unternehmen eine untergeordnete Rolle und wird nicht-durch hauptamtliche Fachkräfte ausgeübt (Transkript 6, 130 f.). Diese personelle Unterbesetzung wird zum einen mit größeren finanziellen Restriktionen begründet, ist jedoch zum anderen auch auf ein unzureichendes Risikobewusstsein zurückzuführen (Transkript 1, 261 ff.).

Neben den geschilderten Defiziten im Mittelstand lässt sich positiv festhalten, dass sowohl die Fachkräfte für Informationsschutz als auch die Sicherheitsverantwortlichen fast aller befragten Unternehmen organisatorisch an den Vorstand oder die Geschäftsführung angebunden sind (Transkript 1, 268; Transkript 3, 94 ff.; Transkript 5, 237 ff.; Transkript 6, 132; Transkript 8, 97 ff.). Dementsprechend arbeiten sie im Auftrag des Vorstands oder der Geschäftsführung, berichten an diese Organe und verfügen zum Teil über umfangreiche Weisungsbefugnisse (Transkript 1, 268; Transkript 3, 94 ff.; Transkript 8, 97 ff.).

Viele Studien zeigen, dass gerade organisatorische Regelungen einen wichtigen Beitrag zum Informationsschutz leisten und im Vergleich zu anderen Spionageabwehrmaßnahmen ein deutlich besseres Kosten-Nutzen-Verhältnis aufweisen (Schaaf, 2009). Auf die Frage, inwieweit formal fixierte Sicherheitsstandards zum Know-how-Schutz etabliert wurden, belegen die Aussagen der Interviewpartner, dass lediglich in Großunternehmen solche systematischen Regelungen vorherrschen (Transkript 3, 271 ff.; Transkript 5, 204; Transkript 8, 201 ff.). Ein Beispiel für einen formal fixierten Sicherheitsstandard bildet hierbei eine Clean-Desk-Policy, die beinhaltet, dass sensible Unterlagen nur während der Arbeitszeit beaufsichtigt auf dem Schreibtisch liegen dürfen und außerhalb der Anwesenheit des Mitarbeiters sicher aufbewahrt werden müssen. So geben, mit Ausnahme eines mittelständischen Unternehmens, nur Großunternehmen an, eine Clean-Desk-Policy zu verfolgen (Transkript 1, 237 ff.; Transkript 5, 257 ff.; Transkript 8, 201 ff.). Für einige der Unternehmen, die nach der ISO 27001 – Informationssicherheit zertifiziert sind, ist die Existenz und regelmäßige Überprüfung einer Clean-Desk-Policy sogar Pflicht (Transkript 3, 271 ff.).

Einen weiteren organisatorischen Aspekt im Informationsschutz bilden Bestimmungen zum Umgang mit sensiblen Informationen. Hierfür ist ein eindeutiges Klassifizierungssystem der im Unternehmen befindlichen Informationen eine notwendige Voraussetzung, da nur so eine sicherheitsadäquate Nutzung, Vervielfältigung und Vernichtung der Informationen durch die

Mitarbeiter erfolgen kann. Befragt nach der Existenz eines solchen Informationsklassifizierungssystems zeigt sich, dass bis auf eine mittelständische Firma nur Großunternehmen über derartige Systeme verfügen (Transkript 3, 282 ff.; Transkript 6, 123 f.; Transkript 8, 210 ff.). Bei näherer Betrachtung der Informationsklassifizierungssysteme ist zu erkennen, dass entweder drei oder vier Vertraulichkeitsstufen bestehen (Transkript 3, 282 ff.; Transkript 5, 227 ff.). Je nach Auswirkungen eines möglichen Informationsabflusses sind die Informationen durch seinen Ersteller zu klassifizieren (Transkript 8, 210 ff.). Hierzu gibt es jedoch Hilfestellungen seitens der Informationsschutzbeauftragten. Umfangreichere Abstufungen in der Vertraulichkeit von Informationen bieten sich aus Sicht eines Interviewpartners nicht an, da mit jeder weiteren Klassifizierungsstufe das Verfahren komplexer wird und letztendlich durch die Mitarbeiter in der Praxis nicht mehr ordnungsgemäß umgesetzt werden kann (Transkript 8, 210 ff.). Ein weiteres Problem besteht darin, da mit steigender Vertraulichkeitsstufe auch der Aufwand im Umgang mit der Information zunimmt. Hier ist das Personal fortlaufend zu sensibilisieren, damit sensible Informationen nicht tiefer klassifiziert werden als es den Inhalten entspricht, damit einfach mit ihnen umgegangen werden kann (Transkript 8, 210 ff.).

Die ordnungsgemäße Klassifizierung von Informationen bei ihrer Erstellung regelt auch die weitere Nutzung. So dürfen in den entsprechenden Unternehmen *vertrauliche* oder *streng vertrauliche* Informationen nicht auf einfache Laufwerke gestellt werden, sondern müssen auf einem verschlüsselten Speicher abgelegt und folgerichtig verschlüsselt verschickt werden (Transkript 3, 282 ff.). Auch die physische Aufbewahrung solcher Informationen, wie Vorstandsprotokolle, erfolgt in besonders gesicherten Räumen (Transkript 8, 225 ff.).

Je nach Klassifizierung der Informationen gelten auch spezielle Regelungen zur Vernichtung. So sind Informationen ab einem bestimmten Vertraulichkeitsgrad mit besonderen Shreddern zu vernichten oder in Datenschutzcontainer zu werfen, die von zertifizierten Entsorgern abgeholt werden (Transkript 3, 292 ff.; Transkript 5, 227 ff.). Trotz der Defizite in der Klassifizierung von Informationen bestehen in den befragten mittelständischen Unternehmen zumindest ausreichende Möglichkeiten zur Vernichtung von Informationsbeständen, allerdings existieren auch hier keine konkreten Verfahrensanweisungen (Transkript 1, 253 ff.; Transkript 4, 250 ff.).

Einen weiteren Baustein im Bereich organisatorischer Know-how-Schutzmaßnahmen bilden Zutritts- und Zugriffsberechtigungskonzepte. Sie stellen sicher, dass nur befugte Personen den Zugang oder Zugriff auf sensible Daten erhalten (Schaaf, 2009). Befragt nach der Existenz von Zutritts- und Zugriffsberechtigungskonzepten, zeigen die Aussagen der Interviewpartner

ein durchaus positives Bild. So liegen in allen der befragten Unternehmen derartige spezifische Konzepte vor, die den Zugang in sensible Bereiche oder den Zugriff auf vertrauliche Daten regeln (Transkript 1, 307 ff.; Transkript 2, 289 ff.; Transkript 5, 294 ff.; Transkript 6, 135 ff.; Transkript 8, 249 ff.). Das reine Vorhandensein dieser Berechtigungskonzepte bietet jedoch keinen ausreichenden Schutz vor Informationsabflüssen. Aufgrund des ständigen Ein- und Austritts von Mitarbeitern sowie unternehmensinternen Umstrukturierungen sind die Berechtigungskonzepte regelmäßig durch enge Zusammenarbeit zwischen Personal- und IT-Abteilung zu prüfen und anzupassen (Transkript 3, 320 ff.).

Dieser angesprochene Prüfungsgedanke ist für einen funktionierenden Informationsschutz unverzichtbar, da oft zwischen der Konzeption und der Umsetzung von Sicherheitsmaßnahmen gravierende Defizite bestehen. Kontrollen zur ordnungsgemäßen Umsetzung der Sicherheitsmaßnahmen sind daher zwingend notwendig. Dabei veranschaulichen die Ausführungen der Gesprächspartner, dass bis auf eine mittelständische Firma nur Großunternehmen über regelmäßige und systematische Kontrollen im Bereich des Informationsschutzes verfügen (Transkript 3, 40 ff.; Transkript 6, 144 ff.; Transkript 8, 258 ff.). Diese Kontrollen in den befragten Großunternehmen werden entweder durch externe Sicherheitsdienstleister oder selbst durch die entsprechenden Stellen durchgeführt. In den angekündigten, aber auch ohne Anmeldung stattfindenden Kontrollen, werden beispielsweise die Clean-Desk-Policy oder Passwortpolitik der Mitarbeiter überprüft. Je nach Einhaltung der Sicherheitsmaßnahmen erhalten die Mitarbeiter ein entsprechendes Feedback (Transkript 3, 271 ff.; Transkript 5, 256 ff.). Neben den firmeninternen Kontrollen finden auch Audits bei Partnerfirmen statt. Hier wird geprüft, ob die geforderten Maßnahmen auch umgesetzt werden, wobei der Umfang solcher Audits mit zunehmender Vertraulichkeit der ausgetauschten Informationen steigt (Transkript 3, 366 ff.; Transkript 8, 258 ff.). Bei einem Großteil der befragten mittelständischen Unternehmen findet keine systematische Überprüfung zur Umsetzung von Know-how-Schutzmaßnahmen statt (Transkript 1, 243 ff.). Vielmehr basieren die Kontrollen auf Erfahrungen (Transkript 4, 282 ff.).

Auf Basis der angesprochenen Kontrollen können Sicherheitsverstöße oder sicherheitsbewusstes Handeln der Mitarbeiter beobachtet werden. Auf die Frage, inwieweit Sanktionierungen beziehungsweise Belohnungen erfolgen, zeigen die Aussagen der Interviewpartner, dass in den untersuchten Großunternehmen entsprechende Systeme vorhanden sind. Bei sicherheitsbewusstem Handeln einzelner Mitarbeiter besteht zum Beispiel die Möglichkeit einer Gehaltserhöhung. Auch positives Feedback oder öffentliches Lob in Form eines Artikels in

der Mitarbeiterzeitung werden ausgesprochen (Transkript 2, 337 ff.; Transkript 8, 283 ff.). In Bezug auf die Sanktionierung kann festgehalten werden, dass je nach Härte des Verstoßes vorgegangen wird. Sanktionen reichen von konstruktiver Kritik bis hin zu arbeitsrechtlichen Konsequenzen (Transkript 1, 272 ff.; Transkript 5, 266 ff.).

Die aufgezeigten organisatorischen Regelungen werden in der Praxis nur dann von den Mitarbeitern umgesetzt, wenn die Führungskräfte entsprechende Rahmenbedingungen schaffen. Dies bedeutet konkret, dass Regelungen durch Führungskräfte kommuniziert und vorgelebt werden müssen (Transkript 8, 201 ff.).

4.3.3 Technik

Wie bereits dargelegt, sind die Angriffsmöglichkeiten im Rahmen von Industriespionage vielfältig. Demensprechend sind neben personellen und organisatorischen auch technische Spionageabwehrmaßnahmen für einen umfassenden Informationsschutz notwendig. Einen wichtigen Baustein bilden hierbei bautechnische Maßnahmen, die zur Absicherung von sensiblen Bereichen und Daten gegenüber Betriebsfremden und unbefugten Mitarbeitern dienen.

Nach den Aussagen der Interviewpartner zeigt sich, dass alle befragten Unternehmen über die gängigen bautechnischen Maßnahmen zum Schutz von Informationen verfügen. Hierzu gehört zunächst die äußere Umfriedung der Standortliegenschaften durch Zäune, Mauern oder ähnliche Vorrichtungen. Dabei orientiert sich die äußere Umfriedung an der Gefährdungslage des jeweiligen Standorts und ist zusätzlich durch die geografische Lage und die Unternehmenshistorie determiniert (Transkript 2, 351 ff.; Transkript 5, 293 ff.). Die zwischen der Umfriedung und den Gebäuden liegenden Bereiche sind je nach Sensibilität videoüberwacht (Transkript 7, 199 f.; Transkript 8, 291 ff.). Die Videoüberwachung findet diesbezüglich im Rahmen der gesetzlichen Bestimmungen statt (Transkript 8, 291 ff.). Ein weiteres ergänzendes bautechnisches Instrument zum Schutz der Außenhaut eines Unternehmens bilden Einbruchmeldeanlagen, die bei Alarmauslösung Werkschutz und Polizei benachrichtigen (Transkript 1, 300 ff.; Transkript 5, 293 ff.). Zutrittskontrollsysteme sind ebenfalls in allen befragten Unternehmen vorhanden. Der Umfang dieser Systeme ist wiederum gefahrenabhängig. So sind zum Beispiel die Forschungs- und Entwicklungsabteilung sowie Rechenzentren besonders sensible Bereiche, die es mittels erhöhter Sicherheitseinrichtungen, beispielsweise biometrischen Zutrittskontrollsystemen, zu schützen gilt (Transkript 1,300 ff.; Transkript 8, 291 ff.). Ebenfalls sind Schlüssel- und Kartensysteme Bestandteile der Zutrittskontrollen (Trans-

kript 3, 263). Zusätzlich zu den genannten Rechenzentren liegen in den Unternehmen auch weitere gefährdete Datenträger und Objekte vor, die durch entsprechende Räumlichkeiten gesichert werden (Transkript 5, 300; Transkript 7, 202). Hierzu gehören beispielsweise die bereits erwähnten Vorstandsprotokolle und Prototypen (Transkript 8, 225 ff.).

Im Gegensatz zu den genannten bautechnischen Maßnahmen werden Abhörschutz- und Sichtschutzmaßnahmen nur durch Großunternehmen durchgeführt (Transkript 3, 347 ff.; Transkript 5, 303 ff.; Transkript 8, 302). So befinden sich in diesen Unternehmen abhörschutzsichere Räume auf der Ebene des Vorstands. Beispielsweise werden die Glasscheiben solcher Räume durch Vibratoren in Schwingung gesetzt, um Abhörversuche von außen zu verhindern (Transkript 3, 347 ff.). Abhörschutzsichere Räume auf Vorstandsebene sind alleine jedoch nicht zielführend. Des Weiteren erfolgen auch temporäre und mobile Abhörschutzmaßnahmen bei wichtigen Zusammenkünften von Führungskräften, in denen beispielsweise keine Funkmikrofone benutzt werden dürfen (Transkript 5, 305 ff.). Allerdings sind die Informationsabflussmöglichkeiten in einem Unternehmen sehr vielfältig, sodass Abhörschutz nur ein Element eines umfassenden Sicherheitskonzepts sein kann. Zudem bieten bautechnische Maßnahmen keinen ausreichenden Schutz, wenn die dahinter stehenden organisatorischen Prozesse nicht aufeinander abgestimmt sind.

Neben diesen physischen Schutzmaßnahmen bilden die Maßnahmen zur Sicherung der Informations- und Kommunikationstechnik ein weiteres Element eines ganzheitlichen Informationsschutzes. Nachgefragt welche Maßnahmen hierbei gegenüber Innen- und Außentätern eingesetzt werden, zeigt sich ein differenziertes Bild. So werden in allen Unternehmen Nutzer-Accounts und Passwörter verwendet (Transkript 1, 325; Transkript 3, 353 ff.; Transkript 4, 306 ff.; Transkript 8, 303 ff.). Allerdings findet lediglich in fünf der acht befragten Unternehmen ein systematischer Passwortwechsel statt (Transkript 1, 325 ff.; Transkript 3, 353 ff.; Transkript 4, 309 ff.; Transkript 6, 166 ff.; Transkript 7, Transkript 8, 166 ff.). Die Regelungen zum Passwortwechsel sind dabei unternehmensspezifisch ausgestaltet. In einem Großunternehmen wird beispielsweise alle 90 Tage das Passwort verpflichtend gewechselt, wobei das Passwort mindestens neun Stellen, unter Zusatz von Ziffern und Sonderzeichen, aufweisen muss (Transkript 3, 353 ff.). In einem anderen mittelständischen Unternehmen dürfen bereits benutzte Passwörter innerhalb eines bestimmten Zeitraums nicht wieder verwendet werden (Transkript 1, 325 ff.). Bei zwei Unternehmen ohne systematischen Passwortwechsel bestehen zumindest Anstrengungen zur Einführung einer solchen Regelung, jedoch gibt es auch

Widerstände aus den Reihen der Belegschaft (Transkript 2, 403 f.; Transkript 4, 309 ff.; Transkript 7, 208 ff.).

In Bezug auf mögliche Angriffe aus dem Internet geben alle Unternehmen der Stichprobe an, über Firewallsysteme und aktuelle Schutzprogramme, wie Anti-Virus oder Anti-Spam, zu verfügen (Transkript 1, 313 ff.; Transkript 2, 429 ff.; Transkript 3, 355 f.; Transkript 4, 318 ff.; Transkript 5, 318 ff.; Transkript 6, 166 ff.; Transkript 7, 217; Transkript 8, 306 ff.). Aufgrund des technischen Fortschritts und dem damit einhergehenden Aufkommen neuer Angriffsmöglichkeiten, sind laufende Anpassungen solcher Maßnahmen unerlässlich (Transkript 5, 317 ff.). Zur Kontrolle der IT-Sicherheit wurden in mehreren Unternehmen auch Penetrationstests durch interne Stellen oder externe Dienstleister gefahren (Transkript 1, 313 ff.; Transkript 6, 170).

Klare Defizite in der Sicherung der Informations- und Kommunikationstechnik sind im Bereich der Verschlüsselung von sensiblen Informationen zu sehen. Gerade die mittelständischen Unternehmen des Samples besitzen, bis auf Ausnahmen, keine Regelungen zur Verschlüsselung von Datenträgern und des Datenverkehrs. Oft fehlt es hier an dem nötigen Bewusstsein für die Gefahren eines ungewollten Know-how-Abflusses (Transkript 4, 301 ff.). Dennoch sind auch in Unternehmen mit Regelungen zur Verschlüsselung von sensiblen Informationen Defizite erkennbar. Diese liegen insbesondere in der konsequenten Umsetzung der Regelungen durch die Mitarbeiter (Transkript 5, 327 f.; Transkript 8, 330 ff.).

Weitere Gefahren für die Informations- und Kommunikationstechnik gehen von infizierten Emails und fremden USB-Sticks aus. So berichten einige Unternehmen über Vorfälle, in denen durch infizierte Email-Anhänge Informationen abgeflossen sind (Transkript 5, 322; Transkript 8, 312 ff.). Die meisten Email-Angriffe werden allerdings durch die Firewall abgefangen, sodass fremde USB-Sticks größere Risiken aufweisen (Transkript 5, 322 ff.). Beispielsweise wurde einem Mitarbeiter im Rahmen eines Verkaufsgesprächs auf einer Messe ein infizierter USB-Stick eines Interessenten überreicht. Der USB-Stick sollte angebliche Informationen zum Käufer beinhalten. Weil das Angebot aus dem asiatischen Raum kam und der Mitarbeiter des Unternehmens sensibilisiert war, schaltete er die Einheit des Informationsschutzes ein, die den USB-Stick untersuchte und tatsächlich ein Angriffsprogramm entdeckte (Transkript 8, 312 ff.). Neben solchen enttarnten Angriffen ist jedoch davon auszugehen, dass eine Vielzahl der Attacken im Dunkeln bleibt (Transkript 3, 359 ff.).

4.3.4 Recht

Rechtliche Spionageabwehrmaßnahmen bilden die vierte Säule eines ganzheitlichen Informationsschutzkonzepts und tragen unterstützend zur Wahrung des firmeneigenen Know-how bei. Geheimhaltungsvereinbarungen stellen hierbei ein wichtiges Instrument dar und bestehen zwischen allen befragten Unternehmen und ihren Mitarbeitern. Ein derart positives Bild zeigt sich auch bei den Geheimhaltungsvereinbarungen mit Geschäftspartnern, wie Lieferanten oder Beratern. So geben nahezu alle Unternehmen an, Geheimhaltungsvereinbarungen mit Partnerunternehmen abgeschlossen zu haben (Transkript 2, 417; Transkript 3, 436 ff.; Transkript 5, 347; Transkript 6, 174; Transkript 7, 237 ff.; Transkript 8, 340 ff.). Neben dem formalen Abschluss ist auch eine regelmäßige Überprüfung zur Einhaltung solcher Vereinbarungen notwendig. Diesbezüglich zeigen sich erhebliche Verbesserungspotenziale bei den befragten Unternehmen. Lediglich zwei Unternehmen geben an, überexplizite Lieferanten-Audits zu verfügen, in denen eine Kontrolle der geforderten Sicherheitsmaßnahmen erfolgt (Transkript 3, 368 ff.; Transkript 8, 258 ff.). Geheimhaltungsvereinbarungen mit der Konkurrenz bestehen nicht (Transkript 2, 417 f.; Transkript 3, 366 ff.).

Im Falle eines Verstoßes gegen geschlossene Geheimhaltungsvereinbarungen werden durch nahezu alle befragten Unternehmen rechtliche Konsequenzen, meist in Form von Schadenersatzansprüchen, eingeleitet (Transkript 1, 363 ff.; Transkript 2, 425; Transkript 3, 375 ff.; Transkript 5, 333; Transkript 6, 175 ff.; Transkript 8, 340 ff.). Die gerichtlichen Verfahren in solchen Fällen sind sehr langwierig, können aber zu empfindlichen finanziellen Regresszahlungen des Täters führen (Transkript 2, 427 f.; Transkript 5, 339 f.). Allerdings ist der Nachweis eines Verstoßes oft sehr schwierig (Transkript 6, 175 ff.). Des Weiteren gibt eines der befragten Unternehmen an, dass es bei Verstößen gegen Geheimhaltungsvereinbarungen durchaus auch zu außergerichtlichen Einigungen kommt, da weder der Täter noch der Geschädigte in der Öffentlichkeit negativ in Erscheinung treten wollen. Zu groß ist auf beiden Seiten die Angst vor nachhaltigen Imageschäden (Transkript 3, 376 ff.). Neben den direkten finanziellen Schäden erleiden verurteilte Unternehmen oder Personen jedoch auch Folgeschäden, da die Akquirierung von neuen Aufträgen beziehungsweise die Suche nach einem neuen Job immens erschwert wird (Transkript 8, 343 ff.).

Ungewollter Know-how-Abfluss kann sich auch bei Zertifizierungsgesellschaften ereignen, die tiefe Einblicke in die firmeninternen Strukturen und Prozesse erhalten. So tauchten in einem der befragten Unternehmen Informationen auf, die nur im Rahmen einer Zertifizierung abgeflossen sein konnten. Als Folge wurden die Zusammenarbeit mit Fremdsachverständigen

aufgehoben und Hausverbote erteilt (Transkript 2, 439 ff.). Auch in einem anderen Unternehmen gibt es immer wieder Vorfälle mit Zertifizierungsgesellschaften (Transkript 5, 348 f.). Umso wichtiger ist es daher, auch mit Zertifizierungsgesellschaften Geheimhaltungsvereinbarungen abzuschließen, damit im Falle eines Informationsabflusses zumindest Schadensersatzansprüche geltend gemacht werden können. Laut Aussagen der Interviewpartner geschieht dies, bis auf eine Ausnahme, auch in allen Unternehmen (Transkript 1, 364 ff.).

Der Bereich der Patentierung bildet ebenfalls vielfältige Möglichkeiten für einen ungewollten Know-how-Abfluss. Zum einen werden Konkurrenten durch die öffentlich einsehbaren Patente auf die Tätigkeiten eines Unternehmens aufmerksam. Zum anderen sind auch Informationsabflüsse bei beteiligten Mitarbeitern oder bei Patentämtern denkbar (Transkript 3, 399 f.; Transkript 8, 353 ff.). Diejenigen Unternehmen der Stichprobe, die Patente zur rechtlichen Absicherung von explizitem Know-how einsetzen, sind sich durchaus der Gefahren der Patentierung bewusst, allerdings sehen sie aufgrund des internationalen Wettbewerbs keine andere Möglichkeit zum Schutz ihrer technischen Erfindungen (Transkript 3, 394 ff.; Transkript 7, 258 ff.). Eines der befragten Unternehmen fährt hierbei eine interessante Strategie (Transkript 4, 350 ff.). So werden Patente nicht zum Schutz der technischen Erfindungen, sondern zur gezielten Desinformation des Wettbewerbs eingesetzt. Das Vorgehen dieses kleineren mittelständischen Unternehmens beruht dabei auf einem negativen Vorfall aus der Vergangenheit, in dem trotz einer Patentanmeldung Produktfälschungen entstanden. Aufgrund der limitierten finanziellen Ressourcen war eine kosten- und zeitintensive Durchsetzung des Patentrechts jedoch nicht möglich.

Die folgende Tabelle 4 veranschaulicht noch einmal die wesentlichen Spionageabwehrmaßnahmen in den befragten Unternehmen. Aufgrund des mehrfach aufgezeigten Gefälles zwischen mittelständischen und großen Unternehmen, findet eine Differenzierung nach Unternehmensgröße statt.

		Unternehmensgröße	
		Großunternehmen	*Mittelständische Unternehmen*
Bereiche	Risikoanalyse	▪ Umfassende, regelmäßige und zum Teil verpflichtende Risikoanalysen: zum Beispiel durch abteilungsinterne Bewertungen, Umfragen und laufende Ermittlungsvorgänge	▪ Weniger strukturierte Risikoanalysesysteme
	Risikobewertung	▪ Systematische Risikobewertung unter Berücksichtigung diverser Parameter : zum Beispiel durch Schadeneintrittswahrscheinlichkeit, Schadenshöhe und Image	▪ Weniger umfangreiche Risikobewertungssysteme
	Personal	▪ Keine Veröffentlichung sensibler Informationen in Stellenausschreibungen ▪ Fallbezogene Überprüfung des Bewerbers im Personalauswahlverfahren ▪ Sicherheitsbelehrungen sowie Datenschutz- und Geheimhaltungsvereinbarungen im Zuge der Personaleinstellung ▪ Umfangreiche und systematisch geplante Sensibilisierungs- und Schulungsmaßnahmen ▪ Systematische Einbindung von Mitarbeitern bei der Entwicklung von Know-how-Schutzmaßnahmen ▪ Mitarbeitermotivation durch materielle und immaterielle Anreize ▪ Systematischer Einsatz von Instrumenten zur Messung der Mitarbeiterzufriedenheit ▪ Fallbezogene Schutzmaßnahmen bei der Beendigung eines Arbeitsverhältnisses ▪ Einsatzgebietsabhängige Sicherheitsmaßnahmen für Fremdpersonal	▪ Keine Veröffentlichung sensibler Informationen in Stellenausschreibungen ▪ Fallbezogene Überprüfung des Bewerbers im Personalauswahlverfahren ▪ Sicherheitsbelehrungen sowie Datenschutz- und Geheimhaltungsvereinbarungen im Zuge der Personaleinstellung ▪ Keine regelmäßigen Sensibilisierungs- und Schulungsmaßnahmen ▪ Weniger systematische Einbindung von Mitarbeitern bei der Entwicklung von Know-how-Schutzmaßnahmen ▪ Mitarbeitermotivation durch materielle und immaterielle Anreize ▪ Vereinzelter Einsatz von Instrumenten zur Messung der Mitarbeiterzufriedenheit ▪ Fallbezogene Schutzmaßnahmen bei der Beendigung eines Arbeitsverhältnisses ▪ Einsatzgebietsabhängige Sicherheitsmaßnahmen für Fremdpersonal

	Organisation	▪ Explizite Fachkräfte für den Bereich des Informationsschutzes ▪ Systematische organisatorische Regelungen zum Informationsschutz: zum Beispiel durch Clean-Desk-Policy, Informationsklassifizierung sowie Zutritts- und Zugriffsberechtigungskonzepte ▪ Regelmäßige Kontrollen zur Überprüfung der Know-how-Schutzmaßnahmen	▪ Keine expliziten Fachkräfte für den Bereich des Informationsschutzes ▪ Weniger umfangreiche organisatorische Regelungen zum Informationsschutz ▪ Vereinzelte Kontrollen zur Überprüfung der Know-how-Schutzmaßnahmen
	Technik	▪ Bautechnische Maßnahmen abhängig von Gefahrenpotenzial, geografischer Lage und Unternehmenshistorie, Abhör- und Sichtschutzmaßnahmen als Add-on ▪ Weitgehende Sicherung der Informations- und Kommunikationstechnik: zum Beispiel durch Passwörter, Schutzprogramme und Verschlüsselung	▪ Bautechnische Maßnahmen abhängig von Gefahrenpotenzial, geografischer Lage und Unternehmenshistorie ▪ Weitgehende Sicherung der Informations- und Kommunikationstechnik: zum Beispiel durch Passwörter, Schutzprogramme, Defizite in der Verschlüsselung
	Recht	▪ Geheimhaltungsvereinbarungen mit den eigenen Mitarbeitern und Geschäftspartnern ▪ Schadenersatzansprüche bei Verstoß gegen Geheimhaltungsvereinbarungen	▪ Geheimhaltungsvereinbarungen mit den eigenen Mitarbeitern und Geschäftspartnern ▪ Schadenersatzansprüche bei Verstoß gegen Geheimhaltungsvereinbarungen

Tabelle 4: Spionageabwehrmaßnahmen der befragten Unternehmen
Quelle: Eigene Darstellung

Die Tabelle 4 zeigt ein bestehendes Gefälle zwischen Großunternehmen und mittelständischen Unternehmen im Bereich des Informationsschutzes. Bereits im Rahmen der Analyse von Spionagerisiken weisen die Großunternehmen weitaus umfassendere Systeme als die mittelständischen Unternehmen auf. In Bezug auf die Bewertung der analysierten Spionagerisiken zeigt sich ein ähnliches Bild. Auch hier finden durch Großunternehmen umfangreichere Risikobewertungen statt, indem zusätzlich zur *Schadenseintrittswahrscheinlichkeit* und *Schadenshöhe* auch weitere Parameter wie *Image* und *Trends* berücksichtigt werden.

Im Bereich personeller Spionageabwehrmaßnahmen bestehen durchaus Gemeinsamkeiten zwischen Großunternehmen und mittelständischen Betrieben. So werden beispielsweise fallbezogene Überprüfungen des Bewerbers im Personalauswahlverfahren und spezifische Schutzmaßnahmen bei der Beendigung eines Arbeitsverhältnisses durchgeführt. Neben diesen

Parallelen zeigen sich jedoch auch Unterschiede. Besonders im Bereich der Sensibilisierung und Schulung von Mitarbeitern gegenüber diversen Spionagerisiken weisen die befragten mittelständischen Unternehmen erhebliche Defizite auf. Ebenfalls findet in den mittelständischen Unternehmen, trotz der hohen Relevanz des Risikofaktors Mensch, keine ausreichende Messung der Mitarbeiterzufriedenheit statt. Ferner sind auch in Bezug auf organisatorische Spionageabwehrmaßnahmen Unterschiede zwischen Großunternehmen und mittelständischen Unternehmen erkennbar. So ist die systematische Umsetzung organisatorischer Regelungen, wie einer Clean-Desk-Policy oder einer Informationsklassifizierung, in den Großunternehmen ausgeprägter. Gleiches gilt auch für die Kontrolle der praktizierten Maßnahmen. Nicht zuletzt weisen nur Großunternehmen explizite Fachkräfte für den Informationsschutz auf. Im Bereich bautechnischer Spionageabwehrmaßnahmen und der Sicherung der Informations- und Kommunikationstechnik zeigen sowohl die Großunternehmen als auch die mittelständischen Unternehmen gute Ergebnisse. Allerdings besitzen die mittelständischen Unternehmen Defizite bei der Datenverschlüsselung sowie bei Abhör- und Sichtschutzmaßnahmen. In Bezug auf rechtliche Spionageabwehrmaßnahmen bestehen sowohl bei den Großunternehmen als auch bei den mittelständischen Unternehmen Geheimhaltungsvereinbarungen mit den eigenen Mitarbeitern und Geschäftspartnern. Eine strafrechtliche Verfolgung bei Verstößen gegen diese Geheimhaltungsvereinbarungen kann jedoch schwierig sein.

5 Diskussion

In den vorherigen Kapiteln wurden auf Basis theoretischer Grundlagen das methodische Vorgehen und die Ergebnisse der Untersuchung dargestellt. Abschließend erfolgt eine Integration der Untersuchungsergebnisse in die bestehende Literatur. Des Weiteren werden methodische Grenzen und die Umsetzbarkeit möglicher Schutzmaßnahmen diskutiert sowie Ausblicke auf zukünftige Spionagegefahren gegeben.

5.1 Integration der Ergebnisse

Die Auswertung der Interviews in Kapitel 4 hat gezeigt, dass gerade bei den befragten mittelständischen Unternehmen zum Teil erhebliche Defizite im Informationsschutz bestehen. In Bezug auf die vorgeschalteten Maßnahmen der Analyse und Bewertung von Risiken, liegen deutliche Verbesserungspotenziale in der Ausgestaltung solcher Systeme vor. So ist es auch für mittelständische Unternehmen möglich, wenn auch nicht in gleichem Umfang, mithilfe von Umfragen und Hinweisgebersystemen die Risiken potenzieller Know-how-Abflüsse im Unternehmen zu identifizieren (Schaaf, 2009). Auf Basis dieser Vorgänge können dann die identifizierten Risiken anhand eines zu erstellenden Katalogs bewertet werden. Neben den klassischen Größenwie *Schadenseintrittswahrscheinlichkeit* und mögliche *Schadenshöhe* sind hier ebenfalls Auswirkungen auf das *Image* und die *Potenziale* des Unternehmens sinnvolle Parameter. Zusätzlich zur Analyse und Bewertung von Risiken sind, nach Meinung von Experten, auch mögliche Indizien, wie schwindende Marktanteile oder das Aufkommen gleichartiger Produkte durch den Wettbewerb, in ein Frühwarnsystem zu integrieren (LfV BW, 1999). Damit jedoch ein nachhaltiger Beitrag zum Know-how-Schutz im Unternehmen entsteht, sind diese Systeme kontinuierlich an die dynamischen Rahmenbedingungen anzupassen (Corporate Trust, 2007).

Das größte Risiko eines ungewollten Know-how-Abflusses liegt nach Aussage der befragten Unternehmen im Faktor Mensch (Transkript 1, 30 f.; Transkript 2, 20 ff.; Transkript 3, 71 ff.; Transkript 4, 19 ff.; Transkript 5, 18 ff.; Transkript 7, 20 ff.; Transkript 8, 28 ff.). Dabei ist der Know-how-Abfluss weniger auf die kriminellen Energien der Mitarbeiter, sondern vielmehr auf das mangelnde Risikobewusstsein und den laxen Umgang mit Sicherheitsrichtlinien zurückzuführen (Transkript 1, 31 ff.; Transkript 5, 20 ff.; Transkript 8, 28 f.). Trotz dieses Sachverhalts finden besonders in den mittelständischen Unternehmen keine regelmäßigen Sensibilisierungs- und Schulungsmaßnahmen für Mitarbeiter statt (Transkript 1, 104 ff.). Ein

häufig in der Literatur genannter Lösungsansatz ist eine anfängliche Grundsensibilisierung, in der Mitarbeiter mit Eintritt in das Unternehmen über die allgemeinen Risiken von Industriespionage, wie zum Beispiel Social Engineering, aufgeklärt werden. Im weiteren Verlauf der Betriebszugehörigkeit sind dann zielgruppenorientierte Auffrischungs- und Ergänzungsmaßnahmen erforderlich (Warnecke, 2010). Ein Beispiel wäre ein im Vorfeld einer Geschäftsreise stattfindendes landesspezifisches Briefing. Die Schulung und Sensibilisierung ist jedoch nicht nur auf das eigene Personal begrenzt. Oft bieten sich solche Maßnahmen auch für Geschäftspartner an, die eng in sensible Prozesse des eigenen Unternehmens involviert sind (SiFo, 2010b). Noch vor dem sicherheitsbewussten Personalmanagement bildet die sorgfältige Auswahl von eigenen Mitarbeitern und Fremdpersonal eine weitere personelle Know-how-Schutzmaßnahme (Meissinger 2005; Warnecke, 2010). So sind bei Fremdpersonal stets Background-Checks zu den jeweiligen Unternehmen und ihren Mitarbeitern eigenständig oder durch verstärkte Zusammenarbeit mit Sicherheitsbehörden durchzuführen (Meissinger, 2005). Gerade bei längerfristigen Fremdmitarbeitern, wie dem Reinigungspersonal, sind auch Integrationsmaßnahmen in die firmeneigene Sicherheitskultur ein sinnvoller Schritt (Warnecke, 2010).

Ein weiteres Defizit besteht in der unzureichenden Einbindung von Mitarbeitern bei der Entwicklung von Spionageabwehrmaßnahmen. Gerade mittelständische Unternehmen verfügen hier über weniger systematisierte Prozesse (Transkript 1, 126 ff.; Transkript 3, 203 ff.). Ein Lösungsansatz liegt in der Einführung eines *betrieblichen Vorschlagswesens (BVW)*, bei dem auch die Sicherheitsarchitektur eines Unternehmens durch den Einbezug der Mitarbeiter ständig optimiert wird. Dabei wird nicht nur die Kreativität der Mitarbeiter zu sicherheitsrelevanten Fragestellungen genutzt, sondern gleichzeitig stärkt ein solches System die Motivation und Identifikation der Mitarbeiter mit dem Unternehmen (Corporate Trust, 2007; Warnecke, 2010). Zur besseren Messung der Mitarbeiterbindung wird in der Literatur ein sogenannter Loyalitätsindex angeführt. Dabei beantwortet eine repräsentative Stichprobe von Mitarbeitern Fragen zu unterschiedlichen Themen, wie Motivation, Vertrauen und Feedback im Unternehmen. Im Anschluss erfolgt eine Auswertung der Umfrage durch Psychologen. Je nach Ergebnis können dann die jeweiligen Schwachstellen im Unternehmen gezielt abgestellt werden (Schaaf, 2009).

Im Bereich organisatorischer Spionageabwehrmaßnahmen weisen mehrheitlich mittelständische Unternehmen Verbesserungspotenziale auf. Gerade das Fehlen expliziter Fachkräfte zum Thema Informationsschutz stellt ein großes Problem dar. Hierbei sollten die betroffenen Un-

ternehmen nicht primär die zusätzlichen Personalkosten berücksichtigen, sondern vielmehr Sicherheit als Chance und strategischen Wettbewerbsvorteil begreifen (Warnecke, 2010).

Zusätzlich sind im Mittelstand klare organisatorische Regelungen zum Informationsschutz zu etablieren. Zu oft fehlen bereits grundlegende Maßnahmen, wie eine Clean-Desk-Policy oder eine Informationsklassifizierung. So wird vorgeschlagen, im Rahmen von Arbeitskreisen den Erfahrungsaustausch zwischen Unternehmen zu fördern und somit den Aufbau solcher Systeme voranzutreiben. Ebenfalls sind die Beratungsangebote der zuständigen Sicherheitsbehörden in einem größeren Maße von Unternehmen in Anspruch zu nehmen (Meissinger, 2005).

Konzipierte Know-how-Schutzmaßnahmen entfalten nur dann ihre Wirkung, wenn sie auch von den Mitarbeitern umgesetzt und gelebt werden. Daher sind die Kontrollen zur Einhaltung von Know-how-Schutzmaßnahmen gerade in den mittelständischen Unternehmen zu intensivieren. Eng damit verbunden ist die Einführung eines Bonus- und Malussystems, was sowohl für Mitarbeiter als auch für Geschäftspartner Anreize zur konsequenten Umsetzung der Maßnahmen bieten kann (SiFo, 2010b). Beispielsweise könnten einem Lieferanten bei mehrmaliger Missachtung von Sicherheitsstandards Folgeaufträge verwehrt werden.

Im Bereich technischer Spionageabwehrmaßnahmen besteht für Unternehmen die größte Gefahr darin, dass die angewandten Maßnahmen nicht mehr den aktuellen technischen Anforderungen entsprechen. Daher wird empfohlen, die Informations- und Kommunikationstechnik regelmäßig entweder durch eigene Fachkräfte oder durch die Einschaltung von seriösen externen Sicherheitsberatern zu überprüfen (Meissinger, 2005). In sogenannten IT-Audits können Schwachstellen in der Informations- und Kommunikationstechnik ausfindig gemacht und gezielt behoben werden. Bei besonders spionagegefährdeten Unternehmensbereichen, wie der Forschung und Entwicklung, sind zusätzlich bautechnische Schutzmaßnahmen zu ergreifen.

Im Bereich rechtlicher Spionageabwehrmaßnahmen bieten die praktizierten Geheimhaltungsvereinbarungen mit Mitarbeitern und Geschäftspartnern keinen vollständigen Schutz vor ungewolltem Know-how-Abfluss. Des Weiteren ist auch die gerichtliche Durchsetzung von Schadenersatzansprüchen nicht immer sichergestellt. Um diesen Gefahren adäquat zu begegnen, bieten Versicherungen seit einiger Zeit entsprechende Versicherungsprodukte an, die zum Beispiel die Kosten für Präventionsberatungen übernehmen und durch Spionage entstandene Vermögensschäden ersetzen (Corporate Trust, 2007). Somit kann der Abschluss einer

Spionageversicherung unter Berücksichtigung des anwachsenden Bedrohungspotenzials durch Wirtschafts- und Industriespionage durchaus sinnvoll für ein Unternehmen sein.

Auf Basis der Verknüpfung von bestehender Literatur und eigenen Untersuchungsergebnissen lässt sich nun, zur Beantwortung der anfangs gestellten Forschungsfrage, ein Katalog an personellen, organisatorischen, technischen und rechtlichen Spionageabwehrmaßnahmen ableiten (Abbildung 7). Dabei erhebt der Maßnahmenkatalog keinen Anspruch auf Vollständigkeit und ist aufgrund der dynamischen Umwelt stetig weiterzuentwickeln.

Personal

Personalrekrutierung

- Diskrete Stellenausschreibungen
- Intensive fallbezogene Bewerberüberprüfung

Personalmanagement:

- Informationsschutz als Chefsache, Vorbildfunktion durch das Management
- Regelmäßige Sensibilisierung und Schulung von Mitarbeitern: Grundlagen und zielgruppenorientierte Add-ons
- Systematische Einbindung der Mitarbeiter bei der Entwicklung von Know-how-Schutzmaßnahmen: zum Beispiel durch BVW
- Materielle und immaterielle Anreizsysteme
- Regelmäßige Messung der Mitarbeiterzufriedenheit: zum Beispiel durch Umfragen und Personalgespräche

Personalfreisetzung:

- Reguläres Ausscheiden:
  - Einzug von Firmeneigentum sowie Deaktivierung von Zutritts- und Zugriffsrechten zum Austrittstermin
- Nicht einvernehmliches Ausscheiden:
  - Individuelle und fallbezogene Vorgehensweise: zum Beispiel durch sofortige Sperrung der Zutritts- und Zugriffsrechte oder Werksverbot

Organisation

Fachkräfte für Informationsschutz:

- Einsatz von Informationsschutzbeauftragten
- Organisatorische Anbindung der Informationsschutzbeauftragten an die Geschäftsführung

Organisatorische Regelungen zum Umgang mit Informationen:

- Clean-Desk-Policy
- Informationsklassifizierung
- Zutritts- und Zugriffsberechtigungskonzepte

Kontrolle und Kooperation:

- Regelmäßige (un-) angekündigte Prüfung auf Umsetzung und Effizienz der Schutzmaßnahmen
- Klare Vorschriften zum Umgang mit Fremdpersonal
- Erfahrungsaustausch durch Arbeitskreise und Zusammenarbeit mit Sicherheitsbehörden

Technik

Bautechnik:

- Äußere Umfriedung des Standorts
- Gesetzeskonformer Einsatz von Videotechnik zur Außen- und Innenraumüberwachung
- Einbruchmeldeanlagen
- Zutrittskontrollsysteme
- Abhör-und Sichtschutz

Sicherung der Informations- und Kommunikationstechnik:

- Nutzer-Accounts mit systematischem Passwortwechsel
- Aktuelle Firewallsysteme und Schutzprogramme
- Verschlüsselung und räumliche Sicherung von sensiblen Informationen
- Ausbau beziehungsweise Deinstallation unnötiger Hard- und Software
- IT-Audits

Recht

Vertragliche und gesetzliche Maßnahmen:

- Geheimhaltungs- und Datenschutzvereinbarungen
- Wettbewerbsklauseln
- Patent- und Lizenzmanagement
- Abschluss von Spionageversicherungen

Abbildung 7: Katalog von Spionageabwehrmaßnahmen
Quelle: Eigene Darstellung

5.2 Grenzen

Die in Abbildung 7 aufgezeigten Spionageabwehrmaßnahmen bieten einen grundsätzlichen Überblick über die Fülle an Maßnahmen zum Schutz gegen einen ungewollten Know-how-Abfluss. Allerdings ist der vorgestellte Katalog nicht als Musterlösung im Kampf gegen Industriespionage zu verstehen, da die Maßnahmen auf das jeweilige Unternehmen, die spezifische Bedrohungslage und die wirtschaftlichen Rahmenbedingungen anzupassen sind. Dazu ist es in einem ersten Schritt sinnvoll die unternehmensspezifischen Spionagerisiken zu analysieren und zu bewerten. Auf Basis der gewonnen Ergebnisse können dann adäquate personelle, organisatorische, technische und rechtliche Spionageabwehrmaßnahmen ergriffen werden. Damit jedoch ein nachhaltiger Schutz vor den Gefahren der Industriespionage gewährt werden kann, sind die ergriffenen Maßnahmen auf Umsetzung und Effizienz zu überprüfen, damit eine fortlaufende Weiterentwicklung der Maßnahmen erfolgen kann.

Die vorliegende Untersuchung zeigt allerdings auch, dass den mittelständischen Unternehmen im Vergleich zu den befragten Großunternehmen weitaus geringere finanzielle und personelle Ressourcen zur Abwehr gegen Industriespionage zur Verfügung stehen (Transkript 4, 39 f.). Dennoch sollten auch mittelständische Unternehmen die Kosten zur Installation von Spionageabwehrmaßnahmen in ein Verhältnis zu den möglichen Konsequenzen eines Spionagevorfalls setzen. Zudem besteht gerade bei personellen und organisatorischen Spionageabwehrmaßnahmen ein günstiges Kosten-Nutzen-Verhältnis, was es auch Unternehmen mit geringerer Kapitalausstattung ermöglicht sich angemessen gegen ungewollten Know-how-Abfluss zu schützen.

Solange jedoch gerade in den mittelständischen Unternehmen kein ausreichendes Bewusstsein über die Risiken von Industriespionage besteht, werden konzipierte Maßnahmen wenig erfolgreich in der Umsetzung sein. Daher bildet insbesondere die Sensibilisierung und Schulung von Mitarbeitern einen wichtigen Aspekt im Rahmen eines ganzheitlichen Informationsschutzkonzepts. Hierzu gehört auch, dass das Management sicherheitsbewusstes Handeln mit dem Ziel vorlebt, dass auch Mitarbeiter unterer Hierarchieebenen die Notwendigkeit der getroffenen Maßnahmen verinnerlichen.

Weitere Grenzen sind in der gesetzeskonformen Umsetzbarkeit von Spionageabwehrmaßnahmen zu sehen. So bestehen Schwierigkeiten in der rechtlichen Umsetzung von nachvertraglichen Wettbewerbsverboten (Transkript 5, 179 ff.). Ebenfalls ist eine vollständige Video-

überwachung des Betriebsgeländes mit den bestehenden Gesetzen nicht zu vereinbaren (Transkript 8, 300).

Es wird schon deshalb keinen vollständigen Schutz vor Industriespionage geben, weil Unternehmen unausweichlich mit ihrer Umwelt, wie Kunden und Geschäftspartnern, interagieren und somit zwangsläufig der Risikofaktor Mensch und die damit verbundenen Gefahren eines ungewollten Know-how-Abflusses bestehen. Zusätzlich ist es für Unternehmen praktisch unmöglich, immer auf dem neuesten Stand der Technik zu sein, weil sie lediglich aus einer defensiven Position auf technische Angriffsmethoden reagieren können. Nicht zuletzt bildet auch die Immaterialität und unendliche Teilbarkeit von Informationen und Wissen ein unvermeidbares Risiko. Spionagegefährdete Unternehmen sollten sich daher auf den Schutz ihrer Kernkompetenzen konzentrieren.

Neben den aufgezeigten Grenzen im Schutz vor Industriespionage sind auch Limitationen im methodischen Vorgehen der vorliegenden Arbeit zu benennen. Zwar wurde bei der Auswahl der Stichprobe bewusst darauf geachtet, dass die befragten Unternehmen aus unterschiedlichen spionagegefährdeten Branchen kommen, allerdings sind die Ergebnisse aufgrund der begrenzten Größe der Stichprobe mit Einschränkungen behaftet und müssen immer unter Berücksichtigung des spezifischen Unternehmenskontextes betrachtet werden. So hätte durch quantitative Erhebungsmethoden, wie den Einsatz von Fragebögen, die Repräsentativität der Untersuchungsergebnisse erhöht werden können. Allerdings bestandbei dieser Arbeit eine besondere Schwierigkeit darin, Unternehmen für eine Befragung über das sensible Thema der Industriespionage überhaupt zu gewinnen, sodass bewusst, in Absprache mit dem Erstprüfer und den Kooperationspartnern, die Erhebungsmethode des Experteninterviews gewählt wurde, um zunächst ein Vertrauensverhältnis zu den Interviewpartnern aufzubauen.

5.3 Ausblick

Die vorliegende Untersuchung zeigt, dass die Angriffs- und Abwehrmöglichkeiten von Industrie- und Wirtschaftsspionage vielfältiger Natur sind. Je nach Unternehmen, der spezifischen Bedrohungslage und den wirtschaftlichen Rahmenbedingungen, ist ein individuelles und ganzheitliches Informationsschutzkonzept zu entwerfen, welches personelle, organisatorische, technische und rechtliche Spionageabwehrmaßnahmen enthält. Trotz dieses situativen Ansatzes bilden gerade personelle und organisatorische Spionageabwehrmaßnahmen eine wichtige Komponente, da der Faktor Mensch im Rahmen von Industriespionage die größten

Risiken aufweist. Diese liegen weniger in den kriminellen Energien von Mitarbeitern, sondern stärker in einem mangelnden Risikobewusstsein und einem leichtfertigen Umgang mit Sicherheitsanweisungen. Daher bilden insbesondere Schulungs- und Sensibilisierungsmaßnahmen einen wichtigen Beitrag zum Informationsschutz.

Mit zunehmendem internationalen Wettbewerbsdruck und globalen Wirtschaftskrisen werden die Gefahren von Industrie- und Wirtschaftsspionage auch in Zukunft für innovative Unternehmen weiter ansteigen (Corporate Trust, 2009; SiFo BW, 2010a). Dabei werden die zukünftigen Gefahren für deutsche Unternehmen weiterhin von chinesischen und russischen Geheimdiensten und Unternehmen ausgehen. Dennoch auch Gefahren aus befreundeten Staaten wie beispielsweise den USA und Frankreich. Trotz dieser Bedrohungen ist gerade in den untersuchten mittelständischen Unternehmen kein ausreichendes Bewusstsein über die Gefahren von Industrie- und Wirtschaftsspionage vorhanden. Zu oft werden die Risiken im eigenen Unternehmen unterschätzt und unzureichende Präventionsmaßnahmen ergriffen, was gerade für mittelständische Unternehmen im Schadensfall existenzbedrohende Auswirkungen haben kann (Corporate Trust, 2007; LfV RlP, 2008).

Unternehmen können die angesprochenen Bedrohungen jedoch auch als Chance verstehen. So ist davon auszugehen, dass Unternehmen, die ihrem Informationsschutz eine höhere Bedeutung zumessen, auch langfristig erfolgreicher als andere Unternehmen sein werden, da sie ihre differenzierenden Wettbewerbsvorteile länger gegenüber der Konkurrenz behaupten können (Huber, 2010a).

Literatur

Baeck, C. (2006). Unternehmensschutz – Zur Stellung des Sicherheitsverantwortlichen. *WIK - Zeitschrift für Sicherheit in der Wirtschaft*, 10. Jg. (3), S. 21-22.

Baeck, C. & Weber, M. (2007). Risikomanagement – Vertrauen ist gut, Kontrolle ist besser. *Personal-Magazin*, 6. Jg. (10), S. 32-35.

Baumgartner, C. (2005). *Social Engineering – trau schau wem.* [Elektronische Ressource]. URL: http://www.isecom.org/press/computerworld-05.08.05_about_social-engineering_author-baumgartner.pdf, Zugriff am 18. März 2011.

Berndt, R., Altobelli, C. & Sander, M. (2010). *Internationales Marketing-Management* (4. Auflage). Berlin: Springer.

Best, E & Weth, M. (2007). *Geschäftsprozesse optimieren – Der Praxisleitfaden für erfolgreiche Reorganisation* (2. überarbeitete Auflage). Wiesbaden: Gabler.

Boyens, K. (1998). *Externe Verwertung von technologischem Wissen*. Wiesbaden: Deutscher Universitätsverlag.

Brellochs, A. (2000). *Competitive Intelligence und Knowledge Management - Information über Markt und Wettbewerber als externe Wissensquelle in einem Wirtschaftsforschungsunternehmen*. München: GRIN.

Bundesamt für Verfassungsschutz (2002). *Wirtschaftsspionage – Information und Prävention.* [Elektronische Ressource]. URL: http://www.sicherheitsforum-bw.de/x_loads/bfv-pdf.pdf, Zugriff am 01. März 2011.

Bundesamt für Verfassungsschutz (2006). *Ihre Verantwortung – Unsere Sicherheit. Über den Umgang mit vertraulichen Informationen.* [Elektronische Ressource]. URL: http://jobo.amarunet.de/media/spio_broschueren/broschuere_0408_ihre_verantwortung_unsere_sicherheit.pdf, Zugriff am 09. März 2011.

Bundesamt für Verfassungsschutz (2008a). *Wirtschaftsspionage – Risiko für Ihr Unternehmen.* [Elektronische Ressource]. URL: http://www.im.nrw.de/sch/doks/vs/wirtschaftsspionage.pdf, Zugriff am 01. März 2011.

Bundesamt für Verfassungsschutz (2008b). *Verfassungsschutzbericht 2008.* [Elektronische Ressource]. URL: http://www.bmi.bund.de/cae/servlet/contentblob/463552/publicationFile/40609/vsb_2008.pdf, Zugriff am 04. März 2011.

Bundesamt für Verfassungsschutz (2009). *Verfassungsschutzbericht 2009.* [Elektronische Ressource]. URL: http://www.verfassungsschutz.de/download/SHOW/vsbericht_2009.pdf, Zugriff am 04. März 2011.

Bundesamt für Verfassungsschutz (2010a). *Sicherheitslücke Mensch – Der Innentäter als größte Bedrohung für die Unternehmen.* [Elektronische Ressource]. URL: http://www.verfassungsschutz.de/download/SHOW/faltblatt_ws_1008_2_sicherheitsluecke_mensch.pdf, Zugriff am 18. März 2011.

Bundesamt für Verfassungsschutz (2010b). *Elektronische Attacken auf Informations- und Kommunikationstechnik.* [Elektronische Ressource]. URL: http://www.verfassungsschutz.de/download/SHOW/faltblatt_ws_1008_3_elektronische_attacken.pdf, Zugriff am 22. März 2011.

Bundesamt für Verfassungsschutz (2010c). *Schrankenlose Offenheit – „soziale Netzwerke im Web.* [Elektronische Ressource]. URL: http://www.ism.rlp.de/fileadmin/ism/downloads/service/publikationen/Verfassungsschutz/pdf/Flyer-Soziale_Netzwerke.pdf, Zugriff am 23. März 2011.

Bundesverband der Deutschen Industrie (2006). *Bedeutung der Sicherheit in der Industrie für Deutschland.* Berlin: Security & Defence.

Corporate Trust (2009). *Gefahrenbarometer 2010 – Risiken für den deutschen Mittelstand.* München: Verlagsgruppe Handelsblatt.

Corporate Trust (2007). *Studie: Industriespionage. Die Schäden durch Spionage in der deutschen Wirtschaft.* München: Verlagsgruppe Handelsblatt.

Creutz, M. (2007). *Ausforschung geistigen Eigentums – Immun gegen Know-how-Klau?* [Elektronische Ressource] URL: http://www.handelsblatt.com/unternehmen/management/strategie/immun-gegen-know-how-klau/2836594.html, Zugriff am 18. März 2011.

Deutscher Industrie- und Handelstag (1997). *Wirtschaftsspionage – Anleitung zur Prävention* (1. Auflage). Bonn: Siewert.

Deutsches Institut für Wirtschaftsforschung (2009). *Innovationsindikator Deutschland 2009.* [Elektronische Ressource]. URL: http://www.innovationsindikator.de/fileadmin/user_upload/Dokumente/innovationsindikator 2009.pdf, Zugriff am 01. März 2011.

Deutsches Patent- und Markenamt (2010). *Patent – Patente fördern Innovationen.* [Elektronische Ressource]. URL: http://www.dpma.de/patent/index.html, Zugriff am 23. März 2011.

Faber, T. (2009). *Angriffsmöglichkeiten im virtuellen Raum* (S. 85-96). In: Bisanz, S. & Gerstenberg, U. (Hrsg.), Raubritter gegen den Mittelstand - Informationsschutz mittelständischer Unternehmen (1. Auflage). Essen: Consulting Plus.

Fick, D., Hohl, K. & Ullrich, L. (2002). *Wettbewerbsvorteil Wissen – Wie Wissensmanagement und Wissenscontrolling zur Gestaltung organisationalen Lernens beitragen können.* Nürtingen: Fachhochschule Nürtingen.

Flick, U. (2005). *Qualitative Sozialforschung. Eine Einführung* (3. Auflage). Reinbeck: Rowohlt.

Frey, B. & Osterloh, M. (2002). *Managing Motivation – Wie Sie die neue Motivationsforschung für Ihr Unternehmen nutzen können* (2. Auflage). Wiesbaden: Gabler.

Friebertshäuser, B. (1997). *Interviewtechniken – ein Überblick* (S. 371-395). In: Friebertshäuser, B. & Prengel, A. (Hrsg.), Handbuch Qualitative Forschungsmethoden in der Erziehungswissenschaft (1. Auflage). Weinheim: Juventa.

Frost, J. (2005). *Märkte und Unternehmen. Organisatorische Steuerung und Theorie der Firma.* Wiesbaden: Deutscher Universitätsverlag.

Fussan, C. (2010). *Bedeutung innerbetrieblicher Veränderungen für Know-how-Schutz in Unternehmen* (S. 1-22). In: Fussan, C. (Hrsg.), Managementmaßnahmen gegen Produktpiraterie und Industriespionage (1. Auflage). Wiesbaden: Gabler.

Gabler (Hrsg.) (2010). *Gabler Wirtschaftslexikon* (17. komplett aktualisierte und erweiterte Auflage). Wiesbaden: Gabler.

Galdy, A. (2008). IT-Kräfte – *Die Rache der Entlassenen.* [Elektronische Ressource]. URL: http://www.manager-magazin.de/unternehmen/it/0,2828,587390,00.html, Zugriff am 18. März 2011.

Goemann-Singer, A., Graschi, P. & Weissenberger, R. (2004). *Recherchehandbuch Wirtschaftsinformationen – Vorgehen, Quellen und Praxisbeispiele* (2. Auflage). Berlin: Springer.

Grund, M. & Fischer, F. (2009). *Know-how-Abfluss durch Kommunikationsinfrastruktur* (S. 71-84). In: Bisanz, S. & Gerstenberg, U. (Hrsg.), Raubritter gegen den Mittelstand - Informationsschutz mittelständischer Unternehmen (1. Auflage). Essen: Consulting Plus.

Harbich, P. (2006). Die wachsende Bedeutung privater Akteure im Bereich der Intelligence. Private Akteure als Quellen, Abnehmer, Konkurrenten und Kooperationspartner staatlicher

Nachrichtendienste. In: *Arbeitspapiere zur Internationalen Politik und Außenpolitik (AIPA)*, 4. Jg. (03), S. 1-82.

Havranek, T. (2010). *Verraten & Verkauft – Bespitzelung, Wirtschaftskriminalität, Industrie-Spionage* (1. Auflage). Wien: Molden.

Hirschmann, K. (2009). *Menschen und Wissen: Eigen- und Fremdpersonal als Risikofaktor* (S. 51-70). In: Bisanz, S. & Gerstenberg, U. (Hrsg.), Raubritter gegen den Mittelstand - Informationsschutz mittelständischer Unternehmen (1. Auflage). Essen: Consulting Plus.

Hitzler, R. (1994). *Wissen und Wesen des Experten. Ein Annäherungsversuch – zur Einleitung* (S. 13-30). In: Hitzler, R., Honer, A. & Maeder, C. (Hrsg.), Expertenwissen. Die institutionalisierte Kompetenz zur Konstruktion von Wirklichkeit. Opladen: Westdeutscher Verlag.

Huber, A. (2009). Spionageabwehr: Von ignorierter Pflicht zum Wettbewerbsvorteil. *intelligenter produzieren*, 6. Jg. (5), S. 40-41.

Huber, A. (2010a). *Wirtschaftsspionage und Konkurrenzausspähung als Phänomene zunehmender Kooperationen und veränderter Loyalität* (S. 109-116). In: Beschorner, T., Schmidt, M., Vorbohle, K. & Schlank, C. (Hrsg.), Kooperation und Ethik (1. Auflage). München: Rainer Hampp.

Huber, A. (2010b). Informationsschutz im Mittelstand – Wie sicher sind Ihre Geschäftsgeheimnisse? *Verein Berliner Kaufleute und Industrieller Spiegel*, 60. Jg. (2), S. 22-23.

Huber, A. (2010c). Informationsschutz und Spionageabwehr. *Beuth Presse*, 7. Jg., (1), S. 11.

Huber, A. (2010d). Ist Spionage ein Risiko für den Mittelstand? *Institut für wertorientierte Unternehmensführung Spektrum*, 5. Jg. (1), S. 9-10.

Hummelt, R. (1997). *Wirtschaftsspionage auf dem Datenhighway – Strategische Risiken und Spionageabwehr* (1. Auflage). München: Hanser.

Institut für Mittelstandsforschung (2007). *Die volkswirtschaftliche Bedeutung der Familienunternehmen.* [Elektronische Ressource] URL: http://www.ifm-bonn.org/assets/documents/IfM-Materialien-172.pdf, Zugriff am 05. April 2011.

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G., Paxson, V. & Savage, S. (2008). *Spamalytics: An empirical Analysis of Spam Marketing Conversion.* [Elektronische Ressource]. URL: http://www.icsi.berkeley.edu/pubs/networking/2008-ccs-spamalytics.pdf, Zugriff am 22. März 2011.

Kondruß, B. (2010). *Der Intelligence Cycle.* [Elektronische Ressource]. URL: http://www.ci-handbuch.de/wettbewerbsanalyse/intelligence-cycle.htm, Zugriff am 04. März 2011.

KPMG (2010). *Wirtschaftskriminalität in Deutschland 2010 – Fokus Mittelstand.* [Elektronische Ressource]. URL: http://www.kpmg.de/docs/20091220_Wirtschaftskriminalitaet.pdf, Zugriff am 07. März 2011.

Kuckartz, U. (1999). *winMAX – Textanalysesystem für die Sozialwissenschaften. Handbuch zum Textanalysesystem winMAX für Windows 95/98/NT* (1. Auflage). Opladen: Westdeutscher Verlag.

Lamnek, S. (1995). *Qualitative Sozialforschung. Bd. 1: Methodologie* (1. Auflage). Weinheim: Beltz.

Landesamt für Verfassungsschutz Baden-Württemberg (1999). *Schutz vor Spionage* (1. Auflage). o.O: o.V.

Landesamt für Verfassungsschutz Baden-Württemberg (2004). *Know-how-Schutz. Handlungsempfehlungen für die gewerbliche Wirtschaft.* [Elektronische Ressource]. URL: http://www.sicherheitsforum-bw.de/downloads/know_how_schutz_2004.pdf, Zugriff am 01. März 2011.

Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006). *Wirtschaftsspionage in Baden-Württemberg und Bayern. Daten – Fakten – Hintergründe.* [Elektronische Ressource]. URL: http://www.verfassungsschutz.bayern.de/imperia/md/content/lfv_internet/service/wirtschaftsspionage_bay_bw_2006.pdf, Zugriff am 01. März 2011.

Landesamt für Verfassungsschutz Rheinland-Pfalz (2008). *Informationsschutz in der gewerblichen Wirtschaft – mit Sicherheit ein Gewinn!* [Elektronische Ressource]. URL: http://www.verfassungsschutz.de/download/SHOW/broschuere_0809_rp_wirtschaftsspionage.pdf, Zugriff am 04. März 2011.

Lux, C. & Peske, T. (2002a). *Competitive Intelligence und Wirtschaftsspionage – Analyse, Praxis, Strategie* (1. Auflage). Wiesbaden: Gabler.

Lux, C. & Peske, T. (2002b). Competitive Intelligence - Zwischen Anspruch und Wirklichkeit. *WIK - Zeitschrift für Sicherheit in der Wirtschaft*, 6. Jg. (2), S. 15-17.

Macharzina, K. (2008). *Unternehmensführung: Das internationale Managementwissen – Konzepte, Methoden, Praxis* (6. vollständig überarbeitete und erweiterte Auflage). Wiesbaden: Gabler.

Marwehe, F & Weißbach, H.-J. (2000). *Der Wissenszyklus. Vom individuellen Wissen zur kollektiven Wissensbasis.* [Elektronische Ressource]. URL: http://www.wiper.de/dokumente/WwZYKLUS.PDF, Zugriff am 15. März 2011.

Mayer, H. (2009). *Interview und schriftliche Befragung – Entwicklung, Durchführung, Auswertung* (5. überarbeitete Auflage). München: Oldenbourg.

Meissinger, J. (2005). *Gefahren und Bedrohungen durch Wirtschafts- und Industriespionage in Deutschland* (1.Auflage). Hamburg: Dr. Kovac.

Merkens, H. (1997). *Stichproben bei qualitativen Studien.* In: Friebertshäuser, B. & Prengel, A. (Hrsg.), Handbuch Qualitative Forschungsmethoden in der Erziehungswissenschaft (1. Auflage). Weinheim: Juventa.

Meuser, M. & Nagel, U. (1991). *Experteninterviews – vielfach erprobt, wenig bedacht. Ein Beitrag zur qualitativen Methodendiskussion* (S. 441-468). In: Garz, D. & Kraimer, K. (Hrsg.), Qualitativ-empirische Sozialforschung: Konzepte, Methoden, Analysen (1. Auflage). Opladen: Westdeutscher Verlag.

Mühlfeld, C. et al. (1981). Auswertungsprobleme offener Interviews. *Soziale Welt*, 32. Jg., S. 325-352.

Nathusius, I. (2001). *Wirtschaftsspionage: Gefahren, Strukturen und Bekämpfung* (1. Auflage). Heidelberg: Kriminalistik.

North, K. (2005). *Wissensorientierte Unternehmensführung* (4. aktualisierte und erweiterte Auflage). Wiesbaden: Gabler.

Osterloh, M. & Frost, J. (2006). *Prozessmanagement als Kernkompetenz – Wie Sie Business Reengineering strategisch nutzen können* (5. überarbeitete Auflage). Wiesbaden: Gabler.

Pfadenhauer, M. (2009). *Das Experteninterview – Ein Gespräch auf gleicher Augenhöhe* (S. 449-461). In: Buber, R. & Holzmüller, H. (Hrsg.), Qualitative Marktforschung: Konzepte - Methoden - Analysen (2. Auflage). Wiesbaden: Gabler.

Pfaff, D. (2005). *Competitive Intelligence in der Praxis – Mit Informationen über Ihre Wettbewerber auf der Überholspur* (1. Auflage). Frankfurt: Campus.

Picot, A., Reichwald, R. & Wigand, R. (2003). *Die grenzenlose Unternehmung – Information, Organisation und Management* (5. aktualisierte Auflage). Wiesbaden: Gabler.

Pittori, P. (1998). *Counterspionage for american business.* Boston: Butterworth-Heinemann.

Polanyi, M. (1966). *The Tacit Dimension.* London: Routledge & Kegan Paul.

Pressetext Nachrichtenagentur (2008). *Industriespionage verursacht 30 Mrd. Euro Schaden.* [Elektronische Ressource]. URL: http://pressetext.de/news/080311018/industriespionage-verursacht-30-mrd-euro-schaden, Zugriff am 08. März 2011.

PricewaterhouseCoopers (2009). *Wirtschaftskriminalität 2009 – Sicherheitslage in deutschen Großunternehmen.* [Elektronische Ressource]. URL: http://www.pwc.de/de/risiko-management/assets/Studie-Wirtschaftskriminal-09.pdf, Zugriff am 08. März 2011.

Probst, G., Raub, S. & Romhardt, K. (1999). *Wissen managen – Wie Unternehmen ihre wertvollste Ressource optimal nutzen* (3. Auflage). Wiesbaden: Gabler.

Rehäuser, J. & Krcmar, H. (1996). *Wissensmanagement im Unternehmen.* In: Schreyögg, G. & Conrad, P. (Hrsg.), Wissensmanagement (1. Auflage). Berlin: Gabler.

Rogge, M. & Ziegler, P. (2007). Social Engineering. *hakin9*, 3. Jg. (11), S. 2-11.

Sack, D. (2008). Das integrierte Informationsschutzkonzept. *WIK - Zeitschrift für Sicherheit in der Wirtschaft*, 12. Jg. (1), S. 19-21.

Schaaf, C. (2009). *Der große Angriff auf den Mittelstand* (1. Auflage). Stuttgart: Boorberg.

Schaumann, P. (2009). *Schutz gegen Social Engineering – neue psychologische Ansätze.* [Elektronische Ressource]. URL: http://www.sicherheitskultur.at/social_engineering, Zugriff am 09. März 2011.

Schildbauer, T., Braun, M. & Schultze, M. (2003). *Corporate Knowledge* (1. Auflage). Göttingen: Business Village.

Schindler, M. (2011). *Wirtschaftsspionage: "90 Prozent aller Fälle im Mittelstand".* [Elektronische Ressource]. URL: http://www.silicon.de/management/cio/0,39044010,41545715,00/wirtschaftsspionage__90_prozent_aller_faelle_im_mittelstand.htm, Zugriff am 17. März 2011.

Schmid, G. (2004). *Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON).* [Elektronische Ressource]. URL: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//DE&language=DE, Zugriff am 10. März 2011.

Sicherheitsforum Baden-Württemberg (2004). *Fall- und Schadensanalyse bezüglich Know-how-/Informationsverluste in Baden-Württemberg ab 1995.* [Elektronische Ressource]. URL:

http://www.sicherheitsforum-bw.de/downloads/Studie-Uni-Lueneburg.pdf, Zugriff am 08. März 2011.

Sicherheitsforum Baden-Württemberg (2005). *Mit Sicherheit erfolgreich – Erfolgsfaktor Know-how-Schutz.* [Elektronische Ressource]. URL: http://www.sicherheitsforum-bw.de/downloads/Sicherheitsforum2.pdf, Zugriff am 18. März 2011.

Sicherheitsforum Baden-Württemberg (2010a). *SiFo-Studie 2009/10 – Know-how-Schutz in Baden-Württemberg.* [Elektronische Ressource]. URL: http://www.sicherheitsforum-bw.de/x_loads/SiFo-Studie.pdf, Zugriff am 01. März 2011.

Sicherheitsforum Baden-Württemberg (2010b). SiFo-Studie 2009/10 - *Handlungsempfehlungen für Unternehmen.* [Elektronische Ressource]. URL: http://www.sicherheitsforum-bw.de/x_loads/Handlungsempfehlungen%20zur%20SiFo-Studie.pdf, Zugriff am 02. März 2011.

Sidler, W. (2008). Angriffsziel Mensch. *IT-Business,* 18. Jg. (2), S. 2-4.

Sobbek, M. & Bühler, B. (2009). *Informationen und unternehmerischer Erfolg: Eine Einführung* (S. 13-24). In: Bisanz, S./Gerstenberg, U. (Hrsg.), Raubritter gegen den Mittelstand - Informationsschutz mittelständischer Unternehmen (1. Auflage). Essen: Consulting Plus.

Spiegel Online (2000). *Die López-Affäre.* [Elektronische Ressource]. URL: http://www.spiegel.de/wirtschaft/0,1518,77898,00.html, Zugriff am 17. März 2011.

Trinczek, R. (1995). *Experteninterviews mit Managern: Methodische und methodologische Hintergründe* (S. 59-67). In: Brinkmann, C., Deeke, A. & Völkel, B. (Hrsg.), Experteninterviews in der Arbeitsmarktforschung. Nürnberg: Institut für Arbeitsmarkt- und Berufsforschung.

Warnecke, G. (2010). *Quellen illegalen Know-how-Abflusses aus Industrieunternehmen und Strategien gegen Industriespionage* (S. 249-332). In: Fussan, C. (Hrsg.), Managementmaßnahmen gegen Produktpiraterie und Industriespionage (1. Auflage). Wiesbaden: Gabler.

Werner, M. (2004). *Einflussfaktoren des Wissenstransfers in wissensintensiven Dienstleistungsunternehmen – Eine explorativ-empirische Untersuchung bei Unternehmensberatungen* (1. Auflage). Wiesbaden: Deutscher Universitätsverlag.

Zentrum für Europäische Wirtschaftsforschung (2007). *IKT-Report: Unternehmensbefragung zur Nutzung von Informations- und Kommunikationstechnologien.* [Elektronische Ressource]. URL: ftp://ftp.zew.de/pub/zew-docs/div/IKTRep/IKT_Report_2007.pdf, [10.März 2011].

Anhang

A Leitfaden für die Experteninterviews 86

B Transkripte 90

B1 Transkript 1 90

B2 Transkript 2 103

B3 Transkript 3 119

B4 Transkript 4 134

B5 Transkript 5 147

B6 Transkript 6 160

B7 Transkript 7 167

B8 Transkript 8 178

A Leitfaden für die Experteninterviews

Leitfaden für die Experteninterviews

Name:	
Position:	
Datum:	
Zeitraum:	

Risikoanalyse

1. Inwieweit wurde bei Ihnen im Unternehmen eine Risikoanalyse durchgeführt, um Maßnahmen zum Know-how-Schutz ergreifen zu können?
2. Wenn eine solche Risikoanalyse durchgeführt wurde, welche Bereiche (Person, Organisation, Technik, Recht) wiesen die größten Risiken auf?

Risikobewertung

3. Hat in Ihrem Unternehmen eine Risikobewertung stattgefunden und wenn ja, welche Faktoren wurden zur Risikobewertung herangezogen?
4. Wurde auf Basis der Analyse und Bewertung der potenziellen Risiken eine Prioritätenliste für notwendige Sicherheitsmaßnahmen entwickelt?

Personelle Maßnahmen

5. Werden im Rahmen der Personalakquisition sicherheitsrelevante Firmeninterna in Stellenausschreibungen veröffentlicht?

6. Findet im Rahmen des Personalauswahlverfahrens eine intensive Überprüfung der Bewerber statt?
7. Kommt es im Zuge der Personaleinstellung zu Sicherheitsmaßnahmen?
8. Ist Informationsschutz bei Ihnen im Unternehmen Chefsache, d.h. geht das Management diesbezüglich mit gutem Beispiel voran?
9. Inwieweit werden die Mitarbeiter für die Gefahren des ungewollten Know-how-Abflusses sensibilisiert und geschult?
10. Inwieweit findet eine Einbindung der Mitarbeiter bei der Entwicklung von Know-how-Schutzmaßnahmen statt?
11. Werden Mitarbeiter leistungsgerecht entlohnt und erhalten sie auch unentgeltliche Anerkennung für ihre beruflichen Leistungen?
12. Gibt es Instrumente zur Messung der Mitarbeiter-Loyalität bzw. des Identifikationsgrads der Mitarbeiter mit dem Unternehmen? Wenn ja, wie sind die Ergebnisse?

13. Welche Sicherheitsmaßnahmen werden bei der Beendigung eines Arbeitsverhältnisses ergriffen?
14. Gibt es bezüglich der angewandten Sicherheitsmaßnahmen Unterschiede zwischen einem regulären und einem nicht einvernehmlichen Ausscheiden?
15. Gelten für Fremdpersonal wie Leiharbeiter, Mitarbeiter von Geschäftspartnern, Sicherheits- und Reinigungspersonal die gleichen Sicherheitsbedingungen wie für das firmeneigene Personal?

Organisatorische Maßnahmen

16. Inwieweit wurden bei Ihnen im Unternehmen formal fixierte Sicherheitsstandards etabliert, die vor Know-how-Abfluss schützen sollen?
17. Gibt es einen Sicherheitsverantwortlichen bei Ihnen im Unternehmen und wenn ja, welche Aufgaben nimmt er im Speziellen wahr?
18. Ist der Sicherheitsverantwortliche organisatorisch an die Geschäftsführung angebunden?
19. Wie sind die Zutritts- und Zugriffsrechte für firmeneigenes und fremdes Personal bei Ihnen zum Schutz von gefährdeten Daten, Objekten und Räumen konzipiert?

20. Werden regelmäßige Kontrollen zur Überprüfung und Anpassung der Sicherheits-maßnahmen durchgeführt und wenn ja, wie genau sind solche Kontrollen ausgestaltet?
21. Inwieweit werden Mitarbeiter bei Sicherheitsverstößen oder sicherheitsbewusstem Handeln sanktioniert bzw. belohnt?

Technische Maßnahmen

22. Welche bautechnischen Maßnahmen bestehen zur Absicherung gegenüber Betriebs-fremden und unbefugten Mitarbeitern?
23. Welche Maßnahmen werden zur Sicherung der Informations- und Kommunikationstechnik gegenüber Innen- und Außentätern eingesetzt?

Rechtliche Maßnahmen

24. Inwieweit werden Geheimhaltungs- und Wettbewerbsvereinbarungen zwischen Ihrem Unternehmen und den Mitarbeitern bzw. zwischen Ihrem Unternehmen und Fremd-firmen abgeschlossen?
25. Werden bei Verstößen gegen solche Geheimhaltungs- und Wettbewerbs-vereinbarungen auch Sanktionen und rechtliche Konsequenzen eingeleitet?

B Transkripte

B1 Transkript 1

Name:	Herr E.
Position:	Geschäftsführer, Firma A.
Datum:	29.03.2011
Zeitraum:	11.00 - 12.00 Uhr

Interviewer (I): Sehr geehrter Herr E., vielen Dank, dass Sie sich Zeit genommen haben. Ich werde Ihnen in den nächsten 60 Minuten Fragen zur Risikoanalyse und Risikobewertung von Industriespionage sowie zu möglichen präventiven und repressiven Spionageabwehrmaßnahmen in Ihrem Unternehmen stellen. Fangen wir mit dem Bereich der Risikoanalyse an. Inwieweit wurde bei Ihnen im Unternehmen eine Risikoanalyse durchgeführt, um spätere Know-how-Schutzmaßnahmen auch ergreifen zu können?

Herr E.: Wir führen einen Risikokatalog beziehungsweise sind wir in das Risikomanagement unserer Muttergesellschaft integriert und betrachten Risiken einmal aus der Sichtweise der Muttergesellschaft und einmal aus der Sicht unserer Firma. Das ist durchaus unterschiedlich, um die möglichen Schadenshöhen zu betrachten und zu bewerten. Sei es ausgehend von den Werten, die wir im Unternehmen haben und den möglichen Risiken, denen wir ausgesetzt sind. Dabei sind auch viele betriebliche Risiken involviert. Wir versuchen Eintrittswahrscheinlichkeiten und Schadenshöhen zu betrachten, um dadurch mögliche Risikoklassifizierungen durchzuführen und dann mögliche Handlungsfelder abzuleiten. Diese Risikoanalyse beziehungsweise dieser Risikokatalog wird vierteljährlich aktualisiert.

I: Herr E., Sie haben gerade schon gesagt, dass die Höhe und auch die Schadenseintrittswahrscheinlichkeit berücksichtigen. Gibt es noch weitere Parameter, die in die Risikobewertung einfließen oder gibt es noch weitere Größen?

Herr E.: Das sind eigentlich die beiden maßgeblichen Stellschrauben, die letztendlich daraus eine Matrix bilden und aus denen wir dann Handlungsfelder ableiten.

I: Wird denn auf Basis der Analyse und Bewertung der Risiken, die Sie vornehmen, dann auch eine Prioritätenliste von den zu ergreifenden Sicherheitsmaßnahmen erstellt?

Herr E.: Ja, es wird noch einmal unterschieden zwischen vier Klassifizierungen. Das eine ist „dringender Handlungsbedarf“, „Handlungsbedarf“, „beobachten“ und ich glaube „kann so bleiben“ oder sinngemäß.

I: Ok. Wenn wir kurz bei der Risikoanalyse stehen bleiben. Können Sie dabei sagen welche Bereiche bei Ihnen im Unternehmen und, da Sie auch Sicherheitsdienstleister sind, auch bei anderen Unternehmen und Geschäftspartnern besonders betroffen sind? Hierbei meine ich die Bereiche Person, Organisation, Technik und Recht.

Herr E.: Also mein Gefühl sagt mir, dass insbesondere bei Menschen die größten Risiken vorliegen. Gar nicht weil die besonders kriminelle Energien entwickeln, sondern einfach weil der Unsicherheitsfaktor am größten ist, weil man unbedarft ist, weil man vielleicht etwas lax mit Richtlinien umgeht und dann am Ende des Tages in der Praxis auch gewisse Dinge nicht umsetzt. Im einfachsten Fall wird das Handy nicht mit einem PIN-Code gesperrt oder dann werden von Firmen die Festplatten nicht verschlüsselt. Und trotzdem reisen die Vertriebler dann nach China und sitzen dann im Hotel und lassen das Laptop liegen. Ich gebe zu, es ist eine Mischung aus Bauchgefühl und Erkenntnissen, die wir dabei bei Kunden haben. Klar, es werden auch sicherlich ein paar technische Dinge, die möglich sind, missachtet und nicht umgesetzt, aber das Maßgebliche ist aus meiner Sicht der Mensch. Das ist für mich der eigentliche Unsicherheitsfaktor. Aber, wie gesagt, gar nicht unbedingt bösgläubig, sondern oftmals unbedarft aus der Praxis heraus. Wenn die Leute im Zug sitzen und auf Toilette gehen, glaube ich dass die meisten Leute ihr Laptop auf den Sitz liegen lassen. Damit haben die meisten Leute keine Schmerzen oder gehen gutgläubig davon aus, dass schon nichts wegkommt.

I: Damit sind wir ja auch schon im Bereich Personal. Diesbezüglich wäre zunächst einmal meine Frage inwieweit man auch im Rahmen der Personalakquisition auf Sicherheitsvorkehrungen achtet. Werden bestimmte sensible Informationen auch in Stellenausschreibungen veröffentlicht?

Herr E.: Also in Stellenausschreibungen sind natürlich keine sicherheitsrelevanten Informationen enthalten. Können Sie die Frage noch ein bisschen konkretisieren? Das habe ich noch nicht ganz verstanden.

I: Selbstverständlich. Und zwar geht es darum, wenn eine Stellenausschreibung formuliert und publiziert wird. Inwieweit nicht nur mögliche Bewerber, sondern auch für mögliche

Wettbewerber gewisse Informationen zu ziehen sind. Zum Beispiel über die Aktivitäten des Unternehmens, dass die Stelle inseriert hat.

Herr E.: Das ist bei uns eher weniger der Fall. Wir beschreiben zwar schon die Technologien mit denen sich der Mitarbeiter zukünftig befasst, aber das kann man auch auf der Homepage herauslesen, wo wir uns darstellen. Oder auch über Unternehmensbroschüren, wo die grundsätzlichen Themen dann auch verfasst sind.

I: Gibt es, wenn wir jetzt einen Schritt weiter zur Personalauswahl gehen, eine intensive Überprüfung der Bewerber?

Herr E.: Bei unserem Unternehmen schon, dadurch, dass wir IT-Dienstleister sind, gibt es eine zusätzliche behördliche Sicherheitsüberprüfung, da wir auch teilweise in Sicherheitsbereichen der Muttergesellschaft unterwegs sind. Sonst erhält der Mitarbeiter auch den entsprechenden Sicherheitsausweis mit den jeweiligen Berechtigungen nicht.

I: Umfasst der von Ihnen angesprochene behördliche Sicherheitscheck auch eine gewisse Überprüfung der Ausbildung und weiterer Daten des Lebenslaufs?

Herr E.: Ja, ich meine schon, aber ich muss zugeben, dass ich nicht ganz tief in dem Thema drin bin.

I: Machen wir jetzt einen weiteren Schritt hin zur Personaleinstellung. Gibt es hier gewisse Sicherheitsmaßnahmen wie Sicherheitsbelehrungen, Datenschutz- und Geheimhaltungsverpflichtungen zwischen Ihrem Unternehmen und den Mitarbeitern?

Herr E.: Ja, zwar nicht beim Einstellungsgespräch, aber im Arbeitsvertrag, den wir gemeinsam unterschreiben. Hier gibt es einen wichtigen Passus zum Thema Datenschutz und zur dauerhaften Wahrung von Betriebsgeheimnissen, unabhängig ob der Mitarbeiter irgendwann einmal ausscheidet. Darüber hinaus gibt es noch für spezielle Berufsgruppen, wie Systemadministratoren im Rechenzentrum, zusätzliche Geheimhaltungsvereinbarungen, die von dem Mitarbeiter auch nochmal gegengezeichnet werden. Es handelt sich dabei ja auch um besonders personenbezogene Daten beziehungsweise technische Themen, die natürlich entsprechende Brisanz haben können. Insbesondere aber auch personenbezogene Daten, die natürlich nicht für irgendwelche Aktionen genutzt werden dürfen. Somit gibt es noch ein zusätzliches Schriftstück und eine Belehrung, was diese Personen dann auch unterzeichnen müssen.

I: Herr E., wird der Informationsschutz in Ihrem Unternehmen, denn als Chefsache betrachtet? Immerhin nehmen Sie sich ja auch die Zeit für die Anfertigung dieses Interviews. Oder gibt es noch weitere Sicherheitsbeauftragte beziehungsweise Sicherheitsverantwortliche?

Herr E.: Also, wir als Geschäftsführer achten dort zum einen darauf und haben darüber hinaus auch Vorgaben von unseren Gesellschaftern. (…). Dabei kommt von einem unserer Gesellschafter ein Management-Handbuch, in dem zum Beispiel Themen, wie Informationssicherheit, ein wichtiges Thema sind. Dort gibt es auch gewisse Erklärungen unsererseits als Geschäftsführung und zusätzlich haben wir auch einen Informationssicherheitsbeauftragten benannt. Dieser ist gleichzeitig Leiter des Rechenzentrums und arbeitet gleichzeitig Aktivitäten ab, die wir als Geschäftsführung initiiert haben. Zum einen haben wir letztes Jahr eine Firma beauftragt, um einen Penetrationstest durchzuführen und haben zusätzlich noch einen weiteren Berater beauftragt, der praktisch eine Überprüfung der Informationssicherheit durchgeführt hat. Daraus ergeben sich dann immer Handlungsbedarf und Empfehlungen, die dann insbesondere von dem Informationssicherheitsbeauftragten bearbeitet werden. Dies wird dann natürlich mit dem Führungsteam durchgesprochen und dann entscheiden wir im Führungsteam oder in der Geschäftsführung, je nach Wertigkeit des Themas, ob wir es durchführen oder ob wir vielleicht auch bewusst damit leben. Dementsprechend müssen wir dann reagieren.

I: Gut. Sie hatten ja bereits angesprochen, dass der Faktor Mensch, wenn oft auch unbewusst, ein Risiko darstellt. Gerade um im Unternehmen für Informationsschutz zu sorgen, ist es daher ja auch wichtig, dass Mitarbeiter für Gefahren geschult und sensibilisiert werden. Inwieweit finden solche Maßnahmen bei Ihnen im Unternehmen statt?

Herr E.: Da müssen wir sicherlich noch besser werden. Das machen wir zum einen über die Regelkommunikation, wenn wir zum Beispiel ausgehend vom Führungsteam über die Prioritätslisten, die ich gerade angesprochen habe, feststellen, dass wir gewissen Handlungsbedarf haben und gewisse Sachen ändern müssen. Aber eine bestimmte Belehrungsveranstaltung haben wir insbesondere nur für Führungskräfte. In dieser Belehrungsveranstaltung spielt das Thema allerdings nur zum Teil hinein. Es geht mehr um Arbeitssicherheit Eine ganzheitliche Mitarbeiterbelehrung für alle Mitarbeiter findet aber derzeit nicht statt. Es gibt lediglich individuelle Auffrischungen, wo der Leiter des Rechenzentrums zum Beispiel noch einmal die Mitarbeiter an bestimmte Themen erinnert (…), aber da ist tatsächlich noch kein regelmäßiger Prozess implementiert.

I: Also meinen Sie schon, dass man in diesem Bereich noch Verbesserungen durchführen könnte?

Herr E.: Ja, das könnte man noch besser machen. Ich denke man könnte den Prozess noch sicherer gestalten.

I: Kommen wir noch einmal auf das Thema Mitarbeiter zurück. Gibt es denn ansonsten auch eine Einbindung der Mitarbeiter bei der Entwicklung von Sicherheitsmaßnahmen? Seien es Sicherheitsmaßnahmen im organisatorischen Bereich, wo der Mitarbeiter zum Beispiel gewisse Informationslecks in Prozessen entdeckt und diese dann an die Geschäftsführung mitteilt, um solche Lecks dann auch zu schließen.

Herr E.: Ja, es gibt hierzu einige Beispiele, wo das genauso erfolgt ist. Wo ein Mitarbeiter gesagt hat, dass im Internet bedenkliche Informationen zur Verfügung stehen, die dann abgeschaltet wurden beziehungsweise sagt ein Mitarbeiter, ganz profan, dass die Einbruchsmeldeanlage ein Zeitfenster hat, das zeitlich zu modifizieren ist. Diese Verbesserungsvorschläge kommen rein, aber das ist kein regelmäßiger Prozess. Das heißt, dass wir keine regelmäßigen monatlichen oder jährlichen Aktivitäten haben, wo wir den Mitarbeiter ermuntern Ideen zu generieren. Das ist eher eine dezentrale Sache, wo dann die Teamleiter in der Regelkommunikation aufmerksam werden, wenn es was zu verbessern gibt. Dann geht es natürlich, je nach Umfang, hoch zu der jeweiligen Entscheidungsebene. Möglicherweise ist es nur eine kleine Anpassung, die vom Team- oder Bereichsleiter selbstständig, sodass es die Geschäftsleitung am Ende des Tages vielleicht noch nicht einmal mitkriegt. Insbesondere wenn es zum Beispiel nur Kleinigkeiten, wie die Videoüberwachung des Geschäftseingangs oder des Lagers, sind. Solche Maßnahmen werden nicht bis zur Geschäftsleitung eskaliert.

I: Sie sind aber trotzdem der Ansicht, dass hier noch Verbesserungspotenziale in der Koordinierung bestehen?

Herr E.: Ja, das ist ein guter Hinweis. Ich könnte mir vorstellen, dass man noch regelmäßiger und aktiver die Mitarbeiter motiviert und anregt, was man unter diesem Aspekt besser machen kann. (…). Vielleicht kann man das auch über das Qualitätsmanagementsystem einbinden, weil wir ja im Sinne von ISO 9001 QM-zertifiziert sind und damit eigentlich einen kontinuierlichen Verbesserungsprozess initiiert haben. Möglicherweise kann man das benutzen, um das Thema Informationssicherheit zu integrieren, weil ich meine, dass dies derzeit nicht maßgeblich dazugehört. Das ist nochmal ein guter Hinweis.

I: Also bestehen Ihrer Ansicht nach auch hier noch Verbesserungspotenziale?

Herr E.: Ja, dort kann man noch besser werden.

I: Beim Stichwort Mitarbeiter ist ja besonders auch die Loyalität und Zufriedenheit der Mitarbeiter ein maßgeblicher Faktor zur Schaffung von Sicherheit. Inwieweit erhalten Mitarbeiter eine leistungsgerechte Entlohnung? Erhalten sie auch immaterielle Anreize?

Herr E.: Ich denke, dass das ein sehr wichtiger Punkt ist, den Sie hier ansprechen, wenn es nicht sogar einer der maßgeblichsten Punkte ist. Das Thema Motivation (…) ist sehr wichtig. Und ich glaube, dass von den Mitarbeitern, die frustriert und genervt sind eine unheimlich große Gefahr ausgeht, was anfangs zu einem sehr luschigen Umgang mit Informationen und bis zu einer absichtlichen Schädigung des Unternehmens theoretisch führen kann. Was heißt theoretisch? Leider auch praktisch dazu führen kann. Insofern bin ich der Meinung, dass man dort unheimlich sensibel sein muss und nicht nur unter dem Aspekt der Leistungssteigerung motivieren sollte, sondern auch das unternehmenswichtige Daten und Informationen dort bleiben, wo sie sind. Das ist ein wichtiger Aspekt, den ich sehr hoch einschätze.

I: Gibt es denn auch einen Loyalitätsindex bei Ihnen im Unternehmen, der auf Basis der Motivation der Mitarbeiter sowie den Feedback- und Kommunikationsmöglichkeiten die Loyalität der Mitarbeiter misst?

Herr E.: Nein, was wir haben ist ein Leitbild und eine vor vier Jahren erarbeitete Vision, damit man mit den Mitarbeitern auch über Ziele sprechen kann, die erreicht werden müssen, um auch dieser Vision zu folgen. (…). Das Leitbild unterteilt sich in die Betrachtungsweisen Kunde, Mitarbeiter, Shareholder und Partner sowie Lieferanten. Insbesondere hier wäre das Thema Mitarbeiter wichtig. Ich gebe zu, dass dies natürlich nur ein Soll-Zustand ist. Hier ist die Feedback-Kultur und das unterstützende Miteinander hervorzuheben, was von allen Führungskräften unterstützt werden soll. Das ist natürlich nur ein Soll-Zustand (…), den es möglichst ideal zu erfüllen gilt. (…). Das ist mit dem Index ist aber ein guter Punkt. Wir haben das versucht mit unserem Leitbild versucht niederzuschreiben und haben viele Workshops und Informationsveranstaltungen für Mitarbeiter durchgeführt. Das sind die wesentlichen Themen, die wir hier gestartet haben.

I: Kommen wir nach Akquisition, Auswahl, Einstellung und Management von Personal nun zur Personalentlassung? Inwieweit gibt es auch Sicherheitsmaßnahmen bei der Beendigung eines Arbeitsverhältnisses?

Herr E.: Was wir zuerst rein materiell machen ist natürlich, dass wir sichergehen, dass die Materialien, die der Mitarbeiter bekommen hat, zurückgegeben werden. Ob das Schlüssel, Ausweise, Laptop und Datenträger angeht. Das wird über einen Laufzettel organisiert und am Ende des Tages wird dann geschaut, ob auch alles zusammengekommen ist. Das ist eher die rein materielle Betrachtungsweise. Was wir zusätzlich ungefähr vor einem halben Jahr neu eingeführt haben ist, dass wir beim Ausscheiden eines Mitarbeiters ein Abschiedsgespräch führen. Das Ganze hat aber weniger einen Aspekt der Informationssicherheit, sondern mehr einen Aspekt der Bereitschaft als Unternehmen dazulernen zu wollen. Das führe ich auch als Geschäftsführer selber durch, unabhängig davon was das für ein Mitarbeiter ist. Ob das eine Führungskraft oder ein handwerklicher Kollege ist. Das ist dabei nicht relevant. Auf der einen Seite möchte ich dem Mitarbeiter dann alles Gute für die Zukunft wünschen und auf der anderen Seite sicherlich auch herausfinden, was wir als Unternehmen besser machen können, weil es ja möglicherweise gute Gründe gibt, warum er das Unternehmen verlässt. Letztendlich ist das dann auch nochmal ein kleiner Check, ob der Mitarbeiter in Greul geht und ob er negative Gefühle äußert und ob man damit rechnen muss, dass er sich Sachen organisiert hat, die er eigentlich nicht haben darf. Ein klassisches Beispiel ist ja immer ein Vertriebler. Ob er die Kundendatei bereits schon abgezogen hat oder nicht und inwieweit er dann auf so etwas in seinem zukünftigen Leben darauf zurückgreift. (…). Wir haben es auch schon mal, nein, zweimal schon gemacht, wo wir von uns aus gesagt haben, dass es das nicht ist. Das war in der Probezeit. Einmal war es auch außerhalb, wo wir gesagt haben, dass jetzt Feierabend ist und von einem auf den anderen Tag hier nicht weitergearbeitet wird und der Mitarbeiter freigestellt wird. Das ist aber nicht bei jedem Mitarbeiter so. Wir haben auch schon einen Systemadministrator gehabt, der gegangen ist, aber der hat ganz normal bis zum letzten Tag weitergearbeitet, weil das Vertrauensverhältnis einfach dagewesen ist. In der IT-Branche sieht man sich sowieso immer mehrfach, sodass wir nicht davon ausgegangen sind, dass es Stressfaktoren gibt und er Informationen absaugt.

I: Herr E., Sie haben erwähnt das alle materiellen Gegenstände am Ende des Arbeitsverhältnisses abzugeben sind.

Herr E.: Ja genau, die hat er abzugeben.

I: Inwieweit funktioniert so etwas auch bei den Zugriffsrechten innerhalb der EDV? Werden hier auch mit Austrittsdatum alle Zugriffe gesperrt?

Herr E.: Ja genau, wir haben das über unseren Personaldienstleister (…) zentralisiert. Der hat dafür zu sorgen, dass am Ende des Tages alles an Bord ist und alle Aktivitäten durchgeführt sind. Dort gehören natürlich auch die Accounts dazu.

I: Gibt es denn auch einen Unterschied zwischen regulärem und nicht einvernehmlichen Ausscheiden?

Herr E.: Ja klar, in dem Moment, wo Stress entsteht. Wir haben auch ein Fall gehabt, wo ein Mitarbeiter auf personenbezogene Daten unberechtigter Weise Zugriff genommen hat und sich darüber Vorteile verschaffen wollte und darüber hinaus noch urheberrechtlich geschützte Kinofilme auf seinem Dienstrechner hatte. Dort wird dann unmittelbar die Reißleine gezogen.

I: Ok. Sprechen wir noch einmal über firmeneigenes und firmenfremdes Personal. Gibt es dort annähernd die gleichen Sicherheitsvorkehrungen und Sicherheitsstandards, die für firmeneigenes und firmenfremdes Personal gelten?

Herr E.: Ich bin gerade am überlegen. Ja, wir haben einige Berater, die für uns tätig sind. Das stimmt, aber genaueres weiß ich hierzu auch nicht. Dort müsste ich mich erst schlau machen. Also die Berater haben natürlich keinen Zugriff auf die Laufwerke und das Datennetz (…). Im Grunde gibt es aber ein Regularium, das für Mitarbeiter und externe Mitarbeiter wie Leiharbeit gilt. Ein Externer, der uns von einer Zeitarbeitsfirma für ein halbes Jahr unterstützt, bekommt natürlich nur eingeschränkte Berechtigungen. Das wird dann immer mit den jeweiligen Vorgesetzen abgestimmt, denn der Rechenzentrumsmitarbeiter wird ja nicht auf einen Anruf von wem auch immer reagieren und irgendwelche Berechtigungen oder auch SAP freischalten. Da gibt es eine klare Vorgehensweise, aber grundsätzlich ist das unabhängig, ob es ein interner oder externer Mitarbeiter ist. Das Prozedere ist bei den Administratoren aber klar formuliert. Darüber gibt es Prozessbeschreibungen.

I: Gut. Damit wären wir mit dem ersten Teil der personellen Sicherheitsmaßnahmen fertig. Nun ist der organisatorische Schutz die zweite Säule in einem ganzheitlichen Informationsschutz. Inwieweit gibt es denn formal fixierte Standards in Ihrem Unternehmen, die vor Know-how-Abfluss schützen sollen?

Herr E.: Können Sie das noch ein wenig präzisieren?

I: Ja. Ein Beispiel wäre ein Clean-Desk-Policy, die besagt, dass nach Arbeitsschluss alle sensiblen Informationen vom Schreibtisch entfernt und verschlossen werden müssen.

Herr E.: Ok. Was wir gemacht haben ist, dass wir Anweisung herausgegeben haben, die beinhaltet, dass keine Angebote auf den Tisch zu liegen haben, wenn Feierabend ist. Das heißt, dass die Unterlagen in den jeweiligen Schränken verschlossen werden. Was wir auch gemacht haben ist, dass wir eine Anweisung herausgegeben haben, die besagt, dass keine Laptops in der Dockingstation über die Nacht oder das Wochenende liegen dürfen. Es sei denn, dass sie wirklich (…) fest verschlossen sind, quasi angekettet. Oder das Laptop muss im Schrank verschlossen werden. Das sind beispielhafte Anweisungen, die herausgegangen sind. Ich bin gerade am überlegen, ob diese Anweisungen auch regelmäßig überprüft werden. Das ist nochmal ein interessanter Hinweis, wer und wann Kontrollen durchführt werden. Ich glaube, dass wir das noch nicht konsequent umgesetzt haben. Es ist natürlich schlau eine Regelung herauszugeben und diese zu wiederholen (…), aber das andere ist das tatsächliche kontinuierliche Nachprüfen

I: Das wäre nämlich noch eine Frage von mir gewesen.

Herr E.: Ja, das machen wir bis jetzt noch nicht. Da haben wir noch Verbesserungspotenzial.

I: Gibt es denn auch Bestimmungen zur Nutzung, Vervielfältigung und Vernichtung von Informationsbeständen?

Herr E.: Was wir gemacht haben ist das Aufstellen dieser schwarzen Kisten, wo man Datenträger wie CDs, DVDs und natürlich auch Papier vernichten kann. (…). Aber eine Verfahrensanweisung zur Vernichtung…nein, das haben wir nicht. Nein, das haben wir noch nicht formuliert. Das wäre noch ein guter Hinweis, dass man das noch einmal niederschreibt.

I: Herr E., Sie hatten bereits erwähnt, dass es einen Sicherheitsverantwortlichen in Ihrem Unternehmen gibt und die Geschäftsführung auch für den Informationsschutz verantwortlich ist. Inwieweit glauben Sie, dass gerade unter dem Druck des Informationsverlustes, unter dem Unternehmen stehen, weitere Personaleinstellungen in diesem Bereich getätigt werden?

Herr E.: Also wir gehen davon aus, dass wir erst einmal damit auskommen. Wir sind nun einmal ein mittelständisches Unternehmen mit 120 Mitarbeitern und gehen auch davon aus, dass wir das auch so über die Bühne kriegen, ohne dass wir weitere Leute einstellen. (…). Der

Sicherheitsverantwortliche tauscht sich aber auch mit Kollegen anderer Unternehmen in Treffen, die mehrmals im Jahr stattfinden, aus.

I: Ist der Sicherheitsverantwortliche denn auch organisatorisch an die Geschäftsführung angebunden?

Herr E.: Ja, zu diesem Thema berichtet er insbesondere an mich. Sein nächster Vorgesetzter aus der Linienorganisation ist natürlich auch immer informiert. Das ist klar.

I: Gibt es denn, wie bei angesprochenen Sicherheitsverstößen, auch Sanktionierungen in Ihrem Betrieb?

Herr E.: Ja, das beginnt bei einer luschigen Handhabung. Wenn zum Beispiel irgendein Blatt auf dem Kopierer liegt, was dort nicht zu liegen hat. Dort weist man natürlich freundlich konstruktiv hin (…) allgemein erntet man dort auch sofort Verständnis. Das funktioniert dann eigentlich auch. Bis hin zu dem genannten Beispiel, wo sich ein Mitarbeiter personenbezogene Daten gezogen hat, um selbst daraus Vorteile zu ziehen. Das kann dann letztendlich bis hin zu fristlosen Kündigung führen.

I: Gibt es denn auch Schadensersatzansprüche, die gestellt werden?

Herr E.: Bisher hat es noch keinen messbaren Schaden diesbezüglich gegeben, sodass solche Forderungen auch nicht gestellt wurden.

I: Gibt es denn auch im umgekehrten Fall, in dem sich ein Mitarbeiter sicherheitsbewusst verhält und bei der Entwicklung von Sicherheitsmaßnahmen einbringt, materielle oder immaterielle Belohnungen?

Herr E.: Nein, materieller Art definitiv nicht. Wir haben uns schon vor drei Jahren gegen ein formales Verbesserungs- und Vorschlagswesen entschieden, weil wir der Meinung sind, dass der administrative Aufwand den Effekt nicht rechtfertigt und darüber hinaus glauben, dass wir durch die vorgelebte Unternehmenskultur Mitarbeiter automatisch motivieren in ihrem Job-Umfeld immer besser zu werden und dementsprechend auch immer Verbesserungen über ihre Vorgesetzten hereinbringen. Insofern gibt es kein Vorschlagswesen, wie man es aus produzierenden Unternehmen kennt. (…). Betrachtet man die immateriellen Reaktionen, so verstehen wir hierunter unsere Feedback-Kultur, die wir so gut es geht vorleben. Ich gebe zu, dass der ein oder andere auch noch höhere Bedürfnisse hat. Also die Anerkennung von guter Leistung,

wie betriebliche gute Leistungen oder im Sinne einer Idee zum Informationsschutz. Diese Feedback-Kultur soll im Idealfall dazu dienen, dass sich Mitarbeiter im Unternehmen gut aufgehoben fühlen und dementsprechend hochgradig loyal dem Unternehmen gegenüber aufgestellt sind.

I: Ja. Damit ist der Bereich der organisatorischen Sicherheitsmaßnahmen abgeschlossen. Gibt es denn auch im Bereich Technik (...) bautechnische Maßnahmen, die den Zugang zu sensiblen Unternehmensdaten schützen?

Herr E.: Also wir haben hier im Unternehmen für unser Lager eine Einbruchsmeldeanlage (…). Zusätzlich haben wir die Außenhaut videoüberwacht. Dann haben wir ein entsprechendes Zutrittskontrollsystem, was nicht nur die Haupttüren, sondern auch die elektronischen Verschließungen für die einzelnen Bürotüren betrifft. Das sind eigentlich die maßgeblichen Dinge. Zusätzlich hatten wir auch unser Rechenzentrum, das gerade umgebaut wird, mit einem biometrischen Zutrittskontrollsystem ausgestattet, also mit einer Iriserkennung. Das ist im Moment aber nicht ganz scharf. (…). Dieses System ist auch im Treppenaufgang installiert, wobei das hier eher einen Marketingeffekt hat. (…). Mit dem normalen Ausweis kann man aber auch die Tür öffnen.

I: Gibt es den auch abhörschutzsichere Räume?

Herr E.: Nein, die haben wir nicht.

I: Kommen wir zum Bereich der Sicherung der Informations- und Kommunikationstechnik. Welche Sicherheitsmaßnahmen bestehen hier?

Herr E.: Wenn wir das Datennetz betrachten, haben wir die entsprechenden Firewalls dieser Welt, Content-Filter sowie Antivirus und Antispam. (…). Das haben wir gerade letztes Jahr wieder über einen Penetrationstest beziehungsweise über einen beauftragten Hackerangriff gecheckt. Einmal von außen und einmal von innen. Das heißt der hat auch hier in den Räumlichkeiten gesessen, einen freien Port genommen und hat geschaut inwieweit er auf welche Systeme kommt. Darüber gibt es natürlich einen Bericht und diesen Bericht sind wir dann auch mit dem entsprechenden Sicherheitsverantwortlichen durchgegangen. Dort haben wir geschaut was wir noch besser machen können und welche Einstellungen noch besser umgesetzt werden können.

I: Herr E., Sie hatten bereits angesprochen, dass jeder Mitarbeiter seinen eigenen Account und sein eigenes Passwort hat. Inwieweit gibt es diesbezüglich auch einen systematischen Passwortwechsel?

Herr E.: Ja, genau. Es gibt einen systematischen Passwortwechsel. Das ist auch nicht mit vier Zahlen getan, sondern muss auch ein bisschen komplizierter mit Groß- und Kleinschreibung sowie Buchstaben, Zahlen und Sonderzeichen aufgebaut werden. Diese Bedingungen habe ich jetzt aber nicht genau parat. (…). Wenn aber zum Beispiel innerhalb von zehn Zeiteinheiten wieder versucht das gleiche Passwort zu nehmen, dann wird das nicht funktionieren. Ich kenne die Richtlinien jetzt nicht genau, aber das ist schon ziemlich aufwendig.

I: Könnten Sie noch einmal sagen welche expliziten Sicherheitsmaßnahmen auf Basis dieses Penetrationstests durchgeführt wurden?

Herr E.: Also was der gecheckt hat?

I: Ja, was der gecheckt hat und was letztendlich auch die Konsequenzen waren.

Herr E.: (…). Es wurde auf jeden Fall von außen die Domain penetriert und es versucht ins Datennetz einzudringen. (…). Dasselbe wurde auch noch einmal von innen durchgeführt, indem versucht wurde auf die virtuelle Netzte, soweit wie möglich, zu gelangen. Zur Erleichterung habe ich ihm dann nach einem halben Tag noch eine IP-Adresse gegeben, um den Angriff zu erleichtern. (…).

I: Würden Sie denn grundsätzlich bestätigen, dass das Ergebnis dieses Test war, dass das Informations- und Kommunikationsnetz sicher ist?

Herr E.: Naja, wir haben schon einige Baustellen identifiziert. Zum Beispiel haben wir (…) einen Automatismus gehabt, durch den man als interner Nutzer sofort einen Port zugewiesen kriegt. Diesen Automatismus haben wir bewusst drinnen gehabt, der aber daraufhin bewusst abgestellt wurde, damit auch nur entsprechend angemeldete Ports freigeschaltet werden. Aber ich muss zugeben, dass ich dort technisch nicht tief genug drin bin. (…).

I: Kommen wir zum Schluss zu den rechtlichen Sicherheitsmaßnahmen. Sie hatten bereits Geheimhaltung- und Wettbewerbsvereinbarungen zwischen Ihrem Unternehmen und den Mitarbeitern angesprochen. Gibt es solche Vereinbarungen auch zwischen Ihrem Unternehmen und Partnerunternehmen?

Herr E.: Das ist ein guter Hinweis. (…) ich weiß darüber aber nichts genaues. Dazu muss ich leider passen.

I: Sie hatten ja bereits im Bereich der Personalfreistellung Sanktionierungen angesprochen. (...). Könnte man sich auch seitens der Geschäftsführung vorstellen, dass Schadensersatzansprüche geltend gemacht werden?

Herr E.: Klar. Das können wir uns auf jeden Fall vorstellen. In dem Moment, wo ein entsprechender Schaden entsteht, muss man rechtlich prüfen, was dort möglich ist. Ich bin natürlich kein Rechtsexperte, aber je nach Vorfall gilt es dies zu hinterfragen und gegebenenfalls rechtlich einzufordern.

I: Herr E., Sie haben im Gespräch auch die QM-Zertifizierung nach ISO 9001 genannt. Gibt es Sicherheitsvorkehrungen zwischen Ihnen und der Zertifizierungsgesellschaft? Letztendlich kann sich ein Informationsverlust auch bei der Zertifizierungsgesellschaft ereignen, was zur indirekten Schädigung Ihres Unternehmens führt.

Herr E.: (…). Stimmt. Im Managementhandbuch sind diverse Prozesse formuliert (…). Um solche Sicherheitsvorkehrungen haben wir uns aber nicht weiter gekümmert. Ich gebe zu, dass wir dort ein bisschen gutgläubig sind.

I: Gibt es denn gewisse Patente auf technische Innovationen, die Sie angemeldet haben?

Herr E.: Nein, wir haben keine Patente. (…).

I: Herr E., damit sind wir am Ende des Interviews. Ich darf mich herzlich bei Ihnen bedanken.

Beurteilung des Interviews:

Dieses Gespräch bildete den Auftakt einer Reihe von Interviews mit Geschäftsführern und Sicherheitsverantwortlichen unterschiedlicher Unternehmen. Mit einer Dauer von circa einer Stunde konnte der angestrebte Zeitrahmen eingehalten werden. Inhaltlich waren die Aussagen gut verwertbar, wenn auch der Interviewpartner zu manchen Fragestellungen nicht genaue Auskünfte geben konnte.

B2 Transkript 2

Name:	Herr B.
Position:	Leiter Risk und Revision, Firma U.
Datum:	31.03.2011
Zeitraum:	10.00 - 11.00 Uhr

Interviewer (I): Herr B., ich darf Sie nochmals herzlich begrüßen und mich bedanken, dass Sie sich die Zeit nehmen an diesem Interview teilzunehmen. Ich werde Ihnen jetzt in den nächsten 60 Minuten Fragen zur Risikoanalyse, zur Risikobewertung und zu den präventiven und repressiven Spionageabwehrmaßnahmen in Ihrem Unternehmen stellen. Ich werde hierbei auf die Bereiche Personal, Organisation, Technik und Recht eingehen. (…). Um Industriespionage wirkungsvoll begegnen zu können, empfiehlt sich zunächst eine Risikoanalyse. Inwieweit wurde bei Ihnen im Unternehmen denn eine Risikoanalyse durchgeführt, um spätere Know-how-Schutzmaßnahmen ergreifen zu können?

Herr B.: Danke. Ich kann Ihnen die Frage beantworten, dass wir hier differenzieren müssen. Zum Know-how-Schutz oder Informationsschutz wurden in unserem Unternehmen bisher keine Risikoanalysen durchgeführt. Unser Unternehmen beschäftigt sich ja mit Geld- und Werttransport sowie -bearbeitung und -einlagerung. Dort auf die physische Sicherheit fokussiert, werden natürlich Risikoanalysen und Gefährdungsanalysen erstellt, aber nochmals in Bezug auf den Know-how-Schutz wurden und werden im Moment (…) keine Analysen durchgeführt.

I: Sie sprachen an, dass auf der materiellen Seite durchaus Risikoanalysen werden.

Herr B.: Das ist korrekt.

I: Können Sie spezifizieren welche Bereiche, das heißt Personal, Organisation, Technik, Recht, hierbei die größten Risiken aufweisen?

Herr B.: Das größte Gefährdungspotenzial, insoweit, dass hieraus der größte Schaden resultieren könnte, wäre der Bereich Personal und Bereich Arbeitsorganisation/Prozessgestaltung an den jeweiligen Standorten, an denen wir unsere Dienstleistung erbringen.

I: Können Sie denn den ein oder anderen Vorfall im Bereich Personal schildern?

Herr B.: Ja, (…). Ein Mitarbeiter oder Bewerber, der bei uns Dienstleistung erbringen will, Arbeit aufnehmen will, wird im Rahmen der behördlichen Verfahren auf Zuverlässigkeit überprüft und hat, wenn er eingesetzt wird und Waffenträger ist, auch das behördliche Verfahren zu durchlaufen. Also waffenrechtliche Zuverlässigkeit vorzuweisen. Darüber hinaus muss jeder Mitarbeiter einmal im Jahr ein polizeiliches Führungszeugnis vorlegen, dass aber (…) nicht hinreichend aussagekräftig ist. So sind uns also in der entsprechenden Überprüfung der Zuverlässigkeit ein wenig die Hände gebunden. Wir müssen uns daher des einen oder anderen Kanals bedienen, um eine nicht personifizierte, aber grundsätzliche Aussage zu erhalten, ob außer auf dem polizeilichen Führungszeugnis ausgewiesene Tatbestände etwas vorläge. Wir fragen an und bekommen „grün" oder „rot" für den Mitarbeiter und fragen auch nicht weiter nach. Der Mitarbeiter scheidet zu diesem Zeitpunkt aus, wenn er „rot" erhält. Das ist aber ein auf Gentleman Agreement basierende Behelfslösung. Es ist uns in Bezug auf Personal mittlerweile durch umfangreichen Streit mit Landesdatenschutzbeauftragten und auch Bundesdatenschutzbeauftragten nicht einmal mehr möglich von den Mitarbeitern SCHUFA-Auskünfte abzufragen. Das ist also pure Freiwilligkeit, wenn diese SCHUFA-Auskünfte zur Verfügung gestellt werden. In Bezug auf die Organisation kann ich sagen, dass wir von der physischen Gestaltung eines Centers das wir neu planen bis hin zur Arbeitsgestaltung innerhalb des Centers, eingehend Risikoanalysen durchführen, um auch den Erfahrungen im europäischen Wettbewerb Rechnung zu tragen, sodass wir etwaige Gefährdungspotenziale und Zugriffsmöglichkeiten auf das Geld minimieren. In Bezug auf Technik kann ich sagen, dass wir eine Netzwerkstruktur über die 21 Standorte gelegt haben. Dies beinhaltet ein Rechenzentrum, was gespiegelt wird. In Bezug auf Recht in Verbindung mit Personal, kann ich sagen, dass wir Risikoanalysen in Bezug auf Vertragsmanagement und ähnliches zwar auch erbringen, die aber eher als Beratung für unser Servicecenter (…) angesiedelt ist.

I: Als nächster Schritt nach der Risikoanalyse erfolgt die Risikobewertung. (...). Gibt es denn nach der Schadenshöhe und der Schadenseintrittswahrscheinlichkeit noch weitere Parameter, die für eine Risikobewertung herangezogen werden(...) oder sind das die maßgeblichen Größen?

Herr B.: Die Schadenswahrscheinlichkeit ist die eigentliche maßgebliche Größe, weil sie hier auch umfasst, dass es hinsichtlich Prozessreifegrad im Arbeitsprozess Prozesse gibt, die einen Schaden wahrscheinlicher machen und dann entsprechend umzuorganisieren wären. (…).

I: In der Literatur werden ja zusätzlich auch Parameter wie ideeller Wert der Betriebsgeheimnisse und Größe des Personenkreises mit Zugriff beschrieben.

Herr B. Ja, das ist bei uns ein wenig differenziert zu betrachten. Anders als ein (…) innovativer Betrieb, der neue Autos, neue Techniken baut, sind Innovationen bei uns auf einen sehr engen Bereich beschränkt. Insofern erbringen wir hauptsächlich Dienstleistung, wiewohl wir innovativ hinsichtlich Geldautomaten weiterdenken. (…). Das sind aber, wenn ich Sie richtig verstehe, keine schützenswerten Informationen wie in einem Automobilkonzern oder ähnlichem. Unser Informationsschutz beschränkt sich an sich auf die Verwaltung der entsprechenden Abrechungsdaten, dass wir sicherstellen, dass die entsprechenden Kontoverbindungen der uns angeschlossenen Auftraggeber, für die wir treuhänderisch deren Konten verwalten, entsprechend sicher in der Hauptverwaltung abgelegt sind, sodass auch kein Zugriff von unternehmensinternen Abteilungen auf diese Daten vorgenommen werden kann. (…).

I: Ergibt sich denn auf Basis der Risikoanalyse und Risikobewertung auch eine Prioritätenliste oder ein Handlungskatalog?

Herr B.: Ja, auch hier wieder differenziert auf die physischen Standorte bezogen. Wir unterziehen diese Standorte mehrmals im Jahr unangekündigt Kontrollen. Diese Kontrollen umfassen circa 170 unterschiedliche Aspekte. Diese Aspekte werden im Sinne einer ABC-Priorisierung bezüglich der Abstellungsnotwendigkeit und des daraus resultierenden Zeitraums priorisiert und bewertet. Darüber hinaus betrachten wir die Prozesse unangemeldet und unangekündigt ebenfalls mehrfach im Jahr hinsichtlich der Geldflüsse, die stattfinden. Die angesprochenen Bereiche werden zeitgleich oder unabhängig von uns auch durch die uns zur Verfügung stehenden Risikoträger wie Versicherer in gleichen Art und Weise durchgeführt.

I: Kommen wir zum Schwerpunktthema Personal. Inwieweit werden Sicherheitsmaßnahmen bezüglich der Personalakquisition durchgeführt? Werden über die Stellenausschreibungen schon sensible Daten publiziert oder wird hier sehr auf Diskretion geachtet.

Herr B.: Wenn Sie die Stellenausschreibung, die dann öffentlich wäre, im Sinne eines neuen Mitarbeiters als sensibel betrachten, wird dies kommuniziert (…). Darüber hinaus wird in der Stellenausschreibung kein sensibles Datum gegeben. Weder wird spezifiziert für welchen Standort gesucht wird. Das ist aber über die entsprechende Pressemitteilung ziehbar. (…). Wenn der Bewerber sich zu erkennen gibt wird, wie gesagt, überprüft und darüber hinaus

lassen wir, bevor er seinen Arbeitsvertrag zur Unterschrift bekommt, auch noch eine Umfeldbeobachtung durchführen. Wir betrachten also auch die persönlichen Lebensumstände.

I: Also sind auch keine Technologien, die der Mitarbeiter später verwendet, in Stellenausschreibungen vorhanden?

Herr B.: In gar keinem Fall.

I: Sie haben gerade angesprochen, dass auch eine intensive Überprüfung der Bewerber stattfindet und hatten angesprochen, dass der Lebenslauf einer Überprüfung unterzogen wird. Gibt es denn weitere Merkmale einer solchen Überprüfung?

Herr B.: Die Merkmale einer solchen Überprüfung lassen sich zusammenfassen auf zuverlässigkeitserhebliche Merkmale, also Umfeldbeobachtung und sonstige auffälligkeitsfestellenden Beobachtungsmerkmale. Wir machen oder lassen das einzelfallbezogen durchführen. Wir können nicht jeden Geld- und Werttransportdienstmitarbeiter in der gleichen Tiefe überprüfen, aber je höher und verantwortungsvollen die Aufgabe wird, umso tiefer wird auch unserer Prüfauftrag.

I: Sie hatten im Vorfeld des Interviews die erhöhte Gewaltbereitschaft von möglichen Tätern im osteuropäischen Raum angesprochen. Gibt es in Ihrem Unternehmen auch Kriterien, die Bewerber aus gewissen Ländern ausschließen?

Herr B.: Das ist eine interessante Frage. Wir haben unseren Mitarbeiterstab oder die Bewerbergruppe noch nicht dahingehend ausgewertet, ob Präferenzen Personen der einen oder der anderen ethnischen Herkunft haben. Generell ist in unserer Branche zu sagen, dass man froh sein muss, wenn sich überhaupt jemand bewirbt. Wir haben also eine Menge (…) an ungelernten Mitarbeitern. (…). Es wird bei uns generell kein Ausschlusskriterium sein, ob jemand einen Hintergrund aus Osteuropa hat, wiewohl ich nicht verhehlen möchte, dass wir dort sehr genau hinschauen wen wir einkaufen und auf etwaige personelle und familiäre Verpflichtungen achten.

I: Gibt es bei der Überprüfung des Lebenslaufs auch Kontakt zu früheren Arbeitgebern des Bewerbers?

Herr B.: Das findet im Einzelfall statt.

I: Bestehen auch Kontakte zu polizeilichen und nachrichtendienstlichen Behörden?

Herr B.: Im Rahmen der offiziellen Anfragen findet das nicht statt.

I: Gut. Kommen wir nachdem wir die Personalakquisition und das Personalauswahlverfahren angesprochen haben, zu der Personaleinstellung. Gibt es dort spezifische Sicherheitsmaßnahmen Ihres Unternehmens? Das heißt also, dass Sicherheitsbelehrungen sowie Datenschutz- und Geheimhaltungsverpflichtungen bestehen.

Herr B.: Die gibt es auf jeden Fall. Sie werden jeweils auch entsprechend dokumentiert, abgefragt und abgelegt.

I: Sie hatten auch den Fall angesprochen, dass Vertriebsmitarbeiter Ihres Unternehmens zum Konkurrenten gewechselt sind. Gibt es denn auch Konkurrenzklauseln und nachvertragliche Wettbewerbsverbote?

Herr B.: Meines Wissens nach nicht rechtswirksam.

I: Ok. Wir hatten gerade angesprochen, dass der Informationsschutz noch Verbesserungspotenziale bei Ihnen im Unternehmen aufweist. Kann man dennoch sagen, dass Informationsschutz als Chefsache betrachtet wird und die Geschäftsführung dementsprechend auch mit gutem Beispiel vorangeht?

Herr B.: Den ersten Teil Ihrer Frage kann ich bejahen. Informationsschutz wird und wurde als Chefsache angesehen. Den zweiten Teil muss ich verneinen, denn der Mitbegründer und Mitgesellschafter hatte zum damaligen Zeitpunkt einer privaten Nutzung der Firmenlaptops zugestimmt, die ich im Zuge der Abwanderung einer kompletten Vertriebsabteilung zeitgleich zu einem großen Mitbewerber, gerne auch ausgewertet gewusst hätte. Das wurde mir allerdings verwehrt, da ich gleichzeitig auch Kenntnis über private auf dem Rechner verbrachte Daten hätte erlangen können, was mich in Konfrontation zu geltendem Recht gestellt hätte.

I: Sie hatten angesprochen, dass der Informationsschutz in Ihrem Unternehmen schon als Chefsache behandelt wird. Inwieweit findet denn auch eine Sensibilisierung und Schulung der Mitarbeiter bezüglich dieses Themas statt?

Herr B.: In Bezug auf Datenschutz und in Bezug auf Geldwäsche ist dies regelmäßig, halbjährlich vorhanden. In Bezug auf Informationsschutz, eines ungewollten oder gewollten Datenabflusses gegenwärtig gar nicht.

I: Das heißt hier wären auf jeden Fall Verbesserungspotenziale in Form von Schulungen und Informationsveranstaltungen für Mitarbeiter möglich?

Herr B.: Absolut. Wir sind gegenwärtig als Fachabteilung dabei unter dem Arbeitsprozessgesichtspunkt dies zu steuern und dort entsprechende Mauern zu ziehen. Es wird in absehbarer Zeit, also noch in diesem Jahr dazu kommen, dass sämtliche Firmenlaptops nicht mehr extern kopiert oder nicht mehr extern auf Firmenlaptops Zugriff genommen werden kann, seitens USB und seitens der vorhandenen technischen Möglichkeiten. Das ist identifiziert, aber es ist noch nicht umgesetzt.

I: Kann man insofern auch sagen, dass noch keine großflächige Einbindung der Mitarbeiter erfolgt ist?

Herr B.: Ja, in Bezug auf diesen Aspekt nicht.

I: Herr B., wir hatten bereits im Vorfeld des Interviews angesprochen, dass die Loyalität und die Zufriedenheit der Mitarbeiter wichtige Punkte sind, die zum Informationsschutz im Unternehmen beitragen. Inwieweit können Sie Auskünfte darüber geben, ob die Mitarbeiter leistungsgerecht entlohnt werden und inwieweit erhalten die Mitarbeiter auch unentgeltliche Anerkennung für ihre beruflichen Leistungen?

Herr B.: Unsere Mitarbeiter, so sie an den Standorten arbeiten und sich nicht im Angestelltenverhältnis befinden, sondern im normalen Lohn stehen, werden tarifgerecht entlohnt. Inwieweit das angemessen ist, lege ich mal in Ihre Beurteilung. Wir haben Bundesländer, deren Tarife bei einem Stundenlohn zwischen 5 und 7 Euro liegen. Das ist sehr herausfordernd hieraus sein Lebensunterhalt zu bestreiten. Unsere Mitarbeiter arbeiten in den Standorten grundsätzlich 170 bis maximal 200 Stunden. (…). Ich halte die tarifliche Entlohnung nicht für ausreichend, gleichwohl gibt es aber auch noch Mitbewerber, der sogar diese tarifliche Entlohnung unterschießt. Wir bewegen uns in der tariflichen Zahlung zwischen 5 und 14 Euro pro Stunde innerhalb von Deutschland. Innerhalb unserer Unternehmensgruppe kann ich sagen, dass wir ausschließlich tarifgerecht oder sogar übertariflich entlohnen, weil wir erkannt und verinnerlicht haben, dass die zu zahlenden Werte zu verbessern sind.

I: Sie hatten gerade den materiellen Gesichtspunkt angesprochen. Gibt es auch unentgeltliche Anerkennung?

Herr B.: Es gibt immaterielle Incentives über einen entsprechenden Versicherungsschutz, den wir unseren Mitarbeitern bieten. Das betrifft zum Beispiel den Aspekt einer rund um die Uhr, weltweitgeltenden Unfallversicherung, die auch den Fall abdecken würde, dass wenn der Mitarbeiter verunfallt und nicht mehr arbeiten kann. Diese stellt sogar sicher, dass der Arbeitnehmer einen anderen adäquaten Arbeitsplatz, selbst wenn er nicht in unserer Unternehmensgruppe liegt, erhält. Der Mitarbeiter wird auch auf entsprechenden Reha-Maßnahmen begleitet und es werden ihm alle administrativen Aufgaben abgenommen. (…). Das betrifft auch Aspekte, dass wir den Mitarbeitern eine Entgeltumwandlung angeboten haben, um auch kapitalbildende Versicherungen zu bedienen und ein Mehr am Ende ihres Berufslebens erwirtschaftet zu haben. Das sind Incentives, die von Seiten des Unternehmens zur Verfügung gestellt werden.

I: Nun hatten wir gerade den Punkt der materiellen und immaterielle Anreize angesprochen. Gibt es denn auch Instrumente in Ihrem Unternehmen, die die Zufriedenheit und die Loyalität der Mitarbeiter messen?

Herr B.: Es finden in regelmäßigen Abständen, jeweils an den Standorten, aber auch in der Hauptverwaltung, Personalgespräche statt. In den Personal- und Mitarbeitergesprächen wird die individuelle Leistung des vorher zu betrachtenden Zeitraums bewertet. Das führt in der Regel dazu, dass wenn dort ein außerordentliches Verhalten gespottet wird, dieses Verhalten auch im wahrsten Sinne des Wortes belohnt wird. Sei es durch eine permanente Lohnanhebung oder sei es durch eine öffentliche Belobigung und Einmalzahlung einer Anerkenntnisprämie.

I: Gut. Kommen wir nun, chronologisch gesehen, zu einer Beendigung eines Arbeitsverhältnisses. Welche Sicherheitsmaßnahmen bestehen hier allgemein und gibt es auch Unterschiede zwischen einem regulärem und einem nicht einvernehmlichen Ausscheiden?

Herr B.: Ja, diese Unterschiede gibt es. (…). Bei einem regulären Ausscheiden würde man dafür Sorge tragen, je nachdem welcher Mitarbeiter betrachtet wird, dass dieser Mitarbeiter nicht mehr die aktuellsten Datenbewegungen hat und aus entsprechender Kundenbeziehung herausgezogen wird, sodass das Arbeitsverhältnis, je nach Individuallage, sanft ausläuft. Das heißt Urlaub und dann Ausscheiden. Davon unabhängig, gerade auch aktuell, sind anlassbe-

zogene Beendigungen von Arbeitsverhältnissen. Hier wird sofort sichergestellt, dass der Mitarbeiter sämtliche Öffnungsgeheimnisse entzogen bekommt und die ihm zur Verfügung gestellten Kombinationen (…) umgestellt werden. Zusätzlich werden Zugangschips sofort und zwar in aller Regel vor dem Benachrichtigen der Mitarbeiter gesperrt. (…). Auch Dienstkleidung, sofern der Mitarbeiter Dienstkleidung trägt, wird eingezogen. All dies erfolgt dokumentiert und umfasst neben der Dienstkleidung auch die Einziehung von Dienstausweisen, mit denen sich unsere Mitarbeiter, sofern sie Außenverkehr haben, ausweisen müssen. Als besonderes Sicherheitsmerkmal hierzu ist vielleicht noch zu erwähnen, dass auch bei den Anlaufstellen unserer Mitarbeiter entsprechende Legitimationslisten hinterlegt sind, auf denen sich die Ausweiskopien, der dort berechtigt auftauchenden Mitarbeiter befinden, sodass ein Abgleich des dort auftauchenden Mitarbeiters auch anhand von Foto, Ausweisnummer und Unterschrift vor Ort erfolgen kann. Dieses Legitimationspapier wird dann eingezogen, die entsprechende Legitimationsliste also aktualisiert. Also wird jede Anlaufstelle auf das Ausscheiden eines Mitarbeiters hingewiesen.

I: Herr B., Sie haben erwähnt, dass relativ strikte Regelungen bei der Beendigung eines Arbeitsverhältnisses bestehen. Gibt es auch nach der Beendigung eines Arbeitsverhältnisses gewisse Überprüfungen der Marktsituation, also von Wettbewerbern und ehemaligen Mitarbeitern?

Herr B.: Grundsätzlich nicht.

I: Betrachten wir neben dem Eigenpersonal auch noch einmal das Fremdpersonal. Vielleicht zunächst einmal die Frage, gibt es überhaupt Fremdpersonal, wie Berater, Reinigungskräfte und Handwerker?

Herr B.: Ja, es gibt Fremdpersonal in unserem Unternehmen, wie zum Beispiel Reinigungskräfte und Handwerker. Jedes Fremdpersonal, wird wie eigenes Personal, in identischer Art und Weise überprüft. (…). Personelle ad-hoc-Veränderungen führen bei uns zum Verweigern des Zutritts.

I: Also wird kein Unterschied gemacht?

Herr B.: Es wird kein Unterschied gemacht. Der Unterschied betrifft nur die Sache, dass ich die Reinigungskraft nicht wie den Waffenträger behandele. Ich habe aber sämtliche Daten und Zuverlässigkeitsprüfungen, wohl aber nicht in die Tiefe wie bei einem Waffenträger. Viel-

leicht das noch als Ergänzung, Reinigungspersonal befindet sich zu keinem Zeitpunkt alleine in einem Center-Bereich, sondern steht immer mindestens unter technischer (…) also unter Kamera. Im Center-Bereich wird das Reinigungspersonal sogar immer begleitet. Lediglich der Verwaltungsbereich wird unbegleitet gereinigt. Dort befinden sich aber keine sensiblen Daten in den Standorten. Diese werden zentral in der Hauptverwaltung verwaltet.

I: Ich würde nun gerne zu den organisatorischen Sicherheitsmaßnahmen Ihres Unternehmens übergehen. Organisatorische Sicherheitsvorkehrungen bilden die zweite Säule eines ganzheitlichen Informationsschutzkonzepts und sind auch eng mit den personellen Sicherheitsmaßnahmen verbunden. Inwieweit wurden bei Ihnen im Unternehmen formal fixierte Sicherheitsstandards etabliert, um einen Know-how-Abfluss zu verhindern?

Herr B.: Auch hier wieder differenziert. Sofern sie formal fixierte Standards abfragen, die bei uns etabliert sind, kann ich das eindeutig bejahen, indem Regelungen des Bundesverbands fixiert wurden. Diese gelten für uns und diese belegen wir auch jährlich als eingehalten. Wenn Sie das auf Know-how-Abfluss beziehen, gibt es keine formal fixierten Sicherheitsstandards, die den Aspekt des Know-how schützen. (…).

I: Sprechen wir im Speziellen Sicherheitsstandards an, die auch in der Literatur genannt werden, wie eine Clean-Desk-Policy. Gibt es diese bei Ihnen im Unternehmen?

Herr B.: Sie wird teilweise gelebt, sie ist aber nicht angeordnet. Ich kann Ihnen aus eigener Erfahrung sagen, dass sie von der Geschäftsführung und Geschäftsleitung gelebt wird und vielleicht auch noch von regionalen Verantwortlichen. Mit Sicherheit wird sie gelebt an den jeweiligen Zählplätzen, denn dort kann kein Geld liegen bleiben. Dort wird gearbeitet bis das Geld ordentlich verwahrt wird. Insoweit muss ich mich vielleicht korrigieren. Ja, es gibt sie, das ist aber nur in Bezug auf die Zählplätze angewiesen. In Bezug auf die Verwaltung wird sie gelebt, ist aber nicht angewiesen.

I: Betrachten wir diesbezüglich auch noch einmal die Bestimmungen zu Nutzung, Vervielfältigung und Vernichtung von Informationsbeständen. Liegen dort gewisse Regelungen vor?

Herr B.: Unser zu vernichtendes Datenmaterial, das betrifft die Hauptverwaltung sowie die Standorte, wird durch einen zertifizierten Datenvernichter entsorgt. Hinsichtlich der Vervielfältigung ist das schon wieder schwieriger zu beantworten, da es bei uns, im Gegensatz zu

Großkonzernen, jedem möglich ist zum Kopierer zu gehen, frei zu kopieren und er sich nicht anmelden und nachhalten muss was er kopiert hat. Das existiert bei uns gegenwärtig nicht.

I: Ist das denn vielleicht geplant?

Herr B.: Ja, es ist auf absehbare Zeit, einhergehend mit einer erstmalig zu erarbeitenden IT-Richtlinie, geplant. Diese betrifft auch die Sicherheit der verwendeten Hardware betrifft. Natürlich ist unser Rechenzentrum, natürlich sind unsere Server zugangsgesichert, aber nochmals, Firmenlaptops oder ähnliches derzeit noch nicht. Dies wird dann in absehbarer Zeit mit Kopierer und Gangkopierer entsprechend eingeschliffen werden.

I: Nun spielt der Sicherheitsverantwortliche eine zentrale Rolle als zentraler Ansprechpartner und Koordinator in Sicherheitsangelegenheiten. Gibt es denn außer Ihrer Person noch weitere Sicherheitsverantwortliche in Ihrem Unternehmen?

Herr B.: (…). Neben meiner Person, und ich bin ja als Geschäftsleitungsmitglieds meinem Geschäftsführer für Personal und Finanzen direkt zugeordnet. Meine Mitarbeiter meiner Abteilung sind ebenfalls in sicherheitsverantwortlicher Dienstleistung draußen unterwegs. Zu verantworten habe ich die Anordnung und ich delegiere den Inhalt der Aufgaben und zum Teil auch die Verantwortung auf Regionalleiter, die dann in der Struktur wieder jeweils einen Cash- und einen Logistikleiter haben. So diversifiziert sich die Aufgabe, die dort übertragen wird und der Cash-Verantwortliche verantwortet die Sicherheit in seinem Center mit allen Mitarbeiter und der Logistik-Verantwortliche mit allen Fahrern. Wir haben pro Standort noch einen Standortsicherheitsverantwortlichen Mitarbeiter, der aber insoweit an den Regionalleiter und nicht an mich berichtet.

I: Das heißt die sicherheitsverantwortlichen Aufgaben werden ausgehend von der Geschäftsführung herunter delegiert?

Herr B.: Sie werden aufgefächert und werden delegiert auf die Standortorganisationen und innerhalb dieser Standortorganisation sind diese Aufgaben umzusetzen. Ich wiederum als übergeordnete Stelle kontrolliere die Umsetzung und gebe das Signal, wenn innerhalb eines festgelegten Zeitraums etwas nicht umgesetzt wurde und koordiniere auch die entsprechenden Folgemaßnahmen, sei es bis zur personellen Einzelmaßnahme des Verantwortlichen.

I: Inwieweit gibt es denn auch Zutritts- und Zugriffsrechte für firmeneigenes und firmenfremdes Personal zum Schutz von gefährdeten Daten, Objekten und Räumen?

Herr B.: In Bezug auf die Standorte, sind Zutritts- und Zugriffsrechte generell gegeben. Unsere Standorte sind zwiebelförmig aufgebaut und je nach Berechtigungsgrad bleiben Sie an der Folgetür stehen. Zutritte in sicherheitserhebliche Bereiche definiere ich als solche Bereiche, in denen unmittelbar Zugriff auf Geld genommen werden kann, können nicht eigenverantwortlich stattfinden. Sie müssen immer mindestens im Vier- oder sogar im Sechs- oder Achtaugenprinzip, sei es durch Zuschaltung von fremden Kamerabildern (…), erfolgen. Wenn wir Zutrittsberechtigungen innerhalb der Hauptverwaltung betrachten, ist lediglich sichergestellt, dass Besucher abgeholt werden. Aber ich weiß nicht wie es Ihnen gegangen ist. Ich glaube Sie standen eben auch alleine, es ist also niemand bei Ihnen geblieben.

I: Ja, das ist richtig.

Herr B.: Das ist natürlich anweisungswidrig. Insofern ist es auch immer das Dilemma, dass Angewiesenes nicht immer auch umgesetzt und gelebt wird. So definieren wir zunehmend unsere Anweisungen im Rahmen von zwingenden Prozessen, die kein Ermessen mehr erlassen. Das ist hier mit Besucherempfang etwas schwierig darzustellen.

I: Sie hatten gerade ja auch angesprochen, dass die besten Sicherheitsvorkehrungen nur greifen, wenn sie vom Personal umgesetzt und gelebt werden. Dementsprechend hatten Sie auch Kontrollen zu Überprüfung der Einhaltung der Sicherheitsmaßnahmen erwähnt. Können Sie Auskunft darüber geben wie die Kontrollen explizit ausgestaltet sind und in welchen Abständen die Kontrollen durchgeführt werden?

Herr B.: Die Kontrollen, und wir betrachten jetzt alle Standorte, finden permanent statt. Jeder Standort wird von uns mindestens zweimal im Jahr auf physische Sicherheit überprüft. Darüber hinaus mindestens zweimal im Jahr auf Salden, also auf Geldfluss, und auf Prozesssicherheit überprüft. Darüber hinaus finden Dienstleistungskontrollen auf den Touren verdeckt statt. Dabei werden Dienstleistungsqualität, Einhaltung von Sicherheitsvorschriften, behördliche oder unternehmenseigene Sicherheitsvorschriften überprüft. Hierüber werden Fotodokumentationen oder Filmdokumentationen gefertigt und gewonnene Erkenntnisse in Kooperation mit der Personalabteilung abgearbeitet. Zudem, ich führte es ja schon aus, führt auch der Versicherer unabhängig von uns, teilweise aber auch in Kooperation mit uns und meiner Fachabteilung, die entsprechenden Kontrollen gleichartig durch, sodass ich hier noch einmal eine Verdichtung ergibt. Zudem finden auch unangekündigte Arbeitgeberkontrollen statt. Auch diese Mitarbeiter und Revisionisten, die dort auftauchen, sind bei uns anzumelden und es sind

entsprechende Personaldaten, wie Personalausweisnummer, zu hinterlegen, dass sie eindeutig zu identifizieren sind. (…).

I: Herr B.: Sie hatten auch bereits angesprochen, dass bei Sicherheitsverstößen rigoros sanktioniert wird und bei sicherheitsbewusstem Handeln belohnt wird. Könnten Sie diesbezüglich noch einmal explizit ausführen wie Sanktionierung und Belohnung aussehen?

Herr B.: Ja, Belohnung, fangen wir mit dem Positiven an. Es findet bei uns in der Unternehmensgruppe eine alle zwei Monate stattfindende Publikation statt. Es wird also im Rahmen einer Mitarbeiterzeitung publiziert. Da jeder Mensch auf Anerkennung fixiert ist, publizieren wir dort natürlich auch positive zwischenzeitlich erfolgte Ereignisse. So hatten wir hier am Standort (…) einen Fahrer, der bei einem Auftraggeber ein Behältnis übergeben bekommen sollten. Unsere Behältnisse, müssen Sie dazu wissen, sind mit Barcode gelabelt und die Besonderheit bestand darin, dass er diesen Code schon hatte. Also wurden seitens des Herstellers zwei Behältnisse mit denselben Barcodes produziert, was eigentlich nicht sein dürfte, weil dieser Hersteller auch zertifiziert arbeitet. (…). Dieser Mitarbeiter hat es über seinen Scanner gemerkt. Er konnte dieses Behältnis nicht annehmen, weil der Scanner das Behältnis schon als angenommen gespeichert hatte. Er hat dann nicht nur das Behältnis abgelehnt, sondern er hat gleichzeitig seinem Gegenüber aufgefordert das Behältnis mitzugeben. Er hat also vorausschauend gedacht. Dieser Mitarbeiter wurde namentlich benannt, ein entsprechender Vermerk in der Personalakte gefertigt und wird in Folge dahingehend überprüft, ob er für Aufgaben außerhalb des Fahrdienstes einsetzbar ist. (…). Gehaltserhöhungen, (…) gibt es natürlich für außergewöhnliche Leistungen im Angestellten- wie im Lohnbereich. Im anderen Bereich kann ich Ihnen aktuell schildern, dass ich vorgestern gerade einen Zugriff in einem Standort ausgelöst habe, da ich atypisches Verhalten des Mitarbeiters gespottet habe und dementsprechend den Mitarbeiter noch aus der laufenden Schicht über einen Einsatztrupp entfernen lassen habe. Das ist die Kehrseite. Wir hatten im letzten Jahr im niedersächsischen Bereich mehrere Fälle mit SEK-Einsatznotwendigkeit (…). Das stellt auch unter Beweis, dass wir hier eine Null-Toleranz-Linie fahren (…).

I: Damit hätten wir auch den organisatorischen Aspekt des Interviews abgeschlossen. Ich würde jetzt gerne auf die technischen Sicherheitsmaßnahmen, die bei Ihnen im Unternehmen zur Verfügung stehen, eingehen. Inwieweit bestehen denn bautechnische Maßnahmen zur Absicherung gegenüber Betriebsfremden und unbefugten Mitarbeitern?

Herr B.: Die äußere Umfriedung unserer Standortliegenschaften stellt sich unterschiedlich dar. Durch eine inhomogene Standortstruktur, die aus dem Vorunternehmen übernommen wurde, haben wir nicht an allen Standorten eine äußere Umfriedungsmöglichkeit, weil die Standorte zum Teil im Stadtzentrum aufgestellt sind. Zum Großteil haben wir äußere Standortumfriedungen, sodass zutrittswillige Besucher schon im Außenbereich in Zaunschleusen laufen und dort abgeholt werden, bevor sie denn überhaupt an das Gebäude herankommen. Die zwischen Umfriedung und Gebäude liegenden Bereiche sind im Rahmen von Bildpunktverfahren überwacht, sodass auch ohne Zutrittsberechtigungen eintretende Personen gespottet werden und eine entsprechende Alarmauslösung stattfindet. Die Standorte sind generell einbruchhemmend bis zur Durchschusssicherheit ausgestattet. Die entsprechenden Einsatzleitungen an den größeren Standorten arbeiten teilweise im Drei- und Vierschichtbetrieb. (…). Öffnungen können nur aus dem gesicherten Bereich heraus freigegeben werden. Die Freigabe erfolgt an nahezu allen Standorten unter Kamerablick und führt, wie gesagt, in Zwiebelbereiche, sodass man nicht unmittelbar vor dem Geld steht. Bevor Sie zum Geld kommen, müssen Sie Personenschleusen durchlaufen, die ebenfalls durchschusssicher gefertigt sind. Sie stehen dann immer noch nicht vor dem Geld, sondern werden dann wieder hinter der Personenschleuse durch bewaffnete Mitarbeiter zum Geld geleitet. Es gehört bei uns in den Standortbegehungen, egal ob intern oder extern, für alle besuchswilligen Mitarbeiter, die am Standort kein dauerhaftes Büro besitzen, dass sich diese Mitarbeiter legitimieren müssen, sich eintragen müssen und auch dokumentiert werden müssen. Sie haben ihren Ausweis zu hinterlegen (…). Der Besuchswillige erkennt auch durch zwingend zu leistende Unterschrift im Besucherbuch, dass etwaige Ersatzansprüche wegen einer Verletzung des Bundesdatenschutzgesetzes (…) gegen ihn geltend gemacht werden kann. Er erklärt auch die Zahlungswilligkeit in einer bestimmten Höhe.

I: Gibt es neben den genannten bautechnischen Maßnahmen auch Räume mit Abhörschutz und Sicherungsräume für gefährdete Datenträger?

Herr B.: Sicherungsräume für gefährdete Datenträger, ja. Unsere Serverräume sind sämtlich klimatisiert und mit entsprechendem Brandmelde- und Löschsystemen ausgestattet. Abhörschutz gibt es derzeit nur über gesicherten Datentunnel, aber Abhörschutz in Bezug auf Telefonie, nein. Datenleitung, ja. Telefonleitung, nein.

I: Es bestehen also keine abhörsicheren Konferenzräume?

Herr B.: Nein.

I: Sie sprachen gerade schon die Informations- und Kommunikationstechnik an. Können Sie noch einmal genau darauf eingehen welche Sicherheitsmaßnahmen in diesem Bereich getroffen wurden?

Herr B.: (…). Der Innentäter kann sich sicher sein das sämtliches Verhalten auf dem Gelände unter Kamera dokumentiert wird. Die Kamerabilder werden in einem definierten Zeitraum aufbewahrt, der ausreichend bemessen ist, um etwaige Auffälligkeiten festzustellen und dann auch auswerten zu können. In Bezug auf Außentäter kann ich Ihnen nur differenzierend antworten. Wenn wir zum Beispiel die Fahrzeuge betrachten, so läuft ein permanenter Datenstrom zwischen den Fahrzeugen und einer externen Notrufleitstelle, die auch nicht unternehmenseigen ist. Das ist eine extern zertifizierte Stelle. Wir haben Abfrageprozedere automatisiert, die bestimmte Gefährdungslagen analysieren, sodass es den Mitarbeitern auch unbemerkt möglich ist einen Alarm abzusetzen und eine entsprechende Intervention durch Einsatzkräfte einzuleiten. Es findet ebenfalls eine externe Steuerung der Öffnungsmöglichkeiten des Fahrzeugs statt. Das Fahrzeug ist mit einer speziellen Technik ausgestattet, die nur bei uns am Standort und bei der Bundesbank geeignet ist, sämtliche Fahrzeugtüren ohne Alarmmeldung zu öffnen. (…). Ich kann aber nicht ausschließen, dass sich im Fahrzeug private Handys befinden (…) und eine Kommunikation möglich wäre. Wir haben in den Standorten leider keine Handyblocker oder ähnliches installiert.

I: Gehen wir kurz auf den Verwaltungsbereich in Ihrem Unternehmen ein. Bestehen an den Firmenrechnern Accounts, Passwortpflichten und ein systematischer Passwortwechsel?

Herr B.: An den Servern und den Standorten, ja. An den Firmenlaptops ist mir das gegenwärtig nicht bekannt.

I: Das heißt, dass hier illegale Zugriffe möglich wären?

Herr B.: Ja, weder ein turnusgemäßer Passwortwechsel oder einer Nachhaltung der bereits verwendeten Passwörter. (…).

I: Und wie sieht es mit der Schutzprogrammen, Antivirus und Antispam, sowie der Verschlüsselung von Datenleitungen?

Herr B.: Es besteht die Möglichkeit, aber nur vereinzelt. (…). Insoweit kann ich zum Beispiel verschlüsselt senden und empfangen. Auf den Firmenrechnern ist es derzeit nicht generell eingerichtet, aber auch das im Sinne einer einheitlichen IT-Richtlinie identifiziert.

I: Kommen wir zum Abschluss des Gesprächs zu rechtlichen Sicherheitsmaßnahmen. Sie sprachen an, dass Geheimhaltungs- und Wettbewerbsvereinbarungen zwischen Ihrem Unternehmen und den Mitarbeitern bestehen. Gibt es auch Vereinbarungen mit ihren Geschäftspartnern und Konkurrenten?

Herr B.: Also zwischen Geschäftspartnern, ja. Zu Konkurrenten oder Mitbewerbern gibt es das meines Wissens nach nicht. Aber Geheimhaltungsvereinbarungen gibt es, wenn Sie zum Beispiel berücksichtigen, dass wir durch externe Sachverständige aufgesucht werden, die im Rahmen ihres Prüfanspruchs Dinge erfahren könnten, die so nicht für sie gedacht sind. In Bezug auf eigene Mitarbeiter führte ich bereits aus, dass es nicht rechtswirksame Wettbewerbsvereinbarungen gibt. (…).

I: Kann man sich bei Ihnen im Unternehmen auch vorstellen bei sicherheitsunbewusstem Handeln auch Schadensersatzansprüche an die Mitarbeiter zu stellen?

Herr B.: Ja, das machen wir.

I: Und wie ist die Erfolgsrate bei solchen Schadensersatzansprüchen?

Herr B.: Man muss es von Fall zu Fall differenziert betrachten (…), aber die Verfahren laufen noch und sind sehr langwierig. Wir haben, als Hintergrundinformation, dieses Vorgehen erstmalig aufgenommen, dass wir sowohl Innentäter als auch unbewusst handelnde Innentäter (…) zivilrechtlich verfolgen.

I: Bestehen denn derzeitig Patente zur rechtlichen Absicherung von explizitem Know-how?

Herr B.: Nein, derzeit nicht. (…). Das Gespräch über ein mögliches angestrebtes Patent würde sich ausschließlich zwischen dem jeweiligen Geschäftsführer und der Fachabteilung befinden. Kein anderer, auch innerhalb der Unternehmung, wäre über die Stellung und den Inhalt der Thematik informiert. (…).

I: Sie hatten bereits angesprochen, dass Zertifizierungen in Ihrem Unternehmen stattfinden. Gibt es denn auch Sicherheitsvorkehrungen zwischen Ihrem Unternehmen und der Zertifizierungsgesellschaft, um Informationsabflüsse zu verhindern?

Herr B.: Das sind genau solche Geheimhaltungsvereinbarungen, die auch rechtswirksam zwischen den Versicherern oder dem Verband eingesetzten Sachverständigen geschlossen wurden. Genau aus diesem Grund haben wir auch die entsprechende Besucherregelung (…) eingeführt, dass dies rechtswirksam verfolgbar wäre. Wir haben in einer Reihe von Fällen erlebt, dass durch Besuch gewonnene Informationen auf nicht prognostizierbaren Wegen wieder aufgetaucht sind. Wir haben dann für uns hausintern auch die Konsequenzen gezogen und haben eine Zusammenarbeit, Zutrittsberechtigungen bei Fremdsachverständigen zurückgezogen und Hausverbote bei allen unseren Standorten erteilt.

I: Damit wären wir am Ende des Interviews (…). Ich darf mich recht herzlich bedanken und die Ergebnisse werden Ihnen spätestens in einem halben Jahr zur Verfügung gestellt.

Herr B.: Ich würde eine Anonymisierung des Gesprächs begrüßen und danke auch für das Gespräch.

Beurteilung des Interviews:

Das zweite Interview dauerte ebenfalls ungefähr eine Stunde. In seinen Ausführungen war der Gesprächspartner sehr kooperativ und hielt vor dem Interview eine Kurzpräsentation zu seinem Unternehmen. Im Interview legte er Wert auf eine saubere Formulierung. Inhaltlich waren die Aussagen gut verwertbar und erlaubten tiefe Einblicke in die Unternehmenspraxis. Im Anschluss an das Gespräch wurden weitere Beispiele aus dem Unternehmensalltag besprochen.

B3 Transkript 3

Name:	Herr S.
Position:	Senior Information Security Manager, Firma F.
Datum:	07.04.2011
Zeitraum:	10.00 - 11.30 Uhr

Interviewer (I): Herr S., ich darf Sie nochmals herzlich begrüßen und mich bedanken, dass Sie sich die Zeit nehmen an diesem Interview teilzunehmen. Ich werde Ihnen jetzt in den nächsten 60 Minuten Fragen zu spezifischen Spionagerisiken Ihres Unternehmens stellen und diesbezüglich auf Risikoanalyse und Risikobewertung eingehen. Anschließend würde ich gerne auf personelle, organisatorische, technische und rechtliche Spionageabwehrmaßnahmen in Ihrem Unternehmen eingehen (...). Um Industriespionage wirkungsvoll begegnen zu können, empfiehlt sich zunächst eine Risikoanalyse. Inwieweit wurde bei Ihnen im Unternehmen denn eine Risikoanalyse durchgeführt, um spätere Know-how-Schutzmaßnahmen ergreifen zu können?

Herr S.: Für uns ist eine Risikoanalyse sogar Zwang, weil wir als Company nach der ISO 27001 - Informationssicherheit zertifiziert sind. Dort ist eine jährliche Risikoanalyse Pflicht. Ohne diese würden Sie gar nicht mehr das Zertifikat bekommen. Das heißt bei uns ist die sowieso Pflicht und zwar über alle Bereiche. Nicht nur der Export oder die Entwicklungsabteilung machen die Risikoanalyse. Bei uns wird eine solche Risikoanalyse bei der Entwicklung, über die Produktion, bis hin zur Auslieferung durchgeführt.

I: Können Sie noch einmal explizit ausführen wie eine solche Risikoanalyse vonstattengeht?

Herr S.: Ja. Zum einen ist es so, dass die Bereiche aufgefordert werden Ihre Risiken zu identifizieren. Das heißt, wo meint die Abteilung könnten Daten oder Know-how abgezogen werden oder abfließen ohne dass es jemand mitbekommt. Diese Risiken müssen zuerst bewertet werden. Das heißt sie müssen aufschreiben, dass dieser Job oder jener Fertigungsprozess Gefahren der Industriespionage beinhaltet. Natürlich ist das Gefährdungspotenzial in der Entwicklung am höchsten. Wenn Sie dort zum Beispiel neue Produkte entwickeln, gerade im Rohstadium sind und das fließt zu Konkurrenten ab, dann ist Ihr Marktvorteil weg (…). Daher ist die oberste Priorität Risiken zu identifizieren und Maßnahmen zu definieren.

I: Gibt es denn bei der Betrachtung der Risikobereiche Personal, Organisation, Technik und Recht schwerpunktmäßig von Spionagetätigkeiten betroffene Bereiche?

Herr S.: Technik ist natürlich die Nummer eins, weil darin unsere Entwicklung zu finden ist (…). Die Risikoanalyse selbst wird durch die Information Security Manager durchgeführt. Wir haben den Corporate Information Security Advisor (…), der dafür verantwortlich ist, dass die Landesverantwortlichen die Risikoanalysen von den Einheiten durchführen lassen. Dann werden die Analysen von den Landesverantwortlichen auf Richtigkeit begutachtet (…). Sehr oft kommt es zum Beispiel vor, dass Führungskräfte eine interne Brille aufhaben und die Risiken verharmlosen (…). Unter Umständen können die Führungskräfte so durch die Landesverantwortlichen aufgefordert werden die Risikoanalysen erneut durchzuführen. Für Deutschland bin ich zum Beispiel der Landesverantwortliche. Das heißt, dass ich den Führungskräften auf die Füße treten muss und ihnen sage, dass die Risikoanalyse durchgeführt werden muss. Das erfreut nicht die meisten Leute, weil es eine Menge an Arbeit macht alle Risiken zu identifizieren. Des Weiteren erfreut es die Führungskräfte nicht, wenn die Risikoanalysen von mir als nicht ausreichend betrachtet werden und Nachbesserungen notwendig sind. Diese Risikoanalysen fließen dann auch in interne und externe Audits ein. Solche Audits führe ich auch selber durch, wo ich die gesamten Abteilungen und Systeme auf den Kopf stelle. Wenn dann die Risikoanalyse nicht gemacht wurde, fällt die Abteilung durch. Das möchte sich keine Führungskraft antun, da der Bericht auch an die oberste Leitung geht (…) und so etwas nicht unbedingt förderlich für die eigene Karriere ist. Aber es gibt auch externe Audits. Wir sind, wie gesagt, ISO 27001 zertifiziert und haben einen externen Auditor, mit dem gewährleistet werden kann, dass die Kontrollen in den unterschiedlichen Ländern auch immer vergleichbar sind (…).

I: Herr S., Sie sprachen gerade auch die Risikobewertung an. Gibt es neben den maßgeblichen Parametern mögliche Schadenshöhe und Schadenseintrittswahrscheinlichkeit noch weitere Parameter zur Risikobewertung?

Herr S.: (…). Ja, hierbei fließt auch die Beschaffenheit der Assets mit in die Bewertung ein. Sind es Software-Assets, sind es physische Assets oder sind es auch Human-Assets, also Mitarbeiter (…). Das größte Risiko beim Know-how-Abfluss ist bei uns die Entwicklung, weil es für Konkurrenten interessant ist die Daten vor Marktveröffentlichung zu erhalten. Hier ist das Risiko besonders hoch, da Entwickler und Informatiker zum Teil sorglos mit sensiblen

Daten umgehen und davon ausgehen, dass nichts passiert. Diese Leute sind dann auch auf den Boden der Tatsachen zurückzuholen (…).

I: Also würden Sie bestätigen, dass beim Personal zum Teil mangelndes Risikobewusstsein vorherrscht?

Herr S.: Ja, auf jeden Fall. Bei manchen Firmen ist es ja auch so, dass in der Leitung kein Risikobewusstsein vorherrscht. Das ist bei uns jedoch nicht der Fall. Wir haben vielmehr das Problem, dass besonders in der Entwicklungsabteilung das Thema nicht so ernst genommen wird wie es eigentlich genommen werden sollte.

I: Das heißt, dass weitere Sensibilisierungs- und Schulungsmaßnahmen notwendig sind?

Herr S.: Ja, es werden zwar jährlich Schulungen, sowohl Präsenzveranstaltungen als auch web-based Trainings, durchgeführt.

I: Aber hier bestehen durchaus Verbesserungspotenziale?

Herr S.: Ja, hier bestehen Verbesserungspotenziale. Deswegen versuchen wir auch undercover an Daten zu gelangen, um zu schauen, ob wir an sensible Daten von uns herankommen. Das heißt, dass wir uns in Foren und Communities herumtoben und regelmäßig nach unseren Firmennamen suchen, um zu gucken ob Daten von Mitarbeitern angeboten werden. Denn es ist ja allseits bekannt, dass nicht der Hacker, sondern der Mitarbeiter das größte Risiko darstellt. Gerade dann wenn Mitarbeiterabbau ansteht und Mitarbeiter innerlich schon gekündigt haben, gibt es ein hohes Risiko des ungewollten Know-how-Abflusses. Deswegen ist es bei uns so, dass wenn ein Mitarbeiter kündigt oder gekündigt wird und sich in exponierter Stelle befindet, wie zum Beispiel Administrator oder Softwareentwickler, in der Regel sofort von seiner Arbeit freigestellt wird. So wird sein Account gesperrt und er hat keine Chancen mehr Daten herunterzuladen. Denn hier hat ja auch die Vergangenheit, wie am Beispiel der Lopez-Affäre, gezeigt, dass beim Weggang von Mitarbeitern hohe Risiken des Know-how-Abflusses bestehen (…).

I: Herr S., wir sind gerade bei der Risikobewertung stehen geblieben und sie erwähnten, dass auf Basis der Analyse der Risiken auch Prioritätenlisten erstellt werden. Gibt es diesbezüglich eine Klassifizierung?

Herr S.: Also wir haben die Stufen eins bis fünf. Von low bis high risk. Von null bis zwei sind die Maßnahmen zwar umzusetzen, haben aber nicht die höchste Priorität. Alles was über zwei ist, muss in eine zentrale Datenbank eingegeben werden. Dort gibt es eine Abteilung, die nichts anderes als Risikobetrachtung und Risikobewertung macht. Diese Abteilung hakt sofort hinterher bis wann das Risiko von Ihnen minimiert wird beziehungsweise bis wann Sie ein Statement zu diesem Risiko abgeben, denn es kann ja sein, dass die Behebung des Risikos teurer als ein Schadensfall ist, sodass man das Risiko akzeptiert. Die Akzeptierung solcher Risiken mit hoher Priorität muss gleichzeitig aber auch durch den Vorstand erfolgen (…). Solche Sachen verfolgt die zentrale Risk-Abteilung, die direkt beim Vorstand angesiedelt ist.

I: Also ist die Risk-Abteilung organisatorisch an die Geschäftsführung angebunden?

Herr S.: Ja, genau. Das ist genau das gleiche wie bei meiner Position. Ich als Verantwortlicher der Informationssicherheit in Deutschland, hänge auch direkt an der deutschen Geschäftsführung (…). Ich habe in diesem Bereich Weisungsbefugnis und kann selbst meinen Geschäftsführer zu Maßnahmen zwingen, auch wenn er es nicht will. So etwas muss jedoch gemacht werden, denn ohne Kenntnis über Risiken, können Sie auch keine Schwachstellen ausschalten.

I: Also wird der Informationsschutz in Ihrem Unternehmen als Chefsache betrachtet und hat dementsprechend einen hohen Stellenwert?

Her S.: Auf jeden Fall. (…). Das hat auch etwas mit unserer Unternehmenshistorie zu tun.

I: Herr S., sie hatten bereits angesprochen, dass der Faktor Mensch das entscheidende Risiko im Bereich der Industriespionage ist. Inwieweit werden denn in Stellenausschreibungen sensible Firmeninterna veröffentlicht?

Herr S.: Wenn sich ein Mitarbeiter bei uns bewirbt, wird er zunächst gegen die Anti-Terrorliste geprüft (…). Wenn Sie dort auffallen, ist es sowieso schon vorbei. Genauso wird der Bewerber natürlich auch von unserer Personalabteilung gegoogelt. Hier wird geguckt, wo der Bewerber überall auftritt. Eine solche Mitarbeiterüberprüfung findet schon statt, wobei demnächst wahrscheinlich eine Datenschutznovelle herauskommt, die Ihnen das untersagt. Sie können weiterhin nach Personen googeln, dürfen aber nicht mehr als viermal in geschlossenen Foren, wie Facebook, Xing und Experteer, suchen. Wenn das so kommen sollte fällt natürlich ein wesentliches Werkzeug der Personalüberprüfung weg. Ob ein Personalleiter

dann trotzdem reinguckt und bei der Ablehnung einen anderen Grund nennt, kann natürlich nicht verhindert werden. (…).

I: Nun hatten wir gerade die Stellenausschreibung angesprochen. Sind Ihrer Meinung nach aus den veröffentlichten Anforderungen, verwendeten Technologien und späteren Tätigkeiten auf der Stelle, Rückschlüsse für Wettbewerber möglich?

Herr S.: Die Stellenausschreibungen sind so allgemein gehalten, dass keine Rückschlüsse möglich sind. (…).

I: Sie hatten gerade die Berücksichtigung individueller Risikofaktoren bei der Personalauswahl angesprochen. Werden im Zuge der Überprüfung der Anti-Terror-Liste auch Kontakte und Aufenthalte von potenziellen Bewerbern in Risikostaaten berücksichtigt?

Herr S.: Ja klar. Bei solchen Fällen werden dann auch schon einmal Botschaften bemüht, um geheimdienstliche Aussagen zu erhalten (…). Das ist aber nicht der Hauptteil der Überprüfungen. Aber natürlich werden Mitarbeiter bei gewisser Gefährdungslage genauestens überprüft.

I: Werden im Rahmen der intensiven Überprüfung der Bewerber auch frühere Arbeitgeber und Ausbildungsstätten überprüft?

Herr S.: Nein, es werden natürlich bei diversen Titeln des Bewerbers Anfragen an Unis gemacht (…). Es werden aber generell keine ehemaligen Chefs oder Unis angeschrieben. Das machen wir nicht.

I: Kommen wir nun zur Personaleinstellung. Welche Sicherheitsmaßnahmen stehen dem Unternehmen hier zur Verfügung? Hierzu gehören zum Beispiel Sicherheitsbelehrungen sowie Datenschutz- und Geheimhaltungsverpflichtungen.

Herr S.: Nach der Einstellung muss der Mitarbeiter zunächst eine Datenschutzerklärung nach Paragraph fünf BDSG abgeben. Dies beinhaltet, dass der Mitarbeiter alle Daten, mit denen er jetzt in Kontakt kommt nicht weitergeben darf. Auch nicht nach Beendigung seiner Tätigkeit, sondern bis zur Beendigung seines Lebens (…). Dann bekommt der Mitarbeiter natürlich auch eine Unterweisung über alle unsere Security-Policies. Das heißt zum Beispiel welche Sicherheitsrichtlinien wir zum Betrieb von Servern und Software haben oder wie er sich auf Dienstreisen zu verhalten hat oder was wir für sicherheitstechnische Einrichtungen haben.

Natürlich gehören hier auch unsere kompletten Guidelines zum Thema Compliance dazu. Sie haben ja nicht nur das BDSG, sondern auch das Wettbewerbsrecht, das KonTraG, das Telekommunikationsgesetz und vieles mehr. Auch das muss der Bewerber lesen und unterschreiben, dass er es verstanden hat und akzeptiert. Erst wenn dieses Prozedere durch ist, wird der Mitarbeiter produktiv.

I: Gibt es denn auch Konkurrenzklauseln oder nachvertragliche Wettbewerbsverbote?

Herr S.: Nein. Das schließt sich dadurch schon aus, dass der Mitarbeiter keine Daten aus unserem Unternehmen in seinem späteren Berufsleben weiterverwenden darf (…). Das wäre rechtlich sonst sehr problematisch (…). Das einzige was wir haben ist, dass Mitarbeiter bei besonderen Schulungen verpflichtet werden noch mindestens drei Jahre im Unternehmen zu bleiben. Gehen Sie vorher, müssen Sie anteilig die Schulungsgebühren zahlen (…). Das ist aber eher eine Sache des Investitionsschutzes und nicht des Know-how-Schutzes.

I: Gehen wir noch einmal auf ein sicherheitsbewusstes Personalmanagement ein. Inwieweit finden denn auch Sensibilisierungs- und Schulungsmaßnahmen bei den Mitarbeitern statt?

Herr S.: Mindestens einmal im Jahr werden durch mich, Mitarbeiter von mir oder durch web-based Trainings Schulungen durchgeführt. Hierbei erhalten die Mitarbeiter Post, dass sie sich bis zu einem Zeitpunkt anmelden müssen, die Schulung durchlaufen und dann die abschließende Prüfung durchlaufen müssen. Dagegen kann sich der Mitarbeiter auch nicht wehren (…). Das wird aber auch durch die ISO 27001 vorgeschrieben.

I: Könnten Sie noch einmal darauf eingehen wie solche Sensibilisierungs- und Schulungsmaßnahmen explizit ausgestaltet sind?

Herr S.: Es gibt einmal Schulungsmaßnahmen für Mitarbeiter und einmal für Führungskräfte. Hierzu gehört was ich zu beachten habe und wie ich mich zum Beispiel auf Dienstreisen verhalte. Das beinhaltet, dass ich in der U-Bahn oder S-Bahn nicht über Projekte spreche oder telefoniere und im Flughafen oder im Flieger nicht mein Laptop ohne Sichtschutzfilter aufklappe. Hier wird definitiv beschrieben, wie Sie sich als Mitarbeiter in der Öffentlichkeit zu verhalten haben, um zu verhindern, dass jemand hinter einem sitzt alles mitschreibt.

I: Und wie sehen die Schulungsmaßnahmen für interne Mitarbeiter ohne Dienstreisen aus?

Herr S.: Diese Mitarbeiter werden regelmäßig über die aktuellen Sicherheitsrichtlinien informiert. (…). Dennoch erhalten alle Mitarbeiter Informationen zum Verhalten auf Dienstreisen. Denn es kann ja durchaus sein, dass ein Kaufmann der sonst keinen Außenkontakt hat, eines Tages zu seinem Chef nach München muss und sich dann adäquat verhalten muss, um keine Informationen an Flughäfen oder Bahnen abfließen zu lassen. Natürlich sagen wir in den Schulungen auch wie Geheimdienste vorgehen, um Mitarbeiter anzuwerben, weil ja durchaus auch befreundete Geheimdienste Daten stehlen. (…). Inhalt der Schulungen ist zum Beispiel wie durch finanzielle Anreize versucht wird Mitarbeiter zu gewinnen oder wie durch kompromittierende Daten Mitarbeiter zur Arbeit für Geheimdienste gezwungen werden. Solche Praktiken müssen die Mitarbeiter wissen, da sie oft kein Risikobewusstsein hierfür haben.

I: Sind das Abhörsystem ECHELON und die damit verbundenen Risiken auch Inhalt von Sensibilisierungs- und Schulungsmaßnahmen?

Herr S.: ECHELON ist fast jedes Jahr auf der Tagesordnung, sodass vertrauliche Daten niemals unverschlüsselt geschickt werden dürfen. Hierbei gibt es jedoch aber auch immer ein paar Probleme, da in einigen Ländern keine ausreichenden Verschlüsselungen zur Verfügung stehen und zum Teil Verschlüsselungen, wie in China oder Indonesien, gar nicht erlaubt sind. (…). Es passiert jedoch auch regelmäßig bei Dienstreisen in die USA, dass Sie (…) mittlerweile bei Mitnahme von verschlüsselten Festplatten gezwungen werden, den Schlüssel herauszugeben. Machen Sie das nicht, gehen Sie in den Bau (…). Bei Herausgabe des Passworts wird Ihr Laptop für maximal eine Stunde einbehalten. In dieser Zeit ist dann Ihre Festplatte bereits kopiert worden. Deswegen gibt es bei uns die Anweisung, dass bei Reisen in die USA oder auch nach Russland, keinerlei sensible Daten auf den Laptop genommen werden, sondern, sobald Sie im jeweiligen Land sind, durch den Aufbau eines VPN-Tunnels die Daten von einem deutschen Server wiedergeholt werden. Dazu gehört aber auch, dass vor der Abreise die Platte auch wieder mit bestimmten Tools geputzt wird, dass nicht bei der Abreise die Daten abgegriffen werden können. Nach solchen Daten sind mittlerweile die USA und auch Russland ziemlich hinterher.

I: Dazu gehört natürlich auch der chinesische Geheimdienst.

Herr S.: Ja, mittlerweile ist China sehr umtriebig auf diesem Gebiet. Alleine die Personalstärke des chinesischen Geheimdienstes ist enorm. (…).

I: Wir hatten gerade die Sensibilisierungs- und Schulungsmaßnahmen für Mitarbeiter angesprochen. Werden denn die Mitarbeiter auch in die Entwicklung von Know-how-Schutzmaßnahmen einbezogen?

Herr S.: Ja. Bei uns gibt es auch Richtlinien wie sich Mitarbeiter bei bestimmten Szenarien, wie Hackerangriffen, zu verhalten haben. Natürlich müssen Mitarbeiter bei entdeckten Problemen die Führungskräfte kontaktieren, die wiederum sicherheitsverantwortliche Mitarbeiter wie mich ansprechen müssen. Dabei werden die Ergebnisse der Risikoanalysen (…) auch in Gruppen diskutiert. Des Weiteren gibt es aber auch die Möglichkeit für Mitarbeiter anonym Risiken mitzuteilen damit das Arbeitsverhältnis zum Vorgesetzten nicht belastet wird. Hierbei bin ich dann oft der Ansprechpartner und regele das mit den Führungskräften.

I: Wenn wir bei dem Punkt der Akzeptanz und Zufriedenheit der Mitarbeiter sind, bilden diese Faktoren ja auch einen wesentlichen Beitrag zum Informationsschutz innerhalb des Unternehmens. Könnten Sie sagen, dass ihre Mitarbeiter leistungsgerecht entlohnt werden und auch unentgeltliche Anerkennung erhalten?

Herr S.: Also ich glaube schon, dass wir in diesem Unternehmen eine sehr gute Entlohnung im Vergleich zum Mittelstand haben. Es gibt natürlich auch Incentive-Maßnahmen, wo Add-ons gezahlt werden. Aber wir haben durchaus die Erfahrung gemacht, dass ein Lob manchmal viel mehr bewegen kann. Es muss nicht immer Geld sein.

I: Werden Lob und Anerkennung für berufliche Leistungen der Mitarbeiter denn auch in Mitarbeiterzeitschriften oder im Intranet veröffentlicht?

Herr S.: Ja, so etwas wird über das Intranet publiziert. Wir haben natürlich auch ein internes Vorschlagswesen, wo nicht nur die Produktion Vorschläge macht, sondern auch Verbesserungen an Prozessen hineingehen. Hierbei werden durchaus materielle Werte wie Gutscheine, Urlaube oder hauseigene Produkte vergeben. Ein solches System haben wir aber schon seit einigen Jahren und sehr gute Erfahrungen damit gemacht.

I: Gibt es denn bei Ihnen im Unternehmen Instrumente zur Messung des Identifikationsgrades der Mitarbeiter oder ihrer Loyalität?

Herr S.: Es gibt bei uns, das ist auch erst vor Kurzem durchgeführt worden, sogenannte Mitarbeiterzufriedenheitsanalysen. Wie stark identifizieren Sie sich mit Ihrem Job? Wie zufrieden sind Sie mit Ihrem Vorgesetzten? Wie akzeptieren Sie Ihre persönlichen Ziele? (…). Die-

se Erhebung hat letzte Woche stattgefunden und wurde durch eine englische Firma online durchgeführt. Sie brauchten circa 60 Minuten zur Beantwortung. Die Auswertung erfolgte natürlich anonym. (…). Dementsprechend werden bei der englischen Firma die Daten nach der Auswertung auch vernichtet. (…).

I: Und welchen Abständen sollen diese Mitarbeiterzufriedenheitsanalysen durchgeführt werden?

Herr S.: Jährlich.

I: Kommen wir nun zur Ausscheidung von Personal. Sie hatte angesprochen, dass es hierbei rigorose Sicherheitsvorkehrungen gibt. Bestehen denn auch Unterschiede zwischen einem regulären und nicht einvernehmlichen Ausscheiden?

Herr S.: Bei Führungskräften und Führungsnachwuchskräften, die mit sensiblen Daten in Kontakt kommen, ist es vollkommen egal ob sie regulär oder nicht einvernehmlich ausscheiden. (…). Dabei startet die Personalabteilung einen Prozess, bei dem geguckt wird in welchen Projekten und Verfahren der Mitarbeiter arbeitet. Diese Informationen erhält dann die zentrale IT-Abteilung, sodass alle Accounts des Mitarbeiters deaktiviert werden. Selbst der Zugang von zu Hause aus (…) wird dann gesperrt. Wie gesagt, ist es vollkommen unerheblich ob selbst gekündigt wurde oder der Mitarbeiter gekündigt wurde.

I: Findet denn eine Beobachtung des Marktes und der Wettbewerber nach Beendigung des Arbeitsverhältnisses statt?

Herr S.: Wenn Mitarbeiter das Unternehmen verlassen dann sind Sie weg. Das halte ich rechtlich auch für fragwürdig. Natürlich gibt es Wettbewerbsbeobachtung und -beurteilung, aber die dient nur der Marktanalyse.

I: Nun hatten wir gerade Sicherheitsmaßnahmen für das firmeneigene Personal behandelt. Gelten für Fremdpersonal, wie Berater, Handwerker, Sicherheits- und Reinigungskräfte, die gleichen Sicherheitsvorkehrungen?

Herr S.: Berater müssen ebenfalls die Erklärungen zum BDSG unterschreiben, Fernmeldegeheimnisse beachten, Policies kennen und noch mehr Erklärungen als normale Mitarbeiter unterschreiben (…). Aber auch die werden wir nach Beendigung ihrer Tätigkeit nicht beobachten und kontrollieren (…).

I: Gab es denn schon Vorfälle, wo Informationen über Sicherheits- und Reinigungspersonal abgeflossen sind?

Herr S.: Das ist schon ein bisschen länger her, hat es aber auch schon gegeben. Dabei hatte eine Führungskraft sensible Daten auf dem Schreibtisch liegen gelassen (…). Im Nachhinein konnte man aufgrund des Zutrittskontrollsystems der Büroräume feststellen, dass eine Reinigungskraft als letztes im Büro war. Die Reinigungskraft hat natürlich alles bestritten, aber natürlich wurde das Vertragsverhältnis sofort aufgelöst. In sensible Bereiche wie die Entwicklungsabteilung kommen Reinigungskräfte aber nicht mehr nach Feierabend hinein. Das heißt, dass sie während der Arbeitszeit putzen müssen. (…).

I: Kommen wir nach den personellen Schutzmaßnahmen zu den organisatorischen Abwehrmaßnahmen. Inwieweit sind denn formal fixierte Sicherheitsstandards, wie eine Clean-Desk-Policy, in Ihrem Unternehmen zum Know-how-Schutz etabliert?

Herr S.: Es gibt eine Clean-Desk-Policy, die auch wieder Bedingung der ISO 27001 ist. Im Rahmen dieses Zertifikats werden Sie auch gezwungen diese Policy regelmäßig zu überprüfen. Das heißt, dass ich die Standorte ohne Ankündigung irgendwann nach Feierabend besuche und durch die einzelnen Bereiche durchgehe. Hierbei mache ich unabgeschlossene Schränke und Schubladen auf, gucke hinein und schaue mir die Schreibtische an. Das mache ich mit der örtlichen Betriebsleitung, die für den Standort verantwortlich ist. Zum Abschluss wird ein Zettel auf den Schreibtischen hinterlassen, wo draufsteht, ob die Sicherheitsvorkehrungen zur voller Zufriedenheit erfolgt sind oder ob es Verbesserungsbedarf (…) gibt. Das wird jährlich durchgeführt.

I: Gibt es auch Bestimmungen zur Nutzung, Vervielfältigung und Vernichtung von Informationsbeständen?

Herr S.: Natürlich. In dieser Policy steht genau wie Informationen zu nutzen sind und wie Informationen einzustufen sind. Es gibt bei uns die Stufen „public“, „internal“, „confidential“ und „strictly confidential“. Informationen, die „public“ sind, sind wie white papers zu behandeln, für Kunden geeignet und können auch ins Intranet gestellt werden. „Internal“ heißt, dass die Informationen nur für Mitarbeiter geeignet sind. „confidential“ heißt nur für einen bestimmten Mitarbeiterkreis und „strictly confidential“ sind meistens Protokolle des Vorstands. In der Policy steht auch, dass Informationen mit der Einstufung „confidential“ nicht mehr auf

ein einfaches Laufwerk gestellt werden dürfen, sondern auf einem verschlüsselten Speicher liegen müssen. Dementsprechend müssen solche Daten auch verschlüsselt verschickt werden.

I: Und wie sieht die Vernichtung von sensiblen Informationsbeständen aus?

Herr S.: Es gibt bei uns die Anordnung, dass Informationen mit Einstufung „internal", „confidential" und „strictly confidential" geschreddert werden müssen oder in Datenschutzcontainer geworfen werden müssen, die es auf jeder Etage gibt (…). Diese Container werden dann von zertifizierten Entsorgern abgeholt und geschreddert. Das ist eine klare Anweisung und Richtlinie, die eingehalten werden muss und auch kontrolliert wird. Wenn zum Beispiel ein Mitarbeiter ein neues Notebook bestellt, muss auch nachgewiesen werden was mit dem alten Gerät passiert (…), sodass kein Missbrauch getrieben werden kann. (…).

I: Herr S. Sie als Sicherheitsverantwortlicher und die zentrale Security-Abteilung sind Ansprechpartner und Koordinatoren in Sicherheitsangelegenheiten. Könnten Sie noch einmal explizit auf Ihre Aufgaben eingehen?

Herr S.: Ja. Die erste Aufgabe besteht darin Policies zu erstellen und diese jährlich zu reviewen und in ihrer Umsetzung zu kontrollieren. Hier werden Führungskräfte angeschrieben, dass Sie ihre Schwachstellen- und Risikoanalysen durchführen müssen. Des Weiteren müssen wir die Audit-Planung vornehmen, wo geplant wird wann welche Abteilung überprüft wird. Das ist natürlich nur uns bekannt, aber wir müssen das der Geschäftsführung vorlegen. Nach der Durchführung der Audits gibt es dann auch ein Audit-Protokoll, was die Geschäftsleitung dann bekommt. Daher sind die internen Audits auch nicht gerne von den Abteilungen gesehen, da diese selber wissen, dass die Audit-Protokolle an die Geschäftsführung gehen. Meistens werden die Abteilungen auch vorgewarnt, weil sie gewisse Vorbereitungen (…) machen müssen. Es gibt aber auch Kontrollen, die komplett unangekündigt stattfinden (…). Das sind die schwerpunktmäßigen Aufgaben. Zusätzlich stehen an den großen Standorten noch sogenannte Local Information Security Advisor unter mir, die Checklisten vorbereiten, Risikoanalysen vorantreiben und mir bei der Koordination helfen. Zeitlich würde ich das alleine gar nicht schaffen. Natürlich kriegen wir auch diverse Anfragen von unseren Kunden wie wir mit ihren Daten umgehen (…). Zum Beispiel hosten wir auch diverse Banken (…).

I: Ok. Ein weiterer organisatorischer Aspekt sind die räumlichen Zutrittsrechte und die Zugriffsrechte innerhalb der EDV. Könnten Sie zu diesen Regelungen in Ihrem Unternehmen Ausführungen machen?

Herr S.: Bei uns gibt es sogenannte Rollenkonzepte, wo jeder Position die Rolle zugeteilt wird, die für ihre Arbeit benötigt wird. Ein SAP-Anwender erhält zum Beispiel nicht die gleichen Befugnisrechte wie ein SAP-Administrator. Diese Rollenkonzepte werden auch regelmäßig, mindestens einmal im Jahr, überprüft (…) und wenn nötig angepasst. Hierbei stehen wir eng mit den Führungskräften und der Personalabteilung in Kontakt.

I: Und wie verhält es sich mit den räumlichen Zutrittskontrollen?

Herr S.: Alle Mitarbeiter haben ein Mitarbeiterausweis, mit dem sie nur für bestimmte und notwendige Räumlichkeiten freigeschaltet sind. Das heißt, dass in die Rechenzentren (…) nur ein kleiner Teil von Administratoren hineinkommt. Selbst die Standortleitungen kommen nicht in die Rechenzentren der Standorte hinein (…). Ich komme mit meinem Profil zum Beispiel in alle Bereiche in Deutschland hinein. Das muss ich aber auch, denn wenn wir einen Vorfall, wie eine Hacking-Attacke, haben, muss ich schnell Zutritt erhalten. (…).

I: Herr S., kommen wir nun zu den technischen Spionageabwehrmaßnahmen. Inwieweit bestehen bautechnische Maßnahmen zur Absicherung gegenüber Betriebsfremden und unbefugten Mitarbeitern an den jeweiligen Standorten?

Herr S.: Hier schreibt wiederum die ISO 27001 alles vor. Sie dürfen zum Beispiel nicht ein Rechenzentrum auf Erdgeschosshöhe einrichten, sodass Sie mit einem Auto problemlos in das Rechenzentrum fahren können. Hier werden Erdwälle und Betonwände gefordert (…). An sensiblen Standorten sind zusätzlich Kartenleser installiert. Externe Personen kommen hier nur in Begleitung eines Mitarbeiters durch und werden durch diese Mitarbeiter auch wieder nach draußen begleitet. Bei kritischen Bereichen müssen Sie dann erneut Ihren Ausweis vorlegen (…). Es handelt sich also um ein mehrstufiges Berechtigungskonzept (…). Zusätzlich sind sensible Bereiche auch videoüberwacht. So dürfen Putzfrauen nur in Begleitung des Werksschutzes in die Serverräume. Somit haben wir also ein dreistufiges System. Von der Anmeldung, über die Abteilungen bis zum Rechenzentrum, wo nur ganz wenige Mitarbeiter hineinkommen.

I: Gibt es denn auch abhörgeschützte Räume bei Ihnen im Unternehmen?

Herr S.: Wir haben nur im Bereich des Vorstands solche Räume, wo es zum Beispiel an den Glasscheiben Vibratoren gibt, die die Scheibe in Schwingung setzen und damit Abhörversuche von außen verhindern. (…).

I: Kommen wir noch einmal zu den Maßnahmen der Sicherung der Informations- und Kommunikationstechnik. Findet denn neben der genannten Verschlüsselung von Datenleitungen auch ein systematischer Passwortwechsel bei Ihnen im Unternehmen statt?

Herr S.: Ja, alle 90 Tage muss das Passwort gewechselt werden. Sie müssen das Passwort mindestens neunstellig halten, mindestens eine Ziffer und ein Sonderzeichen beipacken. Das ist unsere Standard-Vorgehensweise. Des Weitern haben wir natürlich mehrstufige Firewallsysteme (…), die den Datenverkehr überwachen.

I: Gab es denn in der Vergangenheit viele Angriffe auf die Informations- und Kommunikationstechnik?

Herr S.: Nein, eigentlich nicht, aber wenn etwas nicht entdeckt wurde, heißt das ja noch lange nicht, dass nichts passiert ist. Gerade bei Angriffen von Geheimdiensten merken Sie diese Attacken ja in der Regel gar nicht. (…).

I: Kommen wir zum Schluss des Interviews auf rechtliche Spionageabwehrmaßnahmen. Gibt es denn neben den genannten Geheimhaltungsvereinbarungen zwischen Ihrem Unternehmen und den Mitarbeitern auch Geheimhaltungsvereinbarungen zwischen Ihrem Unternehmen und anderen Unternehmen?

Herr S.: Ja, zwischen Lieferanten natürlich. Wir können natürlich unseren Wettbewerbern nichts vorschreiben, aber sämtliche Lieferanten (…) müssen Geheimhaltungsvereinbarungen unterschreiben. Das machen wir eigentlich schon immer. Die Einhaltung dieser Vereinbarungen wird dann auch regelmäßig durch sogenannte Lieferanten-Audits überprüft. Dann werden die Lieferanten besucht und es wird geschaut, ob die Maßnahmen, die wir fordern, auch wirklich umgesetzt werden.

I: Gibt es bei Verstößen gegen solche Vereinbarungen auch rechtliche Konsequenzen?

Herr S.: Natürlich haben wir auch sogenannte Malus-Systeme integriert. Wird gegen Auflagen verstoßen, sind Zahlungen fällig, die ziemlich hoch ausfallen können. Wir hatten bisher nur einen Lieferanten, der kurz vor der Pleite stand, noch versucht hat Sachen zu Geld zu machen und auch von uns Daten verwendet hat. So etwas passiert aber meist außerhalb der Öffentlichkeit und der Presse. Hier wird mit Strafen und Staatsanwaltschaft gedroht, sodass meist von selbst gezahlt wird. Das kommt dadurch, dass weder der Geschädigte noch der Täter negativ in der Presse auffallen wollen. In der Regel versucht man sich meist außergerich-

tlich zu einigen. Gleiches gilt für Mitarbeiter. In der Regel werden die fast nie angezeigt, weil man nicht öffentlich negativ in Erscheinung treten will. Erst wenn nichts mehr geht wird so etwas gemacht. Erst wenn zum Beispiel festgestellt wird, dass ein Mitarbeiter sensible Daten an einen feindlichen Geheimdienst verkauft hat, geht es vor Gericht.

I: Nun ist Ihr Unternehmen sehr forschungsintensiv. Gibt es denn Patente zur rechtlichen Absicherung von explizitem Know-how?

Herr S.: Ja, das sind hunderte.

I: Und inwieweit berücksichtigt man die Risiken einer Patentanmeldung?

Herr S.: (…). Grundsätzlich gilt bei Patenten: Wer zuerst kommt, malt zuerst. Wird zum Beispiel eine noch nicht patentierte Idee von einem Geheimdienst geklaut und an ein einheimisches Unternehmen weitergegeben, wie im *ENERCON*-Fall passiert, dann war es das. Wir hatten bisher mit patentierten Ideen noch keine Probleme. Ich denke, dass dies eher ein Problem in der Telekommunikationsbranche ist (…).

I: Also werden Patente zur rechtlichen Absicherung von Know-how eingesetzt?

Herr S.: Ja. Es bleibt Ihnen ja nichts anderes übrig. Wenn zwei Firmen an der gleichen Sache forschen, hat der Erste den Patentschutz, sodass für den Konkurrenten das Ding gelaufen ist. Es bleibt Ihnen also nichts anderes übrig als bei den jeweiligen Patentämtern die Patente anzumelden.

I: Gab es denn negative Erfahrungen mit asiatischen Patentämtern?

Herr S.: Gott sei Dank hatten wir diesen Fall noch nicht, aber natürlich haben die Chinesen eine ganz andere Auffassung zum Schutz von geistigem Eigentum (…).

I: Nun werden in Ihrem Unternehmen viele Geschäftsprozesse zertifiziert. Gibt es spezielle Vereinbarungen zwischen Ihrem Unternehmen und der Zertifizierungsgesellschaft?

Herr S.: Zertifizierungsgesellschaften kriegen ja alles mit. Insofern müssen diese Gesellschaften natürlich zur Geheimhaltung verpflichtet werden. Die gehen ja auch in die Rechenzentren und die Entwicklung rein. Hier gilt das gleiche wie für Unternehmensberatungen. Sie können die Unternehmen rechtlich verpflichten, aber ob alles eingehalten wird ist eine ganz andere Sache. (…). Das kriegen Sie bei Mitarbeitern, Führungskräften oder Externen nicht hin. Wenn

jemand das machen will, dann macht er es auch. Sie können nur versuchen so gut es geht dagegen zusteuern, Prozesse dicht zumachen, Know-how-Abfluss zu verhindern oder horrende Strafen anzudrohen.

I: Herr S., vielen Dank für das Interview.

Beurteilung des Interviews:

Das zweite Interview dauerte knappe einundeinhalb Stunden. Die Antworten des Gesprächspartners waren sehr umfangreich und zeigten Einblicke in die betriebliche Praxis und getroffene Sicherheitsmaßnahmen. Für die Forschungsfrage irrelevante Äußerungen wurden nicht berücksichtigt.

B4 Transkript 4

Name:	Herr K.
Position:	Geschäftsführer, Firma Up.
Datum:	07.04.2011
Zeitraum:	15.00 - 16.00 Uhr

Interviewer (I): Herr K., ich darf mich nochmals bedanken, dass Sie sich die Zeit nehmen an diesem Interview teilzunehmen. Ich werde Ihnen jetzt in den nächsten 60 Minuten Fragen zu spezifischen Spionagerisiken Ihres Unternehmens stellen und diesbezüglich auf die Risikoanalyse und die Risikobewertung eingehen. Anschließend würde ich gerne auf die in Ihrem Unternehmen befindlichen Sicherheitsmaßnahmen eingehen. (...). Um Industriespionage wirkungsvoll begegnen zu können, empfiehlt sich zunächst eine Risikoanalyse. Inwieweit wurde bei Ihnen im Unternehmen denn eine Risikoanalyse durchgeführt, um spätere Know-how-Schutzmaßnahmen ergreifen zu können?

Herr K.: (…). Wir überlegen schon Schritte für uns, weil wir ja nicht besonders groß sind. Aber wir überlegen uns schon Schritte damit nicht gleich jeder Wettbewerber alles von uns mitkriegt. Wir sind im Laufe der Zeit dann dazu übergegangen, dass wir lieber falsche als gar keine Informationen streuen, da gar keine Informationen Wettbewerber dazu anstacheln sich Informationen zu holen. Falsche Informationen bringen den anderen hingegen dazu in die falsche Richtung zu gucken. Bis diese Fehlinformation bemerkt wird, ist man selber schon wieder ein Stückchen weiter, sodass es einem einen gewissen Vorsprung gibt. Das ist das gleiche wie mit Patenten. Ein falsch deklariertes Patent bringt den Wettbewerb dazu in die falsche Richtung zu gehen. (…). Die Risikoanalyse hieraus ist ja nicht nur auf Patente, sondern auch auf Verarbeitungsteile bedacht. Je nach Nachfrager der Informationen geben wir dann passende oder unpassende Informationen. Somit probieren wir das Risiko zu minimieren, aber das Risiko ist nicht komplett auszuschalten, denn das größte Risiko sind die Mitarbeiter, die speziell mit sensiblen Informationen vertraut sind und von anderen Unternehmen abgeworben werden.

I: Herr K., nun hatten Sie gerade erwähnt, dass der Mensch der größte Risikofaktor im Abfluss von Informationen ist. Könnte Sie noch einmal detailliert erklären wie Risikoanalysen in Ihrem Unternehmen ausgestaltet sind?

Herr K.: Auf der einen Seite wird geschaut, ob ein Mitarbeiter viel Know-how in sich vereint und sich unentbehrlich für das Unternehmen macht. (…). Daher ist es sinnvoll das Know-how auf viele Schultern zu verteilen. Allerdings sind nicht alle Sicherheitsmaßnahmen in einem solch kleinen Unternehmen, wie wir es sind, umzusetzen. Somit sind wir angreifbarer als ein Großunternehmen.

I: Sie hatten im Vorfeld des Interviews erwähnt, dass es bereits zu Betrugsfällen seitens der Mitarbeiter bei Ihnen im Unternehmen gekommen ist. Wiesen denn auch die Bereiche Organisation, Technik und Recht Risiken auf?

Herr K.: Ja, technische Angriffe hatten wir. Unter anderem wurde ein Patent gnadenlos nachgemacht. Aufgrund limitierter finanzieller Ressourcen, hatten wir aber gar nicht die Kraft dagegen anzugehen. Das muss man dann hinnehmen, obwohl man weiß, dass man im Recht ist. Der Ankläger muss ja zuerst in Vorleistung gehen und erhält erst bei Gewinn des Prozesses die Kosten erstattet, was oft nicht machbar ist. Für den Mittelstand sind Forschung und Entwicklung sowieso ein sehr schlimmes Ding. (…). Das liegt vor allem in den begrenzten finanziellen Ressourcen. Ich kann meistens eine Entwicklung nicht allein stemmen, also hole ich mir andere mit ins Boot, die ich beteilige oder die mich beteiligen. Damit habe ich schon das erste Sicherheitsrisiko, dass mich irgendwann ein Partner, bei gut laufendem Geschäft, ausbootet. Das ist natürlich ein großes Problem für den Mittelstand. Für eine große Firma ist das kein Problem. Die sieht ein lukratives Projekt und bewilligt dann schnell noch einmal weitere notwendige Gelder und dann wird das Ding durchgezogen. Das kann ich nicht machen. Wir haben jetzt ein Entwicklungsprojekt mit einem Münchener Unternehmen zusammen, dass einen völlig neuen Datenträger hervorbringt, der rein rechnerisch mit einem einzigen Druck auf einer Fläche von zehn mal zehn Millimeter ein Gigabyte Daten unterbekommt. Das ist natürlich ein heißes Teil. Das machen wir aber mit einem anderen Unternehmen zusammen und inzwischen haben sich weitere Unternehmen heran gehängt. Inzwischen gehen sich schon einige technisch in die Haare. (…). Hier entstehen natürlich Sicherheitsrisiken. Ich wandere also auf einem ganz schmalen Grad und muss aufpassen, dass ich weder links noch rechts herunterfalle.

I: Kommen wir von der Risikoanalyse nun zur Risikobewertung. Grundsätzlich geht man von der möglichen Schadenshöhe und der Schadenseintrittswahrscheinlichkeit aus. Gibt es noch weitere Parameter, die in die Risikobewertung mit einfließen?

Herr K.: Wenn ich etwas mache, fange ich nicht zuerst mit den Risiken an, sondern schaue mir erst einmal die Chancen an. Das Risiko wird erst ganz zum Schluss behandelt. Zum Teil weiß ich ja gar nicht welche Risiken auf mich zukommen. Ich will in erster Linie meine Chancen nutzen und schaue mir hier genau an, wie ich diese Chancen möglichst weit ausbauen kann. Erst dann schaue ich mir die Risiken an. Dabei kann es natürlich auch dazu führen, dass die Risiken höher als die Chancen sind. Das kann man im Detail nicht sagen. Man durchleuchtet Projekte auch auf Risiken, aber es gibt ja nicht nur das Risiko, dass mir jemand etwas wegnehmen will. Es gibt ja auch rechtliche, ökologische und viele weitere Risiken, die man bedenken muss. Solche Risiken kann man aber erst nach Betrachtung der Chancen richtig erkennen.

I: Gibt es denn auf Basis einer Analyse und Bewertung der Risiken eine Auflistung von zu ergreifenden Sicherheitsmaßnahmen in Form einer Prioritätenliste?

Herr K.: In kleineren mittelständischen Unternehmen wie unserem wird so etwas in Arbeitsgruppen festgehalten. Hier hält man Vorgehensweisen und Risiken fest. Man spricht jedoch vielmehr über die Risiken als dass man diese Risiken wirklich analysiert. Man geht eher an die Chancen als an die Risiken. Erst zum Schluss geht man etwas systematischer an die Risiken. Das kann man pauschal aber nicht sagen. (…).

I: Das heißt es werden keine expliziten Prioritätenlisten erstellt, sondern vielmehr geht es über eine zwischenmenschliche Kommunikation?

Herr K.: Ja, und auf eine schnelle Reaktion, was Vorteile für kleine Unternehmen hat (…). Der einzige Nachteil ist wie immer das finanzielle Risiko. Das ist das größte Risiko, weil wir zum Beispiel auch nicht die äußerliche Unterstützung für Forschung und Entwicklung wie Großunternehmen haben. Bis wir Forschungsgelder erhalten vergehen lange Zeiten, sodass die Projekte nicht mehr aktuell sind. Dann kann es auch sein, dass die Kosten der Antragsstellung höher als die Gelder sind, sodass so etwas bei uns nicht so gut funktioniert.

I: Gehen wir nun auf die bei Ihnen im Unternehmen getroffenen Sicherheitsvorkehrungen ein, um Informationsabflüsse zu verhindern und fangen wir mit personellen Maßnahmen an. Inwieweit werden denn im Rahmen der Personalakquisition sicherheitsrelevante Firmeninterna in Stellenausschreibungen veröffentlicht, die es Konkurrenten möglich machen auf Aktivitäten Ihres Unternehmens Rückschlüsse zu ziehen?

Herr K.: Das gibt es bei uns gar nicht. Wir geben bei einer Stellenausschreibung nur bekannt, dass wir jemanden für einen bestimmten Bereich benötigen. Alles weitere erfolgt dann intern, sodass niemand von außen Rückschlüsse ziehen kann. (…).

I: Und wie werden dann Bewerber in einem Personalauswahlverfahren auf sicherheitsrelevante Aspekte überprüft?

Herr K.: Wenn jemand bei uns eingestellt wird, muss er erstmal drei Tage auf Probe arbeiten. (…). In diesem Bereich kann man den Bewerber schon einmal ganz gut einschätzen. Dann kommt eine Probezeit, die wir sehr ernst nehmen und täglich kündigen können, sodass wir sofort eingreifen können. Als nächstes stellen wir, egal ob normaler oder leitender Mitarbeiter, unsere Leute zunächst nur befristet für zwei Jahre ein, um schnellst möglichst aus diesen Verträgen herauszukommen, falls etwas passiert. Wenn nach zwei Jahren keine gute Form mit dem Mitarbeiter gefunden wurde, wird das Arbeitsverhältnis beendet.

I: Werden denn im Rahmen der Überprüfung der Bewerbungsunterlagen auch ehemalige Arbeitgeber befragt oder Informationen zur früheren Ausbildung des Bewerbers eingeholt?

Herr K.: (…) wir fragen nicht bei früheren Arbeitgebern nach. Wonach wir gehen ist, dass wir schauen wie alt der Bewerber ist und wie viel Stellen er zuvor gehabt hat. Das steht ja im Lebenslauf drin. Was hat er dort gemacht? Gibt es darüber Zeugnisse? (…).

I: Das heißt individuelle Risikofaktoren wie Aufenthalte oder Kontakte in Risikostaaten werden nicht berücksichtigt?

Herr K.: Das darf ich ja rechtlich nicht. Ich darf ja nicht jemanden diskriminieren. Das kann zu enormen Konsequenzen führen. (…). Wir gucken aber schon hin, ob jemand rechtslastig ist. Dann greifen schon die sechsmonatige Probezeit und ein auf zwei Jahre befristete Arbeitsverhältnis.

I: Werden die Auswahlgespräche denn selbst von Ihnen durchgeführt?

Herr K.: Nein, ich sitze nur dabei. Grundsätzlich sind immer zwei Mitarbeiter damit beauftragt. Ich erhalte dann die Ergebnisse und bin dann die einzige autorisierte Person, die dann einstellt.

I: Kommt es denn im Fall einer Personaleinstellung auch zu Sicherheitsmaßnahmen wie Sicherheitsbelehrungen, Datenschutz- und Geheimhaltungsverpflichtungen?

Herr K.: Es gibt einmal den Arbeitsvertrag, der inzwischen ausgebaut und rechtlich abgesichert ist. (…). Hier arbeiten wir mit einer hannoverschen Rechtsanwaltskanzlei zusammen und gehen in jede Richtung, um uns rechtlich abzusichern. Das umfasst Arbeitsverträge, Geheimhaltungsverträge zu Kunden, Lieferanten und weiteren Partnern. Da sind wir schon sehr aktiv (…) und müssen aufpassen, dass wir uns für die Größe des Unternehmens nicht zu viel vornehmen (…). Letztendlich ist es doch so, dass wir als mittelständisches Unternehmen fast den gleichen Aufwand wie ein Großunternehmen betreiben müssen (…).

I: Herr K., Sie haben erwähnt, dass durch den Betrugsfall in der Vergangenheit eine Sensibilisierung innerhalb des Unternehmens stattgefunden hat. Wird der Informationsschutz seit diesem Vorfall bei Ihnen im Unternehmen als Chefsache behandelt?

Herr K.: Ganz sicher, auch im Datenschutz. Durch diesen Vorfall sind wir im Unternehmen sensibilisiert worden und schauen genauer hin. Das wissen auch alle. Deshalb ist auch bis auf Kleinigkeiten in der Vergangenheit nichts mehr passiert. Das lässt sich bei knapp 60 Mitarbeitern aber auch nicht verhindern. Insgesamt ist aber das, was uns wehtun würde, nicht mehr an der Tagesordnung.

I: Das heißt seit dem Vorfall wurden diverse Verbesserungen gemacht?

Herr K.: Nicht nur Verbesserungen. Wir haben Sprünge gemacht.

I: Findet denn auch eine Einbindung der Mitarbeiter in die Entwicklung von Know-how-Schutzmaßnahmen statt?

Herr K.: Nicht nur in Know-how-Schutzmaßnahmen. (…). Es geht aber nicht ohne den Druck seitens der Firmenleitung, denn viele Mitarbeiter sehen auf den ersten Blick nicht die Sinnhaftigkeit von Maßnahmen. Ein gutes Beispiel ist hier der Datenschutz. Unser Datenschutzbeauftragter war oft am verzweifeln, weil es Widerstand ohne Ende gab. Ich habe ihn immer motivieren müssen (…). Man muss hier sehr viel Überzeugungsarbeit leisten. Nur wenn jemand von etwas überzeugt ist (…) wird er durchziehen (…). Erst wenn ich jemanden überzeugt habe, hat er auch Spaß an der Arbeit. (…).

I: Herr K., Sie hatten erwähnt, dass nach dem Betrugsvorfall Sprünge im Informationsschutz gemacht wurden. Könnten Sie noch einmal explizit auf Sensibilisierungs- und Schulungsmaßnahmen eingehen?

Herr K.: Zunächst haben alle Mitarbeiter neue Arbeitsverträge erhalten. Zweitens wurden Maßnahmen ergriffen, die nicht restriktiv waren, sondern (…) wurde versucht die Sicherheitslücke im Vorfeld zu schließen und vorzubeugen. Das ist natürlich nicht so einfach, weil man ein Stückchen weiterdenken muss. Ich muss nicht verbieten, sondern es so aufstellen, dass erst gar nichts passiert.

I: Sie hatten angesprochen, dass Sie im Bereich des Informationsschutzes präventiv vorgehen und zufriedene Mitarbeiter Sicherheit für Ihr Unternehmen nach innen und nach außen schaffen. Würden Sie sagen, dass Ihre Mitarbeiter leistungsgerecht entlohnt werden und auch unentgeltliche Anerkennung für ihre beruflichen Leistungen erhalten?

Herr K.: (…). Grundsätzlich kann die Entlohnung aufgrund der Kopfzahl und des Produktes nur soweit erfolgen wie Gewinne vorhanden sind. Das muss man im Verhältnis sehen. Wenn ich über die Stränge lebe, mache ich das Unternehmen und letztendlich auch die Mitarbeiter kaputt. Ich muss es also so installieren, dass es vom Produkt und Gewinn stimmt, sodass die Mitarbeiter noch Spaß an der Arbeit haben und entsprechend Geld kriegen. So habe ich irgendwann umsatzbezogene Prämiensysteme für alle Mitarbeiter eingeführt. (…). Wir sind derzeit auf einem wirtschaftlichen Erfolgskurs, entsprechend hoch sind die Prämien der Mitarbeiter. Wobei Geld ja nur eine zeitliche und nicht die einzige Motivation ist. Grundsätzlich würde ich aber sagen, dass die Entlohnung gut ist. Das Arbeitsumfeld ist dazu auch gut. Ich sage aber bewusst nicht sehr gut, da das ein Superlativ ist, aber ich muss mich auch vor keinem verstecken.

I: Sprechen wir noch einmal die immateriellen Anreize an. Gibt es seitens der Unternehmensleitung ein Feedbacksystem?

Herr K.: Wir haben ein System eingeführt, wo die Leistung der Mitarbeiter durch Kleinigkeiten honoriert wird. Das können Tankgutscheine oder Einladungen für ein Essen sein. Die mache ich meist auch gar nicht selber, sondern das wird durch die Abteilungsleiter und Produktionsleiter durchgeführt (…). Das findet regelmäßig statt. Auch bei kleinen Jubiläen gibt es gleich eine ganze Feier für die Firma, wo zum Beispiel das Mittagessen auf eine Stunde ausgedehnt wird. Es soll immer so sein, dass der Mitarbeiter sieht, dass wir eine Familie sind. Dazu gehört auch, dass jeder Mitarbeiter zu mir oder seinem direkten Vorgesetzen gehen kann (…). Das dient dazu die Probleme der Mitarbeiter aufzunehmen, zu verarbeiten und

Verbesserungsvorschläge hereinzubekommen. Das wird versucht im Vorfeld zu lösen. Erst wenn etwas eskaliert werde ich eingeschaltet.

I: Gab es denn in der Vergangenheit Erhebungen zur Loyalität oder dem Identifikationsgrad der Mitarbeiter mit dem Unternehmen?

Herr K.: Jein. Über die ISO gibt es ja automatisch ein System über das alles bewertet wird, also die Arbeit und die Mitarbeiter. Von daher hat man hier einen guten Überblick. Das Unternehmen ist nicht so groß, dass man den Überblick nicht mehr hätte. Da muss nicht viel geschrieben werden. Das was durch die ISO, also durch das Managementsystem, kommt reicht dort voll aus.

I: Also gibt es keine expliziten Erhebungen?

Herr K.: Nein, direkt ausgerichtete Erhebungen gibt es nicht.

I: Kommen wir nun zur Beendigung eines Arbeitsverhältnisses. Welche Sicherheitsmaßnahmen gibt es bei einem regulären und nicht einvernehmlichen Ausscheiden eines Mitarbeiters?

Herr K.: Ja, den Fall haben wir gerade auch. Ein Mitarbeiter aus dem Labor wurde gekündigt (…) und da wir nicht sicher sind welche Schäden er im Nachhinein verüben könnte, haben wir ihn in eine andere Abteilung versetzt. Daraufhin hat sich der Mitarbeiter für einen längeren Zeitraum krank gemeldet, sodass wir eigentlich gut aus der Affäre gekommen sind. Das ist wirklich von Fall zu Fall unterschiedlich. Grundsätzlich wird bei erhöhter Gefahrenlage ein leitender Mitarbeiter oder ein Mitarbeiter aus dem Labor sofort vom Arbeitsplatz entfernt. Besteht auch das Risiko, dass er Daten herausholen könnte oder vernichten könnte, muss der Mitarbeiter sofort unter Beaufsichtigung einer Person seine Sachen packen und das Unternehmen verlassen. In dem Moment, wo der Mitarbeiter seine Kündigung erhält, sei es fristgerecht oder fristlos, steht sofort jemand bei ihm, sodass keine Schäden eintreten können. Aufgrund des rigorosen Vorgehens hatten wir bis jetzt auch noch keine Schäden in dem Bereich. (…). Wenn jemand geht ziehen wir das gesamte Programm durch.

I: Gibt es auch nach der Beendigung des Arbeitsverhältnisses eine Beobachtung des Mitarbeiters oder von Wettbewerbern?

Herr K.: Das kann man nicht so ganz. Das ist sehr schwierig, gerade wenn es zum Wettbewerb geht. Hier habe ich schon die tollsten Sachen erlebt. Es ist Krieg, das muss man einfach

so sehen. Der Wettbewerb sagt, dass er niemals unsere Mitarbeiter nimmt und kaum sind die Mitarbeiter aus unserem Unternehmen weg, sind sie bei Wettbewerb. Umgekehrt geht das natürlich auch. Wir haben einfach Krieg, das ist so. Dem muss man sich stellen. Man guckt natürlich hin wo wer bleibt. Wir hatten das letztens mit einem leitenden Mitarbeiter und gerade bei leitenden Mitarbeitern erfährt man öfters durch Kontakte, wo der jeweilige Mitarbeiter hingeht (…). Hier hat man schon theoretisch Einflussmöglichkeiten. Die praktische Anwendung möchte ich Ihnen hier nicht erzählen.

I: Anknüpfend an die personelle Sicherheitsmaßnahmen würde ich nun gerne auf die organisatorischen Sicherheitsvorkehrungen in Ihrem Unternehmen eingehen. Inwieweit existieren denn formal fixierte Sicherheitsstandards, wie eine Clean-Desk-Policy, die vor ungewolltem Know-how-Abfluss schützen sollen?

Herr K.: Insgesamt gesehen haben wir im Sicherheitsbereich zwei Teile, die Hardware und die Software. Die Software ist sehr weich, wo man von Fall zu Fall entscheiden muss. Die Hardware fängt bei den Türöffnungen an (…), sodass jeder sein Büro abschließen kann. Die Zutrittsmöglichkeiten sind reglementiert, sodass nur der Mitarbeiter in ein Büro kommt, der auch das Recht dazu hat. Des Weiteren kann ich an meiner Tür sogar kontrollieren wer in mein Büro gegangen ist und mich gleichzeitig auch kontrollieren. Das könnte man auch bei allen anderen Mitarbeitern machen, wobei Kontrolle immer so eine Sache ist. Hier stellt sich ja immer die Frage was ich alles kontrollieren will. Möchte ich alle Daten kontrollieren, die ich kriegen kann, oder nur ganz bestimmte. Ich kann mich auch überkontrollieren (…). Schlussendlich versuchen wir überall in der Firma, wo es notwendig ist, zu kontrollieren. Das heißt von Schließzuständen, über Wachpersonal, das zweimal die Nacht kontrolliert, über zunehmende Aufzeichnungen (…). Das betrifft nicht nur das Abstempeln, sondern auch Autos, deren Benutzung in einem Fahrtenbuch registriert wird. Somit probiert man für alle Bereiche Kontrollmaßnahmen durchzuführen, sodass diese auch noch Sinn machen. (…).

I: Gibt es denn spezielle Bestimmungen zur Nutzung, Vervielfältigung und Vernichtung von Informationsbeständen?

Herr K.: Ja, die gibt es. Hier haben wir im Laufe der Zeit einiges gelernt (…). Wir sind dort so rangegangen, dass wir uns gefragt haben, was uns passieren kann und was wir gar nicht verhindern können. Was wir nicht verhindern können ist, dass jemand mit einem Stick Daten abzieht. Dazu müsste ich alles mit Kameras ausstatten. Das kann ich gar nicht. Schlussendlich

muss man sich jedoch fragen wo schädigt mich jemand im Geld. Das ist der Punkt, der immer am Ende steht. Da komme ich wieder auf den Betrugsfall, wo ich reingefallen bin, wo Sie reingefallen wären, wo jeder andere reingefallen wäre. Diese Firma ist ein Einzelunternehmen, also kriege ich kein Gehalt, also werden mir immer mal Beträge auf mein Konto überwiesen. Ich habe das dann irgendwann regelmäßig in kleinen Mengen gemacht. Also habe ich irgendwann gesagt, dass ich gerne 1000 Euro auf mein Konto überwiesen haben möchte. Andere Tage war es dann 500 Euro. Hierzu wird jedes Mal ein Beleg ausgestellt, der jedoch systematisch in unserem Unternehmen gefälscht wurde. (…). Ich muss mich also in den Angreifer hineinversetzen, um mögliche Angriffspunkte zu entdecken. Das muss man herausfinden und dann in diesem Fall auch noch beweisen. (…). Man muss daher immer und egal in welcher Form auf der Hut sein. Man muss immer darüber nachdenken, dass jemand an mein Geld will. Der denkt über alles nach wie er darankommt. Also muss ich so denken wie mein Angreifer, damit ich weiß was er mir antun könnte. Darüber muss ich ständig nachdenken. Das habe ich daraus gelernt.

I: Gibt es denn auch ausreichende Kapazitäten zur Datenvernichtung?

Herr K.: Ja, Aktenvernichter sind in ausreichendem Maße vorhanden. Dort gibt es noch Unterschiede zwischen Aktenvernichtern. Hier gibt es welche, die etwas kreuz und quer vernichten und andere die Streifen machen, wo man aber auch nichts wiedererkennen kann. (…). Wenn Akten vernichtet werden, wird grundsätzlich eine Firma geholt, die dann die entsprechenden Akten unter Verschluss erhält, sodass wir da verhältnismäßig sicher sind. Ich sage aber immer verhältnismäßig, weil immer Risiken bestehen. Man muss aber auch immer sehen, dass wir nicht Siemens sind und von daher lohnt es sich nicht unbedingt bei uns einzusteigen (…). Man muss also auch immer die Dimensionen sehen, ob es sich für Angreifer lohnt oder nicht lohnt. Gerade das erwähnte Forschungsprojekt mit dem Datenträger ist sehr brisant. Das habe ich auch schon am eigenen Leib erfahren. Dort ging es schon richtig in die Vollen, wo der eine den anderen versucht hat auszubooten.

I: Herr K., Sie hatten ja bereits erwähnt, dass Informationsschutz in Ihrem Unternehmen als Chefsache betrachtet wird und der Sicherheitsbeauftragte mit eingebunden wird. Kann man also sagen, dass der Sicherheitsbeauftragte in Ihrem Unternehmen organisatorisch eng an die Geschäftsführung angebunden ist?

Herr K.: Ja. Dazu gehört nicht nur der Sicherheitsbeauftragte, der hier große Handlungsspielräume hat, sondern auch der Leiter der Qualitätssicherung und des Labors. Die beiden arbeiten sehr eng zusammen (…). Hier findet auch eine gegenseitige Kontrolle nach dem Vier-Augen-Prinzip statt.

I: Sie sprachen ja bereits die Zutritts- und Zugriffsrechte an. Gibt es denn innerhalb der EDV unterschiedliche Zugriffsrechte, je nach Position des Mitarbeiters.

Herr K.: Es gibt einen Hauptverantwortlichen und einen stellvertretenden Administrator, die für die Serveranlage zuständig sind. Hier haben wir versucht alle Maßnahmen zu ergreifen, dass unsere Daten nicht von alleine, wie durch Feuer, Wasser oder ähnliches, verschwinden können. Wir müssen immer wieder auf unsere Daten zurückgreifen können. Zum anderen haben wir einen Tresor und einen Aktenraum, der sehr stabil gebaut ist (…). Hier haben wir die besten Voraussetzungen (…), sodass wir dort die wichtigen Daten drin lagern. Grundsätzlich ist der Serverraum auch mit einer guten Stahltür gesichert. Von außen ist aber nicht ersichtlich, dass es sich um einen Serverraum handelt. Wir wollen also verhindern, dass Fremde es erst gar nicht versuchen dort hineinzugehen.

I: Sie hatten angesprochen, dass Kontrollen in Ihrem Unternehmen durchgeführt werden. Können Sie noch einmal detailliert darauf eingehen wie diese Kontrollen aussehen?

Herr K.: Die Kontrollen laufen auf Basis von Erfahrungen. Hier haben wir zum Beispiel den buchhalterischen Bereich (…), in den auch die sensible Entlohnung der Mitarbeiter fällt. Letztendlich geht es aber immer um das Geld. Das gilt auch für einen Einbruch in das Labor, wo wertvolles Know-how gestohlen wird. Auch hier geht es im Endeffekt um das Geld, egal in welcher Form. (…). Aufgrund unseres Betrugsfalls, würde ich heute speziell in der Lohnbuchhaltung Kontrollen immer durch Externe durchführen, um auf der sicheren Seite zu sein. Häufig ist man ja auch selbst einfach betriebsblind (…).

I: Kommen wir nun zu den technischen Know-how-Schutzmaßnahmen.

Herr K.: Übrigens das fällt mir noch ein. Wir kontrollieren auch Kunden, denn teilweise haben wir es in unserem Bereich auch mit Plagiaten zu tun. (…). Wir liefern ja auch viel an Zulieferer der Industrie (…) und sind dahingehend auch für Sicherheitsfragen sensibilisiert. Zum Beispiel gab es Plagiatsversuche in China (…).

I: Kommen wir zum Ende des Interviews noch einmal auf bautechnische Sicherheitsmaßnahmen. Sie haben erwähnt, dass die Außenhaut videoüberwacht ist. Bestehen hier weitere Sicherheitsmaßnahmen, wie Sicherungsräume für gefährdete Datenträger oder abhörschutzsichere Räume?

Herr K.: Abhörschutzsichere Räume haben wir nicht, denn unsere Informationen sind nicht so wertvoll, dass jemand daraus riesige Summen ziehen kann. Das funktioniert nicht. (…).

I: Gibt es denn verschlüsselte Leitungen zum Austausch von sensiblen Daten?

Herr K.: Warum denn? Hier dreht es sich doch nicht um sicherheitsrelevante Teile. Ich muss einfach den Auftrag durchziehen und kann mich nicht darum kümmern, ob der Auftrag geheimdienstlich überwacht wird. Das ist nicht mein Problem. Für mich ist es einfacherer, wenn ich das so durchziehe (…).

I: Kommen wir noch einmal auf den Punkt der Maßnahmen zur Sicherung der Informations- und Kommunikationstechnik zu sprechen. Ihr Sicherheitsbeauftragter hatte im Vorfeld des Interviews erwähnt, dass es für die einzelnen PCs Accounts sowie eine Passwortpflicht gibt. Existiert denn auch ein systematischer Passwortwechsel?

Herr K.: Ja, der muss nach drei Wochen immer durchgeführt werden, wird manchmal aber nicht durchgeführt, weil es noch nicht gezwungenermaßen besteht. Wir sind aber dabei, dass wir jeden zwingen ein neues Passwort zu machen. (…), wobei ich Passwörtern noch nicht einmal so viel zumesse. Man kann, wenn man es raffiniert macht, auch Tastaturen auslesen. Dann spielt es keine Rolle ob ich ein Passwort habe. Zum anderen können selbst unsere Administratoren Passwörter knacken, die hier nicht wieder auffindbar waren. Selbst die können das machen. Besser ist es, wenn ich den ganzen Computer schütze.

I: Gibt es denn ausreichende Schutzprogramme?

Herr K.: Alles kann ich natürlich nicht schützen, weil wir ja auch über das Internet arbeiten. Wenn uns von dort jemand abzapft habe ich ein Problem. Also muss ich Erschwernisse, aber nicht Verhinderungen einbauen. Dafür sind wir zu klein. Erschwernisse bestehen darin, dass aus bestimmen Computern alle Datenspeichermöglichkeiten heraus gebaut werden. Es gibt keinen USB-Zugang, es gibt keine CD-Lesung oder CD-Brennung. Man kann also nur mit dem PC arbeiten, mehr nicht. Das haben wir ziemlich gut durch alle Computer durchgezogen, sodass jeder Computer einigermaßen auf den Arbeitsplatz abgestimmt ist. Es wird nicht re-

gelmäßig überprüft, aber es muss immer im Verhältnis zu dem sein was wir machen. Alles nur auf Sicherheit auszurichten wären falsch.

I: Aber Sie würden schon sagen, dass es noch Verbesserungspotenziale in der Sicherung der Informations- und Kommunikationstechnik gibt?

Herr K.: Ja, ganz sicher.

I: Kommen wir zum Schluss zu rechtlichen Sicherheitsvorkehrungen. Sie sprachen bereits Geheimhaltungsvereinbarungen zwischen Ihren Mitarbeitern und dem Unternehmen an. Können Sie noch einmal auf Geheimhaltungsvereinbarungen zwischen Ihrem Unternehmen und Geschäftspartnern eingehen?

Herr K.: Das ist unterschiedlich. Grundsätzlich hat jeder, der das Unternehmen betritt eine Datenschutzerklärung zu unterschreiben. Zweitens sind die Sicherheitsvorkehrungen von den Produkten und ihrer Nutzung abhängig (…). In bestimmten Bereichen schicken wir dem Kunden eine Geheimhaltungsvereinbarung und in anderen Bereichen erhalten wir von unserem Kunden eine. Das kann man nicht genau definieren. Es kommt immer auf den Fall und das Produkt an. (…).

I: Werden bei Verstoß gegen Geheimhaltungsvereinbarungen auch Sanktionen und rechtliche Konsequenzen eingeleitet?

Herr K.: Das ist auch unterschiedlich und kommt auf den Fall an. Geht man beispielsweise in den Flugzeugbau, kann man für eine Menge haften und sogar Versicherungen abschließt, die mit in die Kalkulation eingehen. Man muss also oft vor der Auftragsannahme in eine Vertragsprüfung gehen. Oft schießt der Partner über das Ziel hinaus (…), sodass oft Verträge nachverhandelt werden, um einen richtigen Schutz zu gewährleisten. Nicht zu viel, aber auch nicht zu wenig.

I: Sie hatten auch den Bereich der Patente erwähnt, die zur rechtlichen Absicherung von explizitem Know-how dienen. In was für einem Umfang findet eine Patentanmeldung bei Ihnen im Unternehmen statt?

Herr K.: Das hatte mal einen riesigen Stellenwert, bis wir mit einigen Patenten richtig auf die Nase gefallen sind, da trotz Patentanmeldung Produktfälschungen entstanden, sodass wir von Patentanmeldungen weggehen. Wir haben es in einem Patent auch so beschrieben, dass der

Wettbewerb lange suchen muss bis er dort hinterherkommt. Hier habe ich auch gelernt, dass es viele Patente gibt, die gar nicht das patentieren, was sie patentieren sollen, sondern den Wettbewerb in die falsche Richtung schicken sollen. Die Patentämter übernehmen ja nur die Registrierung. Die Überwachung der Patente muss man über einen Patentanwalt machen und das kostet viel Geld. (…). Klagen Sie mal gegen einen Chinesen, der Ihre Patente nachmacht und gehen Sie vor chinesisches Gericht, weil das ausgerechnet auch noch der Erfüllungsort ist (…). Sie bewegen sich hier in einem ganz anderen Rechtsraum und kennen die Sprache Schrift und Kultur nicht. Von daher haben wir davon eher die Finger gelassen. Heute machen wir nicht Patente als Patente, sondern (…) zur Desinformation des Wettbewerbs.

I: Bestehen denn auch spezielle Sicherheitsmaßnahmen zwischen Ihrem Unternehmen und Zertifizierungsgesellschaften?

Herr K.: Zertifizierungsgesellschaften sind für uns nicht das Hauptproblem. Das viel größere Problem sind die Maschinenhersteller, die genau wissen wie wir unsere Produkte fertigen. Hierbei werden ja bei Kauf der Maschine bestimmte Vorgaben von unserer Seite gemacht (…). Damit weiß der Maschinenbauer aber genau was ich haben will. Hier sehe ich das größte Risiko, wenn diese Informationen weitergegeben werden (…). So versuchen wir uns unsere Vorgaben mit Geheimhaltungsverträgen und Regresszahlungen zu schützen. Wir sind zum Teil sogar hingegangen und haben bestimmte Vorgaben dem Maschinenhersteller gemacht, um im Nachhinein die Anordnung von Bauteilen zu verändern, sodass keine Rückschlüsse erfolgen können. Hier sehe ich das größere Risiko drin. (…).

I: Damit sind wir am Ende des Interviews. Ich darf mich nochmals für das Interview bedanken.

Beurteilung des Interviews:

Bereits vor dem Gespräch zeigte sich der Gesprächspartner sehr kooperativ und gewährte einen Rundgang durch sein Unternehmen. Während des Interviews konnten wertvolle Erkenntnisse zum sicherheitsrelevanten Vorgehen kleiner und mittlerer Unternehmen gesammelt werden. Mit einer Dauer von circa einer Stunde konnte der angestrebte Zeitrahmen eingehalten werden. Überflüssige Passagen wurden gestrichen.

B5 Transkript 5

Name:	Herr B.
Position:	Fachbereichsleiter Konzernsicherheit, Firma C.
Datum:	11.04.2011
Zeitraum:	14.00 - 15.00 Uhr

Interviewer (I): Herr B., ich darf mich nochmals bedanken, dass Sie sich die Zeit für dieses einstündige Interview nehmen. Im Rahmen des Interviews werde ich Ihnen Fragen zur Risikoanalyse und Risikobewertung sowie den in Ihrem Unternehmen befindlichen Sicherheitsmaßnahmen stellen. Dabei werde ich auf die Bereiche Personal, Organisation, Technik und Recht eingehen. (…). Um Industriespionage wirkungsvoll begegnen zu können, empfiehlt sich zunächst eine Risikoanalyse. Inwieweit wurde bei Ihnen im Unternehmen denn eine Risikoanalyse durchgeführt, um spätere Know-how-Schutzmaßnahmen ergreifen zu können?

Herr B.: Es ist immer die Frage was man unter Know-how-Schutz versteht. Wo fängt das an, wo hört das auf. Wir führen in verschiedensten Bereichen regelmäßige Risikoanalysen durch. Wenn Sie einmal den klassischen Hardwareteil sehen, macht hier der Bereich IT-Security regelmäßig strukturierte Analysen. Wir führen aber auch weiterführende Analysen zum Bereich Plagiatsschutz durch. Das fängt bei Greenfield-Projekten mit anderen Standorten an, sodass wir gucken wo man hingehen und man nicht hingehen kann. (…). Wir führen also nicht nur eine Risikoanalyse durch, sondern auf verschiedensten Ebenen und Bereichen und führen diese dann zentral zusammen.

I: Herr B., Sie sprachen an, dass Risikoanalysen auf verschiedensten Ebenen durchgeführt werden. Können Sie spezifizieren in welchen Bereichen die Risiken am größten sind?

Herr B.: Die Summe der Risiken macht das Risiko aus. Das fängt im HR-Bereich an, wo ich mich frage wen ich einstelle und wie ich ein vernünftiges Mitarbeiterbindungsprogramm aufbaue. Nicht jeder, der Informationen abfließen lässt, ist kriminell. Das kann zum einen mangelnde Awareness sein, das kann zum anderen auch daran liegen, dass das Unternehmen es nicht geschafft hat einen Know-how-Träger vernünftig an das Unternehmen zu binden. (…). Hier fahren wir ganz klare Programme, wo wir Know-how-Träger identifizieren und mit denen dann langfristige, kostspielige Bindungsprogramme machen. Know-how-Abfluss passiert aber auch beim Consulting. Wenn Sie über Industriespionage lesen, denkt man zuerst an den

klassischen Geheimagenten, der Informationen beschafft. Aber was ist mit dem Consulter? Dort erwarten wir, dass er fragt. Dort geben wir Unterlagen mit. Der arbeitet gleichzeitig für viele Firmen. Joint-Ventures sind natürlich auch ein riesiges Problem. Das ist sehr vielseitig, sodass ich hier keinen Schwerpunkt legen kann.

I: Also ist es die Summe der Risiken.

Herr B.: Ja, es kommt auch immer darauf an was Sie unter Know-how verstehen. Verstehen Sie unter Know-how nur Technologie oder gehört es auch dazu wie man seine Unternehmensfinanzen vernünftig aufstellt? Dort sieht man, dass es sehr viele Angriffspunkte gibt. Ein Unternehmen kann auch sehr viel an Know-how verlieren, wenn gewisse Kennzahlen an falsche Stellen gelangen. Know-how ist auch eine Einkaufsstrategie, die wir haben. Mir ist das immer zu platt, das alles nur auf die Forschungs- und Entwicklungsseite oder nur auf die IT-Seite zu packen. Wir sehen das als ein ganzheitliches Projekt (…), bei dem unterschiedliche Fachabteilungen zusammenarbeiten. (…). Wir gehen hier also ganzheitlich und interdisziplinarisch vor. Dort ist keine Schranke zwischen IT, Recht, HR, Kommunikation oder Sicherheit, sondern ganzheitlich über die gesamten Fachabteilungen hinweg.

I: Werden denn ausgehend von den Risikoanalysen, die auf unterschiedlichen Ebenen stattfinden, im Rahmen der Risikobewertung neben der Schadenseintrittswahrscheinlichkeit und der möglichen Schadenshöhe weitere Parameter berücksichtigt? (...).

Herr B.: Das ist schwer zu beantworten. Sicherlich spielen Eintrittswahrscheinlichkeit und der mögliche Schaden eine Rolle. Haben wir eine geringe Eintrittswahrscheinlichkeit, aber einen hohen Schaden, wird man sich darum kümmern. Haben wir eine hohe Eintrittswahrscheinlichkeit bei geringen Schäden, wird man sich auch darum kümmern. Wir versuchen aber auch schon im Kaffeesatz zu lesen wo Strömungen oder Mega-Trends hingehen können. Das hat nicht unbedingt was mit Eintrittswahrscheinlichkeiten zu tun, sondern man fragt sich wo politische Strömungen hingehen könnten. Das könnte noch ein Parameter sein, aber sicherlich die Eintrittswahrscheinlichkeit und die Höhe der möglichen Schäden die maßgeblichen Größen. Die Risikoarten sind aber sehr unterschiedlich.

I: Wird auf Basis der Analyse und Bewertung von Risiken auch eine Prioritätenliste erstellt, um die Risiken mit entsprechenden Maßnahmen zu bearbeiten?

Herr B.: Es gibt dort je nach Bereich in Nuancen Unterschiede. Wir machen eine Risikoanalyse immer nach sieben Schritten. (…). Die erste Frage ist was ich überhaupt schützen möchte. Was ist also mein Schutzziel? Diese Frage stellen wir uns immer als erstes im Risikomanagement. Angefangen vom Ruf des Unternehmens, dem Know-how, Sabotage, Korruption, Verluste von Marktanteilen, Lieferfähigkeit (…). Wenn wir wissen was wir schützen wollen, überlegen wir uns zunächst was die möglichen Bedrohungen für unsere Schutzziele sind. Wer oder was auf diese Ziele entsprechend einwirken. Wenn wir das haben können wir schon sagen, ob das ein abstraktes oder reales Risiko ist. Dann schauen wir uns an was für Auswirkungen das Risiko bei einem Eintritt hätte. Dann werden Eintrittswahrscheinlichkeit und Auswirkungen in ein Verhältnis gesetzt. Zusätzlich machen wir auch noch den Schritt, dass wir mögliche Gegenmaßnahmen beschreiben. Dort fällt einem auch viel ein und hier erlebt man in Unternehmen auch viel Aktionismus. Wenn wir die Maßnahmen alle beschrieben haben, stellen wir uns die Frage um wie viel wir das Risiko tatsächlich reduzieren, also Eintrittswahrscheinlichkeit oder Auswirkungen. Das ist also eine Art Rückprüfung. Dort muss ich Ihnen aber erschreckenderweise sagen, dass man oft viel macht, es aber nicht viel bringt. Dort beschäftigen wir uns dann auch mit dem was wirklich etwas bringt. (…). Wir arbeiten bei erkannten Risiken aber auch mit der klassischen Ampel. Solange die Ampel auf Grün ist, passiert auch nichts. Manchmal setzen wir aber Themen auf Gelb, weil wir meinen, dass hier irgendetwas passieren könnte. So bereiten wir uns auf jede Eventualität, die uns einfällt, vor. Hier kann man dann Gegenmaßnahmen am Markt oder in der Kommunikation treffen. In der roten Phase wird dann wirklich was unternommen.

I: Ok. Nun würde ich gerne zum Bereich Personal übergehen. Inwieweit werden denn sensible Firmeninterna in Stellenausschreibungen veröffentlicht?

Herr B.: Was meinen Sie damit?

I: Mit Firmeninterna sind zum Beispiel Technologien gemeint, die der zukünftige Arbeitnehmer verwendet und die möglicherweise Wettbewerbern Rückschlüsse auf Tätigkeiten des Unternehmens geben könnten.

Herr B.: Wissen Sie, (…) unsere Kunden sagen uns in der Regel mit welcher Technik wir arbeiten und das sagen sie auch dem Wettbewerb. Von daher ist das aus meiner Sicht eher ein sehr theoretischer Ansatz. Die Instrumentarien, die man verwendet, sind häufig gleich. Die Verfahren, die man dann erst später mitbekommt wenn man hier arbeitet, sind sicherlich un-

terschiedlich. Ich kann Ihnen auch sagen, dass wir mit einem Wettbewerber ganz eng auch auf Konzernsicherheitsebene zusammenarbeiten. Das erwarten auch unsere Kunden. Es gibt natürlich auch Dinge, wo man etwas verschwiegener ist. Dass wir in einer Stellenausschreibung schreiben, dass jemand für den Bereich Einkauf oder HR mit SAP-R/3 umgehen können muss ist nicht wirklich etwas Vertrauliches. (…).

I: Kommen wir nun zum Personalauswahlverfahren. Findet dort eine intensive Überprüfung der Bewerber statt?

Herr B.: Es finden Überprüfungen statt, die im gesetzlich zulässigen Rahmen sind.

I: Werden denn im Rahmen der Überprüfung auch frühere Ausbildungsstätten oder Arbeitgeber des Bewerbers kontaktiert?

Herr B.: Es werden sicherlich im Rahmen der gesetzlichen Maßnahmen Dinge auf Plausibilität abgeprüft. Allein schon die Anti-Terror-Gesetzgebung gibt uns gewisse Prüfpflichten vor. Sie wissen aber auch, dass die Prüfung von sozialen Netzwerken rechtlich nicht ganz einfach ist und das Personalauswahlverfahren sicherlich rechtlich noch erschwert werden wird.

I: Werden denn individuelle Risikofaktoren, wie Kontakte oder Aufenthalte in Risikostaaten berücksichtigt?

Herr B.: Wir haben ein Anti-Diskriminierungsgesetz. Das schließt so etwas aus.

I: Kommt es, wenn der Bewerber das Auswahlverfahren positiv durchlaufen ist, auch zu Sicherheitsmaßnahmen in der Personaleinstellung? Inwieweit finden Sicherheitsbelehrungen, Datenschutz- und Geheimhaltungsverpflichtungen zwischen Ihrem Unternehmen und dem Neueinsteiger statt?

Herr B.: Auf formeller Seite sind natürlich die Geheimhaltungs- und Datenschutzerklärungen zu unterschreiben. Das ist ein gängiger Prozess. Zusätzlich gibt es ein Programm, wo Neueinsteiger vom Gesundheitsschutz bis zur Sicherheit sensibilisiert werden.

I: Wie ist denn der allgemeine Umfang von Sensibilisierungs- und Schulungsmaßnahmen für Mitarbeiter, um Know-how-Abflüsse zu verhindern?

Herr B.: Dort sind wir gerade dabei etwas Größeres auszurollen, aber es ist nicht immer der Mitarbeiter das Problem. Es ist das Gesamtverständnis im Unternehmen. Zum einen möchte

man Geschäfte machen und sieht große Märkte. Auf der anderen Seite sieht man auch das Risiko in den Märkten. Hier muss dann jemand entscheiden was mehr wiegt. (…). Ich muss Ihnen einfach sagen, dass bei einem Engagement in China einfach Know-how abfließen wird. Das können Sie nicht schützen.

I: Also würden Sie sagen, dass der Informationsschutz in Ihrem Unternehmen als Chefsache betrachtet wird?

Herr B.: Ja, auf jeden Fall. Ich habe für ein Sicherheitsprojekt den Vorstand als Sponsor gewinnen können. (…).

I: Gibt es denn auch eine Einbindung der Mitarbeiter bei der Entwicklung von Know-how-Schutzmaßnahmen?

Herr B.: (…). Es ist wichtig, dass Know-how-Träger wissen, dass sie dieses Know-how besitzen. Aber die Schließung von Sicherheitslecks kann nicht Aufgabe einer Abteilung sein. Das muss zentral koordiniert werden. Bei der Entdeckung von Lecks werden dann die jeweiligen Spezialisten eingeschaltet. (…).

I: Loyalität und Zufriedenheit der Mitarbeiter schafft Sicherheit im Unternehmen und auch nach außen. Würden Sie sagen, dass Mitarbeiter in Ihrem Unternehmen leistungsgerecht entlohnt werden?

Herr B.: (…). Ja. Ich glaube, dass wir eine marktkonforme Entlohnung haben. Ich glaube aber nicht, dass Informationsabfluss nur finanziell zu erklären ist. Loyalität hängt von anderen Punkten ab. Wie geht das Unternehmen zum Beispiel in der Wertschätzung mit mir um? Das ist nicht nur Geld.

I: Ja, das stimmt. Daher war meine erweiterte Frage auch welche immateriellen Anreize das Unternehmen stellt, um die Mitarbeiter an das Unternehmen zu binden?

Herr B.: Das ist ganz unterschiedlich. Wir haben aus der Vergangenheit gelernt, dass man den Mitarbeiter nicht nur als Arbeitsressource sehen darf. Von daher haben wir über den Tarifvertrag hinausgehend soziale Regelungen. Wir haben ein hervorragendes Sozialsystem, wenn Mitarbeiter private oder persönliche Probleme haben. Wir machen auch Firmenveranstaltungen mit den Familien. Das ist das eine, was viele Firmen haben. Dann gibt es aber Know-how-Träger, die wir versuchen zu identifizieren (…) um dem Menschen das Arbeitsleben so

schön wie möglich zu machen. (…). Dort werden sehr individuelle Programme gemacht. Es werden Abteilungsleiter und Leiter von Business-Units danach entlohnt wie hoch deren Fluktuation ist. Insbesondere gibt es hier eine Klausel für die Know-how-Träger. (…). Es wird als klares Managementziel auf die einzelnen Ebenen herunter gebrochen, dass die Leute zu halten sind.

I: Also besteht neben der monetären Komponente auch ein weitgefächertes immaterielles Anreizsystem?

Herr B.: Ja.

I: Gibt es denn Instrumente oder Erhebungen zur Messung der Loyalität oder Zufriedenheit der Mitarbeiter?

Herr B.: Ja, wir haben verschiedenste Messinstrumente. Einmal eine Basic-Life-Umfrage, die alle zwei Jahre jedem Mitarbeiter zugestellt wird. Hier werden genau solche Themen abgeklopft. (…). Zusätzlich gibt es abteilungsinterne Untersuchungen, wo die Vorgesetzten, die Führungsebene und das Klima innerhalb der Abteilung bewertet werden. Ein Jahr wird also sehr auf den Bereich und das andere Jahr sehr auf den gesamten Konzern fokussiert.

I: Und wie waren die Ergebnisse dieser Erhebungen?

Herr B.: Das ist von Jahr zu Jahr unterschiedlich. Man merkt bei feindlichen Übernahmen (…) oder in Zeiten der Wirtschaftskrise, dass es nicht so läuft. Allerdings ist die Umfrage nicht das Entscheidende, sondern wir messen danach noch den Umsetzungsgrad der aus der Umfrage entstandenen bereichsspezifischen Aktionsprogramme. Das dient besonders auch der Glaubwürdigkeit solcher Umfragen (…). Mittlerweile haben wir eine Umsetzungsquote von 70 Prozent. Das ist recht gut.

I: Und wie verhält es sich mit den Sicherheitsmaßnahmen bei der Personalfreistellung?

Herr B.: Dort haben wir vor etwa einundeinhalb Jahren eine Analyse gemacht und festgestellt, dass wir hier enorme offene Flanken hatten, die aber nicht ganz einfach zu schließen waren und es auch noch nicht sind. Es gibt Prozesse, wenn man erfährt, dass ein Mitarbeiter das Unternehmen verlassen möchte. Hier prüft man zum Beispiel an welche Daten der Mitarbeiter noch heran darf. Das ist aber ein theoretischer Ansatz, denn in der Regel sind die Daten, schon bevor Sie etwas davon mitbekommen, abgeflossen. Das zweite ist, dass wir den Mitar-

beiter beim Ausscheiden auch auf die Geheimhaltungsvereinbarung und die möglichen rechtlichen Konsequenzen hinweisen. Das geht so weit, dass wir uns von einem Bewerber, der vom Wettbewerb kam und uns Unterlagen angeboten hat, sofort wieder getrennt haben. Obwohl er für uns nützliche Dinge hatte, haben wir das abgelehnt, weil wir gesagt haben, dass das nicht unsere Kultur ist. Die andere Sache ist (…), dass zwar Wettbewerbsvereinbarungen und Geheimhaltungsklauseln in vielen Betrieben gemacht werden, nur die rechtliche Umsetzung sehr schwierig ist. Fassen Sie es zu weit, wird jedes Gericht sagen, dass der Mitarbeiter danach ja gar nichts mehr machen kann. Fassen Sie es zu eng, ist der ausscheidende Mitarbeiter wieder auf der sicheren Seite. Das ist aber zum Teil nur theoretisch, weil man ja immer die getroffenen Maßnahmen auch bezüglich ihrer Wirkung überprüfen muss. Das ist hier sehr bedenklich.

I: Könnten Sie noch einmal Ausführungen zu den Sicherheitsvorkehrungen bei regulärem und nicht einvernehmlichen Ausscheiden machen? Sind die Sicherheitsmaßnahmen dort rigoroser?

Herr B.: Ja, die sind rigoroser. Das hängt aber auch sehr vom Grund des Ausscheidens ab. Es kann sein, dass wir jemanden sofort freistellen und ihm gar keinen Zugang mehr zum Standort und den Unterlagen gewähren. Es kann sein, dass man sich Gedanken darüber macht, was er noch an Unterlagen haben könnte. Man entwickelt dann für die einzelnen Fälle individuelle Lösungen.

I: Findet nach der Beendigung des Arbeitsverhältnisses auch eine intensive Beobachtung des ehemaligen Mitarbeiters und von Wettbewerbern statt?

Herr B.: Dafür gibt es keinen rechtlichen Rahmen.

I: Wie sieht es denn mit firmenfremden Personal, wie Beratern, Sicherheits- und Reinigungspersonal und Handwerkern aus? Gelten für diese die gleichen oder noch strengere Sicherheitsregelungen?

Herr B.: Das ist je nach Einsatzgebiet unterschiedlich, grundsätzlich aber gleich oder strenger.

I: Gab es denn bisher Vorfälle von Know-how-Abfluss durch firmenfremdes Personal?

Herr B.: Wir haben Know-how-Abfluss von firmeneigenem als auch von firmenfremden Personal.

I: Kommen wir nun zu den organisatorischen Schutzmaßnahmen in Ihrem Unternehmen. Inwieweit bestehen bei Ihnen im Unternehmen formal fixierte Sicherheitsstandards, die vor Know-how-Abfluss schützen sollen? Gibt es eine Clean-Desk-Policy?

Herr B.: Ja, die gibt es.

I: (...). Wie hoch ist denn überhaupt die Erfolgsquote solcher organisatorischen Schutzmaßnahmen?

Herr B.: (…). Das ist ein ganz wesentlicher Punkt. (…). Hier muss man sich die Frage stellen, was die Konzernsicherheit überhaupt alles regeln soll. Hier konnte ich feststellen, dass in vielen Konzernen in den Zentralen tolle Dinge ausgedacht werden, die in der Praxis nicht funktionieren. (…). Wir gehen mit unserem Regelwerk eine ganz klare Philosophie. Wir regeln so viel wie nötig und so wenig wie möglich, um den einzelnen unterschiedlich geprägten Geschäftsbereichen die Möglichkeit zu geben möglichst flexibel zu sein. Dann haben wir unsere Guidelines und Policies in zwei Kategorien eingeteilt. Dort werden zum einen Ziele beschrieben, wobei der Weg dorthin den Standorten frei bleibt. Ein Beispiel wäre das Ziel, dass keine Unbefugten auf das Betriebsgelände kommen. (…). Hier wird nur das Ziel beschrieben. Dann haben wir einige wenige Dinge, wo Ziel und Weg genau beschrieben sind. Zum Beispiel die Klassifizierung von Informationen in „öffentlich“, „intern“ und „vertraulich“. Das ist eine ganz strikte Regelung. Wie ich mein Objekt schütze ist jedoch weiter offen. Wir messen uns auch monetär am Umsetzungsgrad der Policies, die wir herausgeben. Nur wenn diese Policies auch im letzten Standort gelebt werden, haben wir einen guten Job gemacht.

I: Herr B., Sie hatten erwähnt, dass aufgrund der Unternehmenshistorie die Standorte zum Teil auf dem Weg der Zielerreichung Freiheiten haben. Wie sieht es bei der Nutzung, Vervielfältigung und Vernichtung von Informationsbeständen aus? Gelten dort auch klare Richtlinien?

Herr B.: Ja, dort gelten klare Richtlinien.

I: Könnten Sie das etwas konkreter ausführen?

Herr B.: Erstmal haben wir eine Dreistufigkeit, in der wir Informationen klassifizieren: „öffentlich“, „intern“, „vertraulich“. (…). Hinter diesen Klassifizierungen stehen jeweils Sicherheitskonzepte wie ich mit den Daten umzugehen habe. Dort ist auch die Vernichtung geregelt, die bis dahin geht, welche Qualität ein Aktenvernichter haben muss. Es ist aber auch ein

Problem, dass viele Bereiche Policies erlassen. Der Endnutzer weiß oft gar nicht wo er die Policies findet. Das haben wir jetzt mit einem Tool gelöst (…), sodass der Endnutzer genau die Informationen erhält, die er braucht.

I: Ist denn Ihr Bereich der Konzernsicherheit auch eng organisatorisch am Vorstand angebunden?

Herr B.: Ja, das ist er. Ich berichte direkt dem Personalvorstand.

I: Werden seitens des Vorstands der Konzernsicherheit auch Freiheiten in der Ausübung der Tätigkeiten gegeben?

Herr B.: Das ist genau das was unser Unternehmen ausmacht. Wir sind ein Unternehmen, das sehr schlanke Hierarchien hat. (…). Man bekommt bei uns klare Zielvorgaben, die man tunlichst einzuhalten hat, aber der Weg dorthin und die Gestaltungsfreiheit ist in diesem Unternehmen genial.

I: Wie sind denn die Zugriffsrechte in Ihrem Unternehmen ausgestaltet?

Herr B.: Zugriffsrechte auf unsere Daten werden durch erheblich organisatorische und technische Maßnahmen sichergestellt. (…), dass man einen ständigen Wechsel von Passwörtern hat, dass man Mindestanforderungen an Passwörter hat, dass es Schutzmaßnahmen zum Datentransfer gibt oder dass es klare Richtlinien bei Joint-Ventures gibt. (…). Wenn ein Mitarbeiter länger nicht an seinem Computer war, wird sein Passwort gesperrt. Des Weiteren hat er auch kein Masterpasswort über alle seine Systeme, sondern er muss sich permanent in unterschiedlichen Systemen anmelden. Wir arbeiten bei mobilen Systemen mit VPN-Verschlüsselung. (…). Hier haben wir aufgrund hoher Sicherheitsmaßnahmen eher Probleme in der Verfügbarkeit der Daten.

I: Herr B., das Aufsetzen von Sicherheitsmaßnahmen und die Umsetzung sind ja zwei verschiedene Paar Schuhe. Werden denn auch zur Überprüfung der Umsetzung auch Kontrollen durchgeführt und wenn ja, in welchen Abständen?

Herr B.: Ja und nein. Zumindest für Deutschland sind solche Themen mitbestimmungspflichtig, sodass man für jeden Standort Genehmigungen haben muss. Das normale Prozedere ist, dass wir einmal im Jahr sogenannte Informationsschutzbegehungen an den Standorten unangemeldet in der Nacht machen. Hier wird die Clean-Desk-Policy, die Passwortpolitik oder

Ähnliches überprüft. Wir haben aber nicht für jeden Standort in Deutschland die Genehmigung von den Sozialpartnern bekommen. Dann können wir das auch nicht tun.

I: Und wie wird das im Ausland gehandhabt?

Herr B.: Dort gibt es keine Mitbestimmung, dort tun wir das.

I: Und inwieweit gibt es bei Sicherheitsverstößen Sanktionen beziehungsweise bei sicherheitsbewusstem Handeln Belohnungen?

Herr B.: Das ist ein abgestuftes Prozedere. Erst einmal ist eine Konzernsicherheit keine Einheit, die bestraft. Wir stellen nur Sachverhalte fest und bestrafen tun andere neutrale Stellen. Wir machen das so, dass bei kleineren Verstößen nur ein Zettel auf dem Schreibtisch liegt (…). Zum Beispiel müssen Mitarbeiter bei unzureichender Sicherung der Notebooks sich diese an einer Stelle wieder holen. Das kann je nach Härte des Verstoßes bis zu arbeitsrechtlichen Konsequenzen führen. Es ist aber so, dass wir die Leute nicht mit der schlagenden Hand gewinnen wollen, sondern vielmehr überzeugen wollen. (…).

I: Inwieweit werden denn Mitarbeiter auch für die Gefahren von Geschäftsreisen sensibilisiert?

Herr B.: (…). Hier gibt es eine grundsätzliche Informationsschulung. Bei Reisesicherheit ist das auch immer ein ständiges Thema. Das ist das allgemeine Tätigkeitsfeld. Wenn man dann in Krisenländer fährt, wird man noch einmal individuell für seinen Job geschult. Dass man zum Beispiel in der Business-Class nicht sein Notebook offen einsehbar hat oder Ähnliches, wird im allgemeinen Teil geregelt. In Russland müssen Sie sich schon genau überlegen, ob Sie das nette Mädchen in das Hotelzimmer herein lassen oder was Sie in den Papierkorb schmeißen. Das sind nicht nur die vertraulichen Unterlagen. Das kann das Kondom oder auch die Flasche Wodka sein. All das womit Sie erpressbar sind. Das machen wir bei gewissen Funktionen in Einzelgesprächen. Das muss nicht unbedingt das oberste Management sein.(…). Es gibt also einen allgemeinen Teil und einen auf die jeweilige Tätigkeit zugeschnittenes Add-on.

I: Gab es denn auch schon Vorfälle, die das Unternehmen geschädigt haben?

Herr B.: Ja, sicherlich. Die Welt ist nicht so brav. Das kann man ganz offen sagen, dass man in gewissen Ländern eher Opfer solcher Kampagnen wird. (…). Das ist natürlich im Geschäftsleben ein Risiko.

I: Gehen wir nun noch einmal auf technische Sicherheitsmaßnahmen in Ihrem Unternehmen ein. Könnten Sie trotz unterschiedlicher Gefahrenpotenziale auf die bautechnischen Maßnahmen der einzelnen Standorte eingehen?

Herr B.: Zunächst muss jeder Standort eine Risikoanalyse nach den geschilderten sieben Schritten durchführen. Daraus muss jeder Standort ein Sicherheitskonzept für sich erarbeiten. Das ist Pflicht. Dann haben wir ein sogenanntes Zonen-Konzept, was die Zutrittskontrollen angeht (…). Grundsätzlich ist eine Umfriedung des Geländes absoluter Standard. Auch Zutrittskontrollen sind Standard. Dann gibt es je nach Schutzzone Videoüberwachungen, Einbruchmeldeanlagen und weitergehende technische Maßnahmen.

I: Gibt es denn auch Sicherungsräume für gefährdete Datenträger?

Herr B.: Selbstverständlich.

I: Und wie verhält es sich mit abhörschutzsicheren Räumen, speziell auf Ebene des Vorstandes?

Herr B.: Eine Umfrage von großen Unternehmen hat ergeben, dass die meisten Unternehmen solche Räume haben. Die Frage Nutzung von solchen Räumen hat einhellig ergeben, dass es gegen null geht. (…). Wir führen temporäre Abhörschutzmaßnahmen durch. Dort gibt es auch eine Klassifizierung wann Themen kritisch sind. Das machen wir mit mobilen Konzepten. Klassisch den Vorstand als Ziel zu sehen, ist eine Scheingeschichte. (…). Ein abhörsicherer Raum beim Vorstand alleine bringt nichts. Dafür sind die Informationsabflüsse zu vielfältig. Ich weiß, dass das ein ganz anderer Ansatz als bei anderen Firmen ist, aber denken Sie mal darüber nach. (…). Wir machen also temporäre Abhörschutzmaßnahmen, wenn wir zum Beispiel einmal im Jahr die Führungskräfte zusammen holen, um die Geschäftsstrategie zu besprechen. Dort wird ganz starker Informationsschutz betrieben, was bis dahin geht, dass Catering-Personal bei bestimmten Themen nicht in die Räume darf oder dass wir keine Funkmikrofone benutzen. (…).

I: Gehen wir kurz noch einmal auf die Sicherung der Informations- und Kommunikationstechnik ein. (...). Bestehen denn aktuelle Schutzprogramme gegenüber technischen Angriffen.

Herr B.: Ich bin davon überzeugt, dass wir hier sehr gut aufgestellt sind, aber es ist ein ständiger Wettlauf. Unser Gegenüber versucht sich immer weiterzuentwickeln und wir müssen nachlegen.

I: Wenn wir uns technische Risiken vor Augen führen, können Mitarbeiter natürlich auch Opfer von infizierten Emails werden. Gab es bisher solche Vorfälle in Ihrem Unternehmen?

Herr B.: Ja, die gab es. Email-Angriffe wurden in der Regel an der Firewall bemerkt. Viel schlimmer sind Sachen, die über USB-Sticks hereingetragen worden, aber solche Vorfälle gab es.

I: Gibt es denn aufgrund des erhöhten Risikos von USB-Sticks auch eine Richtlinie, die den Gebrauch vorgibt?

Herr B.: Die Richtlinie gibt es, aber leider Gottes hapert es manchmal noch an der Umsetzung.

I: Ok. Kommen wir zum Ende des Interviews noch einmal auf rechtliche Sicherheitsmaßnahmen. (...). Gab es aufgrund von Verstößen gegen Geheimhaltungsvereinbarungen rechtliche Konsequenzen, die seitens Ihres Unternehmens initiiert wurden?

Herr B.: Ja, auf jeden Fall.

I: Kann man das auch quantifizieren?

Herr B.: Das ist immer eine Frage. Im Bereich Arbeitsrecht haben Sie sehr viel. Im Bereich Plagiate auch in zunehmendem Maße. Was Sie unter klassischer Spionage verstehen, eher selten. (…).

I: Werden auch Schadenersatzansprüche gestellt?

Herr B.: (…). Im Bereich Plagiate und Know-how-Verluste stellen wir regelmäßig Klagen. Wir haben jetzt einen Fall gehabt (…), wo wir vor Gericht gewonnen haben. Die finanziellen Forderungen waren so hoch, dass die Person wohl in ihrem Leben nicht mehr glücklich wird.

I: Häufig liest man, dass bei Know-how-Abfluss die Parteien sich außergerichtlich einigen, um Imageschäden zu verhindern. Ist das durchaus eine gängige Praxis?

Herr B.: In unserem Hause nicht.

I: (…). Und inwieweit bestehen Sicherheitsvereinbarungen zwischen Ihrem Unternehmen und Zertifizierungsgesellschaften?

Herr B.: Hier gibt es Geheimhaltungsvereinbarungen.

I: Und gab es dort bisher negative Erfahrungen oder Informationsabflüsse?

Herr B.: Es gibt dort immer wieder Vorfälle, aber nicht so tief, dass Sie uns wehtun würden. Es gab aber Vorfälle.

I: Gab es auch Vorfälle mit Geschäftspartnern und Zulieferern?

Herr B.: Ja, die gab es auch.

I: Damit wären wir am Ende des Gesprächs. Vielen Dank.

Beurteilung des Interviews:

Nach anfänglicher Skepsis zur vollständigen Beantwortung der Fragen, entwickelte sich im Laufe des Gesprächs eine produktive Atmosphäre, in der der Interviewte umfangreiche Einblicke in Analyse und Bewertung von Spionagerisiken und dementsprechende Abwehrmaßnahmen gab. Einige Fragestellungen wurden nur indirekt beantwortet. Der angestrebte zeitliche Rahmen konnte erfüllt werden.

B6 Transkript 6

Name:	Herr B.
Position:	Manager IT-Administration, Firma L.
Datum:	18.04.2011
Zeitraum:	10.30 - 11.10 Uhr

Interviewer (I): Herr B., ich darf mich nochmals bedanken, dass Sie sich die Zeit für dieses einstündige Interview nehmen. Im Rahmen des Interviews werde ich Ihnen Fragen zur Risikoanalyse und Risikobewertung sowie den in Ihrem Unternehmen befindlichen Sicherheitsmaßnahmen stellen. Dabei werde ich auf die Bereiche Personal, Organisation, Technik und Recht eingehen. Um Industriespionage wirkungsvoll begegnen zu können, empfiehlt sich zunächst eine Risikoanalyse. Inwieweit wurde bei Ihnen im Unternehmen denn eine Risikoanalyse durchgeführt, um spätere Know-how-Schutzmaßnahmen ergreifen zu können?

Herr B.: Bei uns gibt es umfangreiche Risikoanalysen. Wir haben zum Beispiel vor drei Jahren ein Audit im IT-Bereich gehabt, bei dem durch einen externen Dienstleister unsere gesamten Sicherheitsvorkehrungen im IT-Bereich überprüft wurden. Zusätzlich finden unterstützend jedes Jahr Risikoinventuren statt, in denen die verschiedensten Risiken, denen das Unternehmen ausgesetzt ist, aufgelistet werden. Auf Basis der Auflistung solcher Risiken können dann auch geeignete Maßnahmen getroffen werden.

I: Lässt sich auf Basis der Risikoanalyse sagen welcher der Bereiche Personal, Organisation, Technik und Recht die größten Risiken aufweist?

Herr B.: Die größten Risiken sind in unserem Unternehmen im Bereich der IT und der Organisation zu finden. Daher versuchen wir in diesen beiden Bereichen auch schwerpunktmäßig Sicherheitsmaßnahmen zu fahren. Gerade im Bereich der IT sind ständig Überarbeitungen notwendig, um immer auf dem neuesten Stand der Technik zu sein. Der Bereich Personal ist kein primäres Risiko.

I: Hat in Ihrem Unternehmen denn auch eine Risikobewertung stattgefunden und wenn ja, welche Faktoren wurden zur Risikobewertung herangezogen?

Herr B.: Ja, in unserem Unternehmen gibt es Risikobewertungen. Die wesentlichen Faktoren zur Risikobewertung sind die Schadenseintrittswahrscheinlichkeit und die mögliche Höhe der

Schäden. Neben diesen Größen gibt es jedoch auch Themen, die nicht genau quantifizierbar sind. So gibt es neben finanziellen Risiken auch imageschädigende Risiken, bei denen ein Schaden indirekt eintritt, indem zum Beispiel der Ruf des Unternehmens beschädigt wurde, was die Personalrekrutierung erschwert. Im Rahmen der Risikoanalyse und Risikobewertung nehmen Risiken, die sofortigen Handlungsbedarf mit sich ziehen, sogenannte Top-Risiken, einen besonderen Stellenwert ein. Solche Risiken werden auf Ebene des Vorstands diskutiert und abgearbeitet.

I: Und wurde auf Basis der Analyse und Bewertung der potenziellen Risiken auch eine Prioritätenliste für notwendige Sicherheitsmaßnahmen entwickelt?

Herr B.: Ja, eine solche Prioritätenliste gibt es in Form der Top-Risiken für den Vorstand. (…). Diese Liste wird alle vier Wochen auf Ebene des Vorstands behandelt. Zusätzlich zu dieser Prioritätenliste gibt es auch eine Prüfungsliste für die Revision, wo auch die Einhaltung der beschlossenen Maßnahmen kontrolliert wird. Natürlich gibt es bei enormer Dringlichkeit auch ad-hoc Maßnahmen.

I: Kommen wir nun zu den personellen Know-how-Schutzmaßnahmen. Werden bei Ihnen im Rahmen der Personalakquisition sicherheitsrelevante Firmeninterna in Stellenausschreibungen veröffentlicht?

Herr B.: Nein, in Stellenausschreibungen werden keine Firmeninterna veröffentlicht. Hier sind wir sehr sensibel. Das liegt im Besonderen darin, dass wir ein weltweit agierendes Technologieunternehmen sind und deshalb in solchen Sachen sehr vorsichtig sind. Sicherlich ist aus den Stellenausschreibungen ersichtlich welche Programme der zukünftige Mitarbeiter beherrschen muss, aber sicherheitsrelevante Themen sind nicht enthalten. Solche Programme können zum Beispiel Konstruktionsprogramme sein. (…).

I: Findet im Rahmen des Personalauswahlverfahrens eine intensive Überprüfung der Bewerber statt?

Herr B.: Ja, solche Überprüfungen finden statt. Das gilt besonders für unseren Entwicklungsbereich. (…).

I: Und kommt es im Zuge der Personaleinstellung zu Sicherheitsmaßnahmen wie Sicherheitsbelehrungen, Datenschutz- und Geheimhaltungsverpflichtungen?

Herr B.: Ja, so etwas gibt es bei uns. (…). Wir haben zum Beispiel eine IT-Richtlinie, die von jedem Mitarbeiter bei der Einstellung zu unterschreiben ist. Ebenfalls erhalten die Mitarbeiter eine Arbeitssicherheitsbelehrung. Natürlich haben wir auch Geheimhaltungsvereinbarungen für unsere Mitarbeiter. Solche Geheimhaltungsvereinbarungen gibt es auch für Besucher. Zusätzlich haben wir nachvertragliche Wettbewerbsverbote, um uns nach dem Ausscheiden eines Mitarbeiters abzusichern. Insgesamt gesehen erfolgen diese Sicherheitsmaßnahmen in einem formalen Prozess.

I: Kann man denn auch sagen, dass der der Informationsschutz in Ihrem Unternehmen als Chefsache betrachtet wird und das Management mit gutem Beispiel voran geht?

Herr B.: Das kann seitens des Managements durchaus bestätigt werden. Das Management versucht den Informationsschutz somit auch vorzuleben. Sicherlich gibt es hier individuelle Unterschiede, aber grundsätzlich kann man das bejahen.

I: Und inwieweit werden die Mitarbeiter für die Gefahren des ungewollten Know-how-Abflusses sensibilisiert und geschult?

Herr B.: Die Grundlage hierfür bildet die IT-Sicherheitsrichtlinie. Generell liegt die Sensibilisierungsfunktion innerhalb der Abteilungen. Es ist jedoch auch eine Awareness-Schulung für das Jahr 2012 geplant, die durch einen externen Dienstleister durchgeführt werden soll. Eigentlich sollte diese Schulung schon in diesem Jahr stattfinden, aber leider waren hierfür keine Termine mehr frei. Ziel solcher Trainings soll es sein anhand von nachvollziehbaren Beispielen das Verständnis und das Bewusstsein der Mitarbeiter für Industriespionage zu wecken. Das gilt besonders für Geschäftsreisen, da unsere Mitarbeiter oft im Ausland unterwegs sind. Dementsprechend sind die Laptops der Mitarbeiter besonders gesichert. Der Fokus liegt hier wiederum auf der Prävention.

I: Und wie verhält es sich mit der Einbindung der Mitarbeiter in die Entwicklung von Know-how-Schutzmaßnahmen?

Herr B.: (…). Sicherheitsmaßnahmen können mit hohem Aufwand für die Mitarbeiter verbunden sein. Daher wäre eine direkte Einbindung der Mitarbeiter nicht zielführend Wir haben den Ansatz, dass die Entwicklung solcher Know-how-Schutzmaßnahmen durch Schlüsselmitarbeiter erfolgt.

I: Zufriedenheit der Mitarbeiter schafft Sicherheit im Unternehmen. Werden die Mitarbeiter auch leistungsgerecht entlohnt und erhalten sie unentgeltliche Anerkennung für ihre beruflichen Leistungen?

Herr B.: Ja, unsere Mitarbeiter werden leistungsgerecht beziehungsweise marktkonform entlohnt.

I: Gibt es denn auch Instrumente zur Messung der Mitarbeiter-Loyalität beziehungsweise des Identifikationsgrads der Mitarbeiter mit dem Unternehmen?

Herr B.: Generell kann man sagen, dass die Mitarbeiterzufriedenheit in unserem Unternehmen sehr hoch ist. Das kann man an der Fluktuationsrate beobachten. So läuft die ungewollte Fluktuation gegen null. Des Weiteren haben wir auch branchenunterdurchschnittliche Krankenstände, was ein weiteres Zeichen von Mitarbeiterzufriedenheit ist. Zwar haben wir im Moment eine sehr hohe Arbeitslast, was mit unserem Wachstum zusammenhängt, doch ist die Mitarbeiterzufriedenheit generell sehr gut. Darüber hinaus werden über die Firma auch Freizeitveranstaltungen für die Mitarbeiter angeboten.

I: Die adäquate Beendigung eines Arbeitsverhältnisses gehört ebenfalls zu einem sicherheitsbewussten Personalmanagement. Welche Sicherheitsmaßnahmen werden hier ergriffen?

Herr B.: Das kommt auf die Form des Ausscheidens und den Fall an. Bei einem einvernehmlichen Ausscheiden ist es ein normaler Vorgang, bei dem der Mitarbeiter bis zu seinem letzten Arbeitstag normal weiter arbeiten kann. Bei einem Streit findet eine direkte Freistellung durch den Vorstand statt und jegliche Rechte des Mitarbeiters innerhalb der IT werden gesperrt. Ein solches Vorgehen erfolgt in Kooperation mit der IT-Abteilung und der Personalabteilung.

I: Findet auch eine nachvertragliche Beobachtung ehemaliger Mitarbeiter statt?

Herr B.: Nein, so etwas findet nicht statt. Dafür haben wir ein nachvertragliches Wettbewerbsverbot für Schlüsselmitarbeiter in den Arbeitsverträgen eingebaut. Außerdem würde ein solches Spionieren nicht unserer Firmenphilosophie entsprechen.

I: Gelten denn für Fremdpersonal wie Leiharbeiter, Mitarbeiter von Geschäftspartnern, Sicherheits- und Reinigungspersonal die gleichen Sicherheitsbedingungen wie für das eigene Personal?

Herr B.: Firmenfremde Mitarbeiter erhalten nur die notwendigsten Rechte. Diese Strategie ist bisher sehr erfolgreich, da wir bisher noch keine Datenabflüsse aufgrund von Fremdpersonal feststellen konnten. Das liegt auch darin, dass besonders die Reinigungskräfte schon seit vielen Jahren im Unternehmen arbeiten und daher eng mit dem Unternehmen verbunden sind. Zusätzlich können Reinigungsarbeiten nur während der Arbeitszeit erfolgen. Es gibt also keine Nachtreinigung. Reinigungskräfte, aber auch andere externe Personen, müssen darüber hinaus einen Ausweis tragen. Die Mitarbeiter sind auch dazu angehalten fremde Personen auf ihren Ausweis anzusprechen. (…).

I: Kommen wir nun zu den organisatorischen Know-how-Schutzmaßnahmen. Inwieweit wurden denn bei Ihnen im Unternehmen formal fixierte Sicherheitsstandards etabliert, die vor Know-how-Abfluss schützen sollen? Beispiele wären eine Clean-Desk-Policy oder Bestimmungen zur Nutzung, Vervielfältigung und Vernichtung von Informationsbeständen.

Herr B.: Eine Clean-Desk-Policy gibt es bei uns im Unternehmen nicht. Dafür besteht jedoch eine Klassifizierung von Daten, die den angemessenen Umgang mit den Daten ermöglicht. Zur Vernichtung der Informationsbestände haben wir zentrale als auch dezentrale Shredder. Die weitere Aktenvernichtung wird dann durch zertifizierte Firmen übernommen.

I: Gibt es außer Ihnen noch weitere Sicherheitsverantwortliche im Unternehmen?

Herr B.: Ja, Sicherheitsverantwortliche finden sich in unterschiedlichen Bereichen des Unternehmens wieder.

I: Und sind die Sicherheitsverantwortlichen organisatorisch an die Geschäftsführung angebunden?

Herr B.: Ja, sie sind direkt an die Geschäftsführung angebunden.

I: Wie sind denn die Zutritts- und Zugriffsrechte für firmeneigenes und firmenfremdes Personal zum Schutz von gefährdeten Daten, Objekten und Räumen konzipiert?

Herr B.: Für die räumlichen Zutrittsrechte haben wir ein Transpondersystem. Für unseren IT-Bereich ist dieses Transpondersystem noch durch einen Zahlencode erweitert worden, sodass hier ein zweistufiges Authentifizierungsverfahren stattfindet. In diese sensiblen Bereiche haben nur bestimmte Personen und der Vorstand Zutritt. Diese Sicherheitsvorkehrungen sind

mit der Zeit immer weiter verstärkt worden. Für die Zugriffsrechte gilt ähnliches. Sie werden ebenfalls ständig kontrolliert, sodass man von einem lebendigen System sprechen kann.

I: Sie hatten bereits einige Kontrollen zur Überprüfung von Sicherheitsmaßnahmen angesprochen. Könnten Sie noch etwas genauer darauf eingehen wie die Kontrollen ausgestaltet sind?

Herr B.: Die Kontrollen werden in erster Linie durch die interne Revision übernommen, die einen mehrjährigen Prüfungsplan besitzt. Im Bereich IT haben wir regelmäßig stattfindende IT-Audits, bei denen durch einen externen Dienstleister die IT unserer Firma auf den Prüfstand kommt. Solche IT-Audits werden an allen Standorten durchgeführt. Weitere sicherheitsrelevante Kontrollen werden durch eine Wirtschaftsprüfungsgesellschaft durchgeführt.

I: Und inwieweit werden Mitarbeiter bei Sicherheitsverstößen oder sicherheitsbewusstem Handeln sanktioniert beziehungsweise belohnt?

Herr B.: Sanktionen gibt es durchaus. Das kann zum Beispiel dadurch zum Ausdruck kommen, dass einem Mitarbeiter bei fahrlässigem Verlust seines Laptops in Teilen sein Gehalt gekürzt wird. Natürlich werden auch arbeitsrechtliche Konsequenzen ergriffen. Eine explizite Belohnung gibt es nicht. (…). Sicherheitsbewusstes Handeln wird von den Mitarbeitern erwartet.

I: Kommen wir nun zu den technischen Know-how-Schutzmaßnahmen. Welche bautechnischen Maßnahmen bestehen zur Absicherung gegenüber Betriebsfremden und unbefugten Mitarbeitern?

Herr B.: Hierzu haben wir eine Beratung der lokalen Polizei in Anspruch genommen. Auf Basis der Beratung wurde auf eine Umzäunung verzichtet. Es besteht jedoch ein Kameraüberwachungssystem, eine Alarmanlage und eine Löschanlage. Derzeit wird darüber diskutiert einen nächtlichen Wachschutz einzuführen. Die Rechenzentren selbst sind F90, gasdicht und gegen Vandalismus geschützt.

I: Und welche Maßnahmen werden zur Sicherung der Informations- und Kommunikationstechnik gegenüber Innen- und Außentätern eingesetzt?

Herr B.: Hier finden mehrere Sicherheitsvorkehrungen statt. Das sind Datenverschlüsselungen mit zweifacher Authentifizierung, zwei verschiedene Firewallsysteme und starke Passwortre-

geln. (…). Dateiausführungen können nur über die Administrationsabteilung verwaltet und freigegeben werden. Eine Viren- und Spamfilterung findet hier mit namenhaften Herstellern auf mehreren Ebenen statt. Externe Dienstleister unterstützen uns in diesen Bereichen.

I: Kommen wir zum Schluss des Interviews zu rechtlichen Know-how-Schutzmaßnahmen. Inwieweit bestehen die angesprochenen Geheimhaltungsvereinbarungen auch mit Geschäftspartnern und was passiert bei Verstößen gegen solche Vereinbarungen?

Herr B.: Geheimhaltungsvereinbarungen gibt es selbstverständlich auch mit Partnerfirmen. Der Nachweis eines Verstoßes dieser Vereinbarungen ist jedoch sehr schwierig. Grundsätzlich werden jedoch rechtliche Konsequenzen, in Form von Schadensersatzansprüchen, ergriffen.

I: Vielen Dank für das Interview.

Beurteilung des Interviews:

Mit einer Dauer von nur 40 Minuten war dieses Gespräch eines der kürzeren Interviews. Die Kürze des Interviews entstand durch ein limitiertes Zeitbudget des Gesprächspartners. Grundsätzlich waren die Aussagen relativ gut verwertbar. Zur ausführlicheren Beantwortung mancher Fragestellungen fehlte jedoch die notwendige Zeit.

B7 Transkript 7

Name:	Herr K.
Position:	HR-Manager, Firma V.
Datum:	20.04.2011
Zeitraum:	13.30 - 14.20 Uhr

Interviewer (I): Herr K., vielen Dank, dass Sie sich die Zeit für dieses Interview nehmen. Ich werde Ihnen in den nächsten 60 Minuten Fragen zur Analyse und Bewertung von Spionagerisiken stellen und werde im Verlauf des Interviews auf Know-how-Schutzmaßnahmen eingehen, die in Ihrem Unternehmen getroffen wurden oder geplant sind. Um Industriespionage wirkungsvoll begegnen zu können, empfiehlt sich zunächst eine Analyse der Risiken. Inwieweit wurde bei Ihnen im Unternehmen denn eine Risikoanalyse durchgeführt, um spätere Know-how-Schutzmaßnahmen ergreifen zu können?

Herr K.: Wir haben das mal gemacht, das ist aber schon einige Jahre her. Ich denke, dass es sechs Jahre her ist. Dies hatte einen Anlass, da vermutet wurde, dass es einen Angriff auf unser Unternehmen gegeben hatte. Das hatte sich jedoch nicht in der Form bewahrheitet. In dem Kontext hatten wir dann eine Risikoanalyse durchgeführt.

I: Könnten Sie auf Einzelheiten der Risikoanalyse eingehen?

Herr K.: Ja, wir haben unterschiedliche Dinge untersucht. Zum Beispiel wurden Shredder, die Wege des Papiers oder die Zugänglichkeit der Büros untersucht. Ebenfalls wurde analysiert welche Informationen über die Telefonzentrale gewonnen werden konnten. (…). Das ging bis dahin, dass wir Mitarbeiterschulungen für die Mitarbeiter im Vertrieb, in der Telefonzentrale und am Empfang durchgeführt haben.

I: In der Literatur werden die Risikobereiche Personal, Organisation, Technik und Recht erwähnt. Könnten Sie sagen wo bei Ihnen im Unternehmen die größten Risiken liegen?

Herr K.: (…). Ein Punkt war, dass sich die Mitarbeiter gar nicht der Möglichkeiten und den Umfang staatlich gelenkter Spionage bewusst waren. Hier werden ja insbesondere China, USA, Frankreich und Russland genannt. Zum Beispiel wurde uns auch gesagt, dass chinesische Praktikanten ein Exemplar ihrer Diplomarbeit beim chinesischen Geheimdienst abgegeben müssen. Solche Informationen hatten wir zuvor nicht. Also sind wir insgesamt für diesen

Bereich sensibilisiert worden und auf Sicherheitslücken (…) aufmerksam geworden. Zuvor war dieses Bewusstsein gar nicht vorhanden.

I: Also ist durch die Risikoanalyse und die Risikobewertung erst ein Risikobewusstsein entstanden?

Herr K.: Ja.

I: Aufbauend zur Risikoanalyse findet normalerweise eine Risikobewertung statt. Wurden neben den maßgeblichen Parametern der Schadenseintrittswahrscheinlichkeit und der möglichen Schadenshöhe noch weitere Faktoren berücksichtigt?

Herr K.: Wir haben auch geguckt, wo es Personen gibt, die sehr viel mit Externen zu tun haben. Zum Beispiel Mitarbeiter des Vertriebs oder der Telefonzentrale. Die wurden dann auch speziell geschult.

I: Aber die maßgeblichen Faktoren sind schon die genannten?

Herr K.: Ja.

I: Und wurde auf Basis der Risikoanalyse und Risikobewertung auch eine Prioritätenliste von Maßnahmen erstellt, die zu ergreifen waren?

Herr K.: Also wir haben bestimmte Maßnahmen ergriffen. Prioritäten wurden in diesem Sinne nicht gesetzt, sondern wir haben geguckt was für Maßnahmen zu ergreifen sind und dann auch umgesetzt. Sicherlich müsste man das jetzt aber mal reviewen.

I: Nun würde ich gerne auf die personelle Know-how-Schutzmaßnahmen eingehen. (...). Inwieweit werden denn im Rahmen der Personalakquisition sicherheitsrelevante Firmeninterna in Stellenausschreibungen veröffentlicht?

Herr K.: Wir geben nur die normalen Informationen (…) wie Umsatz und Größe an. Da wir aber eine Aktiengesellschaft sind, kann man die Geschäftszahlen auch sehr gut über die Internetseite herausfinden.

I: Aber spezielle Tätigkeiten der Mitarbeiter oder besondere Technologien sind nicht enthalten?

Herr K.: Nein.

I: Findet denn, wenn ein Bewerber in die Personalauswahl gelangt, auch eine intensive Überprüfung der Bewerber statt, seien es Bewerbungsunterlagen oder individuelle Risikofaktoren?

Herr K.: Letzteres könnte ja rechtswidrig sein, wenn wir über das AGG sprechen. (…). Nein, wir führen keine besonderen Prüfungen durch. Wir machen das übliche, indem wir die Bewerbungsunterlagen überprüfen. In Ausnahmefällen, also bei Führungskräften, lasse ich die Bewerbungsunterlagen auch verifizieren.

I: Das heißt es werden auch ehemalige Arbeitgeber und Ausbildungsstätten kontaktiert?

Herr K.: Ja, die werden gecheckt. (…). Was jetzt auf uns zukommt, ist dass alle neuen Mitarbeiter und temporären Mitarbeiter im Sinne von Anti-Terror-Listen sicherheitsüberprüft werden. Das kommt jetzt auf uns zu.

I: Sonstige staatliche Behörden werden nicht kontaktiert?

Herr K.: Das ist von Fall zu Fall unterschiedlich. Ich habe ja auch einen Kontakt zum Verfassungsschutz und dort habe ich auch schon einmal vor einiger Zeit eine Anfrage gestellt beziehungsweise gesagt, dass eine Person mal genauer angeschaut werden sollte. Das war aber ein Mitarbeiter von dem wir uns einvernehmlich getrennt haben, wo ich aber gesagt habe, dass hier mal geguckt werden soll, ob es eine Nähe zu terroristischen Organisationen gibt.

I: Gehen wir einen Schritt weiter zur Personaleinstellung. Inwieweit werden hier Sicherheitsmaßnahmen, wie Sicherheitsbelehrungen, Datenschutz- und Geheimhaltungsvereinbarungen getroffen?

Herr K.: Ja, Datenschutzvereinbarungen bestehen. Die Geheimhaltungsvereinbarungen ergeben sich aus dem Arbeitsvertrag.

I: Und gibt es auch Konkurrenzklauseln oder nachvertragliche Wettbewerbsverbote?

Herr K.: Wettbewerbsverbote haben wir nicht aber die normalen nachvertraglichen Verschwiegenheitsgebote.

I: Kommen wir zum sicherheitsbewussten Personalmanagement. Inwieweit ist Know-how-Schutz beziehungsweise Informationsschutz Chefsache und wird vom Management vorgelebt, um auch an der Basis ein Risikobewusstsein zu erhalten?

Herr K.: Das ist schon sehr stark verankert. Wir gehen mit internem Firmen-Know-how (…) schon sehr sorgsam um. Wir hatten zum Beispiel neulich ein Projekt, wo bestimmte Prozesse durchleuchtet werden sollten. Die brauchten dann sensible Firmenunterlagen, wo wir aber gesagt haben, dass sie die nicht für die Bearbeitung bräuchten. (…). Hier ist also schon ein großes Bewusstsein vorhanden.

I: Herr K., Sie hatten bereits gesagt, dass auf Basis einer Risikoanalyse Schulungs- und Sensibilisierungsmaßnahmen ergriffen wurden. Könnten Sie noch einmal sagen wie diese Maßnahmen explizit ausgestaltet waren?

Herr K.: Das war in Form von Tagesseminaren für Mitarbeiter der Telefonzentrale, des Empfangs und des Vertriebs, die starke Außenkontakte haben.

I: Also wurde in den Schulungen auch mitgeteilt wie sich Mitarbeiter auf Geschäftsreisen im Ausland zu verhalten haben?

Herr K.: Ja, und wie Leute versuchen an Informationen heranzukommen, indem zum Beispiel unter Legendenbildung hier angerufen wird und versucht wird an Informationen zu gelangen.

I: (...). Inwieweit wurden Mitarbeitern denn auch in die Entwicklung von Know-how-Schutzmaßnahmen mit eingebunden?

Herr K.: Das wurde eher top-down entschieden.

I: Gibt es sonst Fälle bei Ihnen im Unternehmen, wo Mitarbeiter Informationslecks in ihren Abteilungen aufgedeckt haben und mit ihrem Vorgesetzten behoben haben?

Herr K.: Solche Beispiele sind mir nicht bekannt. (…).

I: Loyalität und Zufriedenheit der Mitarbeiter schaffen Sicherheit im Unternehmen und verhindern auch Informationsabflüsse. Werden Mitarbeiter denn leistungsgerecht entlohnt und gibt es auch unentgeltliche Anerkennung für berufliche Leistungen der Mitarbeiter?

Herr K.: (…). Ich denke schon, dass die Mitarbeiter leistungsgerecht beurteilt werden. Die Fluktuationsrate ist in unserem Unternehmen zumindest gering. Das Unternehmen steht aber auch wirtschaftlich auf soliden Füßen, sodass es eine hohe Mitarbeiterbindung gibt. Natürlich gibt es auch hier und dort unentgeltliche Anerkennungen für berufliche Leistungen, aber das

ganze läuft nicht als System ab. Es ist von jedem Vorgesetzten die Führungsaufgabe auch Anerkennung zu geben und das macht der eine mehr und der eine weniger.

I: Gibt es denn auch Instrumente zur Messung der Loyalität und Zufriedenheit von Mitarbeitern?

Herr K.: Nein.

I: Sind solche Erhebungen vielleicht in Zukunft geplant?

Herr K.: Nein.

I: Kommen wir nun zur Beendigung eines Arbeitsverhältnisses. Gibt es dort Unterschiede zwischen einem regulären und einem nicht einvernehmlichen Ausscheiden eines Mitarbeiters?

Herr K.: Nein.

I: Das heißt, dass zum Austrittstermin alle firmeneigenen Geräte und Unterlagen des Mitarbeiters zurückgegeben werden?

Herr K.: Ja, das betrifft Schlüssel und ähnliches. Hierfür gibt es ein Verzeichnis.

I: Und wie sieht es mit den Zugriffsrechten innerhalb der EDV aus?

Herr K.: Die werden zum Austrittstermin gelöscht.

I: Gibt es denn auch eine Beobachtung der Marktsituation nach dem Ausscheiden von Mitarbeitern?

Herr K.: Nein, das gibt es nicht. Wie soll das rechtlich gehen? Wobei ich manchmal schon mit dem Gedanken spiele, warum wir nicht mehr über bestimmte Wettbewerber wissen wollen. Wir machen das aber nicht. Investigativ sind wir nicht unterwegs. Es gibt natürlich Dinge, die man durch über den Wettbewerb erfährt, aber die Wettbewerber selbst plaudern ja auch nicht sensible Daten aus.

I: Wir haben bisher über das firmeneigene Personal gesprochen. Nun möchte ich noch einmal auf das firmenfremde Personal zu sprechen kommen. Gelten für Fremdpersonal, wie Leiharbeiter, Mitarbeiter von Geschäftspartnern, Sicherheits- und Reinigungspersonal, die gleichen Sicherheitsbedingungen wie für das firmeneigene Personal?

Herr K.: Es gelten ja keine besonderen Bedingungen, insofern gelten die gleichen Bedingungen. Für Reinigungspersonal ist es so, dass nicht außerhalb der Geschäftszeiten gereinigt wird. Das findet innerhalb der Geschäftszeiten statt. Das ist eine Maßnahme, die wir aufgrund dieser Risikoanalyse getroffen haben, wobei ja alle Untersuchungen sagen, dass die eigenen Mitarbeiter die Personen sind, die dem Unternehmen am meisten schaden. (…). Deswegen sehe ich diese Maßnahmen nicht unbedingt als zielführend an, aber so ist es zumindest entschieden worden.

I: Gab es denn bislang Vorfälle des Know-how-Abflusses mit Fremdpersonal?

Herr K.: Das ist uns nicht bekannt. (…). Die waren wohl so gut, dass wir nichts mitbekommen haben.

I: Ja, das stimmt. Wenn nichts entdeckt wird, heißt das noch lange nicht das auch nichts passiert ist. Kommen wir nun zu den organisatorischen Sicherheitsmaßnahmen. Gibt es denn formal fixierte Sicherheitsstandard wie eine Clean-Desk-Policy oder Bestimmungen zur Nutzung, Vervielfältigung und Vernichtung von Informationsbeständen?

Herr K.: Es hat im Zuge dieser Geschichten eine Handlungsanweisung gegeben, unter anderem auch in Richtung Clean-Desk. (…). Wir haben zum Beispiel auch eine Entwicklungsabteilung, in die man nur mit Zugangscode hineinkommt. Zusätzlich haben wir das System der Besucherausweise reformiert. Dann haben wir Cross-Cut-Shredder eingeführt, wo noch keine waren. Wir haben auch einen Sicherheitsbeauftragten benannt. Also haben wir schon einige Maßnahmen ergriffen.

I: Wird die Vernichtung von sensiblen Informationen auch durch zertifizierte Aktenvernichter weitergehend durchgeführt?

Herr K.: Das weiß ich nicht genau. Wir haben einen Reißwolf in den vertrauliche Daten gelangen, aber ob die Firmen, die das Material abholen zertifiziert sind, kann ich Ihnen nicht sagen.

I: Also gibt es auch eine Klassifizierung von Informationsbeständen?

Herr K.: Nein, eine klassische Klassifizierung, wie man sie von öffentlichen Stellen kennt, haben wir nicht.

I: Herr K., Sie hatten erwähnt, dass ein Sicherheitsbeauftragter bestimmt wurde. Können Sie mir sagen welche Aufgaben diese Person wahrnimmt?

Herr K.: Er hat die angesprochenen Dinge im Auge und ist die Person, die generell für den Werksschutz zuständig ist.

I: Das heißt, dass diese Person den Informationsschutz nicht hauptberuflich ausübt, sondern generell für die Unternehmenssicherheit zuständig ist?

Herr K.: Genau.

I: Ist der Sicherheitsbeauftragte denn organisatorisch an die Geschäftsführung angebunden?

Herr K.: Nein, das ist ein Mitarbeiter von mir beziehungsweise ein Abteilungsleiter.

I: Sie hatten gerade angesprochen, dass es Zutrittskontrollen bei Ihnen im Unternehmen gibt. Bestehen solche Zutrittskontrollen auch für Räume, wo sensible Daten lagern?

Herr K.: Genau. Für die Entwicklungsabteilung gilt das. Die Mitarbeiter, die dort arbeiten können nur mit Zugangscodes in die Räumlichkeiten. Alle anderen Personen müssen klingeln und werden dort von Mitarbeitern hereingelassen. Das ist der einzige Bereich, wo es spezielle Zutrittskontrollen gibt. Dann gibt es auch noch Bereiche, die von Besucherführungen ausgeschlossen sind.

I: Herr K., Sie haben erwähnt, dass vor Jahren eine Risikoanalyse durchgeführt wurde und entsprechende Maßnahmen eingeleitet wurden. Gab es denn auch Kontrollen zur Überprüfung der Einhaltung der Maßnahmen?

Herr K.: Ja, am Anfang schon, jetzt schon länger nicht mehr.

I: Also würden Sie sagen, dass hier Handlungsbedarf besteht?

Herr K.: Wenn Sie mich so fragen, kann man davon ausgehen, dass hier Handlungsbedarf besteht.

I: Wie sah denn die in der Vergangenheit erfolgte Kontrolle aus?

Herr K.: Wir haben einen Rundgang gemacht und geschaut ob die veranlassten Maßnahmen auch umgesetzt wurden. Hier wurde geguckt wie es mit den Schließregeln, dem Wegpacken

und Vernichten von sensiblen Informationen aussieht. Außerdem wurden Mitarbeiter hierzu befragt und Sicherheitsverstöße direkt angesprochen.

I: Gab es denn bei vorliegenden Sicherheitsverstößen auch Sanktionierungen wie Abmahnungen?

Herr K.: Nein, das gab es nicht.

I: Und dementsprechend wurde sicherheitsbewusstes Handeln auch nicht belohnt?

Herr K.: Nein, ein ausdrückliches Belohnungssystem gibt es nicht.

I: Kommen wir nun zum Themenblock der technischen Know-how-Schutzmaßnahmen. Inwieweit bestehen denn bautechnische Sicherheitsmaßnahmen?

Herr K.: Wir haben natürlich einen Zaun. Hierfür haben wir Pförtner, die das bewachen. Für das Verwaltungsgebäude haben wir eine Alarmanlage, wo alle Fenster und Türen im Erdgeschoss angeschlossen sind. Zusätzlich sind die Bereiche Personal und EDV mit einer eigenen Alarmanlage angeschlossen. Wir haben auch Kameras, die auf Teilbereichen des Betriebsgeländes aufgestellt sind.

I: Gibt es auch Sicherungsräume für besonders gefährdete Datenträger?

Herr K.: Sicherlich gibt es solche Räume, die gegen Feuer oder ähnliches geschützt sind.

I: Und bestehen abhörschutzsichere Räume auf Ebene des Vorstands?

Herr K.: Nein.

I: Ich möchte nun noch einmal auf die Sicherung der Informations- und Kommunikationstechnik eingehen. Gibt es denn für jeden Mitarbeiter einen eigenen Account, dazugehörige Passwörter und einen systematischen Passwortwechsel?

Herr K.: Es gibt Passwörter, aber einen regelmäßigen Passwortwechsel gibt es nicht.

I: Ist so etwas vielleicht für die Zukunft anberaumt?

Herr K.: Wir hatten so etwas mal, wo man automatisch nach vier oder sechs Wochen ein neues Passwort wählen musste. Das ist aber mittlerweile nicht mehr der Fall. Warum das so ist, weiß ich aber auch nicht.

I: Bestehen denn bei der Übermittlung von sensiblen Daten auch Verschlüsselungen?

Herr K.: Nein, wenn Sie zum Beispiel den Email-Verkehr ansprechen, gibt es so etwas nicht.

I: Sie würden aber schon sagen, dass die Firmenrechner und Firmenlaptops mit den neuesten Schutzprogrammen ausgestattet sind?

Herr K.: Ja.

I: Im Bereich Informations- und Kommunikationstechnik werden in der Literatur auch oft Email-Angriffe erwähnt. (…). Gab es solche Vorfälle in Ihrem Unternehmen?

Herr K.: So etwas ist mir nicht bekannt.

I: Sind aus den Firmenrechnern und Firmenlaptops unnötige Hardwarekomponenten, wie Brenner oder USB-Ports, entfernt worden?

Herr K.: Das, was für überflüssig gehalten wird, ist ausgebaut worden. USB-Ports haben wir aber. Im Personalbereich brauchen wir die Ports zum Beispiel für das Online-Banking bei Gehaltsabrechnungen. Die EDV-Abteilung hat zwar immer propagiert, dass solche Dinge ausgebaut oder verriegelt werden müssen, aber sie konnten sich damit aufgrund mangelnder Flexibilität nicht durchsetzen.

I: Wurden in den Schulungsmaßnahmen, denn auch die Gefahren von fremden USB-Sticks angesprochen?

Herr K.: Die Schulungen sind ja schon eine Weile her, aber ich denke schon, dass jedem bewusst ist, was für Gefahren davon ausgehen können. Zumindest ist sich das Management darüber bewusst.

I: Damit wäre auch der technische Aspekt abgearbeitet. Kommen wir nun zum Schluss des Interviews zu rechtlichen Know-how-Schutzmaßnahmen. Sie hatten bereits angesprochen, dass es Geheimhaltungsvereinbarungen zwischen Ihrem Unternehmen und den Mitarbeitern gibt. Bestehen solche Geheimhaltungsvereinbarungen auch mit Partnerfirmen?

Herr K.: Ja, das gibt es schon. Es gibt zum Beispiel Kunden von uns, die wir zur Geheimhaltung verpflichten. Beispielsweise gibt es auch für das genannte Analyseprojekt (…) eine Geheimhaltungsvereinbarung mit dem Beratungsunternehmen.

I: Und wie verhält es sich mit Lieferanten?

Herr K.: Das kann ich Ihnen leider nicht sagen.

I: Gab es denn in der Vergangenheit schon Verstöße gegen Geheimhaltungsvereinbarungen und wurden dementsprechend rechtliche Konsequenzen eingeleitet?

Herr K.: Nein, das ist mir nicht bekannt.

I: Da Ihr Unternehmen ein technologieorientiertes Unternehmen ist, würde ich gerne auf den Aspekt der Patente eingehen. Patente dienen ja zur rechtlichen Absicherung von explizitem Know-how.

Herr K.: Sie können auch zur Veröffentlichung dienen. Das muss man sich genau überlegen.

I: Kann man denn die Patentierung in Ihrem Unternehmen quantifizieren und ist man sich auch über die Risiken der Patentierung bewusst?

Herr K.: Ja, darüber sind wir uns bewusst. Wir haben es in einem konkreten Fall deshalb auch nicht gemacht, weil man dem Wettbewerb sonst auch eine Spur geben würde. Es gibt ja auch viele Möglichkeiten durch geringfügige Veränderungen des Patents am Patent vorbei zu kommen. (…).

I: In den geführten Interviews konnte ich in Erfahrung bringen, dass Patente auch zur Desinformation verwendet werden.

Herr K.: Das ist ein interessanter Aspekt, den ich unserem Entwicklungsleiter mal zukommen lassen werde. Bisher war das bei uns aber noch kein Thema. Einer unserer größten Konkurrenten hat aber zum Beispiel einen großen Teil mit Patenten zugemauert, was auch an deren großer Entwicklungsabteilung liegt. Hier kommen wir dann nicht mehr ran.

I: Herr K., ich gehe mal davon aus, dass bei Ihnen im Unternehmen auch eine Zertifizierung von Geschäftsprozessen stattfindet. Gab es denn zwischen Ihrem Unternehmen und den Zertifizierungsgesellschaften Geheimhaltungsvereinbarungen?

Herr K.: Ja, auch hier gibt es Geheimhaltungsvereinbarungen.

I: Dort sind aber noch keine Know-how-Abflüsse erfolgt?

Herr K.: Nein, das ist uns nicht bekannt.

I: Vielen Dank für das Interview.

Beurteilung des Interviews:

Im vorliegenden Interview ging der Befragte grundsätzlich gezielt auf die gestellten Fragen ein. Allerdings wurden manche Aspekte, trotz mehrfachen Nachhakens, nur spärlich beantwortet. Mit einer Dauer von circa 50 Minuten konnte der angestrebte Zeitrahmen eingehalten werden, was auch auf die gesammelte Erfahrung des Interviewers zurückzuführen ist.

B8 Transkript 8

Name:	Herr K.
Position:	Informationsschutzbeauftragter, Firma Vo.
Datum:	27.04.2011
Zeitraum:	09.00 - 10.10 Uhr

Interviewer (I): Herr K., vielen Dank, dass Sie sich die Zeit für dieses einstündige Interview nehmen. Ich würde Ihnen gerne in den nächsten 60 Minuten Fragen zur Analyse und Bewertung von Spionagerisiken stellen und werde im Verlauf des Interviews auf Know-how-Schutzmaßnahmen eingehen, die in Ihrem Unternehmen getroffen werden. (...). Um Industriespionage wirkungsvoll begegnen zu können, empfiehlt sich zunächst eine Analyse der Risiken. Inwieweit wurde bei Ihnen im Unternehmen denn eine Risikoanalyse durchgeführt?

Herr K.: (…). Grundsätzlich haben wir Analysen gemacht, die überwiegend webbasiert erfolgten. Wir haben also sogenannte web-based Trainings durchgeführt, die für gewisse Personengruppen auch verpflichtend waren. Aus dem Fragenportfolio dieser webbasierte Trainings konnte man relativ schnell erkennen, wo die Mitarbeiter und Führungskräfte Wissenslücken bezüglich Awareness haben. (…). Hier haben wir auch herausgefunden, dass wir in gewissen Bereichen auch noch Nachholbedarf haben, da noch nicht zu allen Mitarbeitern die Relevanz des Themas durchgedrungen ist. Wir haben auch viele Erkenntnisse darüber erlangt, da wir viele Ermittlungsvorgänge haben. Anhand solcher Analysen erkennt man dann auch recht schnell seine Vorteile und seine Nachteile. So bildet sich also unser Wissensstand ab. Auf der einen Seite Umfragen und auf der anderen Seite reale Fälle. (…).

I: Herr K., Sie haben gesagt, dass die Analysen auf Basis von Umfragen und auf Basis von tatsächlichen Vorfällen stattfinden. Können Sie sagen in welchen der Bereiche Personal, Organisation, Technik und Recht die größten Risiken vorhanden sind?

Herr K.: Das ist eine schwierige Frage, da wir es mit einem sehr großen Mengengerüst zu tun haben. Wir haben tausende von Mitarbeitern, unterschiedliche Kulturkreise, unterschiedliche Technologiestände (…). Auf jeden Fall haben wir eine sehr gute IT-Sicherheitstechnik, die state of the art ist, aber die größte Gefahr liegt in der Awareness der Leute. (…). Oft ist es den Leuten einfach nicht bewusst, was sie gemacht haben. Ein Beispiel ist die Nutzung von Verteilerlisten des Vorgängers, wo Leute schon verstorben sind oder jetzt in anderen Unterneh-

men arbeiten. Wir haben auch Fälle, wo Sachen nicht verschlüsselt werden, die eigentlich verschlüsselt sein sollten. Zum Teil wissen die Mitarbeiter auch gar nicht, dass es eine Klassifizierung von Informationen gibt oder wie welche Information einzuordnen ist. Es liegen also rund 90 Prozent des Abflusses in der Awareness der Leute. (…). Das liegt aber auch an einer hohen Arbeitslast, die dazu führt, dass manche sicherheitsrelevanten und zeitaufwendigen Dinge nicht vollständig umgesetzt werden. (…). Ein weiterer Punkt ist, dass wir international agieren. Bei technischen Voraussetzungen, wie Verschlüsselungen, haben Sie zum Teil gesetzliche Vorschriften in den Ländern, die eine Verschlüsselung untersagen. Das macht es uns natürlich auch auf der technischen Seite schwierig gewisse Dinge umzusetzen, aber das ist der geringere Teil. Im Bereich Organisation gibt es neben den Vorteilen des Knowledge-Managements auch Risiken an wen die Informationen gelangen. Hier gilt generell das Need-to-know-Prinzip, aber sicherlich gibt es auch noch Handlungsbedarf.

I: Kommen wir nun zur Risikobewertung. Gibt es denn neben den maßgeblichen Parametern Schadeneintrittswahrscheinlichkeit und mögliche Schadenshöhe auch noch weitere Messgrößen zur Bewertung von Risiken?

Herr K.: Also ich würde das Thema Schadenshöhe noch durch das Thema Image ergänzen, denn es gibt Fälle, wo die finanziellen Schäden weitaus geringer sind als der aus dem Fall entstandene Imageschaden. (…).

I: Wird denn auch der bei einem Informationsabfluss benötigte Rekonstruktionsaufwand bei der Risikobewertung berücksichtigt?

Herr K.: Auf jeden Fall, deshalb speichern wir auch nichts auf lokalen Datenträgern, wie USB Sticks, die man verlieren kann. Wir schauen deshalb auch immer, dass in einem Schadensfall nicht das Backup betroffen ist. (…). Neben dem Image, den Kosten und dem Rekonstruktionsaufwand schauen wir auch immer welche Potenziale wir durch einen möglichen Schaden verlieren würden. (…).

I: Werden denn auf Basis der Analyse und Bewertung der potenzielle Risiken auch Prioritätenlisten für notwendige Sicherheitsmaßnahmen entwickelt?

Herr K.: Ja, sicherlich. Erstmal sind die Prioritäten ja durch den Vorstand vorgegeben. So haben zum Beispiel Prototypen die höchste Priorisierung. Auf der anderen Seite schauen wir natürlich auch auf die Ermittlungsfälle und gucken wo wir Schwächen haben, sodass wir Prio-

ritäten setzen können. (…). Die Prioritäten liegen aufgrund der Größe des Unternehmens jedoch sehr unterschiedlich in den einzelnen Gesellschaften und Abteilungen vor. (…).

I: Kommen wir nun zu den personellen Sicherheitsmaßnahmen in Ihrem Unternehmen. In wieweit werden denn im Rahmen der Personalakquisition sicherheitsrelevante Firmeninterna in den Stellenausschreibungen veröffentlicht?

Herr K.: Das ist genau das, was wir vermeiden wollen. (…). Rückschlüsse aus unseren Stellenausschreibungen sind nicht möglich. Das machen wir nicht. Hier achten wir schon darauf. Die einzige Stelle, die Sachen öffentlich kommuniziert, ist die Öffentlichkeitsarbeit. (…). Natürlich müssen Sie in die Stellenausschreibung reinschreiben, dass Sie zum Beispiel einen Entwickler für Energiezellen brauchen, aber daraus können Sie noch nicht viel entnehmen.

I: Findet denn eine intensive Überprüfung des Bewerbers innerhalb des Personalauswahlverfahrens, wie Kontrolle des Lebenslaufs, statt?

Herr K.: Das ist ja primär eine Frage für den HR-Bereich. Nun ist es ja so, dass wir hier kein Hochsicherheitsunternehmen sind, also nicht geheimschutzüberprüft sind. (…) Natürlich glauben wir aber nicht alles und verifizieren die Unterlagen des Bewerbers. Das können zum Beispiel Kontrollanrufe bei ehemaligen Arbeitgebern oder Ausbildungsstätten sein. (…). So etwas findet zwar nicht in jedem Fall statt, aber grundsätzlich gehen wir so vor.

I: Findet auch eine Berücksichtigung von individuellen Risikofaktoren, wie Kontakten oder Aufenthalten in Risikostaaten, statt?

Herr K.: (…). Ich hatte ja eingangs erwähnt, dass wir sehr viele Mitarbeiter auf unterschiedlicher Ebene haben. Sicherlich ist das bei einer Reinigungskraft etwas anders als bei einem Vorstandsmitglied. Insofern wird bei Leuten im Top-Management auf bestimmte Faktoren geschaut. (…). Dort gibt es unterschiedliche Kriterien. Insbesondere wenn im Ausland neue Standorte aufgemacht werden (…) seien es Russland oder asiatische Länder, vergewissert man sich schon ab einer bestimmten Ebene schon, ob der Bewerber schon einmal im Staatsdienst gearbeitet hat. Das ist aber kein Geheimnis. Das macht jedes Unternehmen.

I: Gibt es im weiteren Schritt der Personaleinstellung ebenfalls Sicherheitsmaßnahmen wie Sicherheitsbelehrungen, Datenschutz- und Geheimhaltungsvereinbarungen?

Herr K.: Ja, auf jeden Fall. Geheimhaltungsvereinbarungen gibt es. Es gibt auch eine Unterweisung in den Datenschutz. (…). Dort sind Sachen, wie das Need-to-know-Prinzip oder Anweisungen zur Klassifizierung von Informationen, enthalten. (…). Was wir verstärkt machen ist, dass wir mithilfe von webbasierten Trainings Auffrischungen und fallbezogene Sensibilisierung anbieten. Also gibt es nicht nur bei der Einstellungen, sondern auch nebenbei. Hier gibt es aber keine genauen zeitlichen Abstände. Das ist auch eine Kostenfrage.

I: Gibt es denn auch Konkurrenzklauseln oder nachvertragliche Wettbewerbsverbote?

Herr K.: Ja, jetzt geht es schon an das Eingemachte. Hier kann ich nur sagen, dass es so etwas sicherlich ab einer bestimmten Ebene gibt. Das hat sich die deutsche Wirtschaft ja auch auferlegt, dass die Leute ab der Vorstandsebene erst einmal eine einjährige Arbeitssperre haben. (…). Das ist ein Agreement der deutschen Wirtschaft, wo wir uns auch daran halten.

I: Herr K., würden Sie es grundsätzlich bejahen, dass der Informationsschutz in Ihrem Unternehmen als Chefsache betrachtet wird und das Management mit gutem Beispiel voran geht?

Herr K.: (…). Auf jeden Fall. Der Informationsschutz ist sehr hoch angesiedelt. Wir sind hier eine Stabsstelle und direkt dem Konzernvorstand unterstellt. Wir arbeiten also im Auftrag des Konzernvorstands. Somit ist das Thema hier hoch angesiedelt. Unsere Abteilung ist auch bei strategischen Entscheidungen, wie Standortwahl, beteiligt. (…). Selbstverständlich geht das Management auch mit gutem Beispiel voran. Das wird alles durch den Bereich Compliance abgedeckt. (…). Das ist auch immer eine personenbezogene Sache. Haben Sie eine Unternehmensleitung, die Informationssicherheit als Chefsache betrachtet, ist das etwas anderes als eine Unternehmensleitung, die dem Thema wenig Beachtung schenkt. (…). Zusätzlich erhalten unsere Führungskräfte auch gesonderte Einweisungen bezüglich Daten- und Informationsschutz. (…). Das machen wir jetzt schon seit zwei Jahren und ich denke, dass das eine ganz gute Sache ist.

I: Sie hatten bereits am Anfang des Interviews die Trainings- und Sensibilisierungsmaßnahmen angesprochen. Könnten Sie hierzu noch einmal detaillierte Ausführungen machen?

Herr K.: Wir haben zum einen webbasierte Trainings. (…). Im Rahmen einer Umfrage konnten wir zum Beispiel feststellen, dass die Leute Bedarf an der richtigen Klassifizierung von Daten haben oder einen Bedarf an Informationen zum Thema Social Engineering haben. Daraufhin haben wir ein webbasiertes Training erarbeitet, wo wir die Inhalte durch Comics ver-

anschaulicht haben. Am Ende des Trainings werden dann Fragen gestellt, die zu beantworten sind. Der Teilnehmer erfährt auch gleich, ob er bestanden oder nicht bestanden hat. Das ist eine Sache die wir freiwillig anbieten, die wir bei neuen Standorten sogar verpflichtend durchführen. Wir haben diese webbasierten Trainings auch in unterschiedlichen Sprachen. (…). Dann haben wir Sensibilisierungen als Vortragsreihen, die wir hier hausintern mit dem Datenschutz, der IT-Sicherheit und der Revision abgestimmt haben. (…). Es gibt also eine Standardpräsentation, die immer wieder angepasst wird. Hierzu gibt es dann Veranstaltungen, wo ganze Hörsäle gefüllt werden. Hier gibt es auch Pflichtveranstaltungen für Mitarbeiter der Forschung und Entwicklung, aber es gibt auch Sensibilisierungen, die aus Ermittlungsvorgängen resultieren. Zusätzlich haben wir auch Flyer entwickelt, die wir in Gehaltsabrechnungen gelegt haben. Hier werden bestimmte Fragestellungen, wie Social Engineering, behandelt und es werden Ansprechpartner genannt. (…). Es gibt auch andere Sachen zum Downloaden. Wir haben zum Beispiel Plakate entworfen, die ausgedruckt werden können und in Büros und Aufenthaltsräumen ausgehangen werden können. Vieles liegt hier mehrsprachig in Dateiform vor, sodass auch andere Standorte diese Angebote nutzen können. (…). Wir haben in Diplomarbeiten auch Comics entwickeln lassen, wo situative Beispiele dargestellt sind. Ich muss Ihnen sagen, dass diese Comics auch in anderen Ländern, vor allem Russland, sehr gut ankommen. Das ist manchmal besser als hochtrabende Präsentationen. Diese Beispiele sind total einfach dargestellt. Dort sehen Sie zum Beispiel ein Schreibtisch, wo eine Figur die Clean-Desk-Policy umsetzt. Damit können wir den Top-Manager, aber auch die einfachen Mitarbeiter ansprechen.

I: In dem Flyer wird das Thema der Risiken auf Geschäftsreisen angesprochen. Ist das ein besonderes Thema, was auch in den Vorträgen zur Geltung kommt?

Herr K.: Sicherheit ist sehr umfangreich. Im Bereich des Know-how-Schutzes sensibilisieren wir auch zum Thema Geschäftsreisen. Wenn Sie zum Beispiel als Top-Manager in bestimmte Länder reisen, ist die Wahrscheinlichkeit sehr groß, dass Sie von Hostessen angesprochen werden, die bestimmte Intentionen besitzen. Es ist ja nicht unbekannt, dass Sie dorthin reisen. Hier führen wir selbstverständlich individuelle Beratungsgespräche. (…). Hier spielen neben den kulturellen auch sicherheitsrelevante Aspekte eine Rolle. (…).

I: Herr K., inwieweit werden Mitarbeiter bei der Entwicklung von Know-how-Schutzmaßnahmen eingebunden?

Herr K.: Bei der Entwicklung der Unterlagen haben die Mitarbeiter eine Menge mitentwickelt. Die Unterlagen sind ja aus dem Feedback der Mitarbeiter entstanden. (…). Da der Inhalt auf dem Bedarf der Mitarbeiter basiert, ist der Inhalt schon sehr gut mit den Mitarbeitern abgestimmt. Die Sensibilisierung der Mitarbeiter findet dann aber top-down statt. Die Sensibilisierung liegt also in der Führungsverantwortung. Sonst würde es keiner machen, da solche Maßnahmen immer mit Aufwand verbunden sind. (…).

I: Loyalität und Zufriedenheit der Mitarbeiter schaffen Sicherheit nach innen und nach außen. Inwieweit werden Mitarbeiter denn leistungsgerecht entlohnt und erhalten auch unentgeltliche Anerkennung für ihre beruflichen Leistungen?

Herr K.: Diese Frage würde ich gerne auslassen, da das ein Thema der Personalabteilung ist.

I: Wissen Sie, ob es in Ihrem Unternehmen Umfragen zur Messung der Mitarbeiterzufriedenheit gibt?

Herr K.: (…). Zur Mitarbeiterzufriedenheit gibt es eine große Kampagne des Personaldirektors. Hierzu gibt es eine jährliche internetbasierte Umfrage, an der jeder Mitarbeiter teilnehmen muss. Diese Umfrage wird dann auch sehr gut verfolgt. Dort werden Stärken- und Schwächenanalysen durchgeführt. Das ist schon sehr aufwendig. (…). Die Ergebnisse sind grundsätzlich sehr gut, aber individuell. (…).

I: Kommen wir nach dem sicherheitsbewussten Personalmanagement zur Beendigung eines Arbeitsverhältnisses. Welche Sicherheitsmaßnahmen werden dort ergriffen?

Herr K.: Das ist relativ gut bei uns. Hier sind wir meiner Ansicht nach auch für viele Benchmark. Wenn jemand aus dem Unternehmen ausscheidet, geht das natürlich über die Personalabteilung. Hier haben wir bestimmte IT-Systeme, wo bestimmte Aktivitäten, wie Ausweisabgabe und Löschung von User-IDs, durchgeführt werden. Somit können wir dann auch sagen, dass beim Ausscheiden des Mitarbeiters auch alle seine Accounts gelöscht sind. So wie ich das mitkriege, läuft das bei vielen anderen Unternehmen nicht so ab.

I: Gibt es auch Unterschiede zwischen einem regulärem und einem nicht einvernehmlichen Ausscheiden des Mitarbeiters bezüglich der Sicherheitsmaßnahmen?

Herr K.: Das ist eigentlich ja egal, da der Arbeitsvertrag ja ausläuft oder gekündigt wird. Damit laufen dann alle Aktivitäten aus. Natürlich gibt es auch Sachen, wo jemand Werksverbot

bekommt, wenn er hier zum Beispiel etwas klaut. Das läuft dann automatisch und schon bevor arbeitsrechtlich hier etwas groß beschlossen werden muss. (…). Im Prinzip ist es aber wirklich so, dass wenn jemand ausscheidet, sei es aus Altersgründen oder sonstigen Dingen, er nichts mehr hat. Dort wird dann alles deaktiviert.

I: Und findet nach der Beendigung des Arbeitsverhältnisses auch eine intensive Beobachtung der ehemaligen Mitarbeiter oder Konkurrenten statt?

Herr K.: Nein. (…). Wir haben ja auch Datenschutzgesetze und ich denke, dass man sich auch die Gegebenheiten halten muss. Wir sind hier ja kein Spionageverein. Wenn es gewisse Dinge gibt, geht das den Weg über die Staatsanwaltschaft, die ihre Konsequenzen durchführt. (…).

I: Herr K., wir haben gerade über das firmeneigene Personal gesprochen. Gelten für das firmenfremde Personal, wie Leiharbeiter, Mitarbeiter von Geschäftspartnern, Berater, Sicherheits- und Reinigungskräfte, die gleichen Sicherheitsbedingungen wie für das firmeneigene Personal?

Herr K.: Ja, hier gelten die gleichen Sicherheitsbedingungen. Es kommt auch immer darauf an was Sie betrachten. Wenn wir zum Beispiel Fremdfirmen haben, die unkritische Sachen machen, schauen wir weniger auf die Leute, da das Risiko gering ist. Wenn Fremdfirmen aber den heißesten Prototypen mit entwickeln, haben die natürlich die gleichen Sicherheitsauflagen wie unsere Mitarbeiter. Das heißt, dass die Firmen Geheimhaltungsvereinbarungen unterschreiben müssen und Fremdfirmen-Sicherheits-Audits kriegen. Hier schauen wir wie die Organisation in der Firma aufgebaut ist und wie sie Daten abgelegen. (…). Also wir unterscheiden schon, welche Informationen firmenfremdes Personal erhält und zu welchen Bereichen sie Zugang bekommen. Je nach Klassifizierungsgrad des Bereichs oder der Informationen, kriegen die dann ihre Sicherheitsauflagen. Zum Beispiel würden wir auch keine Firma nehmen, die unsere Sicherheitsauflagen nicht erfüllt, auch wenn sie preislich billiger ist.

I: Ich würde nun gerne zu den organisatorischen Sicherheitsmaßnahmen übergehen. Sie sprachen ja bereits die Clean-Desk-Policy an. Gibt es weitere formal fixierte Sicherheitsstandards?

Herr K.: Ja, organisatorisch kann man ja unterscheiden. Wir haben die kleinen Dinge, wie die Clean-Desk-Policy. Wir haben aber auch Grundsätze, wie das Thema Sensibilisierung und Führungsverantwortung. Das sind Grundsätze bei uns, wo die Führungskraft dafür verant-

wortlich ist, dass die Mitarbeiter, die auch mit geheimen Sachen arbeiten, die Möglichkeit haben die Sachen sicher abzulegen, zu kommunizieren und zu versenden. Die Führungskraft muss also die Rahmenbedingungen schaffen. Wir haben aber auch organisatorisch-regulatorische Sachen. Wir haben zum Beispiel Regeln im Haus, wo genau beschrieben wird wie mit sensiblen Daten, je nach Klassifikation, umzugehen ist. (…).

I: Könnte Sie kurz auf die Ausgestaltung der Klassifizierung von Informationen eingehen?

Herr K.: Ja. Wir haben versucht die Klassifizierungsstufen möglichst gering zu halten, da mit jeder weiteren Klassifizierungsstufe das Verfahren komplexer wird und keiner mehr durchblickt. (…). Wir haben vier Stufen. Einmal „öffentlich", das alles ist was die Kommunikation schon herausgegeben hat und jeder einsehen kann. Wir haben „intern", das betrifft so etwas wie Telefonverzeichnisse, die einen bestimmten Wertigkeitsgrad haben. Wir haben dann noch „vertraulich" und „geheim". „Geheim" ist natürlich der geringste Satz. Bei uns gibt es auch nicht solche Sachen wie „streng geheim" oder „top secret", da „geheim" für uns schon die höchste Klasse ist. Hierzu gehören Strategiepläne, Prototypen oder Designs. Das hätte schon massive Auswirkungen, wenn solche Informationen an Dritte oder Konkurrenten gelangen würden. Das sind die grundsätzlichen Fragestellungen, die wir haben. Wir gucken immer was der Informationsabfluss für Auswirkungen hat, sei es nun an Dritte, Konkurrenten oder Medien. Dementsprechend gibt es bestimme Einstufungen.

I: Sie hatten gerade die Klassifizierung von Informationen angesprochen. Sind dementsprechend auch die Bestimmungen zur Nutzung, Vervielfältigung und Vernichtung von Informationsbeständen ausgestaltet?

Herr K.: Das ist alles komplett geregelt. Sie haben als Ersteller die Klassifizierungspflicht. Wenn Sie zum Beispiel ein Vorstandsprotokoll als geheim einstufen, wird mit Wasserzeichen und Übergabeprotokollen gearbeitet. Dort wird dann auch geschaut, dass das in einem Panzerschrank abgelegt wird. Das ist alles bei uns eindeutig geregelt. Die Leute tun sich aber trotzdem schwer mit der Klassifizierung, da ja auch der Aufwand für eine höhere Klassifizierung größer ist. (…). Hier muss man die Leute immer ermahnen und sie daran erinnern, dass hier nicht einfach herunter klassifiziert wird. (…).

I: Herr K., Sie hatten erwähnt, dass die Konzernsicherheit organisatorisch direkt an den Vorstand angebunden ist. Könnten Sie in Kürze noch einmal das Aufgabenspektrum der Konzernsicherheit wiedergeben?

Herr K.: (…). Wir haben einen Prototypenschutz, der für den gesamten Umgang mit Prototypen zuständig ist. Wir haben den Bereich technische Sicherheit, der für die Zutrittskontrollsysteme und ähnliches zuständig ist. Dann haben wir die Bereiche Informationsschutz und Ermittlungen. Im Bereich der Ermittlungen haben die Standorte eigene Ermittler, aber wir greifen in bestimmten Fällen ein, wenn eine bestimmte Wertigkeit oder übergreifende Sachen vorliegen. Wir haben dann noch das Thema Konzernbrandschutz. (…). Dann haben wir noch den Bereich Eventmanagement, der bei Großveranstaltungen, wie Hauptversammlungen, mit eingeschaltet wird. (…). Wir haben auch das Thema Reisesicherheit, indem wir auch die Länder bezüglich rechtlicher, politischer, wirtschaftlicher Risiken screenen. Ein aktuelles Beispiel ist Japan, wo wir dann gucken, begleiten, Reisehinweise und Reisesperren ausgeben. (…). Dann ist auch noch das Thema Risikomanagement bei uns angesiedelt. Zusätzlich gibt es den Bereich Personenbegleitung.

I: Sie hatten gerade den Bereich der Zutrittsrechte angesprochen. Könnten Sie hierzu noch weitere Ausführungen machen?

Herr K.: Wir haben für bestimmte Bereiche, wo sich vertrauliche und geheime Daten befinden, in denen es Zutrittsberechtigungssysteme gibt. Grundsätzlich geben wir den Standorten nicht immer die technische Ausprägung vor, sondern die Rahmenbedingungen. Hier weisen wir zum Beispiel die Standorte auf gesetzliche Pflichten, wie die Speicherung von Daten, hin. Wir geben also schon die Vorgaben welche Mindestanforderungen eine Sicherheitstechnik haben muss. (…). Wir haben zum Beispiel auch Videotechnik.

I: Herr K., Sie hatten am Anfang erwähnt, dass Sicherheits-Audits innerhalb des Unternehmens und bei Partnern durchgeführt werden. Was sind denn die genauen Inhalte der Kontrollen und in welchen Abständen erfolgen sie?

Herr K.: (…). Wir machen Sicherheits-Checks immer dann, wenn ein Fachbereich mit einer Fremdfirma zusammenarbeitet und mindestens vertrauliche Informationen weitergibt. Dann erfolgt es so, dass die Abteilung uns die Firma nennt und wir dort eine Abnahme machen. Früher haben wir das selbst in der Konzernsicherheit gemacht. Jetzt wird das durch eine externe Firma nach unseren Sicherheitsstandards gemacht. Wir kriegen dann ein Feedback von der Firma und haben zusätzlich Kontrollrechte. Bei besonderen Projekten kontrollieren wir hier nochmal. Diese Sicherheits-Audits sind auch Voraussetzung der ISO 27001. (…). In dieser Sicherheitsabnahme haben wir organisatorische, räumliche, informationstechnische und

informationsschützende Aspekte drin. Das sind die wesentlichen Facetten, die jeder positiv durchlaufen muss. Hier gibt es dann Berichte zu den Audits, wo zum Beispiel drin steht, dass der Zaun zu niedrig ist, nicht die aktuellen Patches auf den Rechnern sind (…) oder die Server nicht gehärtet sind. Die kriegen dann einen Bericht, der umzusetzen ist, und erst dann kriegen die die Freigabe und Beauftragung. Das machen wir bei großen und kleinen Projekten. Bei Großprojekten, wie Offshoring in Indien, können diese Audits mehrere Wochen lang sein.

I: Findet denn bei durch Kontrollen entdeckte Sicherheitsverstöße eine Sanktionierung statt?

Herr K.: Bei externen Mitarbeitern können wir nur rechtlich vorgehen, wobei wir uns in manchen Fällen eine Geheimhaltung der Gesellschaft und zusätzlich eine personenbezogene Geheimhaltungsvereinbarung geben lassen. Diese personenbezogenen Geheimhaltungsvereinbarungen sind deutlich besser, da bei Geheimhaltungen mit der Gesellschaft oft nur Konventionalstrafen erfolgen. Bei personenbezogenen Vereinbarungen geht es schon an das Eingemachte. Intern gibt es ebenfalls Sanktionen. Wenn Sie zum Beispiel die Emails nicht ordnungsgemäß verschlüsseln oder falsch adressieren, wo Insiderwissen enthalten war, gibt es natürlich arbeitsrechtliche Konsequenzen und Schadensersatzklagen.

I: Gibt es umgekehrt auch eine Belohnung für sicherheitsbewusstes Handeln von Mitarbeitern?

Herr K.: Ja, das ist einer unser Grundsätze. Wenn jemand einen Hinweis gibt, darf er nicht bestraft werden. In den siebziger Jahren ging so etwas ja eher in die Richtung Anschwärzen. Das ist heute ganz anders. Wir haben ja auch ein Ombudsmannsystem, wo wir die Leute loben und ihnen positives Feedback geben. Das geht auch soweit, dass wir uns für gemobbte Mitarbeiter einsetzen, sodass die den Bereich schnell verlassen können.

I: Ich würde gerne nun auf die technischen Sicherheitsmaßnahmen in Ihrem Unternehmen eingehen. Sie hatten ja bereits einige bautechnische Maßnahmen erwähnt. Könnten Sie weitere bautechnische Maßnahmen nennen?

Herr K.: (…). Wir setzen im Rahmen der gesetzlichen Bestimmungen Videotechnik ein. Wir schauen uns bei der Bautechnik natürlich auch Widerstandswerte von Türen an. Wir haben Sichtschutzvereinbarungen. (…). Es nützt Ihnen ja nichts, wenn Sie die tollsten Räumlichkeiten haben und jemand mit dem Fernglas auf Ihren Monitor schaut und geheime Sachen sieht. Das ist ein ganzes Portfolio. Nicht nur Zutritts- und Videoüberwachung, sondern auch Stahl-

schränke, Sonderschließungen, Alarmanlagen und Bewegungsmelder. Das ist aber abhängig von den Bereichen. Zum Beispiel ist bei uns der Bereich Design sehr kritisch, da hier das Neueste von uns stattfindet. Auch die Rechenzentren sind sehr sensibel. Wir haben auch Sicherheitsschleusen und bautechnische Maßnahmen, die vor Sprengstoffanschlägen schützen sollen. Das ist dann aber schon eine Sonderplanung.

I: Und gibt es, speziell auf Ebene des Vorstands, abhörschutzsichere Räume?

Herr K.: Ja, darauf möchte ich aber nicht weiter eingehen.

I: Ok. Im Bereich Technik würde ich gerne noch auf die Maßnahmen zur Sicherung von Informations- und Kommunikationstechnik eingehen. Sie hatten bereits gesagt, dass es Accounts und eine Passwortpflicht gibt. Findet auch ein systematischer Passwortwechsel statt?

Herr K.: Nach ISO 27001 ist das alles geregelt. (…). Grundsätzlich ist hier alles auf dem neuesten Stand. Wir haben ein Team, dass aktuelle Virenscanner und Spam auswertet. Hier findet das komplette Programm statt. Das Problem ist nur eine Technologie zu finden, die den Anwender nicht überfordert. (…).

I: Email-Angriffe und fremde USB-Sticks bilden ja weitere Gefahren für die Informations- und Kommunikationstechnik. Gab es hierzu Vorfälle in Ihrem Unternehmen?

Herr K.: Da kann man über sehr viele Vorfälle berichten. Schlechte Vorfälle haben wir ganz viele von Studenten, Diplomanden und Doktoranden, aber ich möchte Ihnen gerne über einen positiven Fall berichten. Wir hatten eine Messe, wo ein Repräsentant unseres Hause an seinem Stand war. Dort kam eine asiatische Delegation mit vier Managern und zwei Dolmetscherinnen, die gerne 2000 Produkte von unserem Unternehmen kaufen wollten. In dem stattfindenden Smalltalk zwischen unserem Repräsentant, den Dolmetscherinnen und den angeblichen Managern einigte man sich das Gespräch am nächsten Tag fortzusetzen. Man tauschte Visitenkarten aus und der eine Manager überreichte unserem Repräsentanten einen USB-Stick, wo angeblich eine Präsentation der interessierten Firma enthalten sein sollten. (…). Weil das Angebot aus dem asiatischen Raum kam, war der Mitarbeiter schon mehr durch unsere Maßnahmen und die Medien sensibilisiert. Daraufhin rief er bei uns an und fragte uns nach Rat, weil ihm das alles sehr komisch vorkam. Und tatsächlich konnten wir feststellen, dass der USB-Stick verseucht war. Nun werden normale Programme durch unsere Schutzprogramme erkannt. Das Problem war nur, dass das Programm auf dem Stick ein gezielt ge-

schriebenes Programm war, dass vom Scanner nicht entdeckt worden wäre. In unserem Labor konnten wir das schädliche Programm dann entdecken. Zusätzlich waren die Visitenkarten gefälscht. Das war ein gezielter Angriff, sicherlich von einer anderen Nation, um dieses Trojaner-Programm zu implementieren. Das war sehr gutes Beispiel und so etwas verwende ich dann auch immer in meinen Präsentationen. (…). Wir haben aber auch andere Fälle, wo USB-Sticks zum Beispiel auf Kinderspielplätzen verloren werden, irgendjemand das Ding findet und Geld dafür haben will. Normalerweise ist das total unkritisch, wenn die Leute die Daten verschlüsseln würden. Das Problem haben wir immer erst dann, wenn sich die Leute nicht an die Vorgaben halten. (…). USB-Sticks sind echt schlimm.

I: Ganz zum Schluss würde ich gerne noch einmal auf die rechtlichen Sicherheitsmaßnahmen eingehen. Sie hatten bereits angesprochen, dass Geheimhaltungsvereinbarungen zwischen Ihrem Unternehmen und den Mitarbeitern beziehungsweise zwischen Ihrem Unternehmen und Geschäftspartnern bestehen. Könnten Sie noch einmal die rechtlichen Konsequenzen bei Verstoß gegen diese Vereinbarungen schildern?

Herr K.: Die Ergebnisse hierzu hat natürlich unser Rechtswesen. Ich kann Ihnen nur sagen, dass bei Ermittlungsfällen die Geheimhaltungserklärungen herangezogen und Berichte erstellt werden. Die rechtliche Verfolgung übernimmt das Rechtswesen. (…). Personen, die gegen die Geheimhaltung verstoßen, werden schon herangezogen. Wir hatten jetzt ein Beispiel, wo ein Diplomand in der F&E-Abteilung war und Dinge auf seinen USB-Stick gezogen hat, obwohl er das nicht durfte. (…). Dieser Diplomand hatte diese Daten auch mit anderen ausgetauscht, was wir im Nachhinein feststellen konnten. (…). Der Schaden für ihn war, dass er seine Diplomarbeit nicht mehr hier zu Ende schreiben konnte. Der Folgeschaden war aber viel größer, weil es für den richtig schwierig wird wieder einen Job zu finden. Irgendwie sind die Unternehmen ja alle miteinander vernetzt. (…). Das sind die viel größeren Strafen, die jemand hat. Das ist genauso, wenn hier jemand klaut. (…).

I: Als technologieorientiertes Unternehmen werden bei Ihnen ja viele Patente angemeldet. Gab es bisher auch negative Erfahrungen mit der Patentierung?

Herr K.: (…). Wenn Sie hier ein Patent anmelden, habe Sie tausende Mitarbeiter, die an dieser Information mitgearbeitet haben. (…). Dort forschen ganze Teams und Abteilungen dran. Hier ist immer die Frage wo Informationen abfließen. Informationen können aber auch extern abfließen. Wenn zum Beispiel ein Patentanwalt bei irgendeiner anderen Firma vergisst eine

Sperrfrist beim Patentamt einzurichten (…), dann kann das jeder recherchieren. Das sind solche Sachen, wo wir vom Informationsschutz das Patentwesen ansprechen seine Mitarbeiter dafür zu sensibilisieren. (…). Oft ist es ja auch die Unwissenheit oder Schludrigkeit.

I: Herr K., die letzte Frage zielt auf die Zertifizierung von Geschäftsprozessen ab. Gab es mit Zertifizierungsgesellschaften schon Vorfälle im Informationsabfluss?

Herr K.: (…). Man kriegt ja immer nur etwas mit, wenn es entdeckt wird und das ist ja eher zufällig. (…). Da kann ich keine mengenmäßige Aussage zu treffen. Das ist eher Zufall.

I: Vielen Dank für das Interview.

Herr K.: Bitte sehr.

Beurteilung des Interviews:

Dieses Gespräch bildete das achte und letzte Interview mit Geschäftsführern und Sicherheitsverantwortlichen unterschiedlicher Unternehmen. Mit einer Dauer von einer guten Stunde kam es zu keinen zeitlichen Problemen. Inhaltlich gab der Interviewte nach anfänglicher Zurückhaltung im Laufe des Gesprächs weite Einblicke in das praktizierte System von Spionageabwehrmaßnahmen. Gewisse Fragen beantwortete der Interviewte nur knapp oder gar nicht.