



# Fall- und Schadensanalyse bezüglich Know-how-/ Informationsverlusten in Baden-Württemberg ab 1995



Prof. Dr. Egbert Kahle  
Prof. Dr. Wilma Merkel

Universität Lüneburg

im Auftrag des

# Sicherheitsforum Baden-Württemberg

Die Wirtschaft schützt ihr Wissen

# **Fall- und Schadensanalyse bezüglich Know-how-/ Informationsverlusten in Baden- Württemberg ab 1995**

Schlussgutachten

**Stand: 10. 06. 2004**

Prof. Dr. Egbert Kahle

Prof. Dr. Wilma Merkel

Universität Lüneburg

Institut für Betriebswirtschaftslehre

## Vorwort und Projektauftrag

Vom Sicherheitsforum des Landes Baden Württemberg und dem Auftragnehmer wurde im Juli 2002 ein Werkvertrag zur Erstellung eines gutachterlichen Berichts zur Fall- und Schadensanalyse bezüglich Know-how-/Informationsverlusten in Baden-Württemberg ab 1995 mit folgender **Zielsetzung** geschlossen:

- **Ermittlung der potentiellen Schadenshöhe und -relevanz**
- **Aufzeigen von Wegen zur Prävention**

Auslöser des Werkvertrags waren u. a. Einzelerkenntnisse der dem Sicherheitsforum angehörenden Institutionen über das Vorhandensein folgender Schwachstellen in der Wirtschaft Baden-Württembergs:

- „Keine klaren Vorstellungen über Existenz und Wert eigener Betriebsgeheimnisse
- Keine Erfassung der Sicherheitsbelange in den Unternehmenszielen
- Keine oder unzureichende Regeln (Richtlinien, Empfehlungen) für den Umgang mit Betriebsgeheimnissen
- Unsystematische Prävention (kein ganzheitliches Informationsschutzkonzept)
- Menschliche Schwächen: Falsches Verhalten in kritischen Situationen aus Vorsatz, Fahrlässigkeit, Irrtum, Bequemlichkeit oder Überforderung)<sup>1</sup>

Der Werkvertrag war, daraus abgeleitet, auf folgende Schwerpunkte fokussiert:

- Der Auftragnehmer übernimmt die Erstellung eines gutachterlichen Berichts über die inhaltliche Struktur (Schwachstellenanalyse) von ausgewählten Schadensfällen, die der Auftraggeber bereitstellt. Für die Auswahl werden vom Auftragnehmer Anforderungsprofile für die Fallbeschreibung erstellt.
- Bei der Auswertung der Fälle werden neben der Fallbeschreibung und der Einsicht in Akten von den Projektverantwortlichen des Auftragnehmers **Interviews** mit ausgewählten Managern der betroffenen Firmen geführt.
- Im Ergebnis der sich an den Anforderungsprofilen orientierenden Interviews ist vom Auftragnehmer ein **erster gutachterlicher Bericht** zu erstellen, der die Grundlage für die Entwicklung eines Fragebogens durch den Auftragnehmer in Abstimmung mit dem Auftraggeber für eine **repräsentative Fragebogenaktion** zu den ermittelten Schwachstellen ist.
- Auf der Grundlage der Fragebogenaktion wird vom Auftragnehmer ein abschließendes Gutachten (**zweiter Teil des gutachterlichen Berichts**) zu ausgewählten Sicherheitsaspekten in Baden-Württemberg lt. o.g. Zielsetzung erstellt.

---

<sup>1</sup> Verfassungsschutzbericht Baden-Württemberg 2001, Hsg. Innenministerium Baden-Württemberg, Mai 2002, S. 224-225.

Die Realisierung des Projektauftrags dokumentiert sich in folgenden Arbeitsergebnissen des Auftragnehmers, die dem Auftraggeber vorliegen und von diesem bestätigt wurden:

- Erster gutachterlicher Bericht vom 10. Oktober 2002 auf der Grundlage der in der Zeit vom 16. bis zum 18. September 2002 durchgeführten Interviews
- Repräsentative Fragebogenaktion vom 7. Februar bis zum 13. März 2003
- Vortrag und Übergabe der Ergebnisse der nach verschiedenen Aspekten strukturierten Auswertung der Fragebögen am 8. Mai 2003 in Leopoldshafen

Die vorgenannten Arbeitsergebnisse sowie der Projektbericht des Auftragnehmers vom 3. September 2003 sind die Grundlage des nachfolgenden Schlussgutachtens.

Die Zusammenfassung der Hauptergebnisse des Projektauftrags in Beziehung zu den vier herausgearbeiteten Fragestellungen erfolgt unter Punkt 1.

## Inhaltsverzeichnis

<b>Tabellenverzeichnis</b> .....	IV
<b>Abbildungsverzeichnis</b> .....	V
<b>1 Einführung in die Problemstellung und Arbeitshypothesen</b> .....	1
<b>2 Begriffliche Grundlagen und theoretisches Grundverständnis</b> .....	4
<b>3 Methodische Grundlagen und Basisdaten der Untersuchung</b> .....	18
3.1 Aufbau der Messinstrumente und Anforderungsprofile zur Auswertung der Schadensfälle ..	18
3.2 Vorbereitung des Fragebogens durch Interviews mit Geschäftsleitungen betroffener Unternehmen (Pretest) .....	21
3.3 Ergebnisse der Auswertung der Interviews und Gespräche .....	28
3.4 Struktur des Fragebogens .....	30
3.5 Durchführung der Befragung .....	33
3.6 Sicherung des Schutzes personenbezogener Daten .....	35
<b>4 Ergebnisse</b> .....	36
4.1 Die Befunde zu den Einzelfragen (Tabellen und Abbildungen) .....	36
4.2 Nach verschiedenen Aspekten strukturierte Auswertung der Fragebögen .....	60
4.2.1 Allgemeine Ergebnisse .....	60
4.2.2 Einzelne Einflussfaktoren und Verknüpfungen .....	64
<b>5 Gefährdungspotenziale und Handlungsempfehlungen</b> .....	71
5.1 Gefährdungspotenziale .....	71
5.2 Präventionsmaßnahmen im Einzelnen .....	72
5.2.1 Sicherheit braucht ein Konzept und ist Managementaufgabe .....	72
5.2.2 Entwicklung einer „Wissensbilanz“ oder „Informationsinventur“ .....	74
5.2.3 Entwicklung eines Handhabungsschemas für Risikomanagement .....	74
5.2.4 Entwicklung von fachrichtungsübergreifenden Schulungsmaßnahmen für Mitarbeiter der Sicherheitsbehörden und für die Sicherheitsverantwortlichen in den Unternehmen	75
5.2.5 Entwicklung unternehmensspezifischer Präventionsmaßnahmen .....	76
5.2.6 Weiterführende Empfehlungen .....	76
<b>Quellen und weiterführende Literaturhinweise</b> .....	78
<b>Anhang 1: Fragebogen Stand Januar 2002</b> .....	84
<b>Anhang 2: Programmskizze für ein Verbundprogramm</b> „Wissenschaftliche Weiterbildung Security Management“ .....	92

## Tabellenverzeichnis

Tabelle 1	Exemplarische Schadensfälle im Land Baden-Württemberg, Zeitraum 1980-2002.....	19
Tabelle 2	In die schriftliche Befragung einbezogene Wirtschaftszweige.....	34
Tabelle 3	Übersicht der Nennungen zu den 19 Fragen des Fragebogens aus 400 Rückläufen der Fragebogenaktion .....	37
Tabelle 4	Antworten zur Frage 1 „Wie sieht Ihre Produkt-Markt-Position aus? (Produkt schließt hier alle Arten von Dienstleistungen ein)“.....	38
Tabelle 5	Antworten zur Frage 2 „Wie hoch war Ihr durchschnittlicher Umsatz in den letzten drei Jahren?“ .....	39
Tabelle 6	Antworten zur Frage 3 „Worin besteht Ihr wichtigster Wettbewerbsvorteil/-vorsprung?“ .....	40
Tabelle 7	Antworten zur Frage 4 „Wie ist der Wettbewerbsvorteil/-vorsprung entstanden?“ .....	41
Tabelle 8	Antworten zur Frage 5 „Welche ungefähren Aufwendungen haben Sie für die Erstellung bzw. Erarbeitung des Wettbewerbsvorteils/-vorsprungs gehabt? Falls die Angaben nicht in Euro beziffert werden können, bitte Personal- und Zeitaufwand benennen.“ .....	42
Tabelle 9	Antworten zur Frage 6 „Wie hoch schätzen Sie den Wert des Wettbewerbsvorteils/-vorsprungs ein (gemessen in Euro pro Jahr)?“ .....	43
Tabelle 10	Antworten zur Frage 7 „Wie nachhaltig ist der Wettbewerbsvorteil/-vorsprung?“ .....	44
Tabelle 11	Antworten zur Frage 8 „Wie lange hält der momentane Wettbewerbsvorteil/-vorsprung, wenn Sie keine weiteren Investitionen oder andere Maßnahmen dafür tätigen oder wenn er nicht durch adäquate Maßnahmen erhalten wird?“ .....	46
Tabelle 12	Antworten zur Frage 9 „Welche Sicherungsmaßnahmen gegen Informationsverluste werden vorgenommen?“ .....	47
Tabelle 13	Antworten zur Frage 10 „Wie hoch sind Ihre Aufwendungen für Informationssicherheit (in Euro pro Jahr)?“ .....	49
Tabelle 14	Antworten zur Frage 11 „Wer könnte an dem Wissen Interesse haben, das dem Wettbewerbsvorteil/-vorsprung zugrunde liegt?“ .....	50
Tabelle 15	Antworten zur Frage 12 „Waren Sie schon Objekt „unfreundlichen“ Informationsabflusses? (Ausspähung, Abschöpfung, Abwerbung, Mitnahme von Geheimnissen bei Weggang von Mitarbeitern,...)“ .....	51
Tabelle 16	Antworten zur Frage 13 „Wie hoch schätzen Sie den in diesem Fall entstandenen Schaden (in Euro)?“ .....	52
Tabelle 17	Antworten zur Frage 14 „Wie haben Sie den Schadensfall bearbeitet?“.....	53
Tabelle 18	Antworten zur Frage 15 „Welche Sicherheitsmaßnahmen haben Sie als Folge des Schadensfalls ergriffen?“ .....	54
Tabelle 19	Antworten zur Frage 16 „Welche Verdachtsmomente zu Informationsabflüssen hatten Sie bisher?“ .....	55
Tabelle 20	Antworten zur Frage 17 „Wie sind die Beziehungen zu Kooperationspartnern abgesichert?“ .....	56
Tabelle 21	Antworten zur Frage 18 „Gab es bei abgeworbenen/abgewanderten Mitarbeitern Anzeichen für die Illoyalität?“ .....	57
Tabelle 22	Antworten zur Frage 19 „Wie ist die Einschätzung der Arbeit der/Kooperation mit den Sicherheitsbehörden?“ .....	58

## Abbildungsverzeichnis

Abbildung 1 Nachweis der Verteilung der interviewten Unternehmen über die gesamte Region Baden-Württemberg zur Erfassung gegebenenfalls vorhandener regionaler Besonderheiten .....	27
Abbildung 2 Graphische Auswertung der Antwortmöglichkeiten zur Frage 1 .....	38
Abbildung 3 Graphische Auswertung der Antwortmöglichkeiten zur Frage 2 .....	39
Abbildung 4 Graphische Auswertung der Antwortmöglichkeiten zur Frage 3 .....	40
Abbildung 5 Graphische Auswertung der Antwortmöglichkeiten zur Frage 4 .....	41
Abbildung 6 Graphische Auswertung der Antwortmöglichkeiten zur Frage 5 .....	42
Abbildung 7 Graphische Auswertung der Antwortmöglichkeiten zur Frage 6 .....	43
Abbildung 8 Graphische Auswertung der Antwortmöglichkeiten zur Frage 7 .....	45
Abbildung 9 Graphische Auswertung der Antwortmöglichkeiten zur Frage 8 .....	46
Abbildung 10 Graphische Auswertung der Antwortmöglichkeiten zur Frage 9 .....	48
Abbildung 11 Graphische Auswertung der Antwortmöglichkeiten zur Frage 10 .....	49
Abbildung 12 Graphische Auswertung der Antwortmöglichkeiten zur Frage 11 .....	50
Abbildung 13 Graphische Auswertung der Antwortmöglichkeiten zur Frage 12 .....	51
Abbildung 14 Graphische Auswertung der Antwortmöglichkeiten zur Frage 13 .....	52
Abbildung 15 Graphische Auswertung der Antwortmöglichkeiten zur Frage 14 .....	53
Abbildung 16 Graphische Auswertung der Antwortmöglichkeiten zur Frage 15 .....	54
Abbildung 17 Graphische Auswertung der Antwortmöglichkeiten zur Frage 16 .....	55
Abbildung 18 Graphische Auswertung der Antwortmöglichkeiten zur Frage 17 .....	56
Abbildung 19 Graphische Auswertung der Antwortmöglichkeiten zur Frage 18 .....	57
Abbildung 20 Graphische Auswertung der Antwortmöglichkeiten zur Frage 19 .....	59
Abbildung 21 Gefährdungspotenziale berechnet auf der Basis folgender gerundeter Werte in Milliarden €.....	62

# 1 Einführung in die Problemstellung und Arbeitshypothesen

Die Bedeutung von Informationsverlusten für Unternehmen wird in Kreisen von Sicherheitsexperten<sup>2</sup> seit längerem gesehen und als bedeutsam eingestuft, ist aber in der allgemeinen wirtschaftlichen Diskussion weder in der Theorie noch in der Praxis vertieft diskutiert worden. Von ausgewählten Einzelveröffentlichungen abgesehen<sup>3</sup> fehlt es an einem klaren Konzept zur Informationssicherheit ebenso wie an verlässlichen Daten über den tatsächlichen Umfang von Schäden durch Informationsverluste und das weitere Gefährdungspotenzial. Während es zu den Schäden durch Beeinträchtigung der materiellen Ressourcen von Unternehmen wie durch Diebstahl oder Unterschlagung hinreichende empirische Befunde und auch vor allem rechts- und sozialwissenschaftlich fundierte theoretische Ansätze gibt<sup>4</sup>, ist die Ausgangssituation für die Beurteilung von Informationsverlusten konzeptionell und empirisch bestenfalls als vage zu bezeichnen.

Durch die vorgelegte Analyse soll eine Lücke im Kenntnisstand über die Bedeutung und die Art und Weise von Informationsverlusten in Unternehmen geschlossen werden und die Aufmerksamkeit der als gefährdet angesehenen Unternehmen oder Unternehmenstypen auf die Gefährdungspotenziale und auf geeignete Handlungsmöglichkeiten gelenkt werden. Diese Bewusstmachung des Problems der Informationsgefährdung ist dabei deshalb besonders bedeutsam, weil aus Gründen des „Gesichtsverlusts“, aber auch der inneren Betroffenheit von solchen Informationsverletzungen, die davon Betroffenen nicht darüber reden und damit die Öffentlichkeit oder die relevanten „Mitbetroffenen“ - weil zukünftig Gefährdeten - nichts davon erfahren. Ein weiterer „Verdunkelungspunkt“ bei der Gefährdungsanalyse ist die erheblich geringere Offensichtlichkeit des Zusammenhangs von Informationsverlust und ökonomischer Wirkung, während sie bei einem Diebstahl oder einer Unterschlagung von materiellen Gegenständen offenkundig ist; das führt zu einer Unterschätzung der Risikowirkungen von Informationsverlusten. Drittens ist der Begriff des Eigentums nicht nur in unserer Kultur sehr stark auf materielle Objekte bezogen – auch wenn wir den Begriff des geistigen Eigentums kennen, der aber extra durch das Adjektiv geformt wird -, so dass eine Verletzung informationeller Beziehungen gar nicht oder eher dilatorisch als Delikt angesehen wird.

Aus dieser Problemeinschätzung heraus, dass es ja nur ein „Kavaliersdelikt“ sei, dass man die Wirkungen so genau ja gar nicht kenne und man am liebsten gar nicht darüber spricht, ergibt sich die Dringlichkeit der Aufmerksamkeit für das Problem, wenn es denn nachgewiesen werden kann, dass es eine ökonomisch bedeutsame Größenordnung hat; die bisherigen Schätzungen dazu schwanken so sehr, dass sich tragfähige Aussagen darauf nicht aufbauen lassen.

---

<sup>2</sup> Vgl. Hierzu die Vielzahl von Veröffentlichungen in den Fachzeitschriften im Schriftenverzeichnis

<sup>3</sup> z.B. Kahle, E., Security-Management unter HR- und Organisationsaspekten, in: Personalführung, 5/2002, S. 22 - 31.; Sitt, A., Dynamisches Risiko-Management – Zum unternehmerischen Umgang mit Risiken, Wiesbaden 2003

<sup>4</sup> Die aktuellste ist die Studie von Rolfes, M. – Wilmes, K., Wirtschaftskriminalität in Niedersachsen 2003 – Betroffenheit und Bewertung aus der Sicht niedersächsischer Unternehmen, Osnabrück 2003

Daraus ergeben sich die Anforderungen für die inhaltliche Ausrichtung dieser Fall- und Schadensanalyse, die zugleich als Arbeitshypothesen für die zu betrachtenden Problemfelder anzusehen sind:

- Bestimmung des Ausmaßes des Gefährdungspotenzials in einer verlässlichen Bandbreite.
- Untersuchung, ob es unterschiedlich gefährdete Unternehmensgruppen gibt und welche das gegebenenfalls sind bzw. durch welche Kriterien sie von weniger gefährdeten abgegrenzt werden können.
- Beschreibung der Hauptwege der Informationsverluste und Charakterisierung der verschiedenen Wege nach dem Grad der Gefährdungswirkung.
- Darstellung vorhandener und genutzter Sicherungsmaßnahmen und Erarbeitung von Empfehlungen zur Gestaltung der Informationssicherung in Unternehmen.

Diese vier Fragestellungen sollten durch eine breit angelegte empirische Untersuchung aufgeklärt werden und die Befunde mit den bisher vorhandenen Erkenntnissen und Befunden verknüpft werden. Da es noch keine hinreichenden Erkenntnisse über die Sachverhalte gibt, kann es auch keine Hypothesen im Sinne der empirisch-statistischen Hypothesenüberprüfung geben, sondern nur Betrachtungsfelder, in denen nach Vorfällen, Zusammenhängen und Strukturen gesucht wird.

Zu diesen vier Fragestellungen haben sich folgende Hauptergebnisse herausarbeiten lassen, die das Fazit des nachfolgenden Gutachtens hier zusammengefasst vorwegnehmen:

- Das **Gefährdungspotenzial** durch „unfreundlichen Informationsabfluss“ beträgt für Baden-Württemberg 7 Milliarden € und für Deutschland 50 Milliarden €. Es handelt sich dabei um Hochrechnungen auf der Basis unserer Stichprobe, die eine Standardabweichung von  $\sigma = 0,2$  Milliarden € aufweist. Das bedeutet, dass die tatsächlichen Werte um 0,4 bis 0,6 Milliarden € abweichen können.
- Es gibt **unterschiedlich gefährdete Gruppen von Unternehmen**: Kleine Unternehmen sind auf Grund schwächerer Sicherungsmaßnahmen, auf die z. T. aus Kostengründen verzichtet wird, stärker gefährdet. Ein anderes Kriterium der Unterscheidung von Gefährdungsgruppen bildet die Art und Entstehung von Wettbewerbsvorteilen; hier gibt es Vorteile wie den Mitarbeiterstamm oder die Unternehmenskultur, die kaum imitierbar und damit weniger gefährdet sind als neue Produkte oder Verfahren.
- Die **Hauptwege von Informationsverlusten** sind Konkurrenzspionage, ungetreue oder schlampige Kooperationspartner und ungetreue Mitarbeiter; nachweisbare offensichtliche Gefährdung durch ausländische Nachrichtendienste ist gering, aber hinter den entdeckten Informationsverlusten durch Mitarbeiter oder Unbekannte könnte eine Dunkelziffer dieser Dienste verborgen sein, wie es bei den Voruntersuchungen in Einzelfällen sichtbar wurde.
- Die vorhandenen **Sicherheitsmaßnahmen** sind äußerst differenziert, auch nach der Unternehmensgröße. Große Unternehmen haben fast alle umfassende und ausdifferenzierte Sicherheitssysteme und arbeiten mit den Sicherheitsorganen zusammen. Bei kleinen Unternehmen fehlt es oft schon am Sicherheitsbewusstsein und an der Kenntnis über die

Möglichkeiten des Selbstschutzes sowie der Kooperation mit den Sicherheitsorganen. Hier wird verstärkte Aufklärung der Unternehmen empfohlen.

Zielrichtung ist dabei vor allem auch zu klären, ob es für die für die Sicherheit verantwortlichen öffentlichen Stellen spezifischen Handlungsbedarf und unternehmens(gruppen)-spezifische Handlungsmöglichkeiten gibt, wobei sowohl das Problem der Aufklärung nachrichtendienstlicher Aktivitäten gegen die Unternehmen als auch die Bewusstmachung des Informationsproblems als auch die Darstellung von Sicherungsmöglichkeiten einbezogen sind.

Die Vorgehensweise bestand in einer Bearbeitung von neun Schadensfällen als Ausgangspunkt für die Formulierung von umfassenden Fragen für die eigentliche Untersuchung; die Fälle wurden zuerst anhand der Aktenlage analysiert und dann in den Firmen Interviews über den Ablauf der Schadensfälle sowie Hintergründe und Folgerungen geführt. Diese durch eine Datenanalyse vorbereitete Interviewaktion war der „Pretest“ für die Fragebogenaktion selbst. Das Bild, das sich dabei in einer sehr heterogenen und vielschichtigen Weise ergab, ermöglichte die Gestaltung eines umfangreichen Fragebogens, in dem alle relevanten Problemaspekte abgebildet wurden; die Antworten der Firmen zeigten auch bei der Ermöglichung von ergänzenden Antworten keine wesentlichen zusätzlichen Aspekte auf; häufig wurden unscharfe quantitative Angaben qualitativ unterlegt oder Details erläutert. Die Auswertung erfolgte sowohl qualitativ als auch quantitativ, letzteres vor allem auch durch Ermittlung von Korrelationen zwischen einzelnen Fragebereichen.

## 2 Begriffliche Grundlagen und theoretisches Grundverständnis

Sicherheit von Informationen oder Daten hat in der betriebswirtschaftlichen Literatur sehr unterschiedliche Bedeutungen:

- In der allgemeinen und vor allem auch entscheidungstheoretisch geprägten Sicht bezieht sich Sicherheit oder die verschiedenen Ausprägungen des Fehlens von Sicherheit auf den Inhalt von Entscheidungen bzw. die Auswirkungen der damit verbundenen Handlungen; Sicherheit bedeutet insoweit, die Auswirkungen des Handelns genau und zuverlässig zu kennen. Die verschiedenen Ausprägungen des Fehlens von Sicherheit heißen Risiko, Unsicherheit, Rationale Indeterminiertheit und Ignoranz<sup>5</sup>. Ihnen kann mit verschiedenen Entscheidungsregeln begegnet werden. Diese Art von Sicherheit wird mit „certainty“ übersetzt.
- In einer engeren informationstheoretischen Sichtweise bedeutet Sicherheit von Informationen oder Sicherheit von Daten die Unverletzbarkeit von Datenbeständen und Datenflüssen, wobei die vier Aspekte
  - Vertraulichkeit (Schutz vor unbefugter Kenntnisnahme)
  - Integrität der Daten (Schutz vor Falsifizierung)
  - Authentizität (Richtigkeit des Senders)
  - Zugänglichkeit (auf die Daten muss jederzeit und schnell zurückgegriffen werden können)verschiedene Ausprägungen des Fehlens von Sicherheit darstellen, denen auf unterschiedliche Weise begegnet werden kann und/oder muss. Diese Datensicherheit wird mit „certainty“ und/oder mit „validity“ übersetzt.
- In einer sicherheitstechnischen oder -politischen Sicht bedeutet Sicherheit die Unversehrtheit von Leib, Leben und Vermögen des jeweils betrachteten Subjekts; Quellen des Fehlens von Sicherheit können ebenso natürliche Ereignisse wie auch das zufällige oder vorsätzlich schädigende Handeln von Menschen sein. Unternehmensbezogen geht es dabei vor allem um die Sicherung der materiellen Ressourcen der Unternehmung, weniger um Arbeits- und Unfallschutz und auch erst seit neuestem um die Sicherheit der Informationen. Hier ist die Übersetzung „security“.
- In finanzwirtschaftlicher Sicht, insbesondere bei der Kreditgewährung und anderen Finanzgeschäften, werden mit Sicherheit bzw. dem häufiger verwendeten Plural Sicherheiten Instrumente bezeichnet, die beim Eintritt eines Ausfallrisikos eine anderweitige Schadloshaltung des Kreditgebers gewährleisten. Dieses können Güter sein, die dann als dingliche Sicherheit bezeichnet werden, oder Verpflichtungen von Personen, sei es der Kreditnehmer selber oder eine andere Person z.B. durch eine Bürgschaft, was als persönliche

---

<sup>5</sup> Kahle, E., Betriebliche Entscheidungen, 6. Auflage München – Wien 2001, S. 116

Sicherheit bezeichnet wird. Es wird also nicht auf die Beziehung zwischen Information und Handlungswirkung, sondern auf die Vermeidung einer negativen finanziellen Wirkung des Risikos abgestellt, was auch als eine Art Versicherung oder Garantie anzusehen ist. Die dinglichen Sicherheiten, welche Verfügungsrechte oder die Begrenzung von Verfügungsrechten zum Inhalt haben, werden als „securities“ bezeichnet und, soweit sie verbrieft sind, auch als Wertpapiere gehandelt.

Aus den unterschiedlichen Begriffsabgrenzungen und –inhalten resultieren unterschiedliche Problemumfänge und Problemzugänge in den verschiedenen Bereichen; für eine gesamthafte Problemlösung sind alle vier Sichtweisen auf geeignete Weise einzubeziehen. Daraus ergeben sich sowohl für das zu verwendende Sicherheitskonzept als auch für die in dieses Konzept einzubeziehenden Begriffe des Schadens, des Risikos und des Wissens – der thematisch angelegte Begriff des „Know how“ greift eventuell etwas kurz; weil es auch um „Know what“ und „Know who“ geht – einige grundlegende Überlegungen. Aus einer übergreifenden Zusammenfassung der vorgenannten Sicherheitsbegriffe ergibt sich der Arbeitsbegriff für ein Sicherheitskonzept:

**Sicherheit** ist ein Zustand für ein Unternehmen, in dem alle notwendigen Daten für die Planung zukünftiger Handlungen vorhanden sind und in dem keine Beeinträchtigungen der geplanten Ergebnisse zu erwarten ist.

Dieser Zustand liegt in vollem Umfang nie vor, er kann durch unterschiedliche Ereignisse und Prozesse beeinträchtigt werden, was zu unterschiedlichen Arten der „Nicht-Sicherheit“ wie Unsicherheit, Risiko, Rationale Indeterminiertheit usw. führt. Wenn „Nicht-Sicherheit“ der „normale“ Zustand ist, dann sind im Regelfall Abweichungen von den geplanten Ergebnissen zu erwarten. Statistisch gesehen sind Abweichungen zum Guten wie zum Schlechten (nach oben und unten) gleich zu bewerten<sup>6</sup>, ökonomisch sind aber nur Abweichungen zum Schlechten negativ zu beurteilen. Als Risiko wird also nicht das Maß der Abweichung insgesamt – wie etwa die Standardabweichung – sondern das Maß der Abweichung zum Schlechten verwendet. Dabei wird der Umfang der Abweichung vom geplanten Ergebnis als Schaden bezeichnet; dieser Schadensbegriff ist im Gegensatz zum üblichen eher statischen Begriff, bei dem es um die Minderung eines Bestandes oder einen Vorfall geht, dynamisch zu interpretieren<sup>7</sup>, weil der Schaden die gesamte Wirkungskette einer verursachenden Einflussgröße abbildet. Der Schaden wird dabei über die Zeit akkumuliert und in den jeweiligen Zielgrößen, vor allem auch in Geldeinheiten bewertet. Daraus wird folgender Arbeitsbegriff abgeleitet:

**Schaden** ist die bewertete Abweichung vom geplanten Ergebnis, die durch ein Ereignis oder einen Prozess ausgelöst wird.

---

<sup>6</sup> vgl. Bamberg, G. - Coenenberg, A.G., Betriebswirtschaftliche Entscheidungslehre, 7. Auflage, München 1992, S. 66 - 98

<sup>7</sup> zum Begriff der Dynamik vgl. Schneider, E., Einführung in die Wirtschaftstheorie, Band 2, 11. Auflage, Tübingen 1967, , S. 265 ff...; zu einem anders definierten dynamischen Risikokonzept vgl. Sitt, A., Entwicklung ..., a.a.O.

Die Verbindung zwischen diesem dynamischen und dem statischen Schadensbegriff wird dadurch hergestellt, dass das geplante Ergebnis häufig in Form von Beständen an Rechten und Gütern beschrieben wird, so dass dann eine komparativ-statische Betrachtung<sup>8</sup> stattfindet, die aber zur Erklärung der jeweiligen Zustände und der Schadensentwicklung die dynamische Sichtweise benötigt.

Um beispielsweise den Schutz vor Beeinträchtigung von Rechten und Gütern im Sinne von „Security Management“ leisten zu können, werden Informationen benötigt, die sich auf die Rechte und Güter selbst beziehen, d.h. man muss überhaupt erst einmal wissen, was an Rechten und Gütern vorhanden ist und man muss die Möglichkeiten der Beeinträchtigung kennen, die sich immer wieder – auch gerade durch neue Formen der Informationstechnologie – ändern. Hier wird die Verbindung zwischen dem ersten und dem dritten Bedeutungsinhalt sichtbar: Die Informationen über die Güter und Rechte können unvollständig oder falsch sein oder der Entscheidungsträger ist nicht in der Lage, die Informationen sachgerecht zu verarbeiten. Das bedeutet, dass eine Bestandsaufnahme der Rechte und Informationen zu den wesentlichen Voraussetzungen der Sicherheit im Sinne von „security“ gehört, wobei die Formen der Informationserfassung und –verarbeitung<sup>9</sup> und die Möglichkeiten ihrer Beeinflussung durch Dritte – hier kommt der zweite Bedeutungsinhalt zum Tragen - , aber auch die mangelnde Durchdringung von Informationsstrukturen durch den Entscheidungsträger besonders bedeutsam sind. Das bedeutet aber auch, dass immer wieder von neuem die Frage nach der Vollständigkeit der vorliegenden Informationen und nach ihrer Relevanz für die Entscheidungen und für die Sicherheit der Güter und der Prozesse ihrer Verarbeitung zu stellen ist.

Die verschiedenen Ursachen der Unvollkommenheit von Informationen werden mit unterschiedlichen Maßnahmen bearbeitet<sup>10</sup>. Das Fehlen von Informationen kann oft anhand von Strukturbrüchen oder von Lücken in einer Darstellung erkannt werden; schwieriger ist das Fehlen „flächiger“ Informationen zu bemerken, weil etwas, von dem man gar nichts weiß, auch nicht als fehlend bemerkt wird: „Der Beobachter sieht nicht, was er nicht sieht“<sup>11</sup>. Im Reden über die Sachverhalte wird dann aber oft deutlich, dass Informationen fehlen. Ähnliches gilt für falsche Informationen: So lange nur eine Information zu einem Sachverhalt vorliegt und diese falsch ist, lässt sich das nur schwer feststellen; wenn aber mehrere, sich eventuell auf unterschiedliche Aspekte eines Sachverhalts beziehende Informationen vorliegen, dann lassen sich aus Widersprüchen zwischen den Informationen möglicherweise falsche und richtige Informationen differenzieren, wenn nicht „Informationsunterdrückungsmaßnahmen“ wie die laterale Inhibition<sup>12</sup> Platz greifen. Eine solche Einbeziehung unterschiedlicher Information ist im allgemeinen nur durch Kommunikation möglich. Die Regeln und Maßnahmen, die bei einem zufallsgesteuerten Fehlen von Sicherheit empfohlen werden<sup>13</sup>, sind für das Problem der Informationsverluste weniger relevant; sie treffen vor allem für die

---

<sup>8</sup> vgl. Schams, E., Komparative Statik, in: Zeitschrift für Nationalökonomie Band 2, 1931, S. 27 ff.

<sup>9</sup> Kahle, E., Betriebliche ..., a.a.O., S.63 ff.

<sup>10</sup> ders., a.a.O., S. 123 ff.

<sup>11</sup> von Foerster, H., Wissen und Gewissen. Frankfurt 1993, S. 28 und 132

<sup>12</sup> Kahle, E., Betriebswirtschaftliches Problemlösungsverhalten, Wiesbaden 1973, S. 30 und die dort angegebene Literatur

<sup>13</sup> Kahle, E., Betriebliche Entscheidungen..., a.a.O., S. 100ff.

informationstechnische Datensicherung zu. Bedeutsamer ist auf Grund des Mithandelns anderer bei diesem Informationsverlust als theoretischer Ansatz die Spieltheorie<sup>14</sup> oder die Entscheidung bei rationaler Indeterminiertheit als die klassische Form der Analyse wirtschaftlichen Handelns unter Einbeziehung wenigstens eines Mithandelnden anzusehen. Dabei ist neben bestimmten Wettbewerbskonstellationen, die als eine Zwei-Personen-Nullsummen-Spiel- Situation interpretiert werden können, vor allem die Mehr-Personen-Situation mit variablem Spielergebnis einzubeziehen, die Koalitionen und Kooperationen erlaubt und deren Tragfähigkeit zu untersuchen ermöglicht. Mit den Ansätzen dieser Theorie sind die Befunde zu erklären bzw. zu konfrontieren.

Das Verhalten von Menschen in Unternehmen kann jedoch nicht ausschließlich individualpsychologisch beschrieben und erklärt werden, wie es der spieltheoretische Ansatz in seiner Reinform erwarten lässt und wie es auch weit verbreitet angenommen wird<sup>15</sup>. Vielmehr müssen die institutionellen Rahmenbedingungen und die Möglichkeiten der Handlungskoordination explizit berücksichtigt werden. Eine wichtige Frage stellt in diesem Zusammenhang das Phänomen Vertrauen dar, das in der betriebswirtschaftlichen und organisationstheoretischen Literatur erst seit kurzem als institutionelles Phänomen thematisiert wird, während es als Führungsproblem oder als Marketingproblem schon länger gesehen, aber ganz anders behandelt wird. Es spielt in diesem Zusammenhang deshalb eine besondere Rolle, weil Kooperationen sich als eine wichtige Form der Entwicklung von Wettbewerbsvorteilen herausgestellt haben und insoweit Vertrauen als Basis von Kooperation konzeptionell fundiert werden muss.

**Vertrauen** bedeutet – ohne dass es schon eine allgemeinverbindliche Definition gäbe – üblicherweise die Erwartung, dass der Vertrauensempfänger willens und in der Lage ist, eine an ihn gerichtete positive Erwartung auch zu erfüllen. Es ist also nicht allein die Bereitschaft, sondern auch die Befähigung zur Leistungserfüllung zu berücksichtigen und dass es sich immer um eine positive Leistung handelt. Vertrauensempfänger kann sowohl eine – natürliche – Person sein als auch eine Institution; im letzteren Fall spricht man dann explizit vom institutionellen Vertrauen<sup>16</sup> in Unterscheidung vom persönlichen Vertrauen, das im allgemeinen gemeint ist, wenn kein adjektiver Zusatz verwendet wird.

Vertrauen wird als systembestimmendes Merkmal von Netzwerken angesehen<sup>17</sup>, ist aber realtypisch in allen Koordinationsformen der Unternehmung<sup>18</sup> mit vorhanden<sup>19</sup> und darüber hinaus ein sehr stark

---

<sup>14</sup> von Neumann, J. – Morgenstern, O., Spieltheorie und wirtschaftliches Verhalten, Würzburg 1961; Müller-Merbach, H., Operations Research, 3. Auflage München 1973, S. 470 ff. Eine weitergehende Beschreibung der Spieltheorie wird hier nicht gegeben; sie kann der angegebenen Literatur entnommen werden.

<sup>15</sup> Vgl. Picot, A. – Dietl, H. – Franck, H., Organisation – eine ökonomische Perspektive, 3. Auflage Stuttgart 2002, S. 16 f, 95 ff.

<sup>16</sup> Luhmann, N., Vertrauen – Ein Mechanismus der Reduktion sozialer Komplexität, 3. Auflage Stuttgart 1989

<sup>17</sup> Fischer, S., Virtuelle Unternehmen im interkulturellen Austausch – Möglichkeiten und Grenzen von Kooperationen in Netzwerken, Wiesbaden 2001, S. 127 f; 138

<sup>18</sup> zu den Koordinationsformen vgl. Mintzberg, H., The Structuring of Organizations, Englewood Cliffs N.J., 1979 S. 4

<sup>19</sup> Fischer, S., Virtuelle ..., a.a.O., S.140ff.

kulturabhängiges Phänomen<sup>20</sup>. Zum weiteren Zusammenhang von Vertrauen und Koordinationsformen in den Unternehmen, der für die Nutzung der Informationen bzw. für die Anfälligkeit gegen Informationsverluste bedeutsam ist, sei auf weiterführende Literatur verwiesen<sup>21</sup>. Dabei ist vor allem die transaktionskostenmindernde Funktion von Vertrauen zu beachten, die zu einer effizienteren Organisation führt, was bei den Interviews der Voruntersuchung bestätigt wurde.

Als zwei weitere wichtige Ansätze, die für die Interpretation der Befunde bedeutsam sind, haben sich die Ansätze zur Überwindung von Informationsasymmetrien und die Modelle des Wissensmanagements unter besonderer Berücksichtigung der Wissensdiffusion herausgestellt.

**Informationsasymmetrien** bestehen immer dann, wenn die in der allgemeinen Unsicherheitsanalyse als gleichmäßig bzw. zufällig verteilt unterstellten Informationsdefizite systematisch nur auf einer Seite bestehen. Dieser Sachverhalt ist in der neoklassischen Analyse unter der Bezeichnung „principal – agent“- Problem betrachtet worden, bei dem der Auftraggeber (principal) das Verhalten des Auftragnehmers (agent) oder das Ergebnis dieses Verhaltens nicht beobachten kann<sup>22</sup>. Die Informationsasymmetrien können dabei in drei oder auch vier verschiedene Fälle mit verschiedenen Ursachen und Erscheinungsformen unterteilt werden; sie werden im allgemeinen in ihrer englischen Fassung verwendet:

- Hidden Characteristics
- Hidden Actions
- Hidden Informations
- Hidden Intentions

Die verschiedenen Maßnahmen, die vorgeschlagen werden, um negativen Folgen der Informationsasymmetrien zu begegnen, können zum Teil auch genutzt werden, um Informationsverlusten vorzubeugen; sie sollen deshalb unabhängig von ihrer Eignung zur Handhabung bestimmter Asymmetrietypen kurz vorgestellt werden. In allen Fällen geht es darum, opportunistisches Verhalten des Partners – meistens des „agent“ – zu vermeiden. Diese Maßnahmen sind:

---

<sup>20</sup> vgl. Chen, C.C. – Chen, X. – Meindl, J.R., How can Cooperation be Fostered ? The Cultural effects of Individualism – Collectivism, in: Academy of Management Review, vo. 23 no. 2, 1998, S. 291

<sup>21</sup> Kahle, E., Vertrauensbasierte Netzwerke als Chancen für kleine und mittlere Unternehmen, in: Pleitner, H.J., (Hrsg.), Beiträge zu den Rencontres 1998, St. Gallen 1998, S. 535 – 544; ders.; Kooperation und Vertrauen in Organisationen, in: Fischer, A.,(Hrsg.), Arbeit und Bildung im wirtschaftlichen und sozialen Wandel“, Lüneburg 1999, S. 59 –86; ders., Vertrauen als Voraussetzung für bestimmte Formen des Wandels, in: Brauchlin, E. – Pichler, H.J. (Hrsg.), Unternehmer und Unternehmensperspektiven für Klein- und Mittelunternehmen, Berlin – St. Gallen, 2000, S. 535 – 546; ders. Virtuelle Organisationen unter besonderer Berücksichtigung kultureller Barrieren, in: Scholz, CH. (Hrsg.), Systemdenken und Virtualisierung – Unternehmensstrategien zur Vitalisierung und Virtualisierung auf der Grundlage von Systemtheorie und Kybernetik, Berlin 2002, S. 93 - 108

<sup>22</sup> vgl. hierzu und im folgenden Picot, A. et al. a.a.O., S. 96 ff.

- Screening
- Monitoring
- Signalling
- Garantien
- Pfänder/Kautionen
- Verträge
- Reputationsaufbau
- Vertrauen durch Teamwork entwickeln
- Brücken zu opportunistischem Verhalten abbrechen
- Abbrechen der Kommunikation
- Automatische Entscheidungen
- Kleine Schritte gehen
- Professionelle Vermittler einsetzen<sup>23</sup>

**Screening** ist eine Maßnahme des Leistungsempfängers (principal), der sich einen möglichst guten Überblick über die Angebote beschafft, um mögliche Informationsdefizite besser erkennen zu können. Es werden möglichst viele Anbieter in die Betrachtung einbezogen, um auf diese Weise aus einer Vielzahl unterschiedlicher Daten eine Struktur in den Informationen zu erkennen, die es erleichtert, bestimmte Arten oder Aspekte der Informationsasymmetrie im Vorhinein sichtbar zu machen. Unter Sicherheitsaspekten ist dieses eine bekannte und zweckmäßige Vorgehensweise, die als Frühwarnsystem oder als flächendeckende Beobachtung bezeichnet werden kann. Das bedeutet, dass der gesamte relevante Wirklichkeitsausschnitt auf mögliche interessante Beobachtungen untersucht wird, was natürlich mit hohen Transaktionskosten verbunden ist.

**Monitoring** ist ebenfalls eine Maßnahme des Leistungsempfängers, der ein gezieltes Beobachtungssystem für die Leistungsüberwachung einsetzt. Das kann darin bestehen, dass Zwischenberichte verlangt und gegeben werden, dass man zufällig gestreute, unregelmäßige Besuche macht oder auch elektronische Überwachungssysteme einsetzt. Hier liegen die Transaktionskosten bei der Abwicklung der Leistung, während sie beim Screening bei der Geschäftsanbahnung lagen. Beim Monitoring muss auch bezüglich des zu beobachtenden Prozesses relative Klarheit über den Sollablauf herrschen, d.h. der gewünschte Prozess muss in seinem Ablauf hinreichend deutlich beschrieben und von einem Beobachter oder Beobachtungssystem gemessen werden können. Das kann auch für unerwünschte Prozesse oder Handlungen gelten, so dass sich das Monitoring auch auf den Schutz von Objekten oder Personen beziehen kann und dass bestimmte Abläufe und Prozesse dann als „verdächtig“ vorgegeben werden, auf die ein Beobachter reagieren kann.

---

<sup>23</sup> zu den Punkten Verträge und folgende vgl. Dixit, A. K. – Nalebuff, B. J., Thinking Strategically – The competitive Edge in Business, Politics and Everyday Life, New York – London 1993, S. 144 ff.

Um dem Leistungsempfänger die Transaktionskosten des Screening und/oder Monitoring zu ersparen und sich damit als günstiger Leistungsanbieter darzustellen und der Entwicklung einer „adverse selection“<sup>24</sup> oder eines „Market for lemons“<sup>25</sup> vorzubeugen, kann der Anbieter verschiedene Maßnahmen ergreifen die seine Glaubwürdigkeit erhöhen.

Die erste Maßnahme ist das **Signalling**, bei dem Informationen verfügbar gemacht werden, die dem Leistungsempfänger sonst nicht zur Verfügung stehen, d.h. der Anbieter offenbart mehr als er muss. Auch wenn damit die Verlässlichkeit des Informationsgebers nicht garantiert ist, kann man davon ausgehen, dass mehr Daten und Informationen eine bessere Grundlage bieten; wer viel erzählt muss eher bei der Wahrheit bleiben, weil die Wahrscheinlichkeit von Widersprüchen mit wachsender Informationsmenge größer werden. Das gilt vor allem auch für Zahlenangaben, für die es bei großen Zahlenmengen auch mathematisch-statistische Prüfverfahren gibt, die potentielle Verfälschungen erkennen lassen, weil bestimmte systematische Verteilungen in einer verfälschten Zahlenstruktur nicht auftauchen. Durch das Benutzen bestimmter Standards bzw. das freiwillige Bereitstellen von Informationen oder Einsichtsmöglichkeiten erleichtert das Signalling auch im allgemeinen Umgang die Überprüfung sicherheitsrelevanter Prozesse.

Der nächste Schritt, der die Wirkungen der signalisierten Leistung oder Eigenschaft verstärkt, ist die Abgabe von **Garantien**. Diese wirken zwar konkret erst in dem Fall, wenn eine zugesicherte oder erwartete Eigenschaft nicht eingehalten wird, so dass der Leistungsanbieter korrigierend durch Reparatur, Ersatzlieferung oder Ähnliches zu seinen Lasten eingreifen muss, sie hat aber die Signalfunktion, dass der Anbieter von der Qualität seines Angebots so überzeugt ist, dass er mit der Abgabe der Garantie kein wesentliches Risiko einzugehen glaubt. Letztlich erfolgt eine Risikoumkehr, weil der Anbieter das Risiko des Schadens übernimmt; damit macht er seinen Informationsstand über die Qualität seiner Leistung deutlich. Die Informationsasymmetrie wird in ihrer Wirkung teilweise aufgehoben, weil das Risiko vom besser Informierten getragen wird. Garantien haben außer der Signalfunktion auch noch die Wirkung, dass sie den Leistungsempfänger bezüglich des bewerteten Ergebnisses auf ein größeres Sicherheitsniveau versetzen, weil die ökonomische Auswirkung eines zukünftigen schädlichen Ereignisses aufgehoben wird.

Ähnlich sind **Pfänder und Kautionen** zu sehen; sie sind dann einzusetzen, wenn eine Garantie für die Leistung selber schwer möglich ist und das finanzielle Risiko der Leistung stattdessen Gegenstand einer Zusage wird. Der Wirkungszusammenhang ähnelt dem von Garantien, weil nur der ein Pfand geben wird, der sich seiner Sache sicher ist, wenn er das Pfand nicht verlieren will. Es kann natürlich auch sein, dass dem Leistungsanbieter das Pfand nicht viel wert ist oder er mit dem Verlust fest rechnet, so dass man Wert der Leistung und Wert des Pfandes vergleichen muss. Im Regelfall sind aber Pfänder und Kautionen deutliche Signale für zutreffende Informationen. Diese Form der

---

<sup>24</sup> vgl. Picot, A. et al., a.a.O., S. 96f.

<sup>25</sup> Akerlof, G.A., The Market for „Lemons“: Quality Uncertainty and the Market Mechanism, Quarterly Journal of Economics, vol. 89, 1970, S. 488 ff.

Risikoabsicherung ist vor allem für finanzielle Risiken von Bedeutung, bei denen entsprechende „securities“ verpfändet werden, was aber immer mit recht hohen Transaktionskosten verbunden ist.

Eng mit dieser Sicherungsform verknüpft sind **Verträge**, die zum Teil auch hinsichtlich der Garantien, Pfänder oder Kautionen abgeschlossen werden, die aber meistens mehr zum Inhalt haben. Mit einem Vertrag, vor allem in schriftlich fixierter, aber auch in einer anderen im jeweiligen Kontext üblichen Form, bindet sich der Leistungsanbieter an die von ihm angebotene Leistung. Sie wird deshalb im Vertrag im allgemeinen auch in ihren Eigenschaften deutlich beschrieben, so weit das möglich ist. Von einem solchen expliziten „commitment“ ist schwerer herunterzukommen als von allgemeinen Erwartungen (handelsübliche Leistung), weil der Grundsatz „pacta sunt servanda“ im westlichen Kulturkreis mit starken Konnotationen verknüpft ist. Vielfach werden Verträge auch dazu benutzt, die Motivation des Leistungsanbieters zu konformem Verhalten anzuregen, indem die Entlohnung im Vertrag an die erwartungsgerechte Abwicklung gebunden wird. So wird beispielsweise eine gewinnanteilige Entlohnung vereinbart, wenn der „agent“ den Gewinn des „principals“ beeinflussen kann. Die richtige Vertragsgestaltung ist dabei nicht nur ein rechtliches und sprachliches, sondern auch ein kulturelles Problem, wenn man die Grenzen der Kulturen überschreitet.

Während die bisher genannten Instrumente direkt und im Einzelfall eingesetzt werden können, ist der **Aufbau von Reputation** ein eher generelles Instrument und bedarf eines längeren Zeitraums zur Entwicklung. Es ist für alle Typen von Informationsasymmetrien einsetzbar. Reputation bezieht sich ganz allgemein auf die Glaubwürdigkeit der beanspruchten, ggf. signalisierten oder auch nur vermuteten Eigenschaften und Handlungsweisen. Sie kann nur durch wiederholte verlässliche Handlung aufgebaut werden; sie kann teilweise auch durch Referenzen und Zeugnisse über Ausbildungsgänge prognostiziert werden. Das letztere setzt voraus, dass die Ausbildungseinrichtung oder der „Lehrmeister“ eine bestimmte Reputation haben muss, die dann auf die Schüler übertragen wird. Reputation ist eine Art institutionelles Vertrauen, das einer Person oder Institution entgegengebracht wird, ohne dass schon eine persönliche Beziehung zwischen Vertrauensgeber und -empfänger vorliegen muss. Die Reputation des Leistungsanbieters gibt dem potentiellen Leistungsempfänger die Information, dass Andere die Eigenschaften des Reputationsinhabers für gut befunden haben und dass er seine Möglichkeiten zu opportunistischem Handeln nicht genutzt hat. Da dieser Ruf leicht leiden kann, darf der Leistungsempfänger erwarten, dass der Leistungsanbieter auch bei ihm nicht opportunistisch handeln wird, um den Ruf nicht zu verlieren. Für die Gestaltung von Sicherheitsstrukturen ist die Reputation vor allem auf die Verlässlichkeit der Mitarbeiter sowie auf deren Kompetenz zur Handhabung schwieriger Sicherheitssituationen zu beziehen. Dabei ist noch zwischen der Kompetenz, schwierige Situationen erst gar nicht kumulieren zu lassen und geräuschlos zu bereinigen und derjenigen, in Krisensituationen wirkungsvoll handeln zu können, zu unterscheiden. Während man im ersten Fall durch „Unauffälligkeit“ Reputation erwirbt, wird sie im zweiten Fall durch herausragende Aktion sichtbar.

Ähnlich langfristiger Natur ist der Aufbau von **Vertrauen durch Teamwork**. Dieses Teamwork kann zwischen verschiedenen Leistungsanbietern stattfinden, die durch die gemeinsame Aktivität ihre

Eigenschaft als Gruppe verbessern und die durch die soziale Kontrolle der Gruppe den Opportunismus des Individuums eindämmen. Insofern ist das Vertrauen in einen Leistungsanbieter, der als Gruppe sichtbar wird, im allgemeinen größer als in ein Individuum oder in eine Organisation, deren Entscheidungen von einem Individuum getroffen und verantwortet werden. Das Teamwork kann sich aber auch auf die Zusammenarbeit von Leistungsanbieter und -empfänger bei der Leistungserstellung und ggf. im Vorfeld bei der Leistungsdefinition beziehen. Wenn bereits im Vorfeld der Leistungserbringung gemeinsam gearbeitet wird, entsteht möglicherweise Vertrauen, weil man die Arbeits- und Denkweise des Anderen erleben konnte. Beide Fälle sind gerade auch bei Sicherheitsproblemen relevant; die Teamworklösung berücksichtigt, dass einzelne Individuen – gerade im Umgang mit Informationen – ausfallen können, so dass ein Rückgriff auf ein Team mehr Sicherheit gewährleistet als das Vorhandensein eines „Cracks“. Die Zusammenarbeit und das daraus resultierende Vertrauen ist deshalb so wichtig, weil oft ein sehr intensiver persönlicher Kontakt mit einer Vielzahl auch individueller Informationsaustausche erfolgt, der ohne Vertrauen sehr belastend sein würde oder gar nicht stattfände.

In ähnlicher Richtung wirkt die **Vorgehensweise der kleinen Schritte**: Anstatt ein großes Risiko mit einem ganzen Projekt einzugehen, wird die Leistungserbringung in kleinere „Pakete“ aufgeteilt, bei denen das Risiko opportunistischen Verhaltens in absoluter Höhe geringer ist, weil nicht so viel auf dem Spiel steht und zugleich die Folgepakete nicht mehr zugeteilt werden, wenn sich der Leistungsanbieter opportunistisch verhält. Hier kommen spieltheoretische Überlegungen zum Tragen: In einer einmaligen Situation ist das Risiko opportunistischen Verhaltens groß, in einer wiederholten und zeitlich nicht definierten Situation ist es geringer<sup>26</sup>; bei geringeren „Spieleinsätzen“ ist auch die Wahrscheinlichkeit des Opportunismus kleiner. Das Zerlegen eines großen Risikos in mehrere kleine führt bei Unabhängigkeit der Variablen dann auch zu einer Verringerung des Gesamtrisikos.

Da **Abbrechen von Brücken zu opportunistischem Verhalten**, auch „die Schiffe verbrennen“ in Anlehnung an die aus der Geschichte mehrfach bekannte Strategie<sup>27</sup> genannt, soll dem Leistungsempfänger den unbedingten Willen des Leistungsanbieters demonstrieren, sich nicht aus dem Angebot zurückzuziehen. Eigentlich als Zwangsmotivation für den Leistungsanbieter bzw. seine Mitarbeiter gedacht, wirkt es wie eine Garantie, weil Gedeih und Verderb des Anbieters von der Erfüllung abhängen. Diese Maßnahme ist bei Sicherheitsproblemen nicht ganz ohne weitergehende Folgeprobleme; vor allem ist es wichtig, wer die Schiffe verbrennt. Es ist nur hilfreich, wenn der Anbieter es macht; ein Zwang zur Loyalität, indem der Leistungsempfänger die Schiffe des Anbieters verbrennt, wäre kontraproduktiv.

Ähnlich in der Wirkung ist eine endgültige Kommunikation, d.h. der **Abbruch der Kommunikationsverbindung** nach einem letzten Angebot oder einer Zusage. Die Unwiderrufflichkeit einer Aussage bindet zwar den Leistungsanbieter, führt aber auch zu dem Problem, dass nach

---

<sup>26</sup> vgl. Jost, P.J., Theoretische Grundlagen der Spieltheorie in: Jost, P.J., (Hrsg.), Die Spieltheorie in der Betriebswirtschaftslehre, Stuttgart 2001, s. 67 ff.

<sup>27</sup> Dixit, A. K. – Nalebuff, B.J., Thinking ..., a.a.O., S. 152

Abbruch der Kommunikation keine Kommunikation über die Inanspruchnahme der Leistung durch den potentiellen Empfänger stattfindet, es sei denn dafür ständen andere Kommunikationswege zur Verfügung. Diese Maßnahme bietet sich nur in den Fällen an, in denen der Leistungsempfänger klar definiert ist oder eine allgemeine in die Zukunft gerichtete Aussage unbedingt getroffen werden soll.

**Automatische Entscheidungen** signalisieren ebenfalls die unbedingte Bereitschaft des Leistungsanbieters zur sachgerechten Erfüllung und haben damit die gleiche Wirkung wie Garantien. Sie sind aber eher für den Fall negativer Leistung, d.h. für den Fall von Drohungen bei spieltheoretischen Ansätzen wirksam und weniger bei positiver Leistungserbringung. Diese Maßnahme ist bei Sicherheitsproblemen sinnvoll einsetzbar, weil beispielsweise automatische Überwachungs- oder Warnanlagen durch ihre sichtbare Existenz abschreckend wirken, weil sie nicht beeinflussbar sind, es sei denn man unterläuft ihre technischen Möglichkeiten.

Der **Einsatz professioneller Vermittler** oder Repräsentanten ist die letzte der üblichen Maßnahmen zur Eindämmung von Opportunismus oder anderen von der Zielerreichung abweichenden Verhaltens. Der Repräsentant ist an den geäußerten Willen seiner Mandatsgeber gebunden und kann die festgelegte Handlungsrichtung nicht eigenmächtig ändern, wie es der Mandatsgeber selber könnte. Durch diesen Mechanismus schließt sich der Mandatsgeber selber vom abweichenden Verhalten aus. Das ist unter Sicherheitsaspekten besonders bedeutsam, weil Erpressungsversuche oder andere Formen der Beeinflussung in diesem Fall viel weniger leicht anwendbar sind. Schon die Tatsache, dass ein solcher Mandatsträger eingesetzt wird, verringert die Wahrscheinlichkeit der Beeinflussung.

Die verschiedenen Maßnahmen unterscheiden sich in ihrer Eignung zur Lösung von Sicherheitsproblemen einmal durch die Höhe und Verteilung der Transaktionskosten, aber auch durch die situative Angemessenheit. Sie lassen sich aber jeweils gezielt in einzelnen Situationen sinnvoll einsetzen.

Bei der Betrachtung von Informationsdefiziten und Informationsasymmetrien wird ein mehr oder weniger statischer Zustand der Informationsverteilung unterstellt. Es ist aber auch noch die Entwicklung der Informationsbestände und –zustände zu beachten, die unter den Begriffen des Wissensmanagements und der Wissensdiffusion behandelt wird<sup>28</sup>. Dabei sind drei Arten der Wissensentwicklung zu unterscheiden:

- Die integrierte Arbeitsteiligkeit
- Die Wissensdiffusion
- Die gemeinsam Erzeugung neuen Wissens

Bei der integrierten Arbeitsteiligkeit ist das Wissen in einer Organisation auf die einzelnen Individuen verteilt und jeder leistet nach seinem Wissen und seinen Fähigkeiten seinen Beitrag zum

---

<sup>28</sup> vgl. Bouncken, R.B., Organisationale Metakompetenzen, Wiesbaden 2002, Kahle, E., Strategischer Wissenstransfer als Erfolgsfaktor bei KMU, in: Pleitner, H.J. – Weber, W. (Hrsg.), Die KMU im 21. Jahrhundert – Impulse, Aussichten, Konzepte, St. Gallen 2000, S. 459 - 470...

Gesamtergebnis, ohne dass Wissensbestände vom Einen zum Anderen übertragen werden. Erforderlich ist nur das entsprechende „Know who“<sup>29</sup>, um die richtigen Beiträge zu bekommen. Demgegenüber findet bei der Wissensdiffusion eine Übertragung von Informationen statt, die dann wieder zu Wissen bei den Informationsempfängern führt, wobei das Wissen auf Grund seiner Subjektivität auch nach einer treffsicheren Übertragung nicht identisch ist. In vielen Fällen wird es auch bei integrierter Arbeitsteiligkeit zu solcher Diffusion kommen, aber sie ist nicht beabsichtigt und meistens nur partiell. Bei der gemeinsamen Wissenserzeugung werden vor allem neue Verhaltensregeln, Strategien, Interpretationen oder Lösungsmethoden entwickelt, die vorher nicht bekannt waren und die in einem gemeinsamen Prozess entstehen, bei dem die Beiträge der Einzelnen nicht rekonstruierbar sind. Bei realen Wissensprozessen werden oft Elemente von allen drei Typen vorhanden sein, aber der Gesamtprozess lässt sich dann meistens doch als von einem der drei Typen bestimmt charakterisieren. Bei der Erzeugung von Wettbewerbsvorteilen kann jeder der drei Typen vorkommen, es hat aber unterschiedliche Konsequenzen für die Anfälligkeit des Wettbewerbsvorteils gegen Informationsverluste. Am gefährdetsten erscheint die Wissensdiffusion, weil sie leicht „umgelenkt“ werden kann, d.h. ein Unbefugter kann den Strom der Informationen relativ leicht auf sich ziehen, während das gemeinsam erzeugte Wissen meistens nur in der Gemeinschaft nutzbar ist. Dabei bedarf der Begriff des Wissens noch der Klärung:

Auch wenn es bei einem Blick in die jüngste Literatur der Wirtschaftswissenschaften manchmal so scheint, als wäre Wissen deren originäres Erkenntnisobjekt, beschäftigen sich traditionell verschiedene andere Wissenschaften wie Philosophie, Soziologie und Psychologie vorrangig mit dem Thema Wissen<sup>30</sup>. Gilt es eine allgemeine Definition von Wissen herauszuarbeiten, stößt man an Grenzen. Die verschiedenen erkenntnistheoretischen Perspektiven bedingen einen heterogenen Wissensbegriff, der auch in der Betriebswirtschaftslehre anzutreffen ist. In einer kognitionswissenschaftlichen Sicht, die Wissen als die Gesamtheit der subjektiven pfadabhängigen, geistigen Konstruktionen begreift<sup>31</sup> ist menschliches **Wissen** demzufolge abhängig von den Erfahrungen der Vergangenheit und das Ergebnis eines individuellen geistigen Berechnungsvorganges, der von den inneren Zuständen des Subjekts determiniert wird. Wissen unterscheidet sich durch diesen interpretativen Charakter von **Informationen**, die sich aus Daten zusammensetzen, welche das einzelne Individuum persönlich verwerten kann, indem es sie als Grundlage für die Wissensgenerierung verwendet. Somit haben Informationen durch den für den Empfänger relevanten Aussagegehalt eine höhere Ordnung als die Daten, welche die Informationen enthalten<sup>32</sup>. Wissen in diesem Sinne lässt sich im

---

<sup>29</sup> Klages, K., Knowing who- Auswirkungen von Transactive Memory Systems auf und in unterschiedlichen Organisationsformen, Aachen 2003

<sup>30</sup> vgl. van Doren, C., Geschichte des Wissens, Basel 1996

<sup>31</sup> vgl. Varela, F., Ethisches Können, Frankfurt 1994, von Foerster, H., Wissen..., a.a.O., Kahle E., Kognitionswissenschaftliche Grundlagen der Selbstorganisation, Arbeitsbericht 01/95 der Forschungsgruppe Kybernetische Unternehmenssteuerung an der Universität Lüneburg, Lüneburg 1995

<sup>32</sup> vgl. Guldenberg, S., Wissensmanagement und Wissenscontrolling in lernenden Organisationen: ein systemorientierter Ansatz, Wiesbaden 1997, S. 155

Gegensatz zu Informationen eigentlich nicht zwischen Personen transferieren, denn durch die individuellen Deutungsmuster der Personen wird die Information jeweils auf andere Weise als Wissen in die bestehenden mentalen Muster eingeordnet. Gleichwohl kann die gezielte Hingabe von Daten mit intendiertem Informationscharakter Wissensgewinnungsprozesse auslösen, was hier mit dem Begriff des Transfers von Wissen gemeint ist. Dieser Transferbegriff ist vor allem dann berechtigt, wenn der auslösende Akteur die Informationsverarbeitungsmechanismen und Arten der Wissensgenerierung des Anderen abzuschätzen vermag, was eine längere Zusammenarbeit voraussetzt und auch durch den Begriff des "Transactive memory"<sup>33</sup> beschrieben werden kann.

In der Betriebswirtschaftslehre besteht Konsens hinsichtlich bestimmter Differenzierungen des Wissensbegriffs. Große Popularität erlangte die Erkenntnis von Polanyi, dass Menschen mehr wissen, als sie zu sagen vermögen. Beispielhaft führt Polanyi die künstlerischen oder wissenschaftlichen Fähigkeiten eines Genies, den Spürsinn eines Detektivs und die Geschicklichkeiten sportlichen, artistischen oder technischen Ursprungs an. Aufbauend auf dieser Erkenntnis unterscheidet er implizites und explizites Wissen<sup>34</sup>. Implizites Wissen ist nur bedingt dokumentier- und kommunizierbar. Folglich lässt es sich nur bedingt teilen und weitergeben, da es letztlich an Individuen gekoppelt ist<sup>35</sup>, wenn es nicht gemeinsam erworbenes organisationales Wissen darstellt. Das explizite Wissen stellt nach der Explizierung Information bzw. potentielle Information dar.

Darüber hinaus finden sich weitere Differenzierungen von Wissen. Die individuelle Vorstellung der Wirklichkeit findet sich unter Begriffen wie "Know-what"<sup>36</sup> oder der Bezeichnung des Begriffs- oder Faktenwissens, welches das sukzessiv erworbene Wissen repräsentiert<sup>37</sup>. Das "Know-how"<sup>38</sup> dagegen beantwortet die Frage nach dem "Wie" und erklärt, wie Probleme gelöst werden können. Dieser Sachverhalt findet sich auch unter den Begriffen Prozess-, Handlungs- oder Auskunftswissen. Know-how und Know-what umfassen implizite und explizite Facetten. Implizite Facetten des Know-what betreffen dann die Wert- und Glaubensvorstellungen von Menschen. Die nicht vergegenwärtigten oder nicht artikulierten Aspekte von Kommunikationsprozessen und anderen Abläufen dagegen repräsentiert eher das implizite Know-how.

Wichtig für Unternehmen ist die Unterscheidung zwischen individuellen und kollektiven Wissensarten, wobei kollektives Wissen mehr ist als die Summe des Wissens der Einzelnen, vor allem dann, wenn es gemeinsam erarbeitet ist. Kollektives Wissen findet sich im Kontext der Unternehmen häufig unter dem Terminus organisationales Wissen, welches die Gesamtheit des für die Mitarbeiter einer

---

<sup>33</sup> vgl. Brauner, E. – Becker, A., Controlling als transaktives Wissenssystem, Beitrag zur Tagung der Kommission Wissenschaftstheorie in Berlin, 2000; Klages, K., Knowing who-..., a.a.o.

<sup>34</sup> Polanyi, M., The Tacit Dimension, London 1966, S. 14

<sup>35</sup> Rebhäuser, J. – Krcmar, H., Wissensmanagement in Unternehmen, in: Schreyögg, G.C.P. (Hrsg.), Wissensmanagement, Berlin- New York 1996, S.6

<sup>36</sup> Nonaka, I. – Takeuchi, K., The Knowledge Creating Company, New York 1995, S. 18f., 72 f.

<sup>37</sup> Sackmann, S., Culture and Sub-Cultures: An Analysis of Organizational Knowledge, in: Administrative Science Quarterly, 32 (1) 1992, S. 142

<sup>38</sup> Nonaka, I. – Takeuchi, K., The Knowledge ..., a.a.O., S. 18f.

Organisation zugänglichen bzw. geteilten Wissens darstellt<sup>39</sup>. Darunter werden neben anderen Wissensbeständen der "Know-how" und der "Know-what" –Ebene auch die Basisannahmen, wie sie sich in der Unternehmenskultur niederschlagen, subsumiert. Diese legen fest und kanalisieren, was als Wissen für die Organisation angesehen wird<sup>40</sup> und stellen somit eine Form von Wahrheitstheorie für die Unternehmen dar<sup>41</sup>. Neben solchem eher impliziten organisatorischen Wissen zählen zum organisationalen Wissen auch die kodifizierten Wissensbestände wie Akten, Datenbanken, Berichte, Lizenzen, Patente usw.

Die hohe Wettbewerbsrelevanz von Wissen ergibt sich nicht so sehr aus der Existenz von organisatorischem Wissen, sondern vielmehr aus der Fähigkeit neues Wissen zu entwickeln. Diese wird häufig mit dem Begriff Metawissen bezeichnet oder als Lernfähigkeit der Unternehmung begriffen. Neben den individuellen Voraussetzungen des organisatorischen Lernens<sup>42</sup> ist mit dem organisatorischen Lernen oder Metawissen ein so genanntes strategisches Wissen verbunden. Dieses gibt Auskunft über die Art, den Ort und die Verwendungsmöglichkeiten von Wissen im Unternehmen<sup>43</sup>, die sich zum Teil auch als "Know who" bezeichnen ließe, bei dem ein Individuum weiß, wer etwas weiß oder als „Know where“ wenn es die Struktur der Verteilung dieses Wissens kennt.

Wenn es um die Verbesserung der Wettbewerbssituation geht, die auch darin bestehen kann, eine erwartete Verschlechterung abzuwehren, dann ist über den Bestand einer Wissensbasis hinaus vor allem die Entwicklung bzw. der Erwerb von Wissen entscheidend. Mit dieser Thematik beschäftigen sich viele verschiedene Ansätze in der Betriebswirtschaftslehre. Hier wird vor allem auf das Modell von Nonaka et al. zurückgegriffen, da es am deutlichsten zwischen implizitem und explizitem Wissen unterscheidet.

Nonaka et al. sehen die Grundlage für die Entstehung von neuem Wissen in der Konversion von implizitem zu explizitem Wissen und vice versa und gelangen so zu vier Mechanismen: Sozialisation, Externalisation, Internalisation und Kombination<sup>44</sup>. Werden jeweils explizite Wissensbestandteile wie Technologien, Berichte usw. in Verbindung gebracht, bezeichnen Nonaka et al. dies mit Kombination. Für den Vorgang der Explikation oder Artikulation von implizitem Wissen und dessen Reflexion verwenden sie die Bezeichnung Externalisation. Der Prozess der Internalisierung beschreibt den Vorgang, bei dem explizite Wissensbestandteile (geschriebenes oder dokumentiertes Wissen wie

---

<sup>39</sup> Pautzke, G., Die Evolution der organisationalen Wissensbasis: Bausteine einer Theorie des organisationalen Lernens, Herrsching 1989

<sup>40</sup> Kahle, E., Kognitionswissenschaftliche ..., a.a.O.

<sup>41</sup> Schreyögg, G.C.P., Organisationales Lernen und neues Wissen: Einige Kommentare und einige Antworten zum Wissenmanagement aus wissenschaftstheoretischer Sicht, in: Kommission Wissenschaftstheorie im Verband der Hochschullehrer für Betriebswirtschaft (Hrsg.), Innovation in der Betriebswirtschaftslehre, Wiesbaden 1998, S. 194

<sup>42</sup> vgl. Stotz, M., Organisationale Lernprozesse, Wiesbaden 1999

<sup>43</sup> von Krogh, G., Anhaltende Wettbewerbsvorteile durch Wissensmanagement, In: Die Unternehmung, 49 (6), 1995, S.422

<sup>44</sup> Nonaka, I. – Boisjere, R. – Borucki, C.C. – Konno, N., Organizational Knowledge Creation Theory: A First Comprehensive Test, in: International Business Review 3(4), 1994, S. 339f.

Unternehmensgrundsätze) von Individuen aufgenommen, interpretiert und mehr oder weniger unbewusst gelebt werden. Indem implizites Wissen mit explizitem kombiniert wird, können neue Wissensbestände entstehen. Dieser Vorgang - angeregt typischerweise durch Beobachtung, Imitation und gemeinsame Übung - wird Sozialisation benannt.

In diesem Kontext wird davon ausgegangen, dass die Konversion des expliziten und impliziten Wissens jeweils zwischen Individuen erfolgt, so dass die vier Ausprägungen den Raum der Möglichkeiten erschöpfen; so wird z.B. bei der Sozialisation davon ausgegangen, dass das eine Individuum vom anderen etwas übernimmt. Es könnte stattdessen aber auch von beiden gemeinsam geübt werden; es ist zu hinterfragen, ob bei dem gemeinsamen Erarbeiten von impliziten oder expliziten Wissensinhalten in Organisationen oder auch bei der beiderseitigen gleichberechtigten Vereinbarung über die Gültigkeit von Wissen oder Regeln, die angegebene Verteilung ausreicht oder ob weitere Formen definiert und beschrieben werden müssen. Die verschiedenen Formen der Wissenserzeugung und Wissensdiffusion haben für die Interpretation von Informationsverlusten große Bedeutung.

### **3 Methodische Grundlagen und Basisdaten der Untersuchung**

Der explorative Charakter der Untersuchung erforderte eine breite Auswahl an Untersuchungsteilnehmern und ein offenes Untersuchungsdesign. Bei der ersten der vier leitenden Fragestellungen liegt die Ermittlung quantitativer Aussagen über die Größenordnung der Probleme, für die anderen drei (siehe Punkt 1) eine qualitative Abgrenzung von Bedeutungen und Erklärungsmustern im Zentrum. Dabei sollten immer auch andere als die vorgeschlagenen und voruntersuchten Antworten möglich sein. Der Aufbau des Fragebogens erfolgte in drei Schritten:

- Entwicklung eines Leitfadens für die Interviews aus den Unterlagen
- Auswertung der Interviews
- Strukturierung des Fragebogens

#### **3.1 Aufbau der Messinstrumente und Anforderungsprofile zur Auswertung der Schadensfälle**

Vom Auftraggeber wurden dem Auftragnehmer von neun Firmen und Einrichtungen Unterlagen zu Schadensfällen übergeben, die in Tabelle 1 zusammengefasst sind. Es wurden dafür Firmen aus Branchen mit technisch/technologisch relevanter Produktion ausgewählt.

Fall	Auftraggeber/ Nutznießer	Anwerbung/ Anbahnung	Methoden der Aus- spähung	Methoden der Kommuni- kation	Gegenstände der Ausspähung	„Agenten lohn“	Schadenshöhe	Zeit
1	Staat Rumänien	Anw. in Rumänien, Ausreise, Druck auf Angehörige	Filme und Kopien, allgemeine Unterlagen	Telefonat mit Führungs- offizier Brief Funk Pers. Kontakt in vorher vereinbarten Orten Europas	Konstruktions- unterlagen, vor allem aus seinem Arbeitsplatz, benachbarten Bereichen, ganze Entwicklungsvorgänge	Keiner, Reise- kosten, z. T. an seine Führungs- personen weiterge- geben	Im Verfahren nichts geltend gemacht  Millionen DM?	1980 – 1994
2a)	Konkurrenz in Frankreich	Kooperations- vertrag, Mitarbeiterin aus Frankreich	Vermutlich Unter- schlagung von Unterlagen beim Koop.- Partner	Unbekannt	Reinigungssystem	Unbe- kannt	150.000 DM Streitwert	1997 - 2000
2b)	Staat China	Kooperations- angebot: Lehrstuhl in China	Koopera- tionsvertrag für bestimmte Prozesse	Chinesische Gastwissen- schaftler, eigene Tätigkeit in China	Rohrfertigung für Brennelemente	Professur als Angebot	Nicht abschätz- bar, da kein klarer Informa- tionsabfluss	1997 – 2000
3	Konkurrenz	Abwerbung des Mitarbeiters, Methode nicht klar	Mitnahme vorhandener bzw. kopierter Unterlagen	Für die Anwerbung : unbekannt. Danach als Mitarbeiter der Konkurrenz	Kundenkartei	Unbe- kannt Mehr Gehalt?	Sehr hoch, fast ruinös für Firma	2001
4	Konkurrenz in der Schweiz	Abwerbung bzw. Kündigung und Wechsel	Unberech- tigte Kopien von Dateien	Unbekannt	Einspritzsysteme	Unbe- kannt Mehr Gehalt?	Bei Erfolg sehr hoch, Versuch!	2001
5	Konkurrenz Neugrün- dung durch 2 ehem. Mitarbeiter	Ausgründung durch ehem. Mitarbeiter	Unberech- tigte Kopie von Konstruktion sunterlagen, Preiskonkur- renz	Keine nötig, da ehem. Mitarbeiter selber die Informa- tionen verwenden	Zubehör für Maschinen	Gewinne aus der Konkur- renzun- ternehmung	Mehrere Mio. DM, fast ruinös für die Firma	1996- 2002
6	Vermutlich fremde	Kein direkter Kontakt	Diebstahl von	-	Geheimdaten über Rüstungsprojekte	Unbe- kannt	Direkt: Hardware 100000	1998

Fall	Auftraggeber/ Nutznießer	Anwerbung/ Anbahnung	Methoden der Aus- spähung	Methoden der Kommuni- kation	Gegenstände der Ausspähung	„Agenten lohn“	Schadenshöhe	Zeit
	Staaten		Hardware				DM, indirekt: immens	
7a)	Konkurrenz in Österreich	Abwerbung von Mitarbeitern, Nutzung von Partnerfirmen	Nutzung von Mitarbeiter- wissen, ggf. Kopien von Geheimunter- lagen	-	Fahrzeugbau, Neuentwicklungen	Unbe- kannt Mehr Gehalt?	500 –600.000 DM	Vor 2000
7b)	Konkurrenz in Japan	Firmenbesuch durch japanische Ingenieure	Fotografien von Entwick- lungsprojekt	-	Neuentwicklung von Konkurrenz als Eigenentwicklung ausgegeben	Eigene japa- nische Kräfte	Nicht bemessbar, aber immens	Vor 2000
8	Konkurrenz in Frankreich, USA		Unbekannt, vermutet wegen „technischen Sprungs“		Konkurrent tritt plötzlich mit vergleichsweise leistungsfähigen Produkten auf, Patentverletzung in den USA		Noch nicht messbar, da erst Verdachts- stadium	Vor 2000
9a)	Konkurrenz	Abwerbung von Mitarbeitern	Weitergabe von aktuellen Entwicklungs- daten ehemaliger Kollegen	Persönliche Gespräche	unbekannt		Schadenshöhe nicht festgelegt 80.000 bzw. 40.000 DM Buße	1996- 1999
9b)	Ehem. Mitarbeiter mit aus- ländischem Geheim- dienst?		Diebstahl von Produkten/ Hehlerei				Erheblicher Schaden	1996- 1999

**Tabelle 1: Exemplarische Schadensfälle im Land Baden-Württemberg, Zeitraum 1980-2002**

Vom Auftragnehmer wurde zur gründlichen Auswertung der übergebenen neun Fälle folgendes Anforderungsprofil einer komplexen Fallbeschreibung erstellt. Es umfasst:

- Geschäftsberichte
- Firmenprofile einschließlich Produktpalette
- Vorstands/Geschäftsleitungsprotokolle zur strategischen Planung (u. a. zur Produktion und zum Personal)
- Fluktuationsanalysen
- Konkurrenzunternehmen
- Ex-post-Verdachtsmomente (z. B. bezogen auf Mitarbeiter)
- Signale, durch die die Unternehmen/Einrichtungen aufmerksam wurden
- Organisatorische, personalpolitische und informationspolitische Maßnahmen, die im Nachhinein zur Absicherung ergriffen wurden

Die Beschaffung der erforderlichen Unterlagen durch den Auftraggeber stieß auf Schwierigkeiten, die sich aus der Tatsache der Erstmaligkeit einer derartigen wissenschaftlichen Bearbeitung erklären. Zur Vorbereitung der Interviews erhielt der Auftragnehmer hauptsächlich Firmenprofile einschließlich Produktpalette.

### **3.2 Vorbereitung des Fragebogens durch Interviews mit Geschäftsleitungen betroffener Unternehmen (Pretest)**

Insgesamt wurden elf Interviews geführt. Diese sind Bestandteil des ersten gutachterlichen Berichts vom 10.10.2002, der beim Auftraggeber eingesehen werden kann.

Für den Umfang der Stichprobe wurde eine Zielgröße von wenigstens 300 auswertbaren Antworten angestrebt. Bei einer üblichen Antwortrate bei Fragebögen von etwa 10 % wurden Adressen von ca. 3000 Firmen in Baden-Württemberg benötigt. Die IHK Region Stuttgart hat die Vorbereitung der Auswahl des Adressmaterials der zu befragenden Unternehmen technisch und organisatorisch unterstützt, die Festlegung der qualitativen Faktoren erfolgte durch die aus Angehörigen des Sicherheitsforums Baden-Württemberg und der Universität Lüneburg gebildeten Koordinierungsgruppe. Folgende Umfragekriterien wurden festgelegt:

- In den Suchlauf werden ausschließlich baden-württembergische IHK-Handelsregister-Firmen ab 20 Mitarbeitern einbezogen.
- Es wird Adressmaterial im Umfang von ca. 3000 Firmen angestrebt (Trefferquote 10%). Die Auswahl der Firmen erfolgt aus der baden-württembergischen IHK-Datenbank per Zufallsgenerator.
- Es werden Firmen aus Branchen mit technisch/technologisch relevanter Produktion ausgewählt.

Ausgehend von der Auswertung aller vom Auftraggeber übergebenen Unterlagen wurde für die Interviews folgender **Leitfaden** entwickelt:

### **Rahmendaten:**

Was wird hergestellt (Produktpalette)

Wettbewerbssituation (Zahl, Art und Standort der wichtigsten Konkurrenten)

Zahl der Mitarbeiter,

- davon in der Forschung und Entwicklung
- davon Praktikanten, Diplomanden, Doktoranden

Umsatz

Verflechtung mit anderen (ausländischen) Unternehmen

- Kapital
- Partnerschaften/Kooperationen

### **Im Einzelnen:**

#### **Worin besteht der wichtigste Wettbewerbsvorteil?**

- Technik (Maschinen, Mitarbeiter, ...)
- Produkte (Patente, Gebrauchsmuster, Design,...)
- Prozesse (Verfahren, Arbeitsmethoden,...)
- Kunden (Kundenstamm, Beziehungen, Organisation,...)
- Strategie

#### **Inwieweit ist dieser Wettbewerbsvorteil imitierbar?**

- Ist er formal geschützt? (Patente o. ä.)
- Liegt er in den Köpfen der Beteiligten?
- Liegt er in der Organisationsstruktur?

#### **Welche Konsequenz bezogen auf Umsatz/Bilanzsumme hätte ein Verlust dieses Vorteils?**

#### **Wer ist an der Schaffung/Erhaltung des Wettbewerbsvorteils beteiligt?**

- Geschäftsleitung
- Leitende Mitarbeiter
- Forschungs-/Entwicklungsabteilung
- Andere Abteilungen
- Alle Mitarbeiter

### **Wo sind Informationen über den Wettbewerbsvorteil gespeichert?**

- Akten, Zeichnungen,...
- EDV-Dateien
- Nur in den Köpfen der Beteiligten
- In den Fähigkeiten der Beteiligten

### **Wer hat Zugang zu den Informationen?**

#### **Welche Sicherungsmaßnahmen gibt es für die Informationen?**

- Zugangsbeschränkungen (räumlich)
- Zugriffsbeschränkungen (EDV, inhaltlich)
- Sicherheitskopien
- Verteiltes Wissen
- Geheimschutzverfahren/Zusammenarbeit mit Sicherheitsbehörden
- Sicherheitskonzept
- Sicherheitsaspekte bei Personalauswahl/Personalmanagement

#### **Wer könnte an Informationen über den Wettbewerbsvorteil interessiert sein?**

- Gab es weitere Fälle der Ausspähung/Abschöpfung?

#### **Gab es bei den aufgetretenen Fällen vorher Anzeichen für Informationsabflüsse?**

- übermäßiges Kopieren
- verlegte, verstellte Akten
- Anwesenheiten von fremden Personen (auf dem Betriebsgelände, in der Nähe,...)
- Anwesenheit von Betriebsangehörigen zu ungewöhnlichen Zeiten oder an ungewöhnlichen Orten
- Auftauchen von Teilinformation bei Wettbewerbern
- ...

#### **Gab es bei den aufgetretenen Fällen vorher Anzeichen für abweichendes Verhalten von Betriebsangehörigen?**

- Unzufriedenheit
- Engagement nach länger geäußelter Unzufriedenheit
- Plötzlicher „Reichtum“
- Konspiratives Verhalten
- ...

#### **Wie sind die an der Schaffung/Erhaltung des Wettbewerbsvorteils Beteiligten an das Unternehmen gebunden?**

- Arbeits- oder Werkvertrag

- Beteiligung (Eigentum, Miteigentum)
- Ideelle Beteiligung

Die Grundstruktur des Fragebogens war damit vorgegeben. Die Auswertung der Interviews ergab eine Verbreiterung der Fragestellungen und Problembereiche, die sich in der nachfolgenden Problemstruktur abbilden lassen.

Der tatsächliche oder potentielle Verlust von Wissen bzw. Wissensvorsprüngen durch aktive Tätigkeit Dritter und der daraus resultierenden Wettbewerbsvorteile lässt sich nach den vorliegenden Fällen in drei Fallgruppen aufteilen, die zum Teil allerdings auch vermischt auftreten können:

### **Fallgruppe 1**

Tätigwerden einer ausländischen staatlichen (i. w. S.) Einrichtung zur Informationsbeschaffung

### **Fallgruppe 2**

Tätigwerden eines in- oder ausländischen Konkurrenzunternehmens zur Informationsbeschaffung, unterteilbar in 2a) ausländische Konkurrenz und 2b) inländische Konkurrenz, was bei der starken Globalisierung aber nur immer eine Momentaufnahme sein kann.

### **Fallgruppe 3**

Tätigwerden eines Mitarbeiters oder Kooperationspartners zur Informationsweitergabe und -beschaffung

Die Zuordnung zu den Fallgruppen richtet sich nach dem Initiativgeber der Tätigkeit, in einigen Fällen lässt sich das nicht mehr ganz eindeutig erkennen. Bei der Umsetzung der Initiative werden auch in den Fallgruppen 1 und 2 häufig Mitarbeiter oder Kooperationspartner benutzt oder abgeschöpft. Vor allem bei Verdachtsfällen der Fallgruppe 3 könnte eine der anderen Fallgruppen verdeckt im Hintergrund stehen. Die Zuordnung ist beispielsweise im Fall 6 (siehe Tabelle 1) überhaupt nicht klar, weil kein Täter ermittelt wurde; die professionelle Art und Weise, in der die Festplatte ausgebaut und entwendet wurde, lässt auf eine Zuordnung zur Fallgruppe 1 schließen; hier wurde die Datei gezielt entwendet, nicht die Hardware.

Die wirtschaftliche Bedeutung ist in allen drei Fallgruppen sehr hoch, zumindest was das Verlustpotenzial ausmacht; in wenigstens einem der Fälle hat der Informationsverlust zum Ruin geführt. Die Schadenssummen waren nur sehr grob abschätzbar, waren aber des öfteren im Bereich von Hunderttausenden Euro bis hin zu Millionenbeträgen angesiedelt. Für eine genauere Einschätzung bedarf es einer größeren Fallzahl, die durch die geplante Fragebogenaktion erreicht werden soll.

Dabei sollte nicht übersehen werden, dass zwar nach dem Schadenspotenzial im Einzelfall sehr hohe Risiken bestehen, dass aber nach der WIK-Sicherheits-Enquête 2002/2003, SecuMedia Verlag,

Ingelheim<sup>45</sup> nur 6% aller kriminellen Schadensfälle in Unternehmen Konkurrenzspionage betreffen, nur 12% Computersabotage, dagegen 45% Diebstahl, 35% andere Mitarbeiterdelikte und 27% Betrugsfälle auftreten. Jedoch ist bei Diebstahl – so weit es sich um ein Einzeldelikt handelt – schon wegen der physischen Begrenzung des Gutes – der Schaden eher klein bis mittelmäßig, während die hier betrachteten Fälle, wenn die gegen die Unternehmung gerichteten Maßnahmen „erfolgreich“ waren, immer zu hohen Schäden führen.

Für die weitere Analyse muss innerhalb der Fallgruppen tiefer differenziert werden. Dabei werden drei zentrale Probleme begrifflich umfassend und in diesem Feld neuartig definiert, nämlich:

- Wettbewerbsvorteil
- Gefährdungspotenzial
- Unfreundlicher Informationsabfluss
- Schadensbearbeitung

#### **Definition „Wettbewerbsvorteil“**

Unter Wettbewerbsvorteil werden hier nutzbare Potenziale verstanden, die aus dem Einsatz von Wissen, Arbeit und/oder Investitionsmitteln (Kapital) entstanden sind und in Zukunft wirtschaftlich genutzt werden können. Dazu ist notwendig, dass sie von Dritten nicht ohne weiteres genutzt werden können, d.h. auch keine freien oder öffentlichen Güter sind.

#### **Definition „Gefährdungspotenzial“**

Die als Potenzial nutzbaren Wettbewerbsvorteile, die sich eine Firma geschaffen hat und die grundsätzlich von einer anderen Unternehmung im Wettbewerb verwendet werden könnten, stellen das Gefährdungspotenzial dieser Firma dar.

#### **Definition „Unfreundlicher Informationsabfluss“**

Unfreundlicher Informationsabfluss wird als Oberbegriff für alle Verluste an Informationen benutzt, die nicht mit dem Einverständnis der Unternehmung erfolgt sind. Das schließt die Ausspähung ebenso ein wie Nachlässigkeit in Wort und Schrift, die von Dritten genutzt wird.

#### **Definition „Schadensbearbeitung“**

Schadensbearbeitung umfasst alle Arten von Reaktionen des Unternehmens auf einen aufgetretenen Fall von Informationsabfluss, d.h. die Klärung was passiert ist, wie es passiert ist und welche Maßnahmen zur Abwehr in Zukunft und zur Risikoverminderung getroffen wurden.

Die tiefere Differenzierung lässt sich auf der Grundlage der vorstehenden Definitionen wie folgt vornehmen und führt zu der nachfolgenden Operationalisierung der Begriffsinhalte:

---

<sup>45</sup> WIK-Informationen, Sonderheft 2003

### **Art und Inhalt des Wettbewerbsvorteils**

- Produkte (neu, überlegen) (Patente, Gebrauchsmuster, Design,...)
- Prozesse (Verfahren, Arbeitsmethoden,...)
- Technik (Maschinenausstattung, Mitarbeiterstamm,...)
- Marktbeziehungen (Kundenstamm, Lieferanten, Kooperationen,...)
- Know how (Forschung, Organisation, Kultur,...)
- Strategie (Produkt-Markt, Personal, Corporate Strategy,...)

### **Imitierbarkeit/Schützbarkeit des Wettbewerbsvorteils**

- Wie entsteht/entstand der Wettbewerbsvorteil?
- Wie dauerhaft ist er (wird er eingeschätzt)?
- Gibt es formale Schutzrechte?
- Sind spezielle Investitionen zu seiner Nutzung erforderlich und gemacht worden?
- Gibt es inhaltliche Schutzmöglichkeiten? (Speicher, Tresore,...)
- Wie ist die Bindung der beteiligten Mitarbeiter /Kooperationspartner?

### **Umfang der tatsächlichen Schutzmaßnahmen**

- Begrenzung des Kreises der Wissensempfänger/-inhaber
- Verteilung des Wissens auf mehrere Köpfe, die nur zusammen das Ergebnis bewirken können
- Zugriffsbeschränkung EDV/Kontrolle?
- Zugangsbeschränkung Betrieb/Betriebsteil/Mitarbeiter
- Überprüfung der Mitarbeiter bei Einstellung
- Regelmäßige Belehrung zur Vertraulichkeit
- Überprüfung von Kooperationspartnern
- Vertragsgestaltung mit Kooperationspartnern
- Patente/Umgehungspatente/Gebrauchsmuster
- Einrichtung eines Sicherheitssystems im Betrieb mit Schulung der Mitarbeiter

### **Kenntnis über Zusammenarbeit mit für die Sicherheit zuständigen Behörden**

- Zuständigkeit für Wirtschaftsspionage/Konkurrenzspionage (Bekannt?)
- Kenntnis über Sicherheitskonzepte/-programme
- Kontakte mit Polizei/LfV
- regelmäßig
- im Schadensfall
- noch gar nicht
- Kontakte mit anderen Sicherheitsinstitutionen
- Beteiligung an öffentlichen Ausschreibungen/Aufträgen

Die den vorgenannten Erkenntnissen zugrunde liegenden Interviews wurden, wie in Abbildung 1 dargestellt, über das gesamte Land Baden-Württemberg verteilt durchgeführt:

### Verwaltungseinteilung des Landes Baden-Württemberg



Statistisches Landesamt Baden-Württemberg

**Abbildung 1: Nachweis der Verteilung der interviewten Unternehmen über die gesamte Region Baden-Württemberg zur Erfassung gegebenenfalls vorhandener regionaler Besonderheiten**

### 3.3 Ergebnisse der Auswertung der Interviews und Gespräche

Zu den einzelnen unter Punkt 3.2 genannten Aspekten ergaben sich folgende Ergebnisse:

#### **Art und Inhalt des Wettbewerbsvorteils**

- Überlegene neue Produkte schützen sich zum Teil selbst durch ihre Neuheit, weil der Nachbau einfach Zeit kostet. Es wurde empfohlen, lieber viele kleine Schritte zu gehen, um so der Konkurrenz immer wieder voraus zu sein, als einen großen Wurf zu probieren, der länger halten soll.
- Der Schutz von Produkten durch Patente ist bei wichtigen komplizierten Produkten weniger durch ein direktes Patent auf die Idee, als vielmehr durch Umgehungspatente (Patente auf die möglichen Umgehungen der Produktidee) zu leisten.
- Patente sind vergleichsweise teuer.
- Gebrauchsmuster geben nur Schutz im Inland, ein ausländischer Konkurrent ist damit nicht abzuwehren.
- Das Nachahmen von Produkten (reverse engineering) ist zwar grundsätzlich möglich, aber ohne Kenntnis von Verfahren und Arbeitsmethoden doch sehr erschwert; diese sind daher geheim zu halten, auch wenn das Produkt weitergegeben wird.
- Spezifische Investitionen (in Maschinen und Personal) erschweren es der Konkurrenz, sinnvoll nachzuahmen; ohne einen gewissen Mindestmarkt lohnen diese spezifischen Investitionen nicht.
- Die Verfügbarkeit über Kundendaten kann für die Konkurrenz ein erheblicher Vorteil sein, vor allem, wenn es eine große Zahl ist, die auch regelmäßig angesprochen werden muss.
- Bei sehr kleinen Kundengruppen sind die Beziehungen meistens sehr stabil; die potentiellen Kunden sind überwiegend bekannt.
- Im Verhältnis zwischen universitären Forschungseinrichtungen und Wirtschaftsunternehmen muss bei Kooperationen auf die unterschiedliche Kultur (Veröffentlichung vs. Aneignung) geachtet und müssen klare Absprachen (Verträge) getroffen werden.
- Strategien müssen nur geheim sein, wenn sie nachgeahmt oder unterlaufen werden können.
- Gespeicherte Daten sind elektronischem oder physischem Diebstahl ausgesetzt.

#### **Imitierbarkeit/Schützbarkeit**

- Wettbewerbsvorteile entstehen meistens aus dem Zusammenwirken mehrerer Personen, entweder in einer Unternehmung (Forschungs-/Konstruktionsteam), zwischen Unternehmung und Kunde (Kunde hat Wunsch/Unternehmer setzt um) oder in einem Netzwerk.
- Wettbewerbsvorteile sind grundsätzlich nicht dauerhaft, sie erodieren oder werden durch Imitation abgebaut.
- Formale Schutzrechte sind vor allem grenzüberschreitend sehr schwierig durchzusetzen.
- Formale Schutzrechte sind vergleichsweise teuer.

- Mit den meisten Wettbewerbsvorteilen geht eine spezifische Investition einher. Sie ist einerseits ein Risiko (wenn der Vorteil nicht genutzt werden kann oder verloren geht), sie ist aber auch Schutz vor kleinen Nachahmern (- der Nachahmer muss auch viel investieren).
- Zeichnungen und Berechnungen können zwar eingeschlossen werden, aber es müssen viele damit arbeiten, so dass eine enge Kontrolle den Arbeitsfluss hemmen würde.
- Zeichnungen und Muster müssen den Kunden gezeigt werden; wenn diese mit der Konkurrenz zusammenarbeiten, wird es gefährlich.
- Wenn die Mitarbeiter kein Interesse am Unternehmenserfolg (und sei es die Sicherheit der Arbeitsplätze) haben, ist das Risiko der Informationsweitergabe groß. Diese kann absichtlich oder durch Unachtsamkeit erfolgen.
- Von einer bestimmten Größe der Unternehmung/Gruppe an funktioniert die soziale Kontrolle in diesen Sicherheitsfragen nur noch bedingt.

### **Umfang der tatsächlichen Schutzmaßnahmen**

- Der Kreis der Wissensempfänger/-nutzer kann in einem arbeitsteiligen Produktionsprozess ohne Effizienzverluste kaum wesentlich beschränkt werden.
- Arbeitsteiligkeit (jeder weiß etwas) ist ein häufiges Phänomen.
- Der Zugriff auf EDV-Daten (Zeichnungen, Berechnungen) muss den beteiligten Ingenieuren/Meistern und Sachbearbeitern möglich sein; was möglich wäre und scheinbar fehlt, sind Kontrollen, wer welche Informationen wann und wie lange nutzt.
- Bei den kleinen und mittleren Betrieben ist eine Zugangsbeschränkung für Betriebsangehörige kaum machbar; Außenkontrollen hängen von der räumlichen Situation ab.
- Ein ausgearbeitetes Sicherheitskonzept/-system, in dem die Mitarbeiter auch geschult werden, fand sich in der Mehrzahl der Fälle nicht.
- Eine Überprüfung der Mitarbeiter bei der Einstellung auf sicherheitsrelevante Tatbestände (bisheriger Weg, Lücken,...) fand nirgends statt.
- Vertraulichkeit wird erwartet, aber selten explizit verlangt und abgeprüft.
- Kooperationspartner stellen eine große Gefahrenquelle dar; sie werden nur selten sicherheitsrelevant überprüft und auch im Fortgang der Kooperation meistens nur dilatorisch kontrolliert.
- Verträge mit Kooperationspartnern sind oft nur unzureichend in der Frage von Eigentum an Informationen, Weitergabe und Weiterverwertung von Informationen und der Verantwortung für Fehlverhalten abgeschlossen.
- Manche Firmen schützen ihre Produkte erfolgreich durch Umgehungspatente. Andere haben nur Gebrauchsmuster eintragen lassen, die zu wenig Schutz vor ausländischen Konkurrenten bieten.
- Gegen professionelle Abschöpfung/Diebstahl kann man sich kaum schützen.

### **Kenntnis/Zusammenarbeit mit Sicherheitsbehörden**

- Die Zuständigkeit für Wirtschaftsspionage/Konkurrenzspionage ist kaum bekannt; sie ist auch nicht ganz eindeutig festgelegt.
- Die Sicherheitskonzepte und -programme von LfV (Landesamt für Verfassungsschutz), Polizei, ASW (Arbeitsgemeinschaft für Sicherheit in der Wirtschaft) sind kaum bekannt.
- Kontakte mit den Sicherheitsbehörden lagen im Allgemeinen nur im Schadensfall vor; nur bei sicherheitsrelevanten Aufträgen gab es Zusammenarbeit und Kenntnisse.
- Die Behandlung von Wirtschaftsspionage und Konkurrenzspionage durch die Behörden wurde als eher dilatorisch (aufschiebend) angesehen; hier wurde nach erfolgter Spionagetätigkeit mehr Einsatz erwartet.
- Bei öffentlichen Aufträgen wurde mangelnde Sensibilität der öffentlichen Auftraggeber für das Problem der Konkurrenzspionage gesehen. Die starke Bindung an den niedrigsten Preis bei der Auswahl nach einer Ausschreibung geschieht teilweise unter Nichtbeachtung möglicher Konkurrenzspionage.

### **3.4 Struktur des Fragebogens**

Aus diesen Befunden in den Interviews zu diesen Fragen, wobei Befund sowohl eine inhaltliche Aussage zu dem Sachverhalt als auch das Nichtsagen über bzw. Nichtwissen um ein bestimmtes Problem als auch indirekte Aussagen umfasst, wurden die folgenden **Fragen bzw. Fragenkomplexe** abgeleitet :

#### **1. Wie sieht Ihre Produkt-Markt-Position aus?**

- Massenprodukt in einem Markt mit vielen Konkurrenten
- Massenprodukt in einem Markt mit wenigen Konkurrenten
- Einzel/Kleinserienfertigung in einem Markt mit vielen Konkurrenten
- Einzel/Kleinserienfertigung in einem Markt mit wenigen Konkurrenten
- Produkt in Alleinstellung (Monopol)
- ...

#### **2. Worin besteht Ihr wichtigster Wettbewerbsvorteil? (ggf. mehrere ankreuzen, wenn sie gemeinsam wirken, sonst den vorherrschenden)**

- Überlegene Produkte
- Neue Produkte
- Beherrschung spezifischer Produktionsprozesse/Arbeitsmethoden
- Maschinenausstattung
- Mitarbeiterstamm
- Kundenstamm
- Lieferantenbeziehungen
- Kooperationen/Netzwerke

- Forschungsergebnisse
- Organisatorische Vorteile
- Unternehmenskultur
- Strategie (Produkt-Markt, Corporate, Geschäftseinheit)
- ...

### **3. Wie ist der Wettbewerbsvorteil entstanden?**

- Idee einer Person
- Gemeinsame Idee mehrerer Personen in der Unternehmung
- Gemeinsame Idee mit Kunden
- Entwurf einer oder mehrerer Abteilungen
- Gewachsen aus dauerhafter Zusammenarbeit
- Gewachsen durch ständige Investition mit Innovation
- ...

### **4. Wie dauerhaft/imitierbar/schützbar ist der Wettbewerbsvorteil?**

- - Nicht imitierbar und erodiert nicht
- Imitierbar
- Rekonstruierbar
- Durch Patent geschützt
- Durch Umgehungspatente gesichert
- Durch Gebrauchsmuster geschützt
- Setzt erhebliche spezifische Investitionen voraus
- Nachahmung nützt nichts, da keine Kunden vorhanden
- Der Vorteil liegt in der Organisation
- Der Vorteil liegt in der Kultur
- ...

### **5. Welche Sicherungsmaßnahmen werden vorgenommen?**

- Eingangskontrolle
- Zugangsbeschränkungen für bestimmte Bereiche
- Zugriffsbeschränkungen für Daten (wer für was?)
- Werden Sicherheitskopien hergestellt?
- Ist Wissen verteilt, so dass nicht einer alles hat?
- Gibt es ein Geheimschutzverfahren?
- Gibt es ein Sicherheitskonzept für die gesamte Unternehmung?
- Besteht Zusammenarbeit mit Sicherheitsbehörden/-institutionen?
- Werden bei der Personalauswahl Sicherheitsaspekte berücksichtigt?

- Gibt es im Personalmanagement Sicherheits-Checks?
- ...

**6. Wer könnte an dem Wissen Interesse haben, das dem Wettbewerbsvorteil zugrunde liegt?**

- Niemand
- Ein inländischer Konkurrent
- Ein ausländischer Konkurrent
- Mehrere inländische Konkurrenten
- Mehrere ausländische Konkurrenten
- Staatliche (militärische) Institutionen
- Jedermann
- ...

**7. Waren Sie schon Objekt unfreundlichen Informationsabflusses?**

- Nein
- Ja, durch ausländische staatliche Organe
- Ja, durch inländische Konkurrenz
- Ja, durch ausländische Konkurrenz
- Ja, durch „untreue“ Kooperationspartner
- Ja, durch abgewanderte Mitarbeiter
- Ja, durch Unbekannte
- Vielleicht, es bestehen vage Verdachtsmomente
- ...

**8. Welche Verdachtsmomente zu Informationsabflüssen sind Ihnen schon untergekommen?**

- Übermäßiges Kopieren/Kopieren zu ungewöhnlichen Zeiten
- Verlegte/Verstellte Akten
- Anwesenheit fremder Personen auf dem Betriebsgelände oder in der Nähe
- Anwesenheit von Betriebsangehörigen zu ungewöhnlichen Zeiten oder in ungewöhnlichen Betriebsteilen
- Auftauchen von Teilinformationen bei Wettbewerbern
- ...

**9. Wie sind die Beziehungen zu Kooperationspartnern abgesichert?**

- Kooperationsvertrag
- Wechselseitige Kapitalbeteiligung
- Klare Absprachen über Informations- und Verwertungsrechte
- Überprüfung der jeweiligen Leistungsbeiträge

- Regelmäßige Treffen über Arbeitsfortschritte und eventuelle Probleme
- ...

#### **10. Gab es bei abgeworbenen/abgewanderten Mitarbeitern Anzeichen für das Vorhaben?**

- Deutlich geäußerte Unzufriedenheit
- Arbeitsengagement trotz oder nach geäußelter Unzufriedenheit
- Plötzlicher Reichtum
- Konspiratives Verhalten

#### **11. Wie ist die Einschätzung der Arbeit der/Kooperation mit den Sicherheitsbehörden?**

- Arbeit der Sicherheitsbehörden zu Informationsschutz ist weitgehend unbekannt und wird auch nicht benötigt.
- Arbeit der Sicherheitsbehörden zu Informationsschutz ist weitgehend unbekannt, würde aber gebraucht.
- Ansprechpartner bei den Sicherheitsbehörden sind bekannt.
- Es bestehen regelmäßige Informations-/Arbeitskontakte mit den Sicherheitsbehörden.
- Es besteht ein umfassendes, mit den Sicherheitsbehörden abgestimmtes Sicherheitskonzept.
- Die Arbeit der Sicherheitsbehörden ist nicht wirksam genug.
- Die Zuständigkeiten für die verschiedenen Probleme des Informationsabflusses sind nicht klar genug geregelt.
- Es bedarf einer schärferen arbeits- und wettbewerbsrechtlichen Regelung für den Schutz vor unlauterem Informationsabfluss.
- Öffentliche Auftraggeber nehmen wettbewerbsrechtliche Probleme des Informationsschutzes nicht ernst genug.
- ...

### **3.5 Durchführung der Befragung**

In Kooperation mit Prof. Dr. Tscheulin von der Universität Freiburg/Brsg. wurde der Fragebogen durch Unterteilung einiger Komplexe auf insgesamt 19 Fragen umstrukturiert und standardisierte Antworten entwickelt (siehe Anhang). Er wurde an 2400 Firmen IHK-Firmen versandt. Die Auswahl der Firmen erfolgte unter dem Aspekt der potentiellen Betroffenheit, d.h. es wurden Teilnehmer per Zufallsgenerator aus vor allem technologieorientierten gewerblichen Unternehmen ausgesucht. Es wurden folgende in Tabelle 2 dargestellten Wirtschaftszweige einbezogen, deren Differenzierung mit Hilfe von Suchsymbolen und Schlüsselnummern erfolgte:

<b>Wirtschaftszweig</b>	<b>Suchsymbol der IHK zur Differenzierung der Wirtschaftszweige</b>	<b>IHK-Schlüsselnummer</b>
Chemische Industrie	DG	24
Metallerzeugung und -bearbeitung, Herstellung von Metallerzeugnissen	DJ	27, 28
Maschinenbau	DK	29
Herstellung von Büromaschinen, Datenverarbeitungsgeräten und -einrichtungen; Elektrotechnik, Feinmechanik und Optik	DL	30, 31, 32, 33
Fahrzeugbau	DM	34, 35
Verkehr und Nachrichtenübermittlung	I	62, 64
Kredit- und Versicherungsgewerbe	J	65
Grundstücks- und Wohnungswesen, Vermietung beweglicher Sachen, Erbringung von Dienstleistungen überwiegend für Unternehmen	K	72, 73, 74.1-74.3

**Tabelle 2: In die schriftliche Befragung einbezogene Wirtschaftszweige**

Die Umsetzung erfolgte mit Unterstützung der IHK Stuttgart und war mit einigen Ausnahmen treffsicher.

Die Versendung der Fragebögen erfolgte am 15.1.2003, der Rücklauf begann praktisch sofort und erstreckte sich über 8 Wochen. Die letzte berücksichtigte Antwort stammt vom 13.3.2003. In einer Reihe von Fällen kam es zu Rückfragen, die vom Bearbeitungsteam meistens geklärt werden konnten. Teilweise handelte es sich um Firmen, die von der Fragestellung nicht betroffen waren oder sich nicht betroffen fühlten; diesen wurde mitgeteilt, dass auch eine solche Antwort nützlich wäre und es wurde entsprechend geantwortet.

Die erste Auswertung erfolgte mit Hilfe einer Excel-Tabelle, in der die Häufigkeiten zu jeder Antwort bzw. Antwortkategorie absolut und in Prozent (%) dargestellt wurde. Daraus ergaben sich 19 Einzeltabellen mit entsprechenden Werten. Im zweiten Auswertungsschritt wurden die Werte für bestimmte Frageverbindungen untersucht, z.B. die Größenabhängigkeit der Antworten. Hierzu wurden die Klassenwerte in dem Auswahlkriterium – z.B. Größe - jeweils gleich 100% gesetzt und für diese verschiedenen Klassen nun die Ergebnisse auf eine Veränderung der Verteilung überprüft. Die ermittelten Korrelationen wurden verbal beschrieben und zu einer entsprechenden Aussage umgesetzt. In einem weiteren Schritt wurden aufgefundene Korrelationen wiederum in Zusammenarbeit mit Prof. Dr. Tscheulin mathematisch abgesichert.

### **3.6 Sicherung des Schutzes personenbezogener Daten**

Zur Sicherung des Schutzes personenbezogener Daten erfolgten Abstimmungen und Überprüfungen mit dem Landesbeauftragten für den Datenschutz Baden-Württemberg, dem Innenministerium Baden-Württemberg, dem Landesamt für Verfassungsschutz Baden-Württemberg und dem Sicherheitsforum Baden-Württemberg. In Verbindung damit wurden vom Auftragnehmer datenschutzrechtlich relevante Rechtsvorschriften beachtet.

Bei der Versendung des Fragebogens ist allen beteiligten Unternehmen Anonymität der Auswertung und Schutz der Firmendaten zugesichert worden. Die Absicherung dieser Zusage von Datenschutz erfolgte dadurch, dass die Übertragung der Daten aus den Fragebogen in die Excel-Tabelle „Blind“, d.h. ohne Verwendung der Firmendaten vorgenommen wurde. Die vollständigen Fragebögen wurden zur Sicherheit - wenn Rückfrage oder Aufklärungsbedarf besteht – in einem Panzerschrank aufgehoben, zu dem nur die beiden Auftragnehmer Zugang haben. Auf Grund der hohen Fallzahlen und der Breite der vertretenen Branchen ist ein Rückschluss von Aussagen aus der Auswertung auf einzelne Firmen unmöglich. Angaben über Einzelfirmen werden gegenüber Dritten nicht gemacht, die Firmen können uns aber kontaktieren und zu ihren Daten Rückmeldung erhalten.

## **4 Ergebnisse**

### **4.1 Die Befunde zu den Einzelfragen (Tabellen und Abbildungen)**

Von den 2400 an Unternehmen der in Tabelle 2 ausgewiesenen Wirtschaftszweige versendeten Fragebögen kamen 431 zurück. Davon waren 400 Fragebögen für die Auswertung verwertbar. Wie unter Punkt 3.5 bereits ausgeführt, erfolgte die Auswertung mit Hilfe einer Excel-Tabelle, in der die Häufigkeiten zu jeder Antwort bzw. Antwortkategorie absolut und in Prozent dargestellt wurden. Daraus ergaben sich, abgeleitet aus den 19 Fragekomplexen, 19 Einzeltabellen und -abbildungen mit entsprechenden Werten.

Die Auswertung der Fragebögen erfolgte anhand der Nennungen, da die Mehrzahl der Fragen Mehrfachnennungen implizierte. Im Zuge der Auswertung wurde deutlich, dass bis auf die Fragen 11 und 12 die optionalen Antwortmöglichkeiten als separierte Nennungen zu behandeln waren.

Eine Häufung von Nennungen ist bei den Fragen 1, 3, 4, 7, 9, 11, 12 und 17 feststellbar, die in jeder vorgenannten Tabelle nur aus einigen Antwortmöglichkeiten resultieren und an der entsprechenden Stelle genannt werden.

#### **Hinweis:**

Eine ausführlichere Interpretation der Auswertung der Fragebögen erfolgt in Verbindung mit Verknüpfungen zwischen den einzelnen Fragekomplexen in Punkt 4.2.

Die nachfolgende Kopftabelle 3 zeigt die Häufigkeit der Nennungen je Komplex und damit die Intensität der Bearbeitung auch als Kennzeichen der Identifikation der Probanden mit den gestellten Fragen.

Lfd. Nr.	Frage	Anzahl der Nennungen
1	Wie sieht Ihre Produkt-Markt-Position aus? (Produkt schließt hier alle Arten von Dienstleistungen ein)	862
2	Wie hoch war Ihr durchschnittlicher Umsatz in den letzten drei Jahren(in Euro)?	401
3	Worin besteht Ihr wichtigster Wettbewerbsvorteil/-vorsprung?	1453
4	Wie ist der Wettbewerbsvorteil/-vorsprung entstanden?	854
5	Welche ungefähren Aufwendungen haben Sie für die Erstellung bzw. Erarbeitung des Wettbewerbsvorteils/-vorsprungs gehabt? Falls die Angaben nicht in Euro beziffert werden können, bitte Personal- und Zeitaufwand benennen.	396
6	Wie hoch schätzen Sie den Wert des Wettbewerbsvorteils/-vorsprungs ein (gemessen in Euro pro Jahr)?	369
7	Wie nachhaltig ist der Wettbewerbsvorteil/-vorsprung?	916
8	Wie lange hält der momentane Wettbewerbsvorteil/-vorsprung, wenn Sie keine weiteren Investitionen oder andere Maßnahmen dafür tätigen oder wenn er nicht durch adäquate Maßnahmen erhalten wird?	402
9	Welche Sicherungsmaßnahmen gegen Informationsverluste werden vorgenommen?	2486
10	Wie hoch sind Ihre Aufwendungen für Informationssicherheit (in Euro pro Jahr)?	385
11	Wer könnte an dem Wissen Interesse haben, das dem Wettbewerbsvorteil/-vorsprung zugrunde liegt?	803*
12	Waren Sie schon Objekt „unfreundlichen“ Informationsabflusses? (Ausspähung, Abschöpfung, Abwerbung, Mitnahme von Geheimnissen bei Weggang von Mitarbeitern,...)	571*
13	Wie hoch schätzen Sie den in diesem Fall entstandenen Schaden (in Euro)?	245
14	Wie haben Sie den Schadensfall bearbeitet?	275
15	Welche Sicherheitsmaßnahmen haben Sie als Folge des Schadensfalls ergriffen?	303
16	Welche Verdachtsmomente zu Informationsabflüssen hatten Sie bisher?	402
17	Wie sind die Beziehungen zu Kooperationspartnern abgesichert?	618
18	Gab es bei abgeworbenen/abgewanderten Mitarbeitern Anzeichen für die Illoyalität?	261
19	Wie ist die Einschätzung der Arbeit der/Kooperation mit den Sicherheitsbehörden?	434

**Tabelle 3:**

**Übersicht der Nennungen zu den 19 Fragen des Fragebogens aus 400 Rückläufen der Fragebogenaktion**

\* Ohne optionale Nennungen, da diese eine Untersetzung der vorhandenen Antwortmöglichkeiten beinhalten

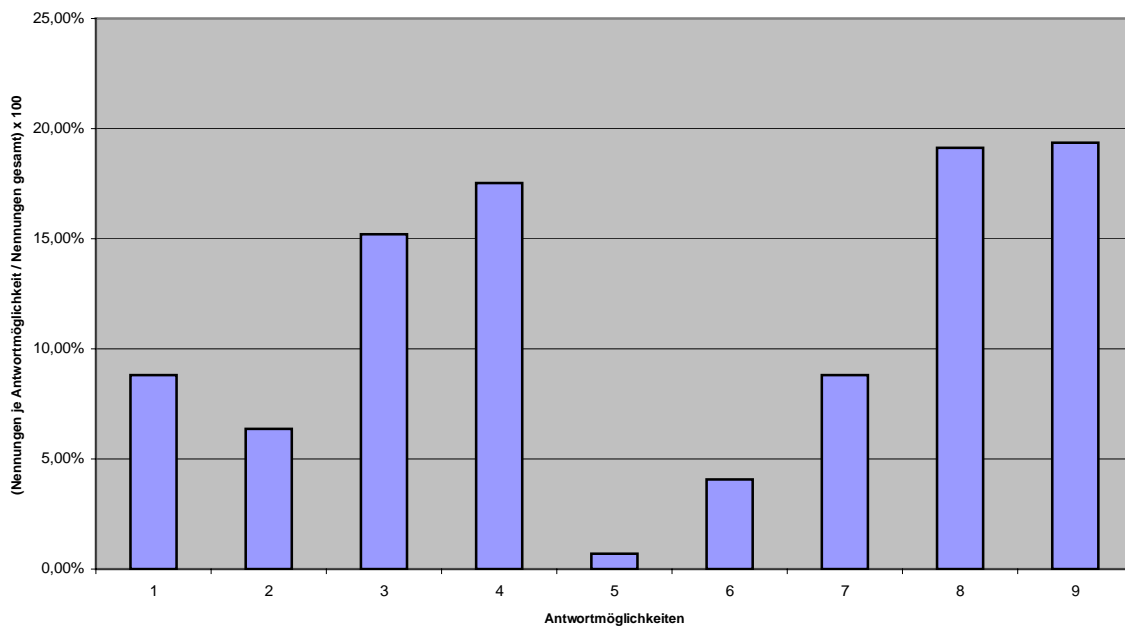
**Zu Tabelle 4 und Abbildung 2:**

Der größte Anteil der Antworten zur Produkt-Markt-Position entfällt hauptsächlich auf die Antwortmöglichkeiten 3 und 4 zur Einzel- und Kleinserienfertigung sowie 8 und 9 bei nationaler und internationaler Marktstellung.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	Massenprodukt in einem Markt mit vielen Konkurrenten	76	8,82
2	Massenprodukt in einem Markt mit wenigen Konkurrenten	55	6,38
3	Einzel-/Kleinserienfertigung in einem Markt mit vielen Konkurrenten	131	15,20
4	Einzel/Kleinserienfertigung in einem Markt mit wenigen Konkurrenten	151	17,51
5	Einziger Anbieter am Markt (Monopol)	6	0,70
6	<i>Optional</i>	35	4,06
7	Unsere Marktstellung ist: eher regional	76	8,82
8	Unsere Marktstellung ist: eher national	165	19,14
9	Unsere Marktstellung ist: eher international	167	19,37
<b>gesamt</b>		<b>862</b>	<b>100,00</b>

**Tabelle 4:**

**Antworten zur Frage 1 „Wie sieht Ihre Produkt-Markt-Position aus? (Produkt schließt hier alle Arten von Dienstleistungen ein)“**



**Abbildung 2:**

**Graphische Auswertung der Antwortmöglichkeiten zur Frage 1**

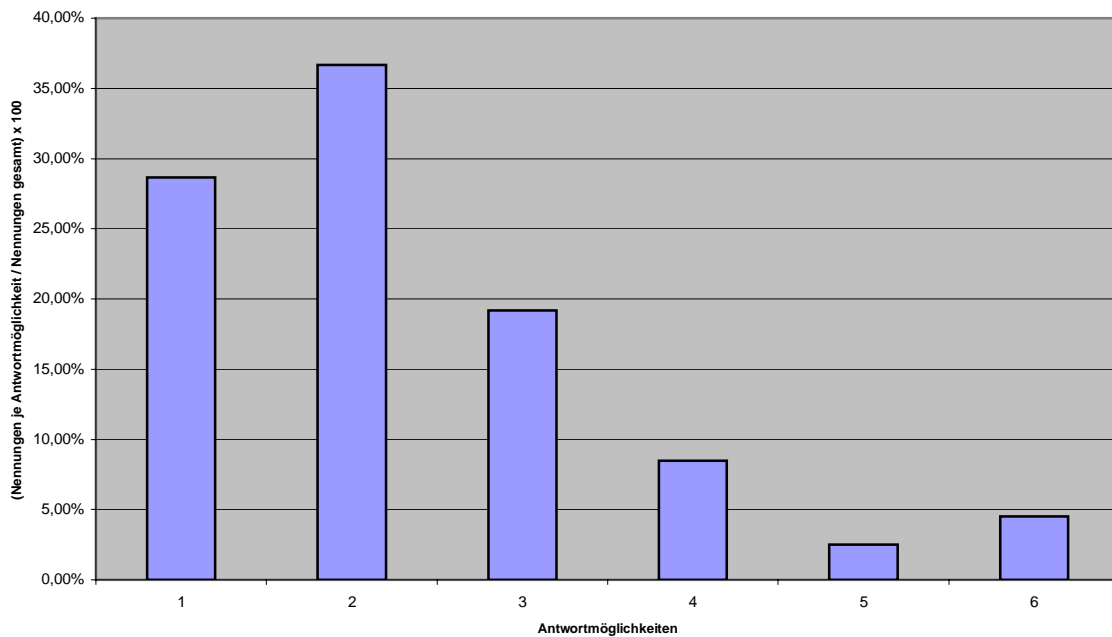
**Zu Tabelle 5 und Abbildung 3:**

Der größte Anteil der Antworten entfällt hauptsächlich auf Umsatzhöhen bis 10 Millionen €, also auf kleine und mittlere Unternehmen.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	unter 2 Millionen €	115	28,68
2	2 bis 10 Millionen €	147	36,66
3	10 bis 50 Millionen €	77	19,20
4	50 bis 200 Millionen €	34	8,48
5	200 bis 500 Millionen €	10	2,49
6	über 500 Millionen €	18	4,49
<b>gesamt</b>		<b>401</b>	<b>100,00</b>

**Tabelle 5:**

Antworten zur Frage 2 „Wie hoch war Ihr durchschnittlicher Umsatz in den letzten drei Jahren?“



**Abbildung 3:**

Graphische Auswertung der Antwortmöglichkeiten zur Frage 2

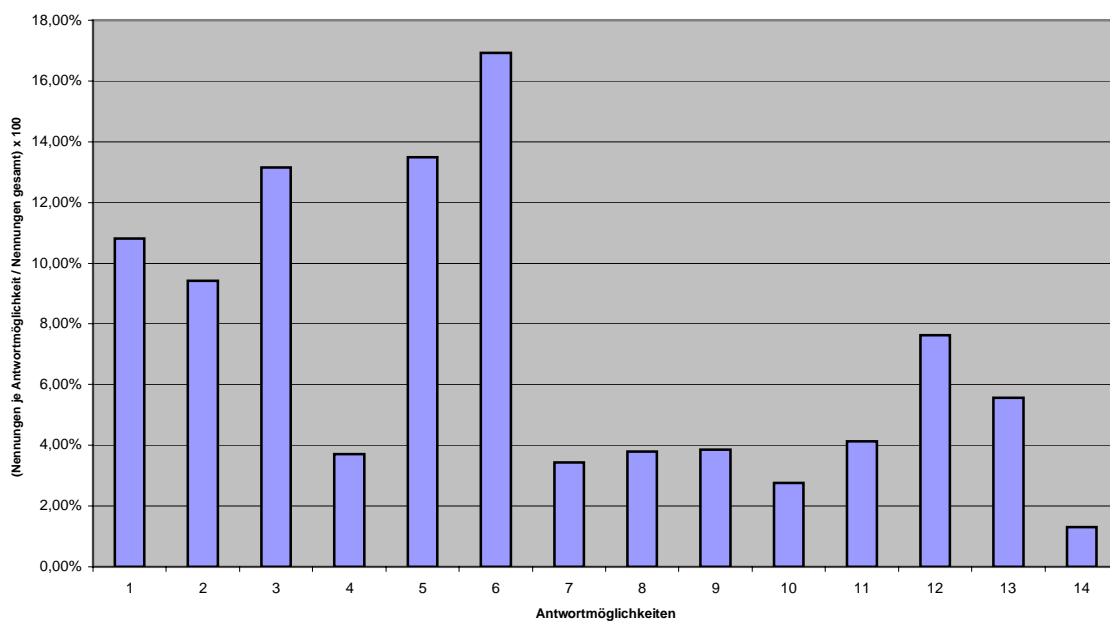
**Zu Tabelle 6 und Abbildung 4:**

Der wichtigste Wettbewerbsvorteil/-vorsprung konzentriert sich auf die Antwortmöglichkeiten 1, 2, 3, 5 und 6.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	Überlegene Produkte	157	10,81
2	Neue Produkte	137	9,43
3	Beherrschung spezifischer Produktionsprozesse/Arbeitsmethoden	191	13,15
4	Maschinenausstattung	54	3,72
5	Mitarbeiterstamm	196	13,49
6	Kundenstamm/Kundenbeziehung	246	16,93
7	Lieferantenbeziehungen	50	3,44
8	Vertriebssystem	55	3,79
9	Kooperationen/Netzwerke	56	3,85
10	Forschungspotenzial/-ergebnisse	40	2,75
11	Organisatorische Vorteile	60	4,13
12	Unternehmenskultur/Betriebsklima	111	7,64
13	Strategie (Produkt-Markt, Corporate, Geschäftseinheit)	81	5,56
14	<i>Optional</i>	19	1,31
<b>gesamt</b>		<b>1453</b>	<b>100,00</b>

**Tabelle 6:**

Antworten zur Frage 3 „Worin besteht Ihr wichtigster Wettbewerbsvorteil/-vorsprung?“



**Abbildung 4:**

Graphische Auswertung der Antwortmöglichkeiten zur Frage 3

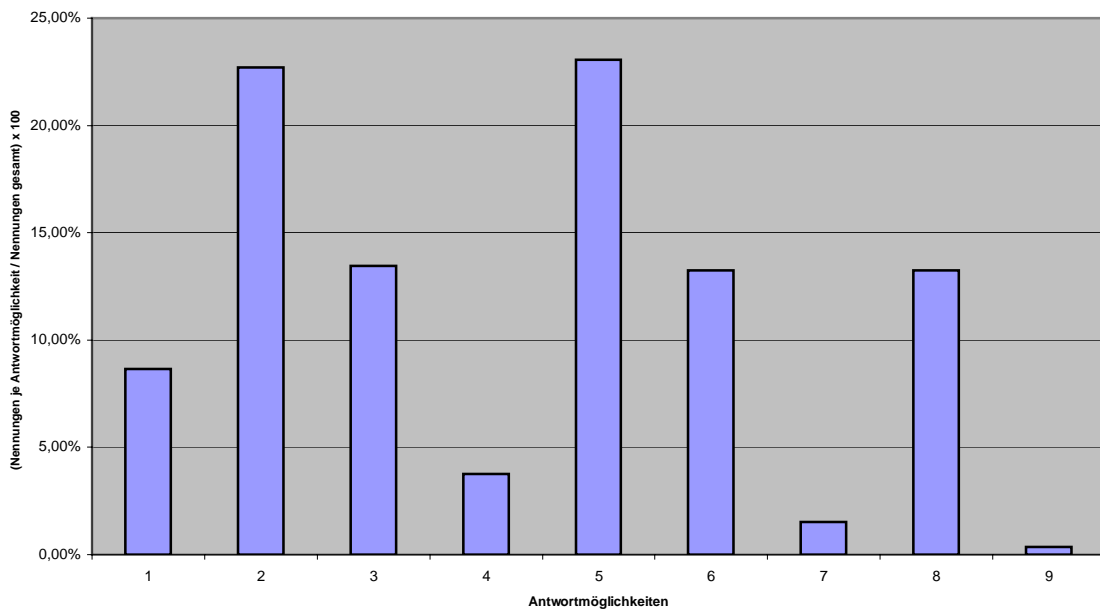
**Zu Tabelle 7 und Abbildung 5:**

Nach Aussage der Unternehmen ist der Wettbewerbsvorteil/-vorsprung hauptsächlich auf die Antwortmöglichkeiten 2, 3, 5, 6 und 8 zurück zu führen.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	Idee einer Person	74	8,67
2	Gemeinsame Idee mehrerer Personen in der Unternehmung (Team)	194	22,72
3	Gemeinsame Idee mit Kunden/Kooperation mit Kunden	115	13,47
4	Entwurf/Projektbearbeitung einer oder mehrerer Abteilungen	32	3,74
5	Gewachsen aus dauerhafter Zusammenarbeit	197	23,07
6	Gewachsen durch strategische Investition in innovative Geschäftsfelder	113	13,23
7	Fremdforschung/Fremdentwicklung	13	1,52
8	Marktbeobachtung	113	13,23
9	<i>Optional</i>	3	0,35
<b>gesamt</b>		<b>854</b>	<b>100,00</b>

**Tabelle 7:**

Antworten zur Frage 4 „Wie ist der Wettbewerbsvorteil/-vorsprung entstanden?“



**Abbildung 5:**

Graphische Auswertung der Antwortmöglichkeiten zur Frage 4

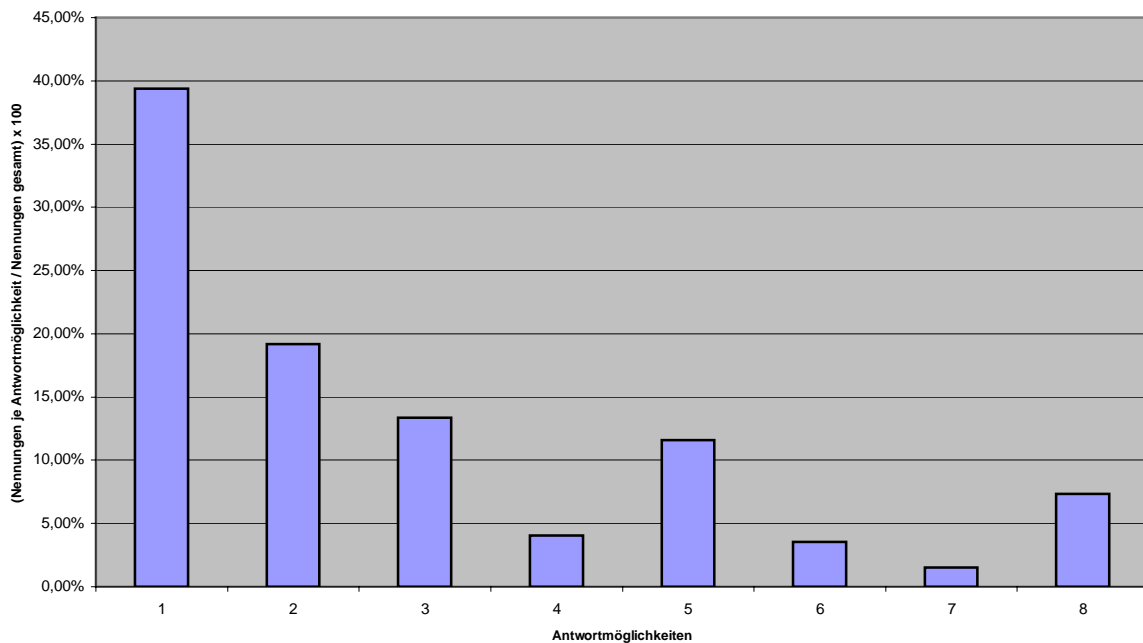
**Zu Tabelle 8 und Abbildung 6:**

Die Aufwendungen zur Erarbeitung dieses Vorsprungs liegen nach mehr als der Hälfte der Nennungen bei maximal 1 Million €

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	unter 500 000 €	156	39,39
2	500 000 bis 1 Million €	76	19,19
3	1 bis 3 Millionen €	53	13,38
4	3 bis 5 Millionen €	16	4,04
5	über 5 Millionen €	46	11,62
6	Optional Personen	14	3,54
7	Optional Stunden	6	1,52
8	Optional	29	7,32
<b>gesamt</b>		<b>396</b>	<b>100,00</b>

**Tabelle 8:**

Antworten zur Frage 5 „Welche ungefähren Aufwendungen haben Sie für die Erstellung bzw. Erarbeitung des Wettbewerbsvorteils/-vorsprungs gehabt? Falls die Angaben nicht in Euro beziffert werden können, bitte Personal- und Zeitaufwand benennen.“



**Abbildung 6:**

**Graphische Auswertung der Antwortmöglichkeiten zur Frage 5**

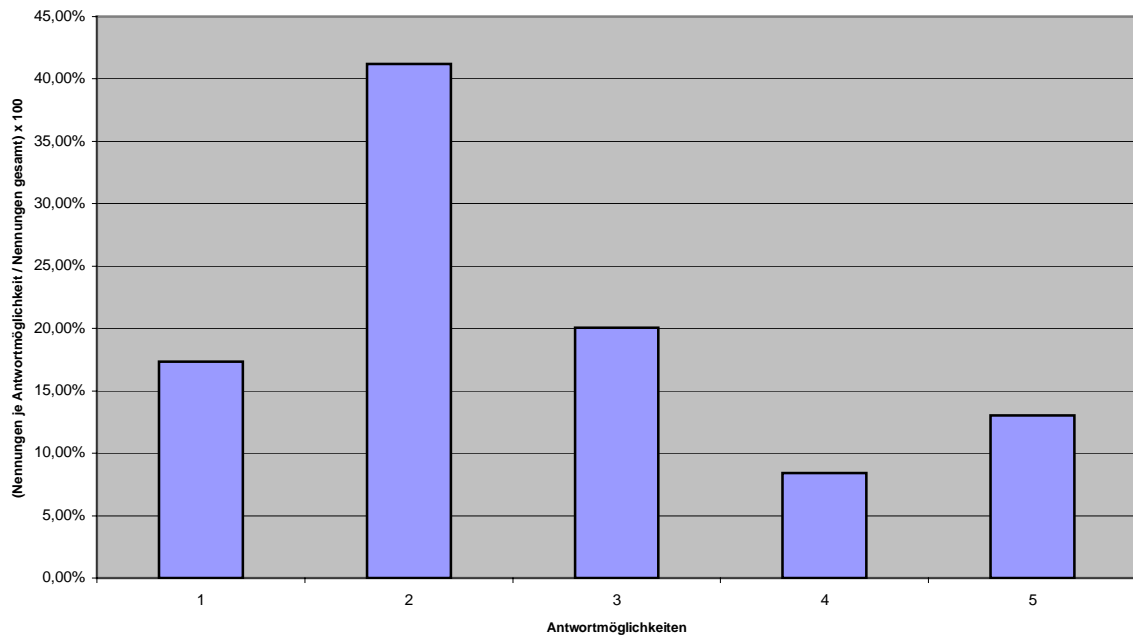
**Zu Tabelle 9 und Abbildung 7:**

Der Wert des Wettbewerbsvorteils/-vorsprungs übersteigt bei vier Fünftel der Nennungen nicht die 2-Millionen-€-Grenze.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	unter 100 000 €	64	17,34
2	zwischen 100 000 und 500 000 €	152	41,19
3	zwischen 500 000 und 2 Millionen €	74	20,05
4	zwischen 2 und 5 Millionen €	31	8,41
5	über 5 Millionen €	48	13,01
<b>gesamt</b>		<b>369</b>	<b>100,00</b>

**Tabelle 9:**

**Antworten zur Frage 6 „Wie hoch schätzen Sie den Wert des Wettbewerbsvorteils/-vorsprungs ein (gemessen in Euro pro Jahr)?“**



**Abbildung 7:**

**Graphische Auswertung der Antwortmöglichkeiten zur Frage 6**

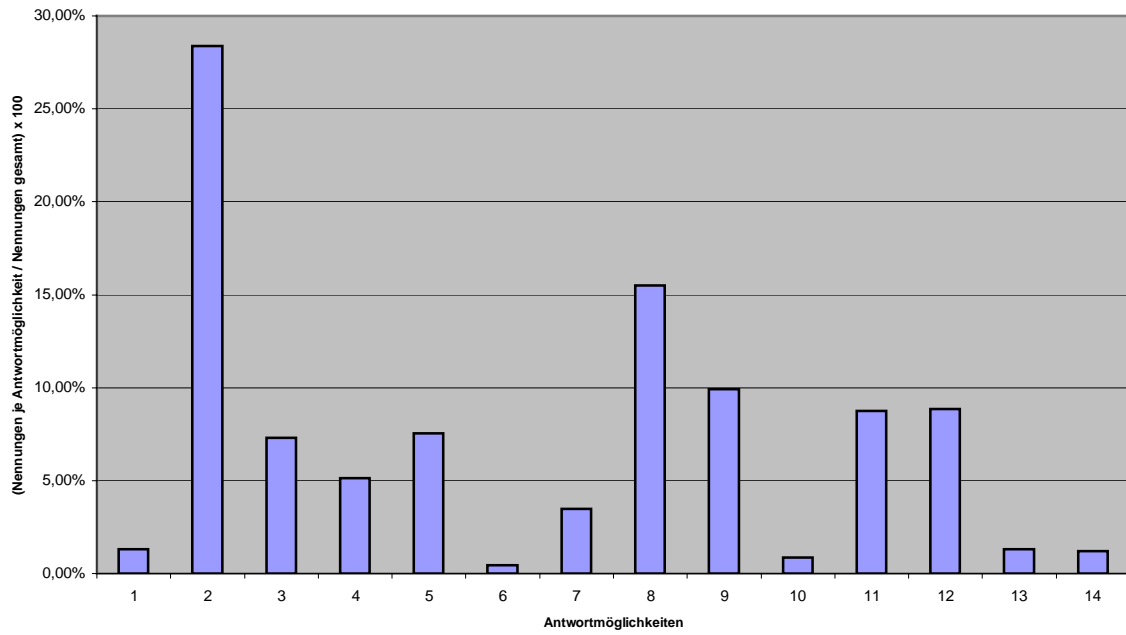
**Zu Tabelle 10 und Abbildung 8:**

Der vorhandene Wettbewerbsvorteil/-vorsprung wird bei 916 Nennungen insgesamt nur von 152 als geschützt ausgewiesen.

<b>Antwort- möglichkeiten</b>	<b>Bezeichnung</b>	<b>Nennungen</b>	<b>Nennungen je <u>Antwortmöglichkeit</u> Nennungen gesamt in Prozent</b>
1	Nicht imitierbar und erodiert nicht	12	1,31
2	Imitierbar (muss stets durch Innovationen verteidigt werden)	260	28,38
3	Rekonstruierbar (leichte Nachahmbarkeit)	67	7,32
4	Geschützt durch: nationales Patent	47	5,13
5	Geschützt durch: internationale Patente	69	7,55
6	Geschützt durch: Umgehungspatente	4	0,44
7	Geschützt durch: Gebrauchsmuster	32	3,49
8	Nicht geschützt	142	15,50
9	Setzt erhebliche spezifische Investitionen voraus	91	9,93
10	Nachahmung nützt nichts, da keine weiteren Kunden vorhanden	8	0,87
11	Der Vorteil liegt in der Unternehmensorganisation (Arbeitsteilung, Struktur)	80	8,73
12	Der Vorteil liegt in der Unternehmenskultur (Werte, Identifikation, Betriebsklima)	81	8,84
13	Es gibt spezielle Sicherheitsmaßnahmen	12	1,31
14	<i>Optional</i>	11	1,20
<b>gesamt</b>		<b>916</b>	<b>100,00</b>

**Tabelle 10:**

**Antworten zur Frage 7 „Wie nachhaltig ist der Wettbewerbsvorteil/-vorsprung?“**



**Abbildung 8:**  
**Graphische Auswertung der Antwortmöglichkeiten zur Frage 7**

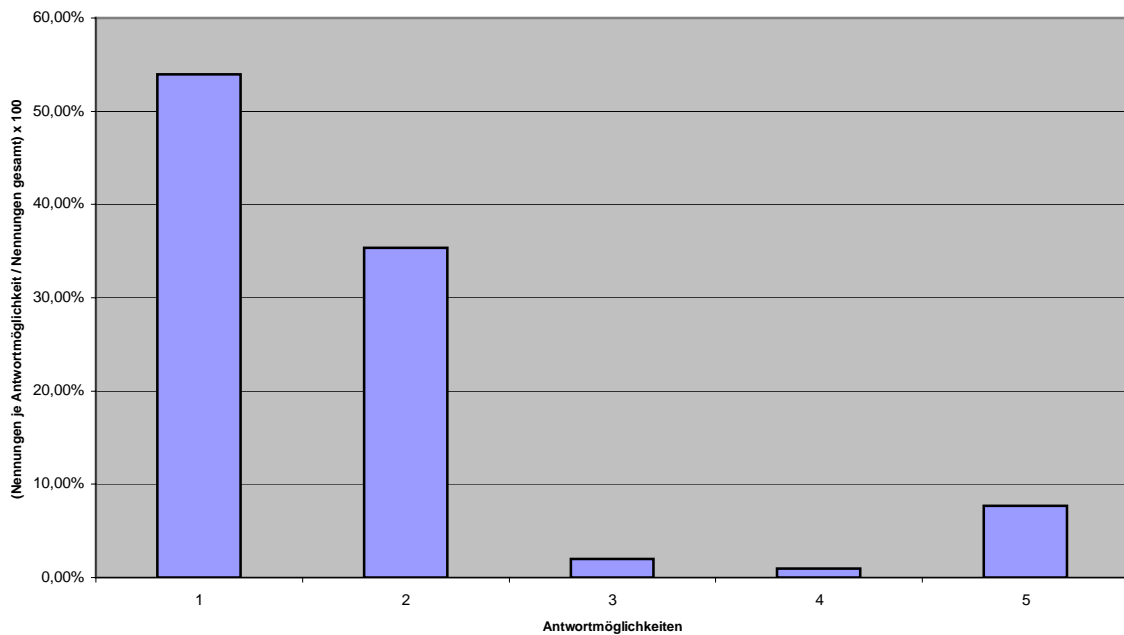
**Zu Tabelle 11 und Abbildung 9:**

Der momentane Wettbewerbsvorteil/-vorsprung hält bei mehr als der Hälfte der Nennungen nicht länger als ein Jahr.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	1 Jahr	217	53,98
2	5 Jahre	142	35,32
3	10 Jahre	8	1,99
4	mehr als 10 Jahre	4	1,00
5	<i>Optional</i>	31	7,71
<b>gesamt</b>		<b>402</b>	<b>100,00</b>

**Tabelle 11:**

**Antworten zur Frage 8 „Wie lange hält der momentane Wettbewerbsvorteil/-vorsprung, wenn Sie keine weiteren Investitionen oder andere Maßnahmen dafür tätigen oder wenn er nicht durch adäquate Maßnahmen erhalten wird?“**



**Abbildung 9:**

**Graphische Auswertung der Antwortmöglichkeiten zur Frage 8**

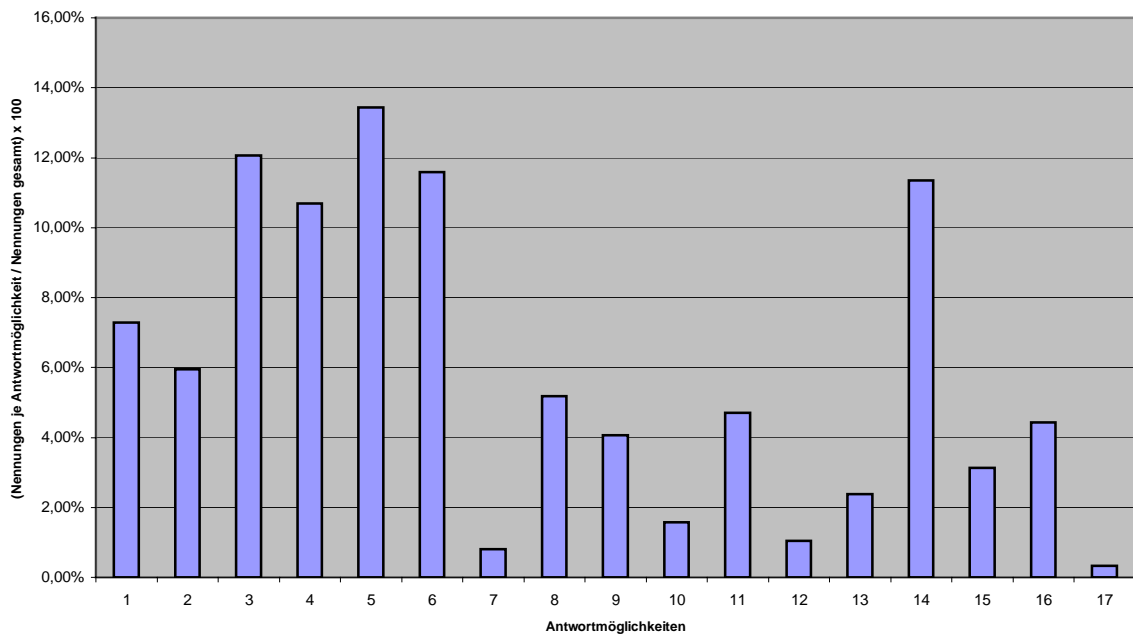
**Zu Tabelle 12 und Abbildung 10:**

Die Sicherungsmaßnahmen gegen Informationsverluste verteilen sich über eine Vielzahl von Einzelaktivitäten und haben ihren Schwerpunkt im Datenschutz und im rechentechnischen Bereich.

<b>Antwort- möglichkeiten</b>	<b>Bezeichnung</b>	<b>Nennungen</b>	<b>Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent</b>
1	Besteht eine Eingangskontrolle/allgemeine Zugangskontrolle?	181	7,28
2	Bestehen Zugangsbeschränkungen für sicherheitsrelevante Bereiche?	148	5,95
3	Gibt es Zugriffsbeschränkungen für Daten?	300	12,07
4	Wird Datenschutz betrieben?	266	10,70
5	Werden Sicherheitskopien hergestellt?	334	13,44
6	Ist Wissen so verteilt, dass nicht eine Person über das gesamte Wissen verfügt?	288	11,58
7	Sind Sie in das amtliche Geheimschutzverfahren einbezogen?	20	0,80
8	Gibt es einen Sicherheitsverantwortlichen im Unternehmen?	129	5,19
9	Gibt es ein Sicherheitskonzept für die gesamte Unternehmung?	101	4,06
10	Besteht Zusammenarbeit mit Sicherheitsbehörden/-institutionen?	39	1,58
11	Werden bei der Personalarbeit Sicherheitsaspekte berücksichtigt (Auswahl, Einsatz, Freisetzung)?	117	4,71
12	Gibt es personenbezogene Sicherheits-Checks?	26	1,05
13	Wird das Personal in Schutzmaßnahmen gegen Informationsverlust geschult?	59	2,37
14	Gibt es Geheimhaltungs-/Wettbewerbsklauseln in den Arbeitsverträgen?	282	11,34
15	Sind beim Ausscheiden von Mitarbeitern spezielle Sicherheitsvorkehrungen vorgesehen?	78	3,14

Antwort- möglichkeiten	Bezeichnung	Nennungen	Nennungen je <u>Antwortmöglichkeit</u> Nennungen gesamt in Prozent
16	Beziehen sich diese Personalmaßnahmen auch auf Fremd-, Leasing- und sonstiges Dienstleistungspersonal?	110	4,42
17	<i>Optional</i>	8	0,32
<b>gesamt</b>		<b>2486</b>	<b>100,00</b>

**Tabelle 12:**  
**Antworten zur Frage 9 „Welche Sicherungsmaßnahmen gegen Informationsverluste werden  
vorgenommen?“**



**Abbildung 10:**  
**Graphische Auswertung der Antwortmöglichkeiten zur Frage 9**

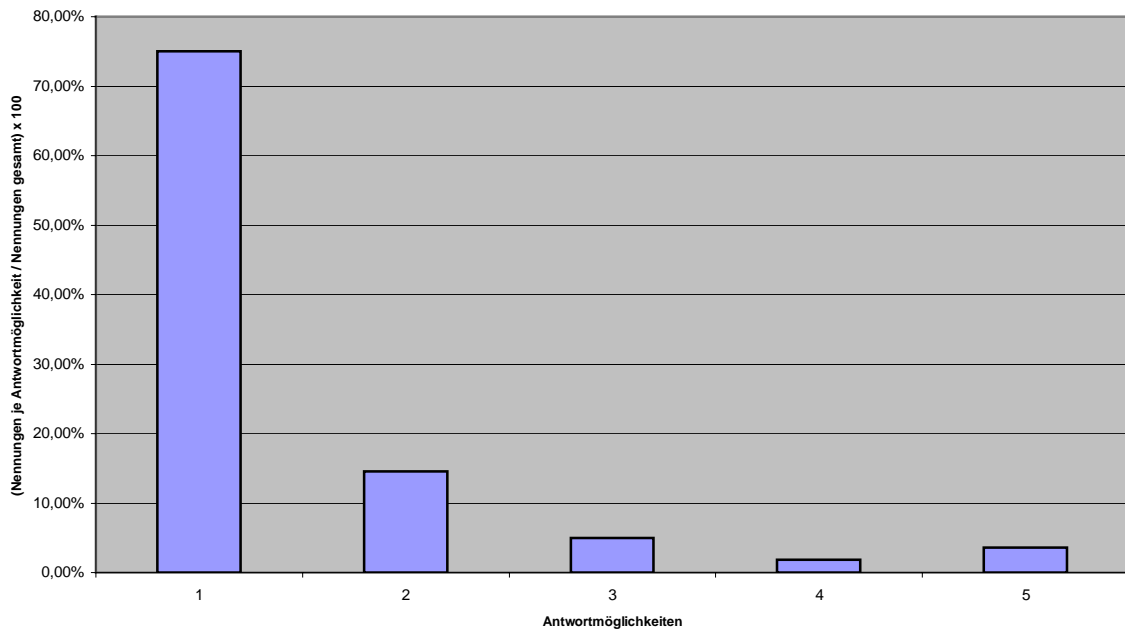
**Zu Tabelle 13 und Abbildung 11:**

Die Aufwendungen für Informationssicherheit sind mit Nennungen bis zu 100000 € pro Jahr als relativ geringfügig einzuschätzen.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	unter 50 000 €	289	75,06
2	50 000 bis 100 000 €	56	14,55
3	100 000 bis 250 000 €	19	4,93
4	250 000 bis 500 000 €	7	1,82
5	über 500 000 €	14	3,64
<b>gesamt</b>		<b>385</b>	<b>100,00</b>

**Tabelle 13:**

**Antworten zur Frage 10 „Wie hoch sind Ihre Aufwendungen für Informationssicherheit (in Euro pro Jahr)?“**



**Abbildung 11:**

**Graphische Auswertung der Antwortmöglichkeiten zur Frage 10**

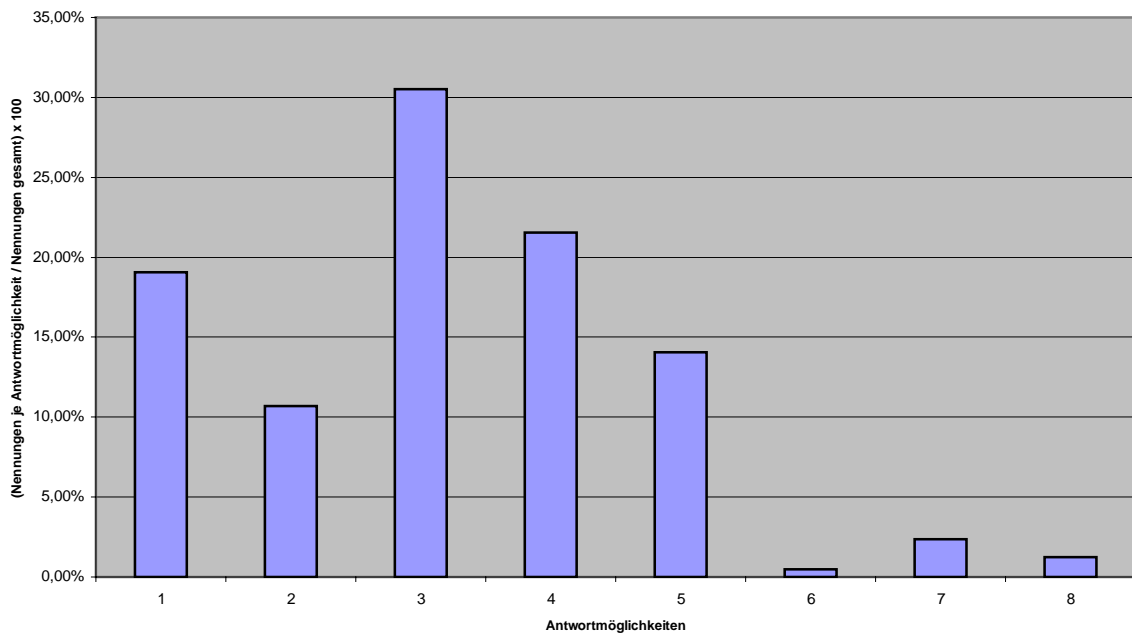
**Zu Tabelle 14 und Abbildung 12:**

Hauptinteressenten am Wissen über den Wettbewerbsvorteil/-vorsprung sind im Wesentlichen sowohl inländische als auch ausländische Konkurrenten.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	Ein inländischer Konkurrent	153	19,05
2	Ein ausländischer Konkurrent	86	10,71
darunter	<i>Optional</i> aus welchem Land oder welchen Ländern	69	
3	Mehrere inländische Konkurrenten	245	30,51
4	Mehrere ausländische Konkurrenten	173	21,54
darunter	<i>Optional</i> aus welchen Ländern	113	
5	Potenzielle Konkurrenten	113	14,07
6	Staatliche (militärische) Institutionen	4	0,50
darunter	<i>Optional</i> aus welchen Ländern	10	
7	Technologie-/Wissenshändler	19	2,37
8	<b>Optional</b>	10	1,25
<b>gesamt</b>		<b>803 (192)</b>	<b>100,00</b>

**Tabelle 14:**

**Antworten zur Frage 11 „Wer könnte an dem Wissen Interesse haben, das dem Wettbewerbsvorteil/-vorsprung zugrunde liegt?“**



**Abbildung 12:**

**Graphische Auswertung der Antwortmöglichkeiten zur Frage 11**

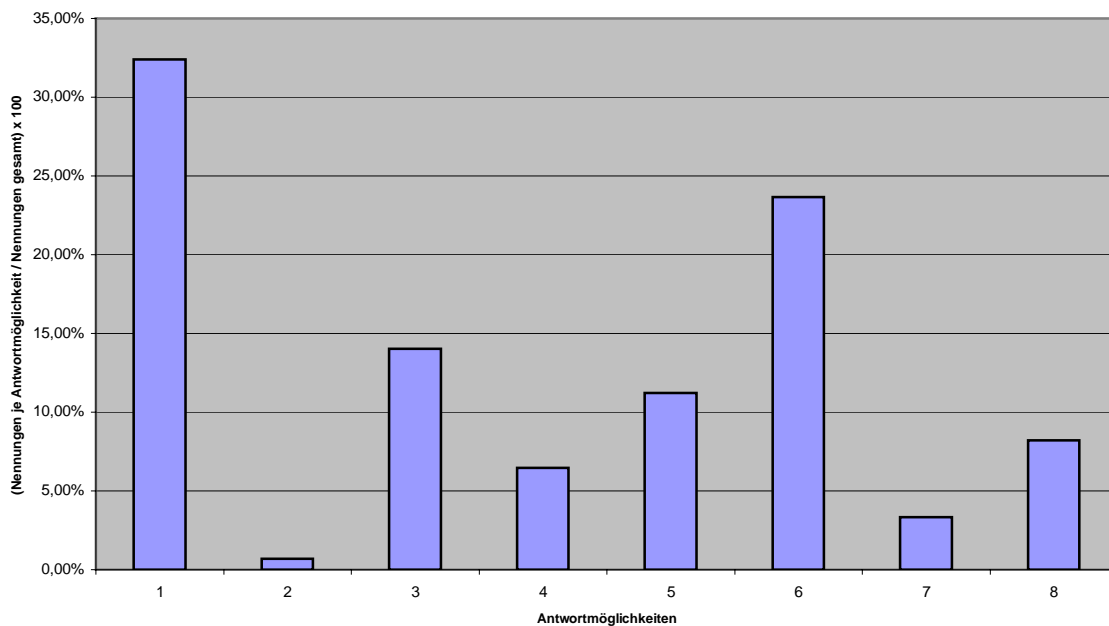
**Zu Tabelle 15 und Abbildung 13:**

In rund 70 Prozent der Antworten signalisierten die Unternehmen Objekte unfreundlichen Informationsabflusses gewesen zu sein.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	Nein	185	32,40
2	Ja, durch ausländische staatliche Organe	4	0,70
darunter	<i>Optional</i> aus welchen Ländern	6	
3	Ja, durch inländische Konkurrenz	80	14,01
4	Ja, durch ausländische Konkurrenz	37	6,48
darunter	<i>Optional</i> aus welchen Ländern	25	
5	Ja, durch „untreue“ Kooperationspartner	64	11,21
6	Ja, durch abgewanderte Mitarbeiter	135	23,64
7	Ja, durch Unbekannte	19	3,33
8	Vielleicht, es bestehen vage Verdachtsmomente	47	8,23
<b>gesamt</b>		<b>571 (31)</b>	<b>100,00</b>

**Tabelle 15:**

**Antworten zur Frage 12 „Waren Sie schon Objekt „unfreundlichen“ Informationsabflusses? (Ausspähung, Abschöpfung, Abwerbung, Mitnahme von Geheimnissen bei Weggang von Mitarbeitern,...)“**



**Abbildung 13:**

**Graphische Auswertung der Antwortmöglichkeiten zur Frage 12**

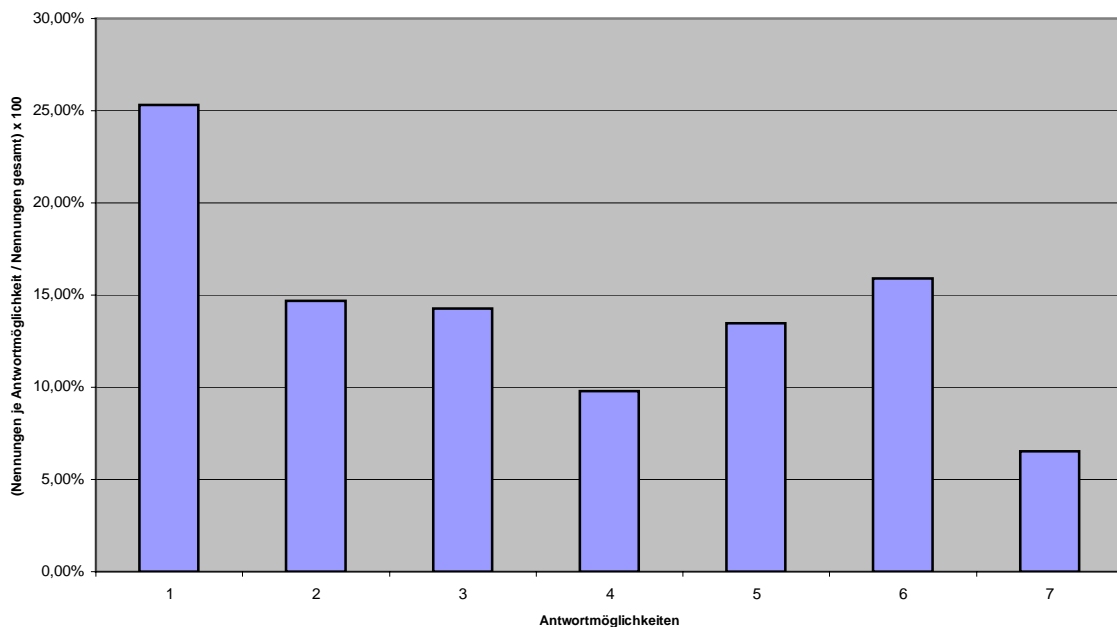
**Zu Tabelle 16 und Abbildung 14:**

Der durch unfreundlichen Informationsabfluss entstandene Schaden ist offensichtlich schwer einschätzbar und verteilt sich relativ gleichmäßig über alle Antwortmöglichkeiten.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	unter 50 000 €	62	25,31
2	50 000 bis 100 000 €	36	14,69
3	100 000 bis 250 000 €	35	14,29
4	250 000 bis 500 000 €	24	9,80
5	über 500 000 €	33	13,46
6	nur in anderen Dimensionen ausdrückbar	39	15,92
7	<i>Optional</i>	16	6,53
<b>gesamt</b>		<b>245</b>	<b>100,00</b>

**Tabelle 16:**

Antworten zur Frage 13 „Wie hoch schätzen Sie den in diesem Fall entstandenen Schaden (in Euro)?“



**Abbildung 14:**

Graphische Auswertung der Antwortmöglichkeiten zur Frage 13

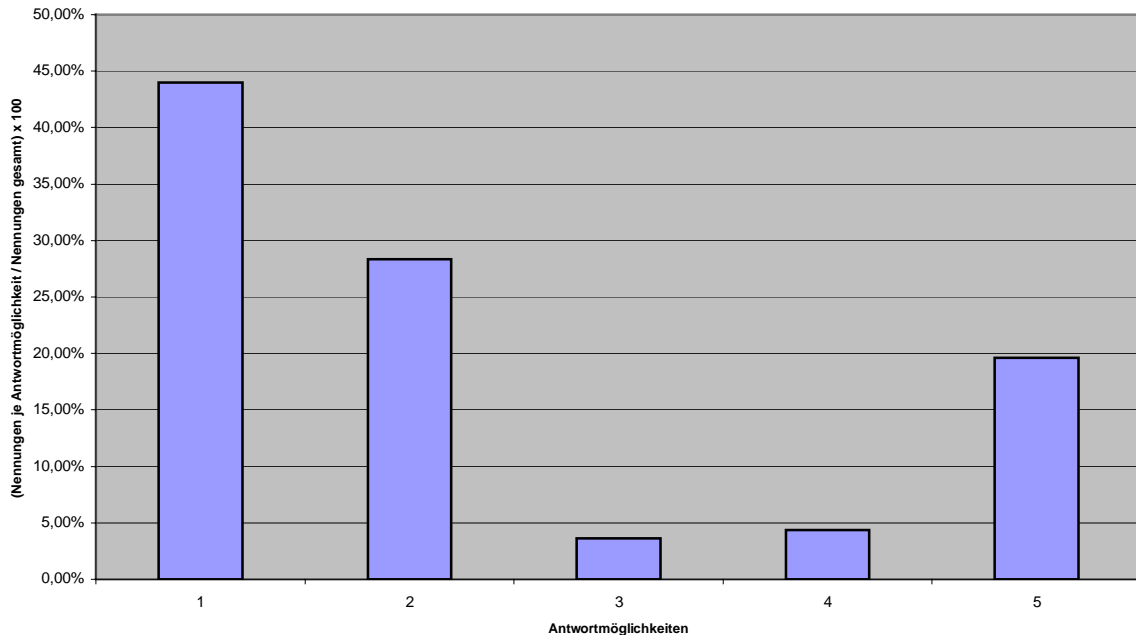
**Zu Tabelle 17 und Abbildung 15:**

Zur Bearbeitung des Schadensfalls erfolgten nur 275 Nennungen, von denen knapp die Hälfte sich zu keiner Bearbeitung bekannte.

Antwort- möglichkeiten	Bezeichnung	Nennungen	Nennungen je <u>Antwortmöglichkeit</u> Nennungen gesamt in Prozent
1	Gar nicht	121	44,00
2	Mit innerbetrieblichen Kräften (Organisations-Abt., Interne Revision, EDV-Abt.)	78	28,36
3	Mit externen Sicherheitsberatern	10	3,64
4	Mit Sicherheitsbehörden (Polizei, Verfassungsschutz)	12	4,36
5	<i>Optional</i> Durchführung einer Schwachstellenanalyse, wobei folgende entdeckt wurden	54	19,64
<b>gesamt</b>		<b>275</b>	<b>100,00</b>

**Tabelle 17:**

**Antworten zur Frage 14 „Wie haben Sie den Schadensfall bearbeitet?“**



**Abbildung 15:**

**Graphische Auswertung der Antwortmöglichkeiten zur Frage 14**

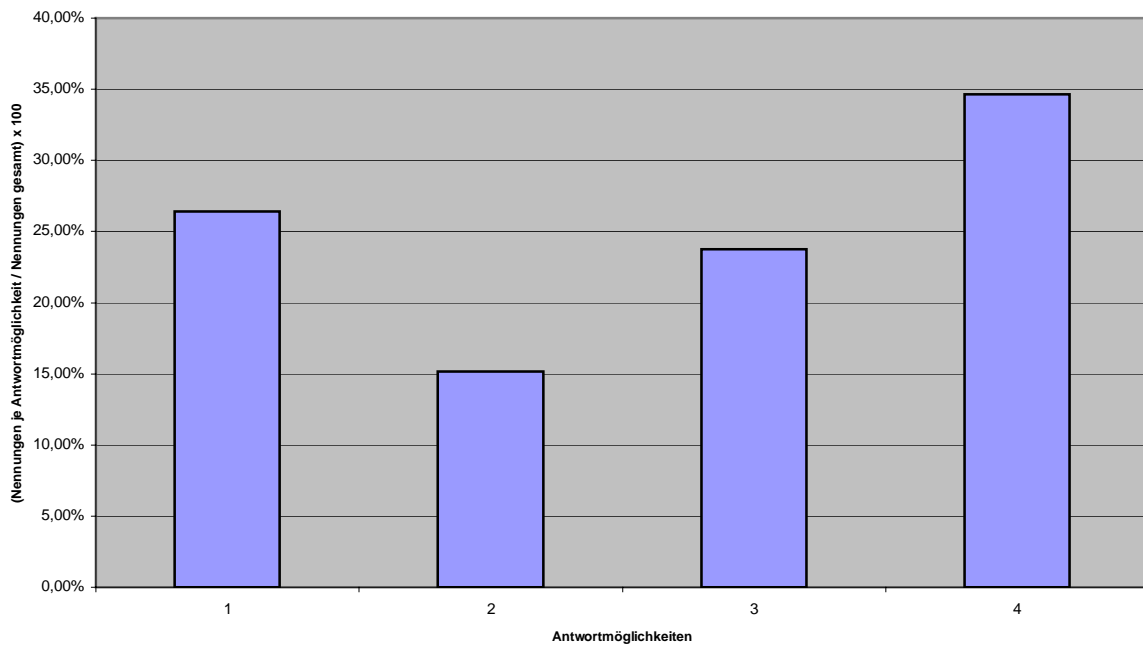
**Zu Tabelle 18 und Abbildung 16:**

Als Folge der eingetretenen Schadensfälle wurden sowohl personelle als auch technische, organisatorische und juristische Maßnahmen zu ziemlich gleichen Anteilen ausgelöst.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	Personelle Maßnahmen (Schulung,...)	80	26,40
2	Technische Maßnahmen (Alarmanlagen, Kontrollsysteme,...)	46	15,18
3	Organisatorische Maßnahmen (Zugangsregelung, Closed Shop,...)	72	23,77
4	Juristische Maßnahmen (Verträge, interne Regeln,...)	105	34,65
<b>gesamt</b>		<b>303</b>	<b>100,00</b>

**Tabelle 18:**

**Antworten zur Frage 15 „Welche Sicherheitsmaßnahmen haben Sie als Folge des Schadensfalls ergriffen?“**



**Abbildung 16:**

**Graphische Auswertung der Antwortmöglichkeiten zur Frage 15**

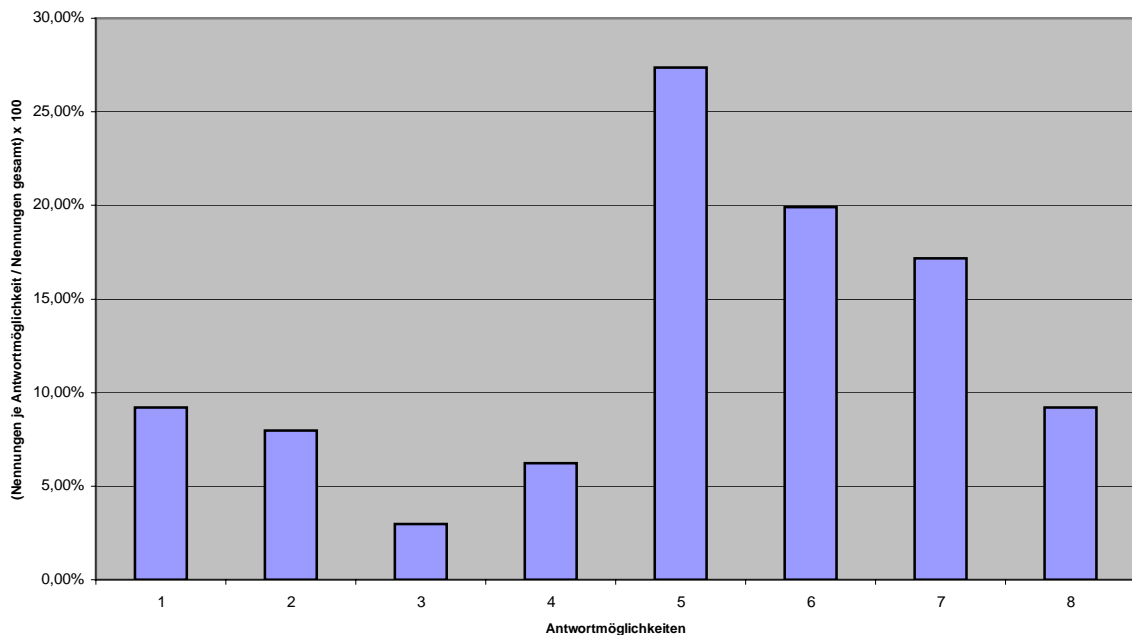
**Zu Tabelle 19 und Abbildung 17:**

Die Verdachtsmomente zu Informationsabflüssen konzentrieren sich auf Auftauchen von Teilinformationen bei Wettbewerbern und nicht erklärbaren Verlusten von Aufträgen.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit / Nennungen gesamt in Prozent
1	Übermäßiges Kopieren/Kopieren zu ungewöhnlichen Zeiten	37	9,20
2	Nicht auffindbare Unterlagen	32	7,97
3	Anwesenheit fremder Personen auf dem Betriebsgelände oder in der Nähe	12	2,99
4	Anwesenheit von Betriebsangehörigen zu ungewöhnlichen Zeiten oder in ungewöhnlichen Betriebsteilen	25	6,22
5	Auftauchen von Teilinformationen bei Wettbewerbern	110	27,36
6	Nicht erklärbarer Verlust von Aufträgen	80	19,90
7	Auftauchen von günstigen Konkurrenzprodukten	69	17,16
8	<i>Optional</i>	37	9,20
<b>gesamt</b>		<b>402</b>	<b>100,00</b>

**Tabelle 19:**

Antworten zur Frage 16 „Welche Verdachtsmomente zu Informationsabflüssen hatten Sie bisher?“



**Abbildung 17:**

Graphische Auswertung der Antwortmöglichkeiten zur Frage 16

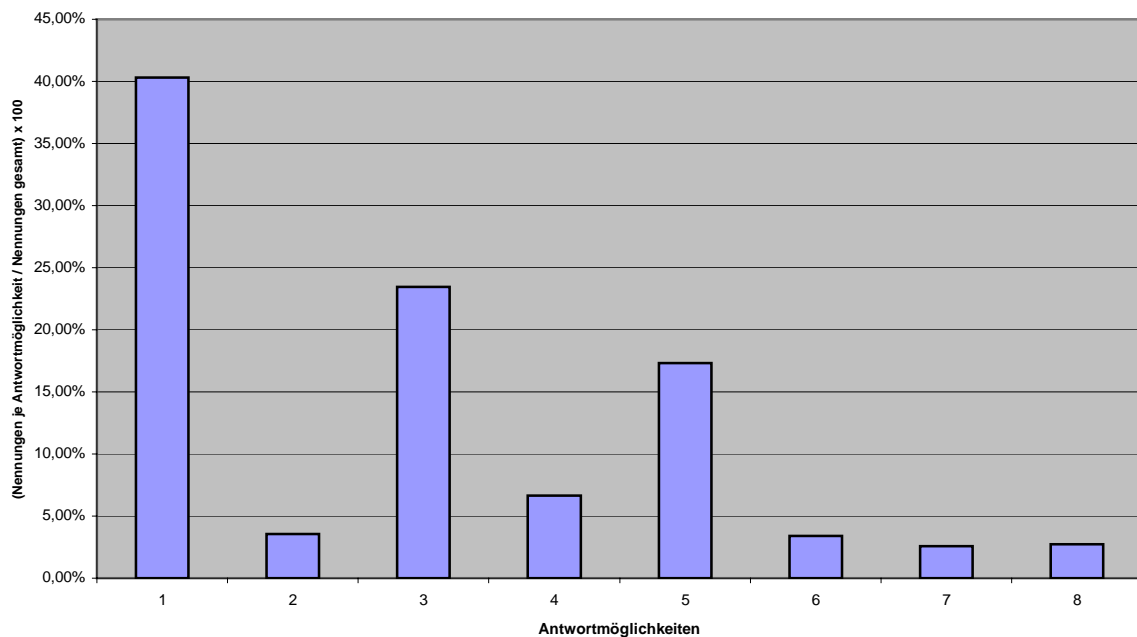
**Zu Tabelle 20 und Abbildung 18:**

Die Absicherung der Beziehungen zu den Kooperationspartnern ergibt sich hauptsächlich aus der Gestaltung der Kooperationsverträge.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	Kooperationsvertrag	249	40,29
2	Wechselseitige Kapitalbeteiligung	22	3,56
3	Klare Absprachen über Informations- und Verwertungsrechte	145	23,46
4	Überprüfung der jeweiligen Leistungsbeiträge	41	6,64
5	Regelmäßige Abstimmungen über Arbeitsfortschritte und eventuelle Probleme	107	17,31
6	Den Partnern werden eigene Sicherheitsstandards vorgegeben	21	3,40
7	Durchführung von Sicherheits-Audits	16	2,59
8	<i>Optional</i>	17	2,75
<b>gesamt</b>		<b>618</b>	<b>100,00</b>

**Tabelle 20:**

Antworten zur Frage 17 „Wie sind die Beziehungen zu Kooperationspartnern abgesichert?“



**Abbildung 18:**

Graphische Auswertung der Antwortmöglichkeiten zur Frage 17

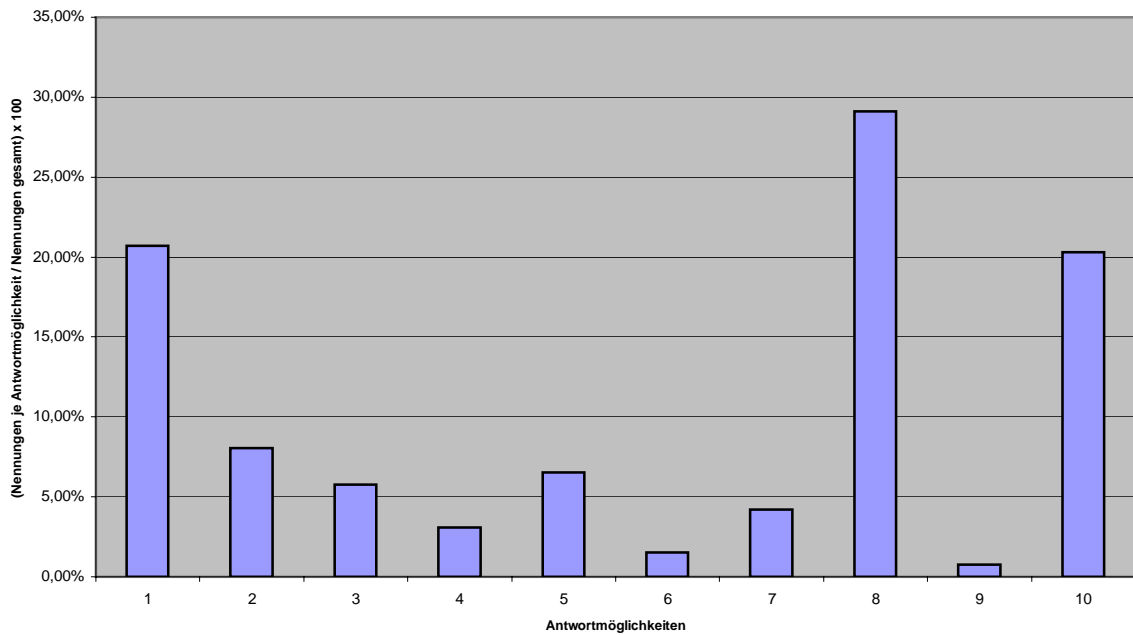
**Zu Tabelle 21 und Abbildung 19:**

Offensichtlich im Nachhinein wurde bei abgeworbenen/abgewanderten Mitarbeitern deutlich geäußerte Unzufriedenheit registriert.

Antwortmöglichkeiten	Bezeichnung	Nennungen	Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent
1	Deutlich geäußerte Unzufriedenheit	54	20,69
2	Arbeitsengagement trotz oder nach geäußelter Unzufriedenheit	21	8,05
3	Auffällige Verbesserung der finanziellen Situation	15	5,75
4	Unerklärlich konspiratives Verhalten	8	3,07
5	Dubiose Kontakte	17	6,51
6	Auffälligkeiten im Lebenslauf	4	1,53
7	Anzeichen für Bestechlichkeit	11	4,21
8	Abnehmende Identifizierung mit dem Unternehmen	76	29,11
9	Besitz von Spionagehilfsmitteln	2	0,77
10	<i>Optional</i>	53	20,31
<b>gesamt</b>		<b>261</b>	<b>100,00</b>

**Tabelle 21:**

**Antworten zur Frage 18 „Gab es bei abgeworbenen/abgewanderten Mitarbeitern Anzeichen für die Illoyalität?“**



**Abbildung 19:**

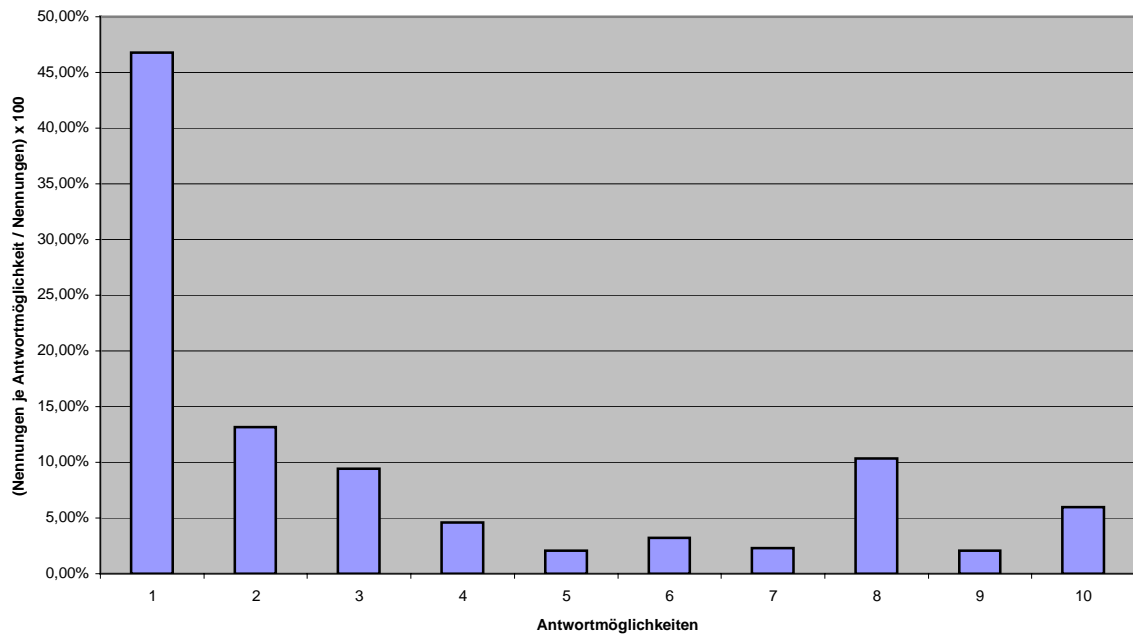
**Graphische Auswertung der Antwortmöglichkeiten zur Frage 18**

**Zu Tabelle 22 und Abbildung 20**

Knapp die Hälfte der Antworten besagt, dass die Arbeit der Sicherheitsbehörden zum Informationsschutz weitgehend unbekannt ist und wird möglicherweise deshalb „auch als nicht benötigt“ bewertet.

<b>Antwort- möglichkeiten</b>	<b>Bezeichnung</b>	<b>Nennungen</b>	<b>Nennungen je Antwortmöglichkeit Nennungen gesamt in Prozent</b>
1	Arbeit der Sicherheitsbehörden zu Informationsschutz ist weitgehend unbekannt und wird auch nicht benötigt	203	46,77
2	Arbeit der Sicherheitsbehörden zu Informationsschutz ist weitgehend unbekannt, würde aber gebraucht	57	13,13
3	Ansprechpartner bei den Sicherheitsbehörden sind bekannt	41	9,45
4	Es bestehen regelmäßige Informations-/Arbeitskontakte mit den Sicherheitsbehörden	20	4,61
5	Es besteht ein umfassendes, mit den Sicherheitsbehörden abgestimmtes Sicherheitskonzept	9	2,07
6	Die Arbeit der Sicherheitsbehörden ist nicht wirksam genug	14	3,24
7	Die Zuständigkeiten für die verschiedenen Probleme des Informationsabflusses sind nicht klar genug geregelt	10	2,30
8	Es bedarf einer schärferen arbeits- und wettbewerbsrechtlichen Regelung für den Schutz vor unlauterem Informationsabfluss	45	10,37
9	Öffentliche Auftraggeber nehmen wettbewerbsrechtliche Probleme des Informationsschutzes nicht ernst genug	9	2,07
10	<i>Optional</i> Welche Maßnahmen der Sicherheitsbehörden hielten Sie für wünschenswert?	26	5,99
<b>gesamt</b>		<b>434</b>	<b>100,00</b>

**Tabelle 22:**  
**Antworten zur Frage 19 „Wie ist die Einschätzung der Arbeit der/Kooperation mit den Sicherheitsbehörden?“**



**Abbildung 20:**  
**Graphische Auswertung der Antwortmöglichkeiten zur Frage 19**

## **4.2 Nach verschiedenen Aspekten strukturierte Auswertung der Fragebögen**

### **4.2.1 Allgemeine Ergebnisse**

#### **4.2.1.1 Repräsentativität und Charakteristik der Stichprobe**

Das Gesamtergebnis ist mit 431 Rückläufen, davon mit 400 brauchbaren Antworten, repräsentativ und mit einer Quote von ca. 16% der versendeten Fragebögen tragfähig. Die Umsatzdaten zeigen: Der gewogene Gesamtwert der Umsätze von 400 Unternehmen beträgt gut 29 Milliarden €. Die stärkste Einzelgruppe nach Fallzahlen sind die Unternehmen mit einem Jahresumsatz von 2 bis 10 Millionen €. Für die großen Unternehmen (über 500 Millionen € Umsatz) wurde als hypothetische (die Skala ist nach oben offen) Klassenmitte 1 Mrd. € angenommen.

Die Erhebung ist nach Umfang und Struktur repräsentativ für die Industrie sowohl in Baden-Württemberg als auch grundsätzlich für die Bundesrepublik Deutschland. Knapp 30% der in die Untersuchung einbezogenen baden-württembergischen Unternehmen bieten ein Massenprodukt an, 65% haben eine Einzel- oder Kleinserienfertigung; eine nur regionale Marktstellung haben etwa ein Sechstel der Firmen, mehr als drei Viertel haben eine nationale oder internationale Marktstellung. Für die Bundesrepublik insgesamt ist jedoch mit einer etwas größeren Streuung zu rechnen, weil die Industriestruktur Baden-Württembergs zwar im Prinzip repräsentativ für die BRD ist, aber doch Abweichungen existieren.

Mit dem ermittelten Umsatzvolumen wurden etwa 10% des Bruttoinlandsprodukts des Landes Baden-Württemberg erfasst, d.h. die vorzustellenden Befunde sind bei Umrechnung auf das Land etwa mit 10 zu multiplizieren; das ist sinnvoll und zulässig, weil die Erhebung eine repräsentative Auswahl des gesamten Landes umfasste. Bei einer Hochrechnung auf die gesamte Bundesrepublik Deutschland – Baden-Württemberg hat etwa 15% des Bruttoinlandsprodukts der Bundesrepublik – müsste man die Werte noch einmal mit 7 multiplizieren; hier wäre aber eine vorsichtiger Hochrechnung angemessen, weil nicht alle anderen Bundesländer eine solche Industriestruktur aufweisen.

Der Wettbewerbsvorteil oder -vorsprung beruht in vielen Fällen auf mehreren Faktoren, im Durchschnitt werden 3,5 Faktoren genannt. Der mit Abstand bedeutendste Faktor ist der Kundenstamm oder die Kundenbeziehung, danach etwa gleichauf der Mitarbeiterstamm und die Beherrschung bestimmter Verfahren und Arbeitsmethoden. Erst danach kommen die am ehesten von Wirtschaftsspionage gefährdeten Faktoren „Überlegene Produkte“ und „Neue Produkte“ und mit noch größerem Abstand „Forschungspotenzial und -ergebnisse“. Das bedeutet, dass die Frage nach dem Verlust von Wettbewerbsvorteilen durch Informationsabfluss immer in dem Dreieck „Kundenkooperation – Mitarbeiter – Konkurrenz“ betrachtet werden muss, was nachfolgend noch differenziert erfolgt.

Die Bedeutung von Kooperation mit den Kunden und zwischen den Mitarbeitern wird auch bei der Entstehung des Wettbewerbsvorteils sichtbar: „Gewachsen aus dauerhafter Zusammenarbeit „und „Gemeinsame Idee mehrerer Personen“ sind mit insgesamt 45% die wichtigsten Faktoren, danach „Gemeinsame Idee mit Kunden“, „Strategische Investition in innovative Geschäftsfelder“ und „Marktbeobachtung“ mit insgesamt 40%.

#### 4.2.1.2 Ausmaß der Gefährdung

Die Aufwendungen für den Wettbewerbsvorteil haben nur 347 Unternehmen in € beziffern können, dabei betragen diese Aufwendungen bei den meisten Firmen unter 500.000 €, aber immerhin bei 46 der Firmen auch über 5 Millionen €. Das gewogene Gesamtergebnis beträgt für die 347 Unternehmen 630 Millionen € und wenn man diesen Wert auf die Zahl der beteiligten Unternehmen umrechnet 730 Millionen €<sup>46, 47</sup>. Der von den Unternehmen genannte Wert des Wettbewerbsvorteils entspricht ziemlich genau den angegebenen Aufwendungen, nämlich 634 Millionen € für die 369 gemachten Angaben und 687 Millionen € für die hochgerechnete Zahl von 400 Unternehmen.<sup>48</sup> Das bedeutet, man kann den Wert des Wettbewerbsvorteils, d.h. die gefährdete Substanz für die Erhebungsgruppe auf 700 Millionen € ansetzen, das sind 2,3% vom Umsatz.

Für das Land Baden-Württemberg beträgt das **Gefährdungspotenzial**<sup>49</sup> dann 7 Milliarden € pro Jahr und für die Bundesrepublik Deutschland insgesamt rund 50 Milliarden € pro Jahr. Damit liegt - erstmalig – ein empirisch abgesicherter Wert für das Gefährdungspotenzial vor, siehe dazu auch Abbildung 21.

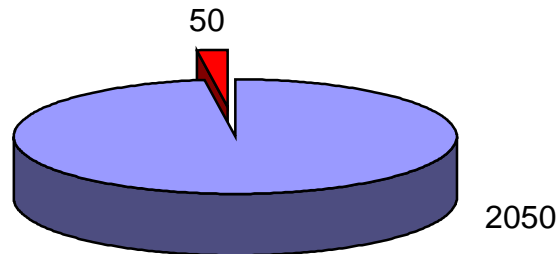
---

<sup>46</sup> Die gewogenen Ergebnisse werden wie folgt ermittelt: Summe über die Klassen (Fallzahl pro Klasse \* Wert der Klassenmitte).

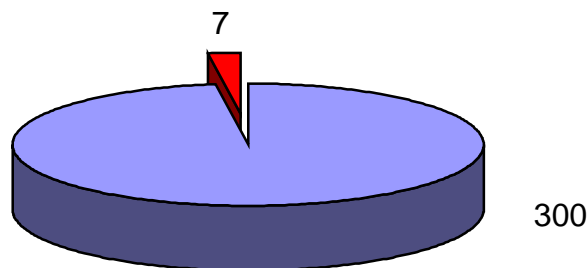
<sup>47</sup> Die Standardabweichung beträgt hier  $\sigma = 1,733$  Mio. €

<sup>48</sup> Die Standardabweichung beträgt hier  $\sigma = 1,681$  Mio. €

<sup>49</sup> Siehe dazu die Definition unter 3.2.



■ BIP Bundesrepublik Deutschland zu Marktpreisen 2002 ohne Gefährdungspotenzial  
■ hochgerechnetes Gefährdungspotenzial Bundesrepublik Deutschland



■ BIP Baden-Württemberg zu Marktpreisen 2002 ohne Gefährdungspotenzial  
■ hochgerechnetes Gefährdungspotenzial Baden Württemberg

**Abbildung 21:**  
**Gefährdungspotenziale berechnet auf der Basis folgender gerundeter Werte in Milliarden €**

BIP Baden-Württemberg zu Marktpreisen 2002 = rund 307 Mrd. €<sup>50</sup>

Anteil des BIP Baden-Württemberg zu Marktpreisen 2002 am BIP Bundesrepublik Deutschland gesamt (2100 Mrd. €) in Prozent = 14,6%<sup>51</sup>

Hochgerechnete Umsätze 2002 aus den 400 verwertbaren Fragebögen rund 30 Mrd. €

Hochgerechneter Wert des Wettbewerbsvorteils 2002 = rund 700 Mio. €

Anteil des Wettbewerbsvorteils an den hochgerechneten Umsätzen in Baden-Württemberg in Prozent = 2,3%

Hochgerechnetes Gefährdungspotenzial Baden-Württemberg = rund 7 Mrd. €

Hochgerechnetes Gefährdungspotenzial Bundesrepublik = rund 50 Mrd. €

<sup>50</sup> Quelle: [www.statistik-bw.de/Veroeffentl/Statistische\\_Berichte/4165\\_02001.pdf](http://www.statistik-bw.de/Veroeffentl/Statistische_Berichte/4165_02001.pdf)

<sup>51</sup> Quelle: [www.statistik-bw.de/Veroeffentl/Statistische\\_Berichte/4165\\_02001.pdf](http://www.statistik-bw.de/Veroeffentl/Statistische_Berichte/4165_02001.pdf)

Bezüglich der Schutzbedürftigkeit des Wettbewerbsvorteils und der vorgenommenen Maßnahmen ist insgesamt bei drei Viertel der Betroffenen Imitierbarkeit oder Nachahmbarkeit gegeben, einen Patent- oder Gebrauchsmusterschutz hat nur ein Viertel aller Unternehmen, fast ein Drittel ist nicht geschützt und die übrigen verweisen auf organisatorisch-kulturelle Eigenschaften des Vorteils, die so nicht geschützt werden müssen. Der Wettbewerbsvorsprung beträgt zeitlich bei der Hälfte der Unternehmen ein Jahr, bei einem weiteren Drittel bis zu 5 Jahre.

Die angefragten Sicherungsmaßnahmen gegen Informationsverluste werden in sehr unterschiedlicher Weise eingesetzt. Hier werden im Detail nach verschiedenen Zusatzaspekten klarere Tendenzen zu erkennen sein. **Die Aufwendungen für Informationssicherheit sind im Vergleich zum Gefährdungspotenzial sehr gering**; zwei Drittel aller befragten Unternehmen geben weniger als 50000 € pro Jahr aus. Die gewogene Summe beträgt für alle 400 Unternehmen 32 Millionen €, also weniger als 5% der Gefährdungssumme. Dem seien die Verluste gegenübergestellt, die bei den aufgetretenen 190 Fällen von Informationsverlusten angefallen sind: die gewogene Gesamtsumme beträgt 52 Millionen €, hochgerechnet auf die 400 sind das 110 Millionen €. Die tatsächlichen Schäden dürften sich demnach für Baden-Württemberg auf etwa 1 Milliarde € belaufen, für die Bundesrepublik Deutschland etwa 7 bis 8 Milliarden €. Auch dieser Wert für tatsächlich entstandene Schäden ist durch seine empirische Absicherung besonders bedeutsam.

Das bedeutet, dass die tatsächlichen Verluste etwa drei Mal so hoch sind, wie die Schutzvorkehrungen kosten. Bei der Verteilung der Schadenshöhe wird auch sichtbar, dass die Kleinschäden zwar die größte Einzelzahl ausmachen, dass aber die Verteilung nach oben deutlich höher verläuft als bei den Sicherheitsausgaben.

Das ist um so erstaunlicher, als nur etwa 30% aller Befragten angeben, noch nicht Objekt eines „unfreundlichen Informationsabflusses“ gewesen zu sein; anders ausgedrückt, mehr als zwei Drittel aller Unternehmen war schon einmal betroffen, wobei manchmal auch nur vage Verdachtsmomente bestehen. Ein Interesse an dem Wettbewerbsvorteil wird sowohl im Inland wie im Ausland gesehen, wobei jedoch den ausländischen staatlichen Organen kaum Bedeutung zugemessen wird. Ungetreue Kooperationspartner und abgewanderte Mitarbeiter machen aber fast die Hälfte aller Fälle aus; dabei ist der dahinter stehende potenzielle Konkurrenzinfluss nicht immer sichtbar.

#### **4.2.1.3 Geographische Verteilung von Wissensabfluss**

Die geographische Verteilung möglicher Interessenten an dem Wettbewerbsvorsprung bzw. möglicher Ausspähungen ist sehr unterschiedlich. Bei den möglichen Interessenten sind 19 aus Fernost, 46 aus Europa, 21 aus USA, Kanada und Israel und 11 global. Bei möglicher Ausspähung sind es 53 aus Fernost, 127 aus Europa, 48 aus Amerika und 14 global. Die Fallzahlen sind hier höher, die strukturelle Verteilung etwa gleich. Bei konkreten Fallzahlen sind es aus Fernost 4, aus Europa 9, aus Amerika 2 und global 4.

Bei tatsächlichem Informationsabfluss sind die staatlichen Organe 4 Mal aus dem (ehemaligen) Ostblock und einmal Spanien genannt. Bei tatsächlicher Ausspähung durch ausländische Konkurrenz wird 9 Mal Fernost genannt, 27 Mal Europa und 5 Mal die USA. Innerhalb der statistischen Streubreite ist das Verteilungsmuster relativ stabil, mit etwa 20% Fernost und 50% und mehr aus Europa. Beachtlich ist, dass Italien innerhalb Europas am häufigsten genannt wird.

#### **4.2.1.4 Schadensbearbeitung und Kooperation mit den Sicherheitsbehörden**

Eine Bearbeitung des Schadensfalles erfolgte in knapp der Hälfte der Fälle überhaupt nicht, nur insgesamt 8% der aufgetretenen Fälle wurden mit externen Sicherheitsberatern oder mit Sicherheitsbehörden bearbeitet. Hier liegt Handlungsbedarf!

Als Folge des Schadensfalls wurden vor allem juristische, personelle und organisatorische Maßnahmen getroffen, technische deutlich weniger.

Die Befunde zu Verdachtsmomenten, Beziehungen zu Kooperationspartnern und Illoyalitätsanzeichen bei abgeworbenen Mitarbeitern werden im Detail mit Zusatzaspekten strukturiert.

Die Einschätzung der Arbeit der Sicherheitsbehörden bzw. die Kooperation mit ihnen zeigt ebenfalls deutlichen Handlungsbedarf: Knapp der Hälfte der Befragten ist die Arbeit der Sicherheitsbehörden nicht bekannt und sie hält sie auch für unnötig. Immerhin 13% kennen sie zwar nicht, würden sie aber benötigen. Nur in knapp 10% der Fälle sind die Ansprechpartner bei den Sicherheitsbehörden bekannt und davon die Hälfte hat regelmäßige Informations- und Arbeitskontakte. Ein umfassendes, mit den Sicherheitsbehörden abgestimmtes Sicherheitskonzept haben ganze 2%!

Die Wirksamkeit der Sicherheitsbehörden wird von 3% als nicht hinreichend angesehen, 2% bemängeln unklare Zuständigkeitsregelungen. Sehr viel mehr Unternehmen sehen einen zu schwachen arbeits- und wettbewerbsrechtlichen Schutz, während eine zu schwache wettbewerbsrechtliche Aufmerksamkeit öffentlicher Auftraggeber nur 2% sehen.

Im Einzelnen werden in den nachfolgenden Punkten verschiedene Maßnahmen vorgeschlagen. Erste Erkenntnis: am meisten fehlt es an Information !

## **4.2.2 Einzelne Einflussfaktoren und Verknüpfungen**

### **4.2.2.1 Größenabhängige Wirkungen**

Kleinere Unternehmen sind eher Einzel- und Kleinserienfertiger mit regionaler Bedeutung, größere haben eher auch Massenprodukte und internationale Bedeutung mit entsprechender internationaler Gefährdung. Bei der Art des Wettbewerbsvorsprungs sind Produktüberlegenheit und Strategie mit zunehmender Größe wichtig, ähnliches gilt – aber auf niedrigem Niveau – für Vertriebssystem und Forschungspotenzial. Demgegenüber sind neue Produkte vor allem für die mittleren Betriebsgrößen

von besonderer Bedeutung und Netzwerke und Unternehmenskultur für ganz Kleine und ganz Große mehr als in der Mitte.

Das lässt sich mit der Art der Entstehung der Vorteile verknüpfen<sup>52</sup>: Bei kleineren Unternehmen mit einem Umsatz bis 50 Mio. € ist häufig eine Person der Ideengeber des Wettbewerbsvorteils, bei einem Teil mittelgroßer Unternehmen mit einem Umsatz zwischen 50 und 200 Mio. € sind meistens mehrere interne Personen; teilweise in Verbindung mit Fremdforschung, beteiligt. Bei größeren und großen Unternehmen ist der Wettbewerbsvorteil überwiegend durch das Vorhandensein einer oder mehrerer Abteilungen sowie strategischer Investitionen in innovative Entwicklungen gewachsen. Unter Sicherheitsaspekten bedeutet das, dass bei Beteiligung mehrerer Personen oder Abteilungen das Risiko, das die zugehörige Kommunikation abgehört wird oder dass andere Formen des Informationsabflusses erfolgen größer ist, als wenn eine Person allein eine Idee erarbeitet. Die Aufwendungen für den Wettbewerbsvorteil und der Wert des Wettbewerbsvorteils steigen – natürlich – mit der Größe; aber es geben auch 40% der Firmen bis 2 Mio. € Umsatz mehr als 500000 € für den Wettbewerbsvorteil aus, davon sogar 4% mehr als 3 Mio. €. Hier muss für die Beratung und Information darauf hingewiesen werden, dass das Risiko in den Fällen mit hohen Aufwendungen bzw. Werten des Wettbewerbsvorsprungs besonders hoch ist. Das sollte ein Feld für eine intensive Aufklärung und Beratung sein.

Die Schutzwürdigkeit des Vorteils nimmt mit der Größe zu. Internationale Patente und Umgehungspatente sind für die Großen bedeutsamer, nationale Patente mehr für mittlere Unternehmen. Direkt auf den Wettbewerbsvorteil bezogene Sicherheitsmaßnahmen sind insgesamt unbedeutend.

Bei den vorhandenen Sicherheitsmaßnahmen besteht ein klares Größengefälle: Die ersten fünf Punkte (Eingangskontrolle, Zugangsbeschränkungen, Zugriffsbeschränkungen, Datenschutz, Sicherheitskopien) werden bei Großen zu 100% angewandt und sinken bei Kleinen auf z.T. sehr niedrige Werte wie 23 oder 27%<sup>53</sup>. Die für die Sicherheitsbehörden besonders wichtigen Aspekte wie Geheimschutzverfahren, Sicherheitskonzept, Zusammenarbeit mit Sicherheitsbehörden und Sicherheitsschulung sind nur bei großen Unternehmen relevant. Das korreliert auch mit den Ausgaben für Sicherheit: Außer den ganz großen Unternehmen geben 90 % aller Unternehmen weniger als 100000 € im Jahr für Informationssicherheit aus; das ist in den meisten Fällen weniger als 1 % des Umsatzes, im Durchschnitt sogar nur 0,1 % des Umsatzes.<sup>54</sup>

Das Gefährdungspotenzial wird durch die Unternehmen unterschiedlich eingeschätzt, die Bedrohung durch einen inländischen Konkurrenten nimmt mit der Größe ab, die durch einen ausländischen

---

<sup>52</sup> Die Berechnungen zu den Verknüpfungen sind im Projektbericht vom 3. September 2003 enthalten und können beim Auftraggeber eingesehen werden.

<sup>53</sup> Der Korrelationskoeffizient „r“ ist beispielsweise für die Eingangskontrolle „r = 0,75“, für die Zugangsbeschränkungen „r = 0,92“.

<sup>54</sup> Die Ausgaben unter 50000 € korrelieren mit der Größe der Unternehmen mit „r = -0,89“ und die der über 500000 € mit „r = 0,97“.

Konkurrenten wird in der Mitte am stärksten empfunden. Die Bedrohung durch mehrere Konkurrenten nimmt mit der Größe zu und zwar mehr bei ausländischen als bei inländischen. Staatliche Institutionen und Wissenshändler werden nur wenig als Bedrohung gesehen.

Der tatsächliche Informationsabfluss nimmt mit der Größe zu; ausländische staatliche Organe sind nur von großen Unternehmen bemerkt worden; der negative Abfluss nimmt mit der Größe zu, wobei die inländische Konkurrenz bedeutsamer ist als die ausländische. Ungetreue Kooperationspartner und Mitarbeiter gibt es in allen Größenklassen, wobei die Mitarbeiter die größere Bedrohung sind. Beachtenswert ist, dass vor allem große Unternehmen einen Abfluss durch Unbekannte und vage Verdachtsmomente in erheblichem Umfang sehen, der Anteil steigt hier auf bis zu 50%. Zusammen mit dem erkannten Tätigwerden staatlicher ausländischer Organe zeigt sich hier doch ein Aufklärungs- und Handlungsbedarf. Die Höhe der Schäden folgt hier der Unternehmensgröße.

Im Umgang mit dem Schaden ist auch eine größenspezifische Tendenz zu erkennen: „Keine Bearbeitung“ nimmt mit der Größe ab (Große machen immer eine Schadensbearbeitung), eine „Zusammenarbeit mit Sicherheitsbehörden“ ist insgesamt schwach ausgeprägt, nimmt aber mit der Größe zu. Bei den ergriffenen Sicherheitsmaßnahmen gibt es eine schwache Tendenz zur Zunahme mit der Größe; nur personelle Maßnahmen sind auch bei kleineren Unternehmen stärker vertreten.

Bei den Verdachtsmomenten für eine Ausspähung sind die Tendenzen unterschiedlich, so dass eine generelle Aussage über betriebsinterne Verdachtsgründe nicht getroffen werden kann; wichtiger, aber ohne größenbezogene Differenzierung, sind die außerbetrieblichen Verdachtsgründe wie Auftauchen von Teilinformationen bei Wettbewerbern, Unerklärliche Auftragverluste oder Auftauchen von günstigen Konkurrenzangeboten.

Die Absicherung von Kooperationsbeziehungen erfolgt über Verträge, über klare Absprachen und regelmäßige Abstimmungen; diese drei Sicherungsverfahren werden mit zunehmender Größe zunehmend genutzt und sind alle sehr wichtig. Kapitalbeteiligung wird nur von kleinen bis mittleren Unternehmen als hilfreich angesehen, hat aber auch dort nachrangige Bedeutung.

**Sicherheitsaudits**<sup>55</sup> sind insgesamt weniger üblich, nehmen aber auch mit der Größe zu. Die Illoyalitätsanzeichen bei Abwanderung von Mitarbeitern haben insgesamt nur mäßige bis geringe Bedeutung und sind nicht größenabhängig.

Die Zufriedenheit mit der Arbeit der Sicherheitsbehörden bzw. die Kooperation mit ihnen ist demgegenüber klar größendifferenziert. Während bei den kleineren und mittleren Unternehmen (bis 200 Mio. €) etwa die Hälfte die Arbeit nicht kennt und auch nicht für nötig hält, ist der Anteil dieser Meinung bei den großen nur noch 20% oder weniger. Nicht bekannt, aber für nötig halten die Arbeit der Sicherheitsbehörden immerhin 25 bis 40% der Unternehmen von 50 bis 500 Mio. Dass die noch größeren eine relativ geringe Quote bei dieser Antwort haben, ist dadurch zu erklären, dass diese in

---

<sup>55</sup> s. Ergänzende Literaturhinweise: Thoenissen, Michael: Erfolgversprechender Audit-Aufbau, KES Nr. 6, 2002, S. 65-68

mehr als der Hälfte der Fälle ihre Ansprechpartner kennen und in fast 40% der Fälle regelmäßige Informationskontakte haben. Deswegen konnten sie bei „Nicht bekannt,...“ auch passen. Dass Ansprechpartner bekannt sind, regelmäßige Informationskontakte bestehen oder bemängelt wird, dass Zuständigkeiten nicht klar genug geregelt seien, wird mit zunehmender Größe häufiger bekundet. Umfassende Sicherheitskonzepte gibt es erst ab 200 Mio. € Umsatz.

Der Wunsch nach schärferen wettbewerbs- oder arbeitsrechtlichen Regeln ist wenig ausgeprägt und ohne Größendifferenz; Kritik an der Nichtbeachtung wettbewerbsrechtlicher Regeln durch öffentliche Auftraggeber kommt im Wesentlichen von kleineren Unternehmen, aber insgesamt sehr wenig. Wünschenswerte Maßnahmen werden sehr verschiedene genannt, aber nicht von den großen Unternehmen, die scheinen mit der Arbeit der Sicherheitsbehörden zufrieden zu sein.

Am häufigsten tritt dabei der Wunsch nach mehr Informationen auf, z.B. in Fachzeitschriften, über mögliche Zusammenarbeit, über Aktivitäten, Leitfäden, Vertragsmuster. Andere wünschen zusätzliche Lösungen z.B. über EDV oder ein Leumundszeugnis, ein schnelleres Eingreifen des Staates bei Nachbau und Patentverletzungen, ein Sicherheitscheck für Unternehmen nach einer „Sterne“-Klassifikation, eine Anlaufstelle für Betroffene und mehr Zusammenarbeit zwischen staatlichen Stellen und der Wirtschaft. Eine dritte Ebene wird angesprochen bei dem Wunsch nach mehr Informationen durch die Staatsanwaltschaft über den Stand von entsprechenden Ermittlungen und eine Verbesserung der rechtlichen Auflösung des Konflikts zwischen Datenschutz und Datensicherheit.

#### **4.2.2.2 Marktstellung**

Die Marktstellung – regional, national oder international – variiert mit der Größe, aber nicht sehr ausgeprägt; 70% der Firmen, die nationale Geltung beanspruchen und 50 der international orientierten sind klein, d.h. bis 10 Millionen € Umsatz. Überlegene Produkte, neue Produkte und Forschungspotenzial sind um so wichtiger, je weiter das Verbreitungsgebiet; demgegenüber sind Maschinenausstattung, Mitarbeiterstamm, Kundenstamm, Lieferantenbeziehungen, organisatorische Vorteile und Netzwerke eher regional bedeutsam. Daraus lässt sich schließen, dass die ersten drei Arten von Wettbewerbsvorsprung vor allem ausländischer Konkurrenz und/oder Spionage ausgesetzt sind. Mit der Verbreitung steigt auch der Aufwand für den Wettbewerbsvorsprung und dessen Wert.

Die Nutzung von Patenten und Gebrauchsmustern steigt mit der Verbreitung und zwar sowohl die nationalen als auch die internationalen Patente; Umgehungspatente werden nur von Unternehmen mit internationaler Verbreitung genutzt. Die Sicherungsmaßnahmen differenzieren nur wenig nach der Marktstellung, außer bei der Teilnahme an Geheimschutzverfahren, der Existenz eines Sicherheitsverantwortlichen und der Zusammenarbeit mit den Sicherheitsbehörden, die bei Unternehmen mit internationaler Geltung größer ist. Das liegt auch daran, dass diese teilweise von Amts wegen einbezogen werden. Damit einher geht auch ein Zuwachs der Sicherheitsaufwendungen bei weiterer Verbreitung der Unternehmen.

Bei den potentiellen Interessenten gibt es keine Differenzierung nach der Marktstellung, wohl aber beim tatsächlichen unfreundlichen Informationsabfluss. Mit der Verbreitung der Unternehmen nimmt

die Betroffenheit allgemein zu und insbesondere die durch ausländische Organe, durch ausländische Konkurrenz, durch Unbekannte und vage Verdachtsmomente. Alle zusammen machen bei international tätigen Unternehmen immerhin 41% aller Unternehmen aus. Die dabei auftretenden Schäden nehmen ebenfalls zu und die Intensität der Schadensbearbeitung.

Als typische Verdachtsmomente sind zunehmend mit der Verbreitung das Auftauchen von Teilinformationen und von günstigen Konkurrenzangeboten zu sehen; nicht erklärbarer Verlust von Aufträgen nimmt hingegen mit der Verbreitung ab.

Unternehmen mit internationaler Geltung sehen eher einen Bedarf an Informationen über und Kooperation mit den Sicherheitsbehörden. 30% dieser Firmen sehen einen Handlungsbedarf bei der Kooperation.

#### **4.2.2.3 Typen des Wettbewerbsvorteils**

Bei der Verknüpfung der drei Typen von Wettbewerbsvorteilen durch Bündelung der Teilfragen – produkt- und verfahrensbezogen, externe Faktoren und interne Faktoren – mit anderen Aspekten zeigt sich, dass die Überlegenheit von Produkten und Verfahren mit der Marktverbreitung an Bedeutung zunimmt, während die externen Faktoren vor allem national von Bedeutung sind und zwar besonders bei Einzel- und Kleinserienfertigung bei starker Konkurrenz. Die internen Faktoren sind am wichtigsten bei oligopolistischen Strukturen.

Bei der Entstehung des Wettbewerbsvorteils haben die verschiedenen Typen einige Unterschiede: Produkt- und Verfahrensüberlegenheit entsteht am ehesten durch mehrere Personen in der Unternehmung, dann aus dauerhafter Kooperation und auf dem dritten Platz aus Zusammenarbeit mit Kunden. Bei den externen Faktoren ist die Reihenfolge zwischen Platz 1 und 2 vertauscht, während bei den internen Faktoren auf dem dritten Platz die Kunden von der strategischen Investition in innovative Bereiche verdrängt werden. Dem entspricht auch der Schutz durch Patente und Gebrauchsmuster, der bei Produkt- und Verfahrensüberlegenheit deutlich ausgeprägter ist als bei den anderen beiden Typen.

Das Wissensinteresse gibt wenig Differenzierung, jedoch sind ausländische staatliche Institutionen und Konkurrenten bei Produktüberlegenheit etwas mehr genannt als in den anderen Fällen. Der tatsächliche Informationsabfluss wurde am meisten bei Produkt- und Verfahrensüberlegenheit bemerkt und zwar durch ausländische Konkurrenten.

Die Absicherung von Kooperationsbeziehungen erfolgt bei Produkt- und Verfahrensüberlegenheit mehr durch Vertrag, Absprachen und regelmäßige Abstimmungen als bei den beiden anderen Typen.

#### **4.2.2.4 Entstehung des Wettbewerbsvorteils**

Bei der Verknüpfung des externen Faktors der Wettbewerbstypen mit der Entstehung durch gemeinsame Idee mit Kunden, dauerhafte Kooperation oder Marktbeobachtung zeigt sich, dass die

dauerhafte Kooperation bei kleinen Unternehmen wichtiger ist, die anderen beiden eher bei großen. Kundenstamm und Lieferantenbeziehungen sind für Kooperationen am wichtigsten, die Marktbeobachtung dann, wenn das Vertriebssystem der Überlegenheitsfaktor ist.

Gemeinsame Ideen von Unternehmen und Kunden sind besonders imitierbar und werden am häufigsten durch Patente und Gebrauchsmuster geschützt, Kooperationsvorteile bedürfen dieser am wenigsten. Die Schutzmechanismen „Spezialinvestitionen“, „Arbeitsorganisation“ und „Unternehmenskultur“ wirken besonders bei der Entstehung des Vorteils durch Marktbeobachtung, der erste am wenigsten bei Kooperationsvorteilen, die anderen beiden am wenigsten bei Vorteilen aus gemeinsamen Ideen.

Die Gefährdung durch einen oder mehrere Konkurrenten wird am stärksten bei Vorteilen aus Marktbeobachtung empfunden, bei einem werden die Ideen, bei mehreren die Kooperationsvorteile als am wenigsten gefährdet gesehen. Staatliche Stellen werden nur bei Vorteilen aus gemeinsamen Ideen als relevant angesehen.

Die Absicherung der Kooperation ergibt den überraschenden Befund, dass alle Sicherheitsinstrumente zur Absicherung bei Vorteilen aus Kooperation deutlich unterausgeprägt sind. Das gilt auch für die Kooperation mit bzw. Kenntnis über die Sicherheitsbehörden, aber es werden hier mehr wettbewerbs- und arbeitsrechtliche Konsequenzen eingefordert.

#### **4.2.2.5 Quellen unfreundlichen Informationsabflusses**

Hier wurden vier Gruppen gebildet: Mitarbeiter (135), Kooperationspartner (64), inländische Konkurrenz (80) und Ausland einschließlich Unbekannte und vage Verdachtsmomente (107)

Hier zeigt sich eine deutliche Betonung des Auslands bei Unternehmen mit internationaler Verbreitung und mit Einzel- und Kleinserienfertigung im Oligopol. Das Ausland ist auch am stärksten bei großen Unternehmen als Quelle genannt und bei kleinen deutlich weniger.

Die Differenzierung nach Art des Wettbewerbsvorteils zeigt nur bei den überlegenen Produkten einen bedeutsamen Anteil des Auslands (2. Platz), alle anderen Wettbewerbsvorteile sind vor allem durch inländische Konkurrenz oder durch Kooperationspartner am stärksten gefährdet, soweit überhaupt eine Differenzierung möglich ist. Auch bei der Entstehung des Wettbewerbsvorteils werden die Inländische Konkurrenz und Kooperationspartner deutlich als gefährlicher empfunden. Wenn jedoch der Aufwand für und der Wert des Wettbewerbsvorteils sehr hoch ist, dann steigt die Gefahr durch ausländische Institutionen erheblich. Weiterhin ergibt sich als wichtiger Hinweis, dass nationale Patente vor allem durch ausländische Konkurrenz gefährdet sind, daneben auch durch Kooperationspartner.

Bei den Sicherungsmaßnahmen gibt es nur wenige klare Unterschiede: Bei Gefährdung durch ausländische Konkurrenz ist die Zusammenarbeit mit den Sicherheitsbehörden häufiger und es erfolgt auch mehr Schulung in Schutzmaßnahmen. Es wird bei Konkurrenzgefährdung (In- und Ausland) auch mehr für Informationssicherheit ausgegeben. Tendenziell ist man also auf dem richtigen Wege.

Die Arbeit der Sicherheitsbehörden wird nach diesen Kriterien sehr differenziert beurteilt. „Unbekannt“ und „unnötig“ ist deutlich höher bei Mitarbeiter- und Kooperationsgefährdung als bei Konkurrenzgefährdung, dabei ist Auslandsgefährdung noch einmal deutlich niedriger. Ebenso ist der Bedarf trotz fehlender Kenntnis der Arbeit bei Auslandsgefährdung am höchsten, hier aber zusammen mit der Kooperationsgefährdung. Ebenso sind Ansprechpartner bei Konkurrenzgefährdung, vor allem aus dem Ausland, bekannter und auch regelmäßige Informationskontakte und umfassende abgestimmte Konzepte finden sich am häufigsten bei Auslandsgefährdung. Das bedeutet, dass die auslandsgefährdeten Unternehmen schon sehr viel mehr über die Arbeit der Sicherheitsbehörden wissen und mit ihnen kooperieren, dass aber auch dort noch erhebliche unbearbeitete Felder sind: 36% sagen, Arbeit ist unbekannt und unnötig, 21% haben Bedarf, kennen sie aber nicht, nur in 14% der Fälle sind Ansprechpartner bekannt, regelmäßige Kontakte und umfassende Konzepte liegen zwischen 5 und 10%.

#### **4.2.2.6 Schadensbearbeitung und Sicherungsmaßnahmen**

Es wurden die Gruppen „keine Schadensbearbeitung“, „mit innerbetrieblichen Kräften“, „mit externen Sicherheitsberatern“, „mit Sicherheitsbehörden“ und „Schwachstellenanalyse“ gebildet, wobei die Gruppen mit externen Beratern und mit Sicherheitsbehörden sehr klein und damit statistisch kaum aussagefähig sind. Die Art der Schadensbearbeitung korrespondiert deutlich mit den ermittelten Schwächen in den Sicherungsmaßnahmen, dort wo eine Schadensbearbeitung – welcher Art auch immer – erfolgt, ist die relative Anwendung von Sicherheitsmaßnahmen deutlich höher.

Die „Gar nicht Bearbeiter“ haben am seltensten eine Eingangskontrolle oder Zugangsbeschränkungen, betreiben die geringsten Zugriffsbeschränkungen für Daten und Datenschutz. Sie sind nie in das amtliche Geheimschutzverfahren eingebunden. Sie haben am seltensten ein Sicherheitskonzept oder wenden bei der Personalarbeit Sicherheitsaspekte an oder schulen das Personal in Informationsverlustschutz. Auch Geheimhaltungsklauseln kommen am seltensten vor, wenn auch auf hohem Niveau. Fremdes Personal wird selten in Sicherheitsüberlegungen einbezogen.

In den nicht aufgeführten Punkten entsprechen die Anteile denen, die bei der Schwachstellenanalyse vorliegen, die den zweitschwächsten Platz bei den meisten Punkten aufweist.

Die Zahlen bei externen Sicherheitsberatern und Sicherheitsbehörden sind wegen der kleinen Anzahl nur bedingt aussagefähig; allerdings sind sie in der Tendenz deutlich höher als bei den anderen Aspekten. Als Schlussfolgerung lässt sich daraus ableiten, dass die Zusammenarbeit mit externen Sicherheitsberatern oder den Sicherheitsbehörden zu einem höheren Sicherheitsbewusstsein verhilft und dass dann auch mehr geeignete Sicherheitsmaßnahmen ergriffen werden.

## 5 Gefährdungspotenziale und Handlungsempfehlungen

### 5.1 Gefährdungspotenziale

Als Ergebnis lässt sich feststellen, dass ein erhebliches Gefährdungspotenzial vorliegt, das für Baden-Württemberg etwa 7 Milliarden € und für Deutschland insgesamt etwa 50 Milliarden € ausmacht.

Dabei ist darauf hinzuweisen, dass vor allem kleine Unternehmen mit einem erheblichen Wettbewerbsvorteil überproportional gefährdet sind. Die Aufwendungen für Sicherheitsmaßnahmen betragen nur 0,1% des Umsatzes und nur etwa 1/3 des Werts der aufgetretenen Schäden. Schon einzelbetrieblich lohnt sich also ein Mehraufwand für Sicherheit.

Von Bedeutung ist, dass ein erheblicher Teil der Schäden und Probleme aus Fehlverhalten von Mitarbeitern und Kooperationspartnern entstehen, die hier nicht im Vordergrund der Betrachtung stehen. Für die Analyse der Wirkungen ausländischer Konkurrenzspionage und eventueller Schutzmaßnahmen sind spezifische Arten der Wettbewerbsvorteile und die Faktoren Unternehmensgröße und Marktverbreitung einzubeziehen; dort gibt es dann deutlich abweichende Schadensbilder. Bei den hier erhobenen Schadensgrößen sind nur direkte Schäden angesprochen; besonders bei Fällen von Produkt- oder Markenpiraterie kommen noch zusätzliche Imageschäden hinzu, weil den (potenziellen) Kunden durch minderwertige Plagiate ein falsches Qualitätsbild übermittelt wird.

Ein allgemeiner Handlungsbedarf ergibt sich aus dem Befund, dass nur etwa 8% der Unternehmen entweder mit einem externen Sicherheitsberater oder mit Sicherheitsbehörden die aufgetretenen Schadensfälle bearbeitet haben. Die Arbeit der Sicherheitsbehörden ist knapp der Hälfte der Unternehmen unbekannt und sie hält sie auch nicht für nötig (eine etwas befremdliche Sichtweise); immerhin hat aber gut 1/7 der Unternehmen trotz fehlender Kenntnis dieser Arbeit einen Bedarf an ihr. In den Zusatzantworten war vor allem ein Bedarf an Information erkennbar.

Wenn auch in kleinen Zahlen, so ist doch von einer nicht vernachlässigbaren Zahl die Wirksamkeit der Arbeit der Sicherheitsbehörden oder unklare Zuständigkeitsregelungen bemängelt worden. 24 Nennungen dieser Art sind nicht alarmierend, aber doch ein Hinweis, dass in Fällen des Informationsabflusses vielleicht nicht immer optimal vorgegangen wird.

Ganz deutlich sind die Größenunterschiede bezüglich Sicherheitsbewusstsein und entsprechenden Maßnahmen zu erkennen. Bei den kleinen und mittleren Unternehmen tut sich da ein großes „Schwarzes Loch“ auf. Größere Unternehmen sehen die Gefahren mehr und sehen auch größere Gefahren als die kleinen, obwohl gerade kleine Unternehmen mit einem relativ großen Wettbewerbsvorteil geradezu existenziell gefährdet sind.

Als Folge davon sollten die allgemeine Informationsstrategie und die Maßnahmen zur Erhöhung des Sicherheitsbewusstseins, deren Notwendigkeit sich aus den Zahlen zum Gefährdungspotenzial, zu den

Schäden und zu den Schutzvorkehrungen ergibt, größenabhängig strukturiert werden. Dabei sind die verschiedenen genannten Items in den Zusatzantworten zu Frage 19 zu berücksichtigen.

Für die konkrete Sicherheitspolitik von Unternehmen müssen diejenigen im Vordergrund stehen, die besonders spionagegefährdet sind, d.h. diejenigen, deren Wettbewerbsvorteil auf überlegenen Produkten, neuen Produkten und Forschungspotenzial beruht und die eine internationale Geltung haben oder anstreben; sie haben oft eine Einzel- oder Kleinserienfertigung und stehen in einem oligopolistischen Wettbewerb. Die Produkt-/Verfahrensüberlegenheit führt zu deutlich höherer Gefahr und auch zu mehr und größeren Schäden; damit geht eine intensivere Aufklärungs- bzw. Schadensbearbeitung einher. Viele Unternehmen mit dieser Gefährdungslage sind sich der Problematik bewusst und machen auch deutlich mehr als der Durchschnitt; sie wissen mehr über die Lage und über die Möglichkeiten der Sicherheitsbehörden und kooperieren auch mehr mit den Behörden. Trotzdem besteht hier noch erheblicher Handlungsbedarf, weil noch längst nicht alle, die gefährdet sind, sich dessen bewusst sind und entsprechend reagieren. Mehr als die Hälfte auch der durch Auslandskonkurrenz gefährdeten Unternehmen kennen die Arbeit der Sicherheitsbehörden nicht, weniger als 10% haben regelmäßige Kontakte oder umfassende Konzepte.

Die überwiegende Haltung ist nach wie vor, Schäden gar nicht zu bearbeiten und keine Sicherheitsmaßnahmen zu ergreifen. Die präventive Vorgehensweise ist bisher noch die Ausnahme und man sollte daran arbeiten, dass sie zur Regel wird.

## **5.2 Präventionsmaßnahmen im Einzelnen**

### **5.2.1 Sicherheit braucht ein Konzept und ist Managementaufgabe**

Wesentliche Erkenntnisse sowohl aus den Interviews, den Befragungen der Unternehmen und der Diskussion mit Mitgliedern des Sicherheitsforums Baden-Württemberg lassen sich wie folgt pragmatisch zusammenfassen:

- Konzeptlos auf dem Gebiet der Sicherheit ist kopflos
- Aus Schaden wird man klug/Informationen schützen ist klüger
- Sicherheit ist Managementaufgabe
- Wettbewerbsvorteile müssen gesichert und erhalten werden
- Innovationen und Informationen sind zu schützen

Eine existenzielle Schlussfolgerung sowohl für Unternehmen als auch für die Sicherheitsbehörden daraus ist: Informationen sind unser Kapital.

Aus den vorliegenden Befunden, nämlich

- Existenz eines erheblichen Gefährdungspotenzials
- Geringes Sicherheitsbewusstsein und wenige Sicherheitsmaßnahmen bei KMU
- Differenzierte Situation der Gefährdung von Wettbewerbsvorteilen

lassen sich die nachfolgenden Aufgaben für die Arbeit auf dem Gebiet der Sicherheit ableiten:

- Wissen um die Risiken ist die Voraussetzung, um für Maßnahmen zum Schutz gegen diese Risiken zu ergreifen
- Schutzbedürftigkeit ist für jedes einzelne Unternehmen zu ermitteln
- Bedrohungen sind zu analysieren
- Risiken müssen bewertet werden
- Informationsschutzkonzepte sind zu entwickeln, zu implementieren und fortzuschreiben

Ergo: Prävention ist erforderlich. „Sinn und Zweck der Prävention ist es, durch sorgfältig aufeinander abgestimmte personelle und organisatorische, technisch/bauliche und rechtliche Schutzmaßnahmen den Eintritt potenzieller Risiken zu verhindern oder wenigstens zu minimieren“<sup>56</sup>. Der Weg dazu sind komplexe Informationsschutzkonzepte:

#### **personelle Maßnahmen**

- Sensibilisierung durch Schulung
- Periodische Awareness-Kampagnen/ Preisausschreiben/ Bildschirmschoner/Plakataktionen/ Infostände/give aways
- Personaldiagnostik durch eigene Mitarbeiter und Externe

#### **organisatorische Maßnahmen**

- Kontrollsysteme/-mechanismen (vier Augen Prinzip)
- Verbindliche Sicherheitsgrundsätze und -standards (codices)
- Direkte Anbindung an die Managementebene
- Geregelte Entsorgung (Schriftstücke, CD, Festplatte)
- Fotografierverbot einschließlich Fotohandys

#### **technische/bauliche Maßnahmen**

- Zugangsberechtigungen (Firmenausweise und Einlasskontrolle)
- Betriebsinterne Sicherheitsinseln (DV, Forschung, Vorstand/Geschäftsführung)
- Räumliche Sicherheit/Schließsystem für Schreibtische, Schränke, Archive
- Vorrang/Optimierung der organisatorischen Maßnahmen vor technischem Einsatz
- IT-Sicherheit durch effizienten Passwortschutz, Netzwerksicherheit (Firewall, W-LAN Problematik), Protokollierungsverfahren, Softwaremanipulationen

#### **rechtliche Maßnahmen**

- Patent-/Gebrauchsmusterschutz
- Geheimhaltungs- und Wettbewerbsklauseln für Mitarbeiter während und nach dem Arbeitsverhältnis sowie für Fremdfirmen

---

<sup>56</sup> Verfassungsschutzbericht Baden-Württemberg 2001, Hsg. Innenministerium Baden-Württemberg, Mai 2002, S. 225.

### 5.2.2 Entwicklung einer „Wissensbilanz“ oder „Informationsinventur“

Um den Schutz vor Beeinträchtigungen von Rechten und Gütern in Unternehmen zu gewährleisten, werden Informationen benötigt. Diese Informationen beziehen sich auf die Rechte und Güter selbst, d.h. man muss überhaupt erst einmal wissen, was an Rechten und Gütern vorhanden ist, und man muss die Möglichkeiten der Beeinträchtigung kennen, die sich immer wieder – auch gerade durch neue Formen der Informationstechnologie – ändern. Eine Aufstellung und ständige Aktualisierung aller Wissensbestände/Informationen in den Unternehmen nach dem Prinzip „Know how, Know who“ ist eine Voraussetzung des Schutzes von Informationen. Der Schutz der Informationen bezieht sich auf vier Aspekte:

- Sicherung der Vertraulichkeit (Schutz vor Einblick)
- Sicherung der Daten vor Verfälschung (Verbindlichkeit)
- Sicherung der richtigen Datenherkunft (Authentizität und Integrität)
- Sicherung der Verfügbarkeit<sup>57</sup>

Empfohlen wird dazu den Sicherheitsbehörden die Entwicklung eines Erfassungsbogens für die Gefährdungstatbestände insbesondere der Wirtschaftsspionage in Unternehmen und deren regelmäßige Auswertung durch das Sicherheitsforum des Landes Baden-Württemberg (Was könnte gefährdet sein? Wer könnte spionieren? Wie kann man das sichern?).

### 5.2.3 Entwicklung eines Handhabungsschemas für Risikomanagement

An dieser Stelle wird empfohlen, die Dissertationsschrift von Sitt zum Thema Entwicklung eines „Dynamischen Risiko-Managements“ unter Berücksichtigung von „Nicht-Markt Risiken“<sup>58</sup> für die Entwicklung eines Handhabungsschemas zugrunde zu legen.

In dieser Arbeit werden unter anderen folgende Schritte zur Entwicklung und Durchsetzung eines Risiko-Management-Systems herausgearbeitet.

#### **Erster Schritt:** Vorgaben der Unternehmensleitung

- Voraussetzung für den Erfolg eines Risiko-Managements ist die deutliche Signalisierung, dass die Unternehmensführung dem Thema verpflichtet ist.

#### **Zweiter Schritt:** Erstellung des Risiko-Portfolios

- Nach der Fixierung der Vorgaben erfolgt zwingend eine Inventur der Risiken, diese besteht aus den Teilschritten Identifikation und Bewertung der Risiken, Zuordnung der Gegenmaßnahmen sowie Analyse der Kontrollen

---

<sup>57</sup> Kahle, Egbert: Security-Management unter HR- und Organisationsaspekten, Personalführung, Nr. 5 2002. S. 22ff.

<sup>58</sup> Sitt, Axel: Dynamisches Risikomanagement, Deutscher Universitäts-Verlag, Wiesbaden 2003, S. 29ff.

**Dritter Schritt:** Festlegung der Eskalationskriterien und des Berichtswesens

- Eskalationskriterien sind vorher definierte Schwellenwerte im Verlauf des Risiko-Management-Prozesses, bei deren Über- oder Unterschreitung eine Eskalation des Sachverhaltes unterstellt wird. Eine Eskalation kann in diesem Zusammenhang die reine Information von Vorgesetzten sein, die Übertragung der Verantwortung auf eine höhere Ebene oder auf eine tatsächliche Reaktion.

**Vierter Schritt:** Integration des Risiko-Managements in die Steuerungsprozesse

- Hierzu gehört u. a. die Erarbeitung von Leitlinien, Maßnahmen und Regeln.

**Fünfter Schritt:** Risiko-Controlling

Die fünf genannten Schritte sind eine wesentliche Voraussetzung zur Risiko-Reduktion in den Unternehmen.

#### **5.2.4 Entwicklung von fachrichtungsübergreifenden Schulungsmaßnahmen für Mitarbeiter der Sicherheitsbehörden und für die Sicherheitsverantwortlichen in den Unternehmen**

Die generelle und durchgängige Verwirklichung eines Sicherheitsmanagements in Behörden und Unternehmen verlangt eine gezielte und aufeinander abgestimmte Weiterbildung sowohl der Mitarbeiter der Sicherheitsbehörden als der Sicherheitsverantwortlichen in den Unternehmen. Als Weg dazu wurde von der Universität Lüneburg ein Weiterbildungsstudiengang Security Management u. a. mit Unterstützung des Landesamtes für Verfassungsschutz des Landes Baden-Württemberg entwickelt, der sich gegenwärtig in der Diskussion befindet. Anfragen und Voranmeldungen auch aus Baden-Württemberg zu diesem durch die Diskussion bekannt gewordenen Studiengang liegen dem Zentrum für Wissenschaftliche Weiterbildung der Universität Lüneburg bereits vor.

Nachfolgend dazu der bisher erreichte Stand:

- Programmskizze für ein Verbundprogramm „Wissenschaftliche Weiterbildung Security Management“:

##### **1. Gegenstand**

Der Weiterbildungsstudiengang Strategisches Management mit dem Schwerpunkt Security Management (kurz Security Management) mit dem Abschluss MBA – ist über vier Semester konzipiert, verläuft berufsbegleitend und ist modular aufgebaut.

##### **2. Wissenschaftliche Leitung**

Die wissenschaftliche Verantwortung und Leitung des Studiengangs trägt der Fachbereich Wirtschafts- und Sozialwissenschaften der Universität Lüneburg, Lehrstuhl Recht insbesondere Wirtschafts- und Umweltrecht.

### 3. Organisation, Koordinierung und Durchführung

Verantwortlich dafür ist das ZWW (Zentrum für Wissenschaftliche Weiterbildung) der Universität Lüneburg.

### 4. Verbund

Im Sinne gemeinsamer Weiterbildungsangebote von Hochschule und Wirtschaft werden mehrere Universitäten, Landesämter, Arbeitskreise und auch Unternehmen in die Weiterbildung einbezogen. Jeder Partner wird sich mit einem seiner Qualifikation entsprechenden Modulanteil einbringen. Die Weiterbildung wird länderübergreifend und in einem effizienten Verbund erfolgen.

Die Gesamtübersicht über den bisher dazu erreichten Stand befindet sich im Anhang.

#### 5.2.5 Entwicklung unternehmensspezifischer Präventionsmaßnahmen

Unternehmensspezifische Präventionsmaßnahmen verlangen unternehmensspezifische Analysen und Untersuchungen. Hierzu sollten die Potenziale der sich mit diesen Fragen befassenden Universitäten und Hochschulen genutzt werden. Als Beispiel dazu wird die Diplomarbeit von Hartmann zum Thema Risikomanagement als Führungsaufgabe von Unternehmen (Studiengang Betriebswirtschaftslehre der Universität Lüneburg, 2002)<sup>59</sup> vorgestellt.

Ausgangspunkt der Diplomarbeit sind Risikomanagement und KonTraG. Es folgen Ausführungen zur Organisation des betrieblichen Risikomanagements einschließlich einer Abgrenzung des Krisenmanagements vom Risikomanagement. Der Abschluss sind vertiefende Betrachtungen ausgewählter Risiken wie das Lieferisiko, Managementrisiken als Ausprägungsform des Risikos der Wirtschaftskriminalität sowie Risiken durch Electronic-Commerce.

Den Unternehmen sollte über das Sicherheitsforum empfohlen werden, sicherheitsrelevante unternehmensspezifische Themen als Haus- oder Diplomarbeiten auf der Grundlage von Vereinbarungen mit Universitäten und Hochschulen zu vergeben.

#### 5.2.6 Weiterführende Empfehlungen

Ausgangspunkt hierfür ist die Frage: „Was tun, wenn trotz aller Präventionsmaßnahmen Schadensfälle auftreten?“

Hierzu wird empfohlen,

- umgehend mit dem Landesamt für Verfassungsschutz Baden-Württemberg Verbindung aufzunehmen um gemeinsam die eigenen Prozesse nach den **Vorgaben des Regelkreises der Prävention** zu überprüfen,
- professionelle externe Unterstützung durch Mitglieder des Sicherheitsforums des Landes Baden-Württemberg einzuholen.

---

<sup>59</sup> Hartmann, Sebastian: Risikomanagement als Führungsaufgabe von Unternehmen, Wissenschaftliche Arbeitsberichte des ZWW zum Security Management, Lüneburg 2003.

Dem Sicherheitsforum wird als weitere Maßnahme empfohlen, die **Sicherheitsstruktur des Landes Baden-Württemberg** pyramidenförmig und durchgängig zu gestalten (Sicherheitsforum als Spitze der Pyramide). Das Sicherheitsforum übernimmt hierbei die Rolle eines **Security-Council** als Kopf regelmäßig durchzuführender, „erweiterter“ **Sicherheitsforen** mit Unternehmen, Einrichtungen und Behörden u. a. mit dem Ziel der **Verstärkung der Öffentlichkeitsarbeit**. **Der Auftragnehmer bietet an**, seine vorhandenen Erfahrungen in der Vorbereitung und Organisation bundesweiter Sicherheitsforen einzubringen.

Ein Weg der besseren Einbeziehung der Unternehmen, Einrichtungen und Behörden sollten künftig **regelmäßige Unternehmensbefragungen** à la WIK-Enquête werden.

Komplexe einer derartigen ersten Unternehmensbefragung könnten die bisher im Abschnitt 5.2 genannten „Präventionsmaßnahmen im Einzelnen“ sein.

Da ein hoher Anteil der festgestellten und analysierten Schadensursachen den Charakter wirtschaftskrimineller Handlungen trägt, wird an dieser Stelle auf eine Studie aus Niedersachsen zu diesem Komplex verwiesen, deren Vorschläge zur Prävention auf Anforderungen der Unternehmen an Politik und Institutionen zulaufen und voll übernehmbar sind:

„Anforderungen der Unternehmen an Politik und Institutionen

- Strafverfolgung verstärken, mehr Abschreckung, Strafen erhöhen
- Gesetze verbessern bzw. anpassen
- Mehr und mehr qualifizierte Ermittlungspersonal
- Schnellere Prozessabläufe, Bürokratie abbauen
- Konsequenter Verfolgung und Bestrafung von Bagatelldelikten
- Harmonisierung internationaler Gesetze, internationale Strafverfolgung
- Politik muss ihrer Vorbildfunktion besser gerecht werden
- Bessere Informationspolitik zuständiger Behörden und Institutionen
- Verbesserung der Rechtslage von Unternehmen im Zusammenhang mit Kündigungen
- Bessere Vernetzung und Kommunikation zwischen Betrieben und Institutionen
- Unterstützung bei der Entwicklung von Kontroll- und Sicherheitskonzepten
- Aufklärungs- und Öffentlichkeitsarbeit durch Institutionen“<sup>60</sup>

Abschließend wird empfohlen künftig die aktuellen **Grundsätze für geheimsschutzbetreute Betriebe** schrittweise und differenziert nach Schutzwürdigkeit auf alle Unternehmen und Einrichtungen des Landes Baden-Württemberg anzuwenden.

---

<sup>60</sup> Rolfes, M.; Wilmes, K.: Wirtschaftskriminalität in Niedersachsen 2003. Betroffenheit und Bewertung aus der Sicht niedersächsischer Unternehmen (Studie). Universität Osnabrück, 14. November 2003, S. 23.

## Quellen und weiterführende Literaturhinweise

- Akerlof, G. A.: The Market for „Lemons“: Quality Uncertainty and the Market Mechanism, Quarterly Journal of Economics, vol. 89, 1970
- ASW-Sicherheitsforum 2001 „Schutz der deutschen Wirtschaft vor globaler Kriminalität“, Berlin 2001, [www.asw-online.de](http://www.asw-online.de)
- Bamberg, G. - Coenenberg, A. G.: Betriebswirtschaftliche Entscheidungslehre, 7. Auflage, München 1992
- Bewacherrecht: Verschärfte Vorschriften für die Sicherheitsbranche, UNSERE WIRTSCHAFT; Nr. 10/2002, [www.ihk24-lueneburg.de](http://www.ihk24-lueneburg.de)
- Biometrische Verfahren – eine Chance für mehr Sicherheit und besseren Datenschutz?, forum kriminalprävention, Nr. 3 2003, Verlag Deutsche Polizeiliteratur GmbH, [www.forum-kriminalprävention.de](http://www.forum-kriminalprävention.de)
- Bockslaff, Klaus: Notfallplanung, Kern eines ganzheitlichen Risikomanagements, WIK, Nr. 2 2002 SecuMedia Verlags-GmbH Ingelheim, [www.wik.info/wik/news](http://www.wik.info/wik/news)
- Bouncken, R. B.: Organisationale Metakompetenzen, Wiesbaden 2002, Kahle, E., Strategischer Wissenstransfer als Erfolgsfaktor bei KMU, in: Pleitner, H. J.; Weber, W. (Hrsg.), Die KMU im 21. Jahrhundert – Impulse, Aussichten, Konzepte, St. Gallen 2000
- Brauner, E.; Becker, A.: Controlling als transaktives Wissenssystem, Beitrag zur Tagung der Kommission Wissenschaftstheorie in Berlin, 2000; Klages, K., Knowing who-..., a.a.ao.
- Chen, C. C.; Chen, X.; Meindl, J. R.: How can Cooperation be Fostered ? The Cultural effects of Individualism – Collectivism, in: Academy of Management Review, vo. 23 no. 2, 1998
- Cox, Peter: Schutzschild gegen Spam, KES, Nr. 1 2003, SecuMedia Verlags-GmbH Ingelheim, [www.kes.info](http://www.kes.info)
- Das Niedersächsische Datenschutzgesetz, Der Landesbeauftragte für den Datenschutz Niedersachsen, Hannover 2001
- Datenschutz in der BOSCH-Gruppe, Stuttgart
- Der Dokumententresor für Ihre vertraulichen Unterlagen, Brainloop Secure Dataroom, München, 2003, [www.brainloop.com](http://www.brainloop.com)
- Dixit, A. K.; Nalebuff, B. J.: Thinking Strategically – The competitive Edge in Business, Politics and Everyday Life, New Vork – London 1993
- Donner, Hartwig (Universität Lüneburg, Präsident); Kaden, Ulrich: Sicherheit in der Wirtschaft unter europäischer Perspektive: Nach Europarecht mögliche Formen der polizeilichen Zusammenarbeit, Wissenschaftliche Arbeitsberichte des ZWW der Universität Lüneburg 12/2002, [www.uni-lueneburg.de/einricht/zww/wabzww](http://www.uni-lueneburg.de/einricht/zww/wabzww)
- Fischer, Derk; Mohs, Joachim: Hacker auch im Mittelstand – Wirtschaftskriminalität mit Hilfe der IT, PriceWaterhouseCoopers, Frankfurt am Main, November 2002, [www.pwcglobal.com/de/ger/main/home/index.html](http://www.pwcglobal.com/de/ger/main/home/index.html)
- Fischer, S.: Virtuelle Unternehmen im interkulturellen Austausch – Möglichkeiten und Grenzen von Kooperationen in Netzwerken, Wiesbaden 2001

Geheimhaltungshandbuch, Informationen für geheimhaltungsbetonte Unternehmen, 2003

Gerke, Wolfgang: Das Pflichtenheft des Risikomanagements, Frankfurter Allgemeine Zeitung, Nr. 98, 28.04.2003, [www.faz.net/s/homepage.html](http://www.faz.net/s/homepage.html)

Güldenbergh, S.: Wissensmanagement und Wissenscontrolling in lernenden Organisationen: ein systemorientierter Ansatz, Wiesbaden 1997

Hammes, Michael: Prävention wirtschaftskrimineller Handlungen, WIK, Nr. 5 2002, SecuMedia Verlags-GmbH Ingelheim, [www.wik.info/wik/news](http://www.wik.info/wik/news)

Hänsgen, Matthias: Auch Risikomanagement-Systeme brauchen Schutz, WIK, Nr. 7 2003 SecuMedia Verlags-GmbH Ingelheim, [www.wik.info/wik/news](http://www.wik.info/wik/news)

Hartmann, Sebastian: Risikomanagement als Führungsaufgabe von Unternehmen, Wissenschaftliche Arbeitsberichte des ZWW zum Security Management, Lüneburg 2003, [www.uni-lueneburg.de/zww/wabzww](http://www.uni-lueneburg.de/zww/wabzww)

Heil, Artur: Panikmache oder akute Bedrohung?, KES, Nr. 5 2002, SecuMedia Verlags-GmbH Ingelheim, [www.kes.info](http://www.kes.info)

Herrmann, Jürgen: Integrierte Managementsysteme, WIK, Nr. 7 2003 SecuMedia Verlags-GmbH Ingelheim, [www.wik.info/wik/news](http://www.wik.info/wik/news)

Hugo, Jürgen: Unternehmensschutz im Umbruch, WIK, Nr. 6 2002 SecuMedia Verlags-GmbH Ingelheim, [www.wik.info/wik/news](http://www.wik.info/wik/news)

Ihre Verantwortung für unsere Sicherheit – Über den Umgang mit vertraulichen Informationen, Bundesamt für Verfassungsschutz, Köln 2002

Indikatorenbericht zur technologischen Leistungsfähigkeit Deutschlands, Zentrum für Europäische Wirtschaftsforschung GmbH, [www.zew.de](http://www.zew.de)

Informationsschutz bei ABB – Kommunizieren und Schweigen, Mannheim 2000

Informationsschutz: Leitfaden für Mitarbeiter der BOSCH-Gruppe, Stuttgart 1999

IT-Security kompakt, CEFIS (CeBIT 2003), KES, Nr. 1 2003, SecuMedia Verlags-GmbH Ingelheim, [www.kes.info](http://www.kes.info)

Jost, P. J.: Theoretische Grundlagen der Spieltheorie in: Jost, P. J., (Hrsg.), Die Spieltheorie in der Betriebswirtschaftslehre, Stuttgart 2001

Kahle, E.: Betriebliche Entscheidungen, 6. Auflage München – Wien 2001

Kahle, E.: Betriebswirtschaftliches Problemlösungsverhalten, Wiesbaden 1973

Kahle, E.: Security-Management unter HR- und Organisationsaspekten, in: Personalführung, 5/2002; Sitt, A., Dynamisches Risiko-Management – Zum unternehmerischen Umgang mit Risiken, Wiesbaden 2003

Kahle, E.: Vertrauensbasierte Netzwerke als Chancen für kleine und mittlere Unternehmen, in: Pleitner, H. J., (Hrsg.), Beiträge zu den Rencontres 1998, St. Gallen 1998; ders.; Kooperation und Vertrauen in Organisationen, in: Fischer, A.,(Hrsg.), Arbeit und Bildung im wirtschaftlichen und sozialen Wandel“, Lüneburg 1999; ders., Vertrauen als Voraussetzung für bestimmte Formen des Wandels, in: Brauchlin, E. – Pichler, H.J. (Hrsg.), Unternehmer und Unternehmensperspektiven für Klein- und Mittelunternehmen, Berlin – St. Gallen, 2000; ders. Virtuelle Organisationen unter besonderer Berücksichtigung kultureller Barrieren, in: Scholz, CH. (Hrsg.), Systemdenken und

- Virtualisierung – Unternehmensstrategien zur Vitalisierung und Virtualisierung auf der Grundlage von Systemtheorie und Kybernetik, Berlin 2002
- Kahle, Egbert (Universität Lüneburg, Dekan des Fachbereichs Wirtschafts- und Sozialwissenschaften): Entscheidungs- und organisationstheoretische Grundlagen des Security Managements in Unternehmen, Wissenschaftliche Arbeitsberichte des ZWW der Universität Lüneburg 12/2002, [www.uni-lueneburg.de/einricht/zww/wabzww](http://www.uni-lueneburg.de/einricht/zww/wabzww)
- Klages, K.: Knowing who- Auswirkungen von Transactive Memory Systems auf und in unterschiedlichen Organisationsformen, Aachen 2003
- Konferenzmaterial des ZWW der Universität Lüneburg: 1. Lüneburger Sicherheitsforum für die Wirtschaft, Wirtschaftsspionage und Korruption, 26. Juli 2000, [www.uni-lueneburg.de/zww/sicherheitsforum/sfprogramm00.htm](http://www.uni-lueneburg.de/zww/sicherheitsforum/sfprogramm00.htm)
- Konferenzmaterial des ZWW der Universität Lüneburg: 2. Lüneburger Sicherheitsforum für die Wirtschaft, Gefahr für Unternehmen durch Euro-Kriminalität, 20. Juni 2001, [www.uni-lueneburg.de/zww/sicherheitsforum/sfprogramm01.htm](http://www.uni-lueneburg.de/zww/sicherheitsforum/sfprogramm01.htm)
- Konferenzmaterial des ZWW der Universität Lüneburg: 3. Lüneburger Sicherheitsforum für die Wirtschaft, Unternehmen und Terrorismus, 19. Juni 2002, [www.uni-lueneburg.de/zww/sicherheitsforum/sfprogramm02.htm](http://www.uni-lueneburg.de/zww/sicherheitsforum/sfprogramm02.htm)
- Konferenzmaterial des ZWW der Universität Lüneburg: 4. Lüneburger Sicherheitsforum für die Wirtschaft, Notfall- und Krisenmanagement im Katastrophenfall - mit Empfehlungen für die Wirtschaft, 18. Juni 2003, [www.uni-lueneburg.de/zww/sicherheitsforum/sfprogramm03.htm](http://www.uni-lueneburg.de/zww/sicherheitsforum/sfprogramm03.htm)
- Krause, Alexander: Die Überprüfung des Personals auf Zuverlässigkeit, WIK, Nr. 5 2002, SecuMedia Verlags-GmbH Ingelheim, [www.wik.info/wik/news](http://www.wik.info/wik/news)
- Kriminalität in den Bundesländern: Zahl der Straftaten stieg erneut, WIK, Nr. 2 2003, SecuMedia Verlags-GmbH Ingelheim, [www.wik.info/wik/news](http://www.wik.info/wik/news)
- Leiner, Klaus-G.: Dem Mitbewerber keine Blöße zeigen, WIK, Nr. 6 2002 SecuMedia Verlags-GmbH Ingelheim, [www.wik.info/wik/news](http://www.wik.info/wik/news)
- Luhmann, N.: Vertrauen – Ein Mechanismus der Reduktion sozialer Komplexität, 3. Auflage Stuttgart 1989
- Meding, Dietmar: Innentäter außen vor, KES, Nr. 5 2002, SecuMedia Verlags-GmbH Ingelheim, [www.kes.info](http://www.kes.info)
- Mintzberg, H.: The Structuring of Organizations, Englewood Cliffs N. J., 1979
- Mitarbeiter sind für IT-Sicherheit gefährlicher als Viren, Financial Times Deutschland, 06.03.2003, [www.ftd.de](http://www.ftd.de)
- Neumann, J.; Morgenstern, O.: Spieltheorie und wirtschaftliches Verhalten, Würzburg 1961; Müller-Merbach, H., Operations Research, 3. Auflage München 1973
- Nonaka, I.; Boisiere, R.; Borucki, C. C.; Konno, N.: Organizational Knowledge Creation Theory: A First Comprehensive Test, in: International Business Review 3(4), 1994
- Nonaka, I.; Taguechi, K: The Knowledge Crating Company, New York 1995
- Pautzke, G.: Die Evolution der organisationalen Wissensbasis: Bausteine einer Theorie des organisationalen Lernens, Herrsching 1989

- Picot, A.; Dietl, H.; Franck, H.: Organisation – eine ökonomische Perspektive, 3. Auflage Stuttgart 2002
- Polanyi, M.: The Tacit Dimension, London 1966
- Prävention durch Technik, forum kriminalprävention, Nr. 3 2003, Verlag Deutsche Polizeiliteratur GmbH, [www.forum-kriminalprävention.de](http://www.forum-kriminalprävention.de)
- Proliferation – das geht uns an!, Bundesamt für Verfassungsschutz, Köln 2001
- Rannacher, Helmut: Verfassungsschutz schaltet „Vertrauliches Telefon“, Magazin Wirtschaft, IHK Region Stuttgart, Nr. 2/99
- Rebhäuser, J.; Krcmar, H.: Wissensmanagement in Unternehmen, in: Schreyögg, G.C.P. (Hrsg.), Wissensmanagement, Berlin- New York 1996
- Rechtsvorschriften zum Geheimschutz, CD-ROM, Bundesamt für Verfassungsschutz, Köln 2002
- Rolfes, M.; Wilmes, K.: Wirtschaftskriminalität in Niedersachsen 2003. Betroffenheit und Bewertung aus der Sicht niedersächsischer Unternehmen (Studie). Universität Osnabrück, 14. November 2003.
- Sackmann, S.: Culture and Sub-Cultures: An Analysis of Organizational Knowledge, in: Administrative Science Quarterly, 32 (1) 1992
- SAP Security Policy, Version 0.60, SAP AG Juli 2003, [www.sap-ag.de](http://www.sap-ag.de)
- Schäffter, Markus: IT-Entscheider in der Verantwortung, KES, Nr. 4 2002, SecuMedia Verlags-GmbH Ingelheim, [www.kes.info](http://www.kes.info)
- Schams, E.: Komparative Statik, in: Zeitschrift für Nationalökonomie Band 2, 1931
- Schmidt, Eike Ingwer (Verwaltungsgericht Stade, Präsident): Der Beitrag der gesetzgebenden staatlichen Gewalt zur Sicherheit der Wirtschaft durch einfach- gesetzliche Regelungen auf nationaler Ebene, Wissenschaftliche Arbeitsberichte des ZWW der Universität Lüneburg 12/2002, [www.uni-lueneburg.de/einricht/zww/wabzww](http://www.uni-lueneburg.de/einricht/zww/wabzww)
- Schmitt, Michael: Tiger Teams – Hacker mit weißer Weste, WIK, Nr. 5 2002, SecuMedia Verlags-GmbH Ingelheim, [www.wik.info/wik/news](http://www.wik.info/wik/news)
- Schneider, E.: Einführung in die Wirtschaftstheorie, Band 2, 11. Auflage, Tübingen 1967; zu einem anders definierten dynamischen Risikokzept vgl. Sitt, A.
- Schreyögg, G. C. P.: Organisationales Lernen und neues Wissen: Einige Kommentare und einige Antworten zum Wissenmanagement aus wissenschaftstheoretischer Sicht, in: Kommission Wissenschaftstheorie im Verband der Hochschullehrer für Betriebswirtschaft (Hrsg.), Innovation in der Betriebswirtschaftslehre, Wiesbaden 1998
- Schutz vor Spionage – Ein praktischer Leitfaden für die gewerbliche Wirtschaft, Landesamt für Verfassungsschutz Baden-Württemberg, Stuttgart 1999
- Schutzmaßnahmen gegen illegales Abhören, Bundesamt für Sicherheit in der Informationstechnik, [www.bsi.bund.de](http://www.bsi.bund.de)
- Schweigler, Berthold: Kriminalität belastet Wirtschaft direkt und indirekt, WIK, Nr. 7 2003 SecuMedia Verlags-GmbH Ingelheim, [www.wik.info/wik/news](http://www.wik.info/wik/news)
- Sicherheit in der Wirtschaft, Studie mit Abhandlungen zum Thema aus verschiedenen Blickwinkeln als Grundlage eines modular aufgebauten Bildungskonzepts mit präventivem Ansatz zur

- Zusammenarbeit von Polizei und Wirtschaft, Universität Lüneburg, Zentrum für Wissenschaftliche Weiterbildung, 12/2000, [www.uni-lueneburg.de/zww/sicherheitsforum](http://www.uni-lueneburg.de/zww/sicherheitsforum)
- Sitt, Axel: Dynamisches Risikomanagement, Deutscher Universitäts-Verlag, Wiesbaden 2003
- Sitt, Axel: Entwicklung eines „Dynamischen Risiko-Managements“ unter Berücksichtigung von „Nicht-Markt Risiken“, Dissertation, Universität Leipzig, 2003
- Stephan, Hans Jürgen: Rechtsschutz und Kompensation bei Wirtschaftskriminalität und Produktpiraterie durch Schutzrechtsmanagement und Rückgewinnungshilfe (Forensic Services), Unterlagen zum Seminar Entscheidungstheorie/Security Management an der Universität Lüneburg, 2003
- Stotz, M.: Organisationale Lernprozesse, Wiesbaden 1999
- Thoenißen, Michael: Erfolgversprechender Audit-Aufbau, KES, Nr. 6 2002, SecuMedia Verlags-GmbH Ingelheim, [www.kes.info](http://www.kes.info)
- Trotz Milliardeninvestitionen: Große IT-Sicherheitslücken in deutschen Unternehmen, Mummert + Partner Unternehmensberatung, Hamburg 2002, [www.mummert.de](http://www.mummert.de)
- Ulfkotte, Udo: Angriffsziel Betrieb: Vorsicht vor Spionen, Magazin Wirtschaft, IHK Region Stuttgart, Nr. 2/99
- Unternehmen sparen an IT-Sicherheit, Global Information Security Survey 2003, Ernest & Young, Stuttgart, August 2003, [www.ey.com/GLOBAL/content.nsf/Germany/Studien](http://www.ey.com/GLOBAL/content.nsf/Germany/Studien)
- van Doren, C.: Geschichte des Wissens, Basel 1996
- Varela, F.: Ethisches Können, Frankfurt 1994, von Foerster, H., Wissen..., a.a.O., Kahle E., Kognitionswissenschaftliche Grundlagen der Selbstorganisation, Arbeitsbericht 01/95 der Forschungsgruppe Kybernetische Unternehmenssteuerung an der Universität Lüneburg, Lüneburg 1995
- Verbindliche Regeln für Computer-Nutzer, Stuttgart 2000
- Verfassungsschutzbericht Baden-Württemberg 2001, Hsg. Innenministerium Baden-Württemberg, Mai 2002
- Volkman, Regina: Security Awareness bei SAP, SAP AG 2003
- von Foerster, H.: Wissen und Gewissen. Frankfurt 1993
- von Krogh, G.: Anhaltende Wettbewerbsvorteile durch Wissensmanagement, In: Die Unternehmung, 49 (6), 1995
- Voßbein, Reinhard; Voßbein, Jörn: Lagebericht zur IT-Sicherheit, Teil 1 und 2, KES/KPMG Sicherheitsstudie 2002, KES, Nr. 3 und 4 2002, SecuMedia Verlags-GmbH Ingelheim, [www.kes.info](http://www.kes.info)
- Wachholz, R.-P. (Landeskriminaldirektor): Notwendigkeit der Kooperation mit der Wirtschaft im Bereich der inneren Sicherheit, Wissenschaftliche Arbeitsberichte des ZWW der Universität Lüneburg 12/2002, [www.uni-lueneburg.de/einricht/zww/wabzww](http://www.uni-lueneburg.de/einricht/zww/wabzww)
- Weilep, Volker: Das Risikomanagementsystem, UNSERE WIRTSCHAFT; IHK Lüneburg-Wolfsburg, [www.ihk24-lueneburg.de](http://www.ihk24-lueneburg.de):
- Teil 1: Unverzichtbares Instrument zur Insolvenzvermeidung (Nr. 9 2002)
  - Teil 2: Frühwarnsystem und Funktionsweise des Risikomanagementsystems (Nr. 11 2002)

- Teil 3: Elemente und Funktionsweise des Risikomanagementsystems (Nr. 12 2002)
- Teil 4: Das Risikomanagementsystem in der Praxis (Nr. 1 2003)

Wieben, Hans-Jürgen (Leitender Kriminaldirektor): Polizei (Justiz, Verfassungsschutz) und Wirtschaft:

- Kritische Gedanken zu einem Bildungs- und Präventionskonzept, Wissenschaftliche Arbeitsberichte des ZWW der Universität Lüneburg 12/2002, [www.uni-lueneburg.de/einricht/zww/wabzww](http://www.uni-lueneburg.de/einricht/zww/wabzww)

WIK - Zeitschrift für die Sicherheit der Wirtschaft Nr. 1, Februar 2003, [www.wik.info/wik/news](http://www.wik.info/wik/news)

WIK-Informationen, Sonderheft 2003

WIK-Sicherheits-Enquête 2002/2003, SecuMedia Verlag, Ingelheim (WIK-Informationen Sonderheft 2003), [www.wik.info/wik/news](http://www.wik.info/wik/news)

Wirtschaftsdaten Region Stuttgart, IHK Region Stuttgart, 2002

Wirtschaftskriminalität 2003, PwC Deutsche Revision, PriceWaterhouseCoopers, Frankfurt am Main, 2003,

<http://www.pwc.com/Extweb/ncpressrelease.nsf/docid/F966E39AFBFC883B80256D8E00472FB2>

Wirtschaftsschutz-Info Nr. 4 – 07/03, Niedersächsisches Amt für Verfassungsschutz

Wirtschaftsspionage – Information und Prävention, Bundesamt für Verfassungsschutz für die Verfassungsschutzbehörden, 2002

Wirtschaftsspionage: Der Verfassungsschutz hilft Ihnen!, Niedersächsisches Landesamt für Verfassungsschutz, Hannover, 2003

Wolff, Jörg: Grundlagen des Strafrechts – das vorsätzliche Begehungsdelikt, Skriptum zur Vorlesung an der Universität Lüneburg, 2002

Woll, Harald: Wettbewerbsverzerrung durch Wirtschaftsspionage – Gegenmaßnahmen, Unterlagen zur Vorlesung an der Fachhochschule Reutlingen im Europäischen Studiengang für Betriebswirtschaft, 2002

[www.statistik-bw.de/Veroeffentl/Statistische\\_Berichte/4165\\_02001.pdf](http://www.statistik-bw.de/Veroeffentl/Statistische_Berichte/4165_02001.pdf)

Zschunke, Peter: Spionage in undichten Funknetzen, Wiener Zeitung, 08.05.2003, [www.wienerzeitung.at](http://www.wienerzeitung.at)

Zur technologischen Leistungsfähigkeit Deutschlands, Bundesministerium für Bildung und Forschung, [www.bmbf.de](http://www.bmbf.de)

## Anhang 1:

### Fragebogen Stand Januar 2002

Angaben zum Ansprechpartner		
<b>Name:</b> .....	<b>Vorname:</b> .....	<b>Titel:</b> .....
Funktion:.....		
Firma: .....		
Straße:.....		
Ort: .....		
Tel: .....		
Fax: .....		
E-mail: .....		

## Angaben zur Firma

<b>1) Wie sieht Ihre Produkt-Markt-Position aus?</b> <b>(Produkt schließt hier alle Arten von Dienstleistungen ein)</b>	
Massenprodukt in einem Markt mit vielen Konkurrenten	
Massenprodukt in einem Markt mit wenigen Konkurrenten	
Einzel-/Kleinserienfertigung in einem Markt mit vielen Konkurrenten	
Einzel/Kleinserienfertigung in einem Markt mit wenigen Konkurrenten	
Einzigiger Anbieter am Markt (Monopol)	
.....	
Unsere Marktstellung ist:   eher regional	
eher national	
eher international	

<b>2) Wie hoch war Ihr durchschnittlicher Umsatz in den letzten drei Jahren (in Euro)?</b>	
unter 2 Millionen €	
2 bis 10 Millionen €	
10 bis 50 Millionen €	
50 bis 200 Millionen €	
200 bis 500 Millionen €	
über 500 Millionen €	

<b>3) Worin besteht Ihr wichtigster Wettbewerbsvorteil/-vorsprung? (ggf. mehrere ankreuzen, wenn sie gemeinsam wirken, sonst den vorherrschenden)</b>	
Überlegene Produkte	
Neue Produkte	
Beherrschung spezifischer Produktionsprozesse/Arbeitsmethoden	
Maschinenausstattung	
Mitarbeiterstamm	
Kundenstamm/Kundenbeziehung	
Lieferantenbeziehungen	
Vertriebssystem	
Kooperationen/Netzwerke	
Forschungspotenzial/-ergebnisse	
Organisatorische Vorteile	
Unternehmenskultur/Betriebsklima	
Strategie (Produkt-Markt, Corporate, Geschäftseinheit)	
.....	

<b>4) Wie ist der Wettbewerbsvorteil/-vorsprung entstanden?</b>	
Idee einer Person	
Gemeinsame Idee mehrerer Personen in der Unternehmung (Team)	
Gemeinsame Idee mit Kunden/Kooperation mit Kunden	
Entwurf/Projektbearbeitung einer oder mehrerer Abteilungen	
Gewachsen aus dauerhafter Zusammenarbeit	
Gewachsen durch strategische Investition in innovative Geschäftsfelder	
Fremdforschung/Fremdentwicklung	
Marktbeobachtung	
.....	

<b>5) Welche ungefähren Aufwendungen haben Sie für die Erstellung bzw. Erarbeitung des Wettbewerbsvorteils/-vorsprungs gehabt? Falls die Angaben nicht in Euro beziffert werden können, bitte Personal- und Zeitaufwand benennen.</b>	
unter 500 000 €	
500 000 bis 1 Million €	
1 bis 3 Millionen €	
3 bis 5 Millionen €	
über 5 Millionen €	
... Personen	
... Stunden	
.....	

<b>6) Wie hoch schätzen Sie den Wert des Wettbewerbsvorteils/-vorsprungs ein (gemessen in Euro pro Jahr)?</b>	
unter 100 000 €	
zwischen 100 000 und 500 000 €	
zwischen 500 000 und 2 Millionen €	
zwischen 2 und 5 Millionen €	
über 5 Millionen €	

<b>7) Wie nachhaltig ist der Wettbewerbsvorteil/-vorsprung?</b>	
Nicht imitierbar und erodiert nicht	
Imitierbar (muss stets durch Innovationen verteidigt werden)	
Rekonstruierbar (leichte Nachahmbarkeit)	
Geschützt durch: nationales Patent	
internationale Patente	
Umgehungspatente	
Gebrauchsmuster	
Nicht geschützt	
Setzt erhebliche spezifische Investitionen voraus	
Nachahmung nützt nichts, da keine weiteren Kunden vorhanden	
Der Vorteil liegt in der Unternehmensorganisation (Arbeitsteilung, Struktur)	
Der Vorteil liegt in der Unternehmenskultur (Werte, Identifikation, Betriebsklima)	
Es gibt spezielle Sicherheitsmaßnahmen	
.....	

<b>8) Wie lange hält der momentane Wettbewerbsvorteil/-vorsprung, wenn Sie keine weiteren Investitionen oder andere Maßnahmen dafür tätigen oder wenn er nicht durch adäquate Maßnahmen erhalten wird?</b>	
1 Jahr	
5 Jahre	
10 Jahre	
mehr als 10 Jahre	
.....	

<b>9) Welche Sicherungsmaßnahmen gegen Informationsverluste werden vorgenommen?</b>	
Besteht eine Eingangskontrolle/allgemeine Zugangskontrolle?	
Bestehen Zugangsbeschränkungen für sicherheitsrelevante Bereiche?	
Gibt es Zugriffsbeschränkungen für Daten?	
Wird Datenschutz betrieben?	
Werden Sicherheitskopien hergestellt?	
Ist Wissen so verteilt, dass nicht eine Person über das gesamte Wissen verfügt?	
Sind Sie in das amtliche Geheimschutzverfahren einbezogen?	
Gibt es einen Sicherheitsverantwortlichen im Unternehmen?	
Gibt es ein Sicherheitskonzept für die gesamte Unternehmung?	
Besteht Zusammenarbeit mit Sicherheitsbehörden/-institutionen?	
Werden bei der Personalarbeit Sicherheitsaspekte berücksichtigt (Auswahl, Einsatz, Freisetzung)?	
Gibt es personenbezogene Sicherheits-Checks?	
Wird das Personal in Schutzmaßnahmen gegen Informationsverlust geschult?	
Gibt es Geheimhaltungs-/Wettbewerbsklauseln in den Arbeitsverträgen?	
Sind beim Ausscheiden von Mitarbeitern spezielle Sicherheitsvorkehrungen vorgesehen?	
Beziehen sich diese Personalmaßnahmen auch auf Fremd-, Leasing- und sonstiges Dienstleistungspersonal?	
.....	

<b>10) Wie hoch sind Ihre Aufwendungen für Informationssicherheit (in Euro pro Jahr)?</b>	
unter 50 000 €	
50 000 bis 100 000 €	
100 000 bis 250 000 €	
250 000 bis 500 000 €	
über 500 000 €	

<b>11) Wer könnte an dem Wissen Interesse haben, das dem Wettbewerbsvorteil/-vorsprung zugrunde liegt?</b>	
Ein inländischer Konkurrent	
Ein ausländischer Konkurrent	
aus welchem Land oder welchen Ländern .....	
Mehrere inländische Konkurrenten	
Mehrere ausländische Konkurrenten	
aus welchen Ländern .....	
Potenzielle Konkurrenten	
Staatliche (militärische) Institutionen	
aus welchen Ländern .....	
Technologie-/Wissenshändler	
.....	

<b>12) Waren Sie schon Objekt „unfreundlichen“ Informationsabflusses? (Ausspähung, Abschöpfung, Abwerbung, Mitnahme von Geheimnissen bei Weggang von Mitarbeitern,...)</b>	
Nein	
Ja, durch ausländische staatliche Organe	
aus welchen Ländern .....	
Ja, durch inländische Konkurrenz	
Ja, durch ausländische Konkurrenz	
aus welchen Ländern .....	
Ja, durch „untreue“ Kooperationspartner	
Ja, durch abgewanderte Mitarbeiter	
Ja, durch Unbekannte	
Vielleicht, es bestehen vage Verdachtsmomente	

<b>13) Wie hoch schätzen Sie den in diesem Fall entstandenen Schaden (in Euro)?</b>	
unter 50 000 €	
50 000 bis 100 000 €	
100 000 bis 250 000 €	
250 000 bis 500 000 €	
über 500 000 €	
nur in anderen Dimensionen ausdrückbar	
.....	

<b>14) Wie haben Sie den Schadensfall bearbeitet?</b>	
Gar nicht	
Mit innerbetrieblichen Kräften (Organisations-Abt., Interne Revision, EDV-Abt.)	
Mit externen Sicherheitsberatern	
Mit Sicherheitsbehörden (Polizei, Verfassungsschutz)	
Durchführung einer Schwachstellenanalyse, wobei folgende Schwachstellen entdeckt wurden (personelle, technische, organisatorische, juristische, sonstige): .....	
.....	
.....	

<b>15) Welche Sicherheitsmaßnahmen haben Sie als Folge des Schadensfalls ergriffen?</b>	
Personelle Maßnahmen (Schulung,...)	
Technische Maßnahmen (Alarmanlagen, Kontrollsysteme,...)	
Organisatorische Maßnahmen (Zugangsregelung, Closed Shop,...)	
Juristische Maßnahmen (Verträge, interne Regeln,...)	

<b>16) Welche Verdachtsmomente zu Informationsabflüssen hatten Sie bisher?</b>	
Übermäßiges Kopieren/Kopieren zu ungewöhnlichen Zeiten	
Nicht auffindbare Unterlagen	
Anwesenheit fremder Personen auf dem Betriebsgelände oder in der Nähe	
Anwesenheit von Betriebsangehörigen zu ungewöhnlichen Zeiten oder in ungewöhnlichen Betriebsteilen	
Auftauchen von Teilinformationen bei Wettbewerbern	
Nicht erklärbarer Verlust von Aufträgen	
Auftauchen von günstigen Konkurrenzprodukten	
.....	

<b>17) Wie sind die Beziehungen zu Kooperationspartnern abgesichert?</b>	
Kooperationsvertrag	
Wechselseitige Kapitalbeteiligung	
Klare Absprachen über Informations- und Verwertungsrechte	
Überprüfung der jeweiligen Leistungsbeiträge	
Regelmäßige Abstimmungen über Arbeitsfortschritte und eventuelle Probleme	
Den Partnern werden eigene Sicherheitsstandards vorgegeben	
Durchführung von Sicherheits-Audits	
.....	

<b>18) Gab es bei abgeworbenen/abgewanderten Mitarbeitern Anzeichen für die Illoyalität?</b>	
Deutlich geäußerte Unzufriedenheit	
Arbeitsengagement trotz oder nach geäußelter Unzufriedenheit	
Auffällige Verbesserung der finanziellen Situation	
Unerklärlich konspiratives Verhalten	
Dubiose Kontakte	
Auffälligkeiten im Lebenslauf	
Anzeichen für Bestechlichkeit	
Abnehmende Identifizierung mit dem Unternehmen	
Besitz von Spionagehilfsmitteln	
.....	

<b>19) Wie ist die Einschätzung der Arbeit der/Kooperation mit den Sicherheitsbehörden?</b>	
Arbeit der Sicherheitsbehörden zu Informationsschutz ist weitgehend unbekannt und wird auch nicht benötigt	
Arbeit der Sicherheitsbehörden zu Informationsschutz ist weitgehend unbekannt, würde aber gebraucht	
Ansprechpartner bei den Sicherheitsbehörden sind bekannt	
Es bestehen regelmäßige Informations-/Arbeitskontakte mit den Sicherheitsbehörden	
Es besteht ein umfassendes, mit den Sicherheitsbehörden abgestimmtes Sicherheitskonzept	
Die Arbeit der Sicherheitsbehörden ist nicht wirksam genug	
Die Zuständigkeiten für die verschiedenen Probleme des Informationsabflusses sind nicht klar genug geregelt	
Es bedarf einer schärferen arbeits- und wettbewerbsrechtlichen Regelung für den Schutz vor unlauterem Informationsabfluss	
Öffentliche Auftraggeber nehmen wettbewerbsrechtliche Probleme des Informationsschutzes nicht ernst genug	
Welche Maßnahmen der Sicherheitsbehörden hielten Sie für wünschenswert?  .....	

## **Anhang 2:**

### **Programmskizze für ein Verbundprogramm „Wissenschaftliche Weiterbildung Security Management“**

#### **1. Gegenstand**

Der Weiterbildungsstudiengang Strategisches Management mit dem Schwerpunkt Security Management (kurz Security Management) mit dem Abschluss MBA – ist über vier Semester konzipiert, verläuft berufsbegleitend und ist modular aufgebaut.

#### **2. Wissenschaftliche Leitung**

Die wissenschaftliche Verantwortung und Leitung des Studiengangs trägt der Fachbereich Wirtschafts- und Sozialwissenschaften der Universität Lüneburg, Lehrstuhl Recht insbesondere Wirtschafts- und Umweltrecht.

#### **3. Organisation, Koordinierung und Durchführung**

Verantwortlich dafür ist das ZWW (Zentrum für Wissenschaftliche Weiterbildung) der Universität Lüneburg.

#### **4. Verbund**

Im Sinne gemeinsamer Weiterbildungsangebote von Hochschule und Wirtschaft werden mehrere Universitäten, Landesämter, Arbeitskreise und auch Unternehmen in die Weiterbildung einbezogen. Jeder Partner wird sich mit einem seiner Qualifikation entsprechenden Modulanteil einbringen. Die Weiterbildung wird länderübergreifend und in einem effizienten Verbund erfolgen.

Verbundpartner, mit denen bisher verbindliche Absprachen getroffen wurden:

- Universität Saarbrücken
- Universität Hamburg
- Polizeiführungsakademie Münster
- Fachhochschule Nordostniedersachsen
- Landesamt für Verfassungsschutz Niedersachsen
- Landesamt für Verfassungsschutz Baden-Württemberg
- DIHK Bonn/Berlin
- Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW) Bonn/Berlin
- Bundesarbeitskreis der Sicherheitsbevollmächtigten (BAK Sibe)
- TÜV Saarland
- Prevent AG Hamburg

## **5. Grundsätzliches zum Weiterbildungsstudiengang „Security Management“**

Der Studiengang wird als Weiterbildungsstudiengang angeboten. Zielgruppe sind Spitzenmanager und potentielle Spitzenmanager, die sich mit der grundsätzlichen Orientierung ihrer Unternehmung sowie mit Sicherheits- und Risikoaspekten auseinandersetzen wollen. Der geplante Weiterbildungsstudiengang soll als Präsenzstudiengang in Blockform mit einem Umfang von 720 Präsenz- und Fernstudienstunden durchgeführt werden.

## **6. Ziele**

Unter der Prämisse, dass es die zentralen Aufgaben der Führung sind, die strategische Ausrichtung der Unternehmung zu bestimmen und Situationen mit außergewöhnlicher Bedeutung und unter außergewöhnlichen Umständen zu beherrschen, sollen Absolventen dieses MBA in die Lage versetzt werden, die Ziele (Vision und Mission) einer Unternehmung zu bestimmen, alternative Strategien zu entwickeln und Risiken potentieller Krisen und langfristiger Änderungen zu erkennen und Instrumente zu ihrer Handhabung einzusetzen.

## **7. Konzept**

Der Studiengang ist viersemestrig konzipiert. Die Themen umfassen sowohl verhaltenswissenschaftliche Tatbestände und Analysen als auch mathematisch-formale Optimierungsansätze, die jeweils neben der theoretischen Fundierung eine fallbezogene praktische Anwendung finden. In den ersten beiden Semestern werden Grundlagen der verschiedenen Teilgebiete (Ziele, Strategien, Corporate Governance, Früherkennung, Krisenmanagement, Security Management) allgemein und an Fallstudien erarbeitet. Im dritten Semester erfolgt die Entwicklung eines ganzheitlichen Strategie- und Risikokonzepts („Lüneburger Modell“), im vierten Semester die tutorierte Erarbeitung von Fallanalysen. Das an der Universität Lüneburg entwickelte VILES-Konzept (virtuelles Lernsystem) wird für diesen Studiengang herangezogen und als spezielle Plattform ausgebaut

## **8. Curriculum**

Der Aufbau der ersten drei Semester erfolgt modular, so dass gegebenenfalls auch Elemente anderer Masterstudiengänge bei Bedarf integriert bzw. gegen einzelne Module ausgetauscht werden können. Es werden folgende Module geplant, die u.a. unter Nutzung multimedialer Instrumente zu bearbeiten sind und im folgenden beispielhaft dargestellt werden:

## 9. Module

### Modul I: Normatives Management

- Unternehmensziele  
Typische Ziele, Zielbeziehungen, „Vision and Mission“, Leitbilder, Managementphilosophien, Kollegienmanagement
- Unternehmensethik und Unternehmenskultur  
Ethische Grundlagen des Managements, Analyse und Gestaltung von Unternehmenskultur, Konfliktmanagement
- Interkulturelles Management  
Analyse unterschiedlicher Management-Kulturen, Management von kulturellen Unterschieden, Internationales Management
- Corporate Governance  
Inhalte von CG, Steuerungskonzepte, Balanced Scorecard, europäische und deutsche Rechtsentwicklung (im Verbund mit der Universität Hamburg, FORSI)

### Modul II: Management Strategien

- Unternehmensstrategien  
Strategietypen, Arten von Strategien, spieltheoretische Ansätze, Strategie-Mix
- Strategisches Marketing  
Positionierung, Innovationsstrategien, Kommunikationsstrategien, Netzwerke
- Finanzstrategien und Strategisches Human Resource Management

### Modul III: Risikomanagement

- Früherkennung strategischer Risiken und vorbeugende Planung  
(im Verbund mit der Polizeiführungsakademie Münster)
- Security Management  
Datensicherheit, Wirtschaftsspionage, „Guerre Economique“, Sicherheit am Arbeitsplatz, andere Gefährdungspotenziale
- Krisenmanagement  
Krisenursachen, Krisenbeherrschung, Notfallpläne, Krisenkommunikation  
(im Verbund mit der FH Nordostniedersachsen)
- Ursachen und Formen organisatorischen Wandels  
„Dynamics of International Competition“, Kultureller Wandel, New Economy, Organisationales Lernen, „Cognitive Maps“

**Modul IV:** Technische Sicherheit

(im Verbund mit der Universität Saarbrücken)

**Modul V:** Entwicklung eines ganzheitlichen Strategie- und Risikokonzepts

(im Verbund mit Landesämtern und Unternehmen)

- Grundkonzept vernetzter Unternehmensplanung (Fokus-Konzept)

- Ganzheitliches, Risikomanagement

- Unternehmenssimulation (Planspiel)

Die Absolvierung der einzelnen Module und Untermodule wird mit Credit Points gemessen. Als Leistungsnachweise innerhalb des Studiengangs sind hauptsächlich Hausarbeiten vorgesehen. Der Studiengang wird mit einer Masterarbeit abgeschlossen, die im Regelfall eine schwerpunktbezogene Fallanalyse umfassen soll.

Informationen zum Studiengang sind über

<http://www.uni-lueneburg.de/zww/sicherheitsforum>

abrufbar.