

Um welches Wissen geht es bei Wirtschafts- und Industriespionage? Was genau ist Wirtschafts- und Industriespionage? Wo liegen die Grenzen zu regulärer Informationsbeschaffung, und wie können die Antworten auf diese Fragen ein Unternehmen vor den Abfluss von Know-How schützen? Schutz wird durch Wissen über Fakten und Prozesse ermöglicht und kann nur durch eine ganzheitliche Betrachtung eines Unternehmens sowie seiner internen und externen Umwelten stattfinden.

Die Diskussion über den Umfang und die Definition des schützenswerten Wissens in einem Unternehmen, den Geschäfts- und Betriebsgeheimnissen, kurz den Wirtschaftsgeheimnissen, und die Debatte über die Methoden der legalen oder illegalen Abflüsse von Wissen ist alles andere als neu. Sie wird seit mehr als hundert Jahren intensiv geführt.<sup>10</sup> Außer Frage steht dabei zunächst, dass sämtliches Wissen eines Unternehmens, welches der Öffentlichkeit zugänglich gemacht wurde, nicht in den Schutzbereich von Geschäfts- und Betriebsgeheimnissen fällt. Strafbar ist die Verwendung, Verwertung und Ausspähung von Geschäfts- und Betriebsgeheimnissen, wenn es sich dabei um internes Wissen handelt, welches der Unternehmer keinem Anderen bzw. keinem Fremden zugänglich machen möchte.

In diesem Zusammenhang ist die in den Gesetzesmaterialien zu § 125 TKG 2003 enthaltene Definition zu Wirtschaftsgeheimnissen aufschlussreich:

„Betriebs- oder Geschäftsgeheimnisse sind Tatsachen kommerzieller oder technischer Art, die nur einem eng begrenzten, im Wesentlichen geschlossenen Personenkreis bekannt und für andere nicht oder nur schwer zugänglich sind. Der Berechtigte muss an der Geheimhaltung jedenfalls ein schutzwürdiges wirtschaftliches und objektiv berechtigtes Interesse haben.“

---

10 siehe hierzu: Wassermann (1931).

Die Geheimnisdefinition erschließt sich daher zunächst aus einer Negativabgrenzung: kein Geheimnis stellen sohin all jene Unternehmensdaten dar, die in Registern, Datenbanken udgl. öffentlich zugänglich sind. Patente oder geschützte Marken sind somit nicht Gegenstand des Schutzes vor Wirtschafts- und Industriespionage. Ihr Schutz unterliegt eigenen gesetzlichen Normen.

In der Wirtschafts- und Unternehmenswelt gibt es unterschiedliche Möglichkeiten, Informationen zu gewinnen und zu verwerten. Der nachfolgende Überblick zeigt, welche wirtschaftlich bzw. unternehmerisch relevanten Informationen und Daten durch legale Methoden gewonnen werden können – und welcher Informationsabfluss erst durch die Anwendung illegaler Mittel möglich ist. Die „Spionagepyramide“ beginnt daher bei regulärer Marktforschung – und endet bei echter Wirtschafts- und Industriespionage.

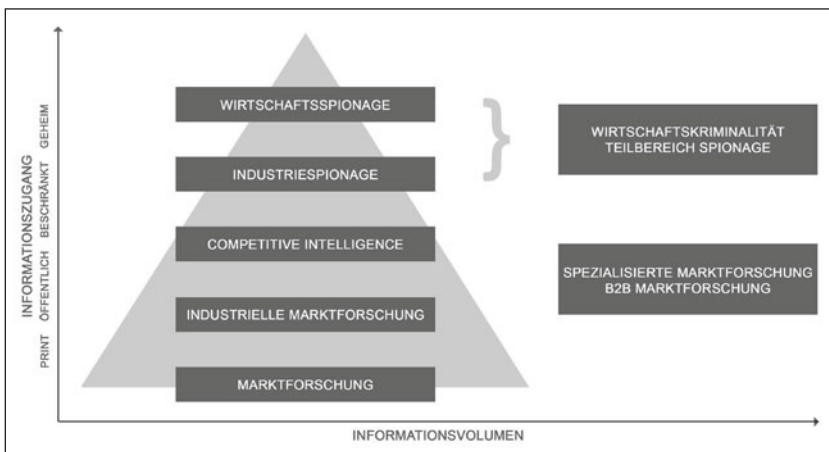


**Abb. 8** Die Spionagepyramide

© Eigene Darstellung

## 2.1 Marktforschung: Grundlage für Marketing

Für viele Unternehmen ist es eine Selbstverständlichkeit, Marktforschung zu betreiben. Sie ermöglicht es dem Betrieb, auf Marktentwicklungen möglichst zeitnah zu reagieren und die eigene Wettbewerbsfähigkeit zu sichern: „Marktforschung ist die systematische Sammlung, Aufbereitung, Analyse und Interpretation von

Daten über Märkte und Marktbeeinflussungsmöglichkeiten zum Zweck der Informationsgewinnung für Marketingentscheidungen.<sup>11</sup> Die damit möglichen differenzierten Marketingentscheidungen betreffen alle Austauschbeziehungen eines Unternehmens: Sie beziehen sich sowohl auf unternehmensinternes Marketing, als auch auf Maßnahmen, die sich auf die Rohstoff-, Kapital- und Arbeitsmärkte (Beschaffungsmarketing), gegen Konkurrenzunternehmen (wettbewerbsorientiertes Marketing) sowie in Richtung der unmittelbaren Absatzmärkte (handelsgerichtetes Marketing) richten.<sup>12</sup>

Deshalb verfolgt die Marktforschung heute ein ganzheitliches Konzept, das die früher getrennten Methoden der Marktforschung und der Marketingforschung zu einem integrierten Marketing zusammenführt. So können die Unternehmen rasch auf sich verändernde interne und externe Bedingungen reagieren. Dazu zählen ebenso notwendige Reaktionen auf Aktivitäten von Konkurrenzunternehmen.

Eine Sonderform der Marktforschung, die sich von der Konsumgüter-Marktforschung – dem Business-to-Consumer-Segment (B2C) unterscheidet, ist die Business-to-Business-Marktforschung (B2B). Sie sorgt als Teil der Industrienmarktforschung für die systematische und kontinuierliche Beobachtung, Analyse, Diagnose und Prognose der Situation und Entwicklung des Umfelds von Investitionsgüterunternehmen. Dabei stehen Beschaffungsmanagement, Absatzmärkte, aktuelle und potentielle Kunden und Wettbewerber im Mittelpunkt.

---

## 2.2 Competitive Intelligence: Konkurrenz am Prüfstand

Eine deutlich intensivere Auseinandersetzung mit der Konkurrenz findet auf der nächsten Stufe der „Spionagepyramide“ statt: der sogenannten Competitive Intelligence. Während sich die Marktforschung zumeist auf vollständig erhobene Daten stützt, die in unmittelbarem Zusammenhang mit den untersuchten Märkten (Absatz-, Beschaffungsmärkte etc.) stehen, werden bei der Competitive Intelligence auch mittelbar marktrelevante sowie marktexterne Variablen und Daten in die Analyse miteinbezogen.

„Unter Competitive Intelligence versteht man die systematische, andauernde und legale Sammlung und Auswertung von Informationen über Konkurrenzunternehmen, Wettbewerbsprodukte, Marktentwicklungen, Branchen, neue Patente, neue Technologien oder Kundenerwartungen. Diese Konkurrenz- oder Wettbe-

---

11 Fantapié (2011), S. 4.

12 Vgl. Koch (2012), S. 4ff.

werbsaufklärung soll dazu dienen, frühzeitig ihre Strategien an die sich veränderten Wettbewerbsstrukturen anzupassen und aufgrund besserer Informationen einen Wettbewerbsvorteil zu erlangen,<sup>13</sup> lautet *Schaafs* Definition von Competitive Intelligence, dem CEO von Corporate Trust.

Der Begriff Intelligence stammt ursprünglich aus dem militärischen Sprachgebrauch. Er kann am treffendsten mit (Früh- bzw. Feind-) „Aufklärung“ beschrieben werden. Oftmals wird bei der Beschreibung des Begriffes der von der CIA entwickelte „Intelligence Cycle“ verwendet. Mit Blick auf Competitive Intelligence stellt er sich folgendermaßen dar:

In der Planungsphase erfolgt die Festlegung und Eingrenzung des Informationsbedarfs sowie die Benennung der maßgeblichen Ziele.<sup>14</sup> Anschließend werden die geplante Vorgehensweise skizziert, Meilensteine definiert und beteiligte Personen festgelegt. Im nächsten Schritt, der Beschaffungsphase, erfolgt die Sammlung der Informationen aus unterschiedlichen Quellen. Primärquellen sind u. a. Kunden, Interessenten, Lieferanten, Berater und Mitbewerber. Sekundärquellen umfassen die Beschaffung der Informationen aus Medien, Fachzeitschriften, Datenbanken (z. B. Internet, Bibliotheken, Archiv) dem gesellschaftlichen Umfeld sowie Banken und Versicherungen. Durch gezielte Abfragen können somit bereits verfügbare bzw. bekannte Informationen gewonnen werden, die Bestandteil der unternehmensinternen Datenbanken oder des von den Mitarbeitern gehaltenen Humankapitals sind.

Informationslieferanten für Intelligence werden in drei große Kategorien unterteilt: in Open Source Intelligence (OSINT), Human Intelligence (HUMINT) und Technical Intelligence (TECHINT).

Bei Open Source Intelligence wird auf Basis von frei verfügbaren Daten eine Informationsgrundlage geschaffen, welche im weiteren Verlauf durch anders gewonnene Informationen und Daten ergänzt wird. Das können beispielsweise gezielte Fragestellungen im Bereich Human Intelligence sein.<sup>15</sup> Human Intelligence beschreibt die Informationsgewinnung durch die Nutzung von bestehenden oder aufgebauten Vertrauensverhältnissen und ist eng mit psychischen Faktoren bzw. mit dem Faktor Mensch im Unternehmen verbunden. Human Intelligence stellt – obgleich in der aktuellen Debatte der bestehenden Bedrohungen für ein Unternehmen anders dargestellt<sup>16</sup> – die bedeutendste, zumeist genutzte und erfolgreiche Methode zur Informationsgewinnung dar. SOMINT (Social Media

---

13 Schaaf (2009), S. 124.

14 Vgl. ÖNORM S 2430:2011, S. 10f.

15 Vgl. Lux/Peske (2002), S. 83ff.

16 siehe hierzu: Kapitel 1.

Intelligence) stellt in diesem Zusammenhang eine neue Methode der Generierung von Wissen über Personen durch die Nutzung von Sozialen Netzwerken dar.

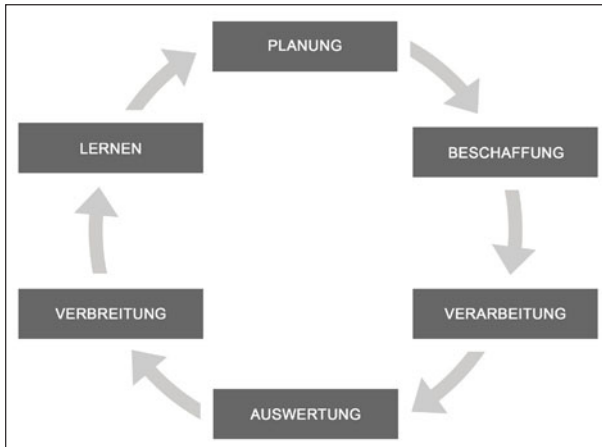


**Abb. 9** Der Intelligence Cycle

© Eigene Darstellung

Technical Intelligence meint die Beschaffung von Informationen mittels technischer Hilfsmittel, worunter auch Hacking subsummiert werden kann. Dieses Verfahren ist abgesehen von seiner strafrechtlichen Relevanz und Kostenintensivität nur bestimmten Akteuren vorbehalten, da die derart generierten Informationen im Regelfall einer intensiven Aufbereitung bedürfen.

Die Vorgangsweise im Bereich Competitive Intelligence auf einen Blick:

- In der Phase der *Verarbeitung* werden die zuvor gesammelten Informationen zunächst in eine auswertbare Form übersetzt, geordnet, hinsichtlich ihrer Richtigkeit und Glaubwürdigkeit überprüft und für die weitere Verwendung archiviert.
- Diese strukturiert vorliegenden Rohinformationen werden in der Phase der *Auswertung* analysiert und bewertet sowie mit bereits vorhandenem Wissen verglichen, kombiniert und verarbeitet. Das ermöglicht ein konsolidiertes Bild und ist die Grundlage dafür, um Hypothesen entsprechend der anfangs festgelegten Zielsetzungen formulieren zu können.<sup>17</sup> Dadurch wiederum wird die

<sup>17</sup> Vgl. Lux/Peske (2002), S. 27f.

Darstellung von Zukunftsszenarien ermöglicht, die das Unternehmen in die Lage versetzt, Vorhersagen über mögliche Entwicklungen und Vorgehensweisen zu tätigen. Entscheidend ist, dass die Interpretation der Analyse im Hinblick auf die Ausgangssituation und die anstehenden Entscheidungen getroffen wird, und dass eine möglichst lückenlose Dokumentation der angewandten Analysemethoden sowie der Analyseergebnisse erfolgt.

- Im Anschluss werden die zuvor erhobenen und gewonnenen Ergebnisse in der *Verbreitungsphase* präsentiert. Durch entsprechendes Feedback wird in der Lernphase die Grundlage für die Neubewertung einer bestehenden Analyse und vorgenommenen Informationsbeschaffung geschaffen. So werden Möglichkeiten der Prozessverbesserung identifiziert – und durch die inhaltliche Reflexion schlussendlich wieder der Ausgangspunkt des Intelligence Cycles erreicht.<sup>18</sup>

Ziel der Competitive Intelligence ist jedenfalls eine umfassende Marktanalyse durch die Erhebung der unterschiedlichsten Daten und deren Analyse und Verknüpfung mit grundsätzlich nicht unmittelbar relevanten Daten. Dieses Verfahren profitiert zudem davon, dass durch den Trend zur Zertifizierung von Unternehmen vermehrt Unternehmensdaten einer breiten Öffentlichkeit – und somit auch der Konkurrenz – zugänglich gemacht werden. Wesentlicher Erfolgsfaktor der Competitive Intelligence ist jedoch die Kompetenz, mittels der erhobenen Daten zielgerichtete Analysen durchführen zu können und daraus neue bzw. optimierte Wettbewerbsstrategien zu erarbeiten. All diese Aktivitäten bzw. gesetzten Schritte sind vollkommen legal.

Es kann jedoch vorkommen, dass die Competitive Intelligence betreibenden Akteure die Grenzen der legalen Informationsbeschaffung überschreiten. Damit greifen – abhängig von der tatsächlich angewandten illegalen Methode der Informationsbeschaffung bzw. deren konkreter Ausgestaltung – entsprechende zivilrechtliche bzw. strafrechtliche Normen. Die Beeinflussung von (Vertriebs-)Mitarbeitern während geschäftlicher Termine im In- und Ausland beispielsweise durch Luxus-Konsum, und die damit mögliche Beeinflussung des Mitarbeiters sowie „Erschleichung“ vertraulicher Informationen (social engineering/social hacking) sind hingegen Verfahren, wie sie bei Wirtschafts- und Industriespionage angewandt werden. Damit ist die nächste und entscheidende Stufe der „Spionagepyramide“ erreicht.

---

18 Vgl. ÖNORM S 2430:2011, S. 14 f.

## 2.3 Industriespionage: Spionage bei der Konkurrenz

Die Industriespionage wird in Deutschland auch als Konkurrenzausspähung, Betriebsspionage oder Werksspionage bezeichnet. Dabei wird ein Unternehmen durch einen inländischen Konkurrenten bzw. eine Einzelperson ausgespäht. Bei der Konkurrenzausspähung ist es in Deutschland Sache des Unternehmens, geeignete Maßnahmen der Unternehmenssicherheit zu ergreifen und gegen das unrechtmäßige Vorgehen der Person bzw. des Konkurrenzunternehmens vorzugehen. (Straf-) Rechtlich relevant ist hier die Norm § 17 dt. UWG (Gesetz gegen den unlauteren Wettbewerb) – Verrat von Geschäfts- und Betriebsgeheimnissen. Es handelt sich hierbei um ein Antragsdelikt.

Unternehmen und mitunter Einzelpersonen, die Industriespionage betreiben, verfolgen das Ziel, die eigene Wettbewerbsfähigkeit bzw. ihre Marktmacht zu erhalten und zu steigern: Sie versuchen Informationen und Kenntnisse zu erlangen, die sie in die Lage versetzen, sich am Markt deutlich vor den anderen Unternehmen zu positionieren, beispielsweise durch gestohlene Innovationen oder die Ausspähung von Preiskalkulationen insbesondere im Zusammenhang mit (Projekt)Ausschreibungen und Kooperationsbestrebungen mit anderen Unternehmen. In letzterem Fall bezieht sich der wirtschaftliche Schaden nicht auf den Verlust der Innovation (z. B. durch Diebstahl) sondern auf den Verlust des gesamten potentiellen Auftragsvolumens.

Bei der Industriespionage zeigt sich in der Praxis, dass die relevanten Aktionen eher punktuell und kurzfristig ausgerichtet sind. Mit ein Grund dafür: Produktlebenszyklen sind heute sehr kurz. Das Zusammenspiel zwischen Entwicklungsprozessen und Wettbewerbsposition ist sehr dynamisch, weshalb Akteure der Industriespionage entsprechend rasch und flexibel handeln müssen.

In Österreich wird unter Industriespionage jene Konkurrenzforschung verstanden, bei der die Grenze der legal erlaubten Methoden überschritten wird. Ziel ist der Erwerb von Informationen, die geeignet sind, die eigene Marktposition zu stärken bzw. die Wettbewerbsvorteile anderer Unternehmen zu schmälern oder zu beseitigen. Dies erfüllt den Tatbestand des Treuebruchs eines Beschäftigten in Bezug auf den Verrat von Geschäfts- und Betriebsgeheimnissen. Nach herrschender Lehre und Rechtsprechung setzt § 11 UWG ein „Handeln zum Zwecke des Wettbewerbs“ voraus. Damit ist das Verhalten eines Täters gemeint, der mit der Intention handelt, nicht eigenen, sondern fremden Wettbewerb zu fördern.<sup>19</sup>

---

<sup>19</sup> Vgl. OGH 28.08.2012 12 Os 38/12y.

## 2.4 Wirtschaftsspionage: Staatlicher Hintergrund

Das deutsche Bundesamt für Verfassungsschutz (BfV) definiert Wirtschaftsspionage als „Teil der Spionage, der die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Forschungseinrichtungen beinhaltet.“<sup>20</sup>

Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (.BVT) in Österreich versteht unter Spionage allgemein die Auskundschaftung von Geheimnissen durch nachrichtendienstlich gesteuerte Personen oder Gruppen sowie die Auskundschaftung von Geschäfts- und Betriebsgeheimnissen zu Gunsten des Auslandes. Die Verantwortung des .BVT zur Strafverfolgung liegt vornehmlich bei § 124 StGB – Auskundschaftung eines Geschäfts- und Betriebsgeheimnisses zugunsten des Auslands<sup>21</sup>. Dabei handelt es sich um eine Spezialbestimmung gegen den wirtschaftlichen Landesverrat<sup>22</sup> und somit um ein Officialdelikt. Die Behörden sind deshalb bei Bekanntwerden eines Vorfalls zur Strafverfolgung verpflichtet. Konkret bedeutet dies, dass das .BVT nach der aktuellen Rechtslage einen bekannt gewordenen Vorfall jedenfalls der zuständigen Staatsanwaltschaft anzeigen muss. Dieser Umstand ist der Zusammenarbeit zwischen Behörden und Wirtschaft zur Optimierung des Wirtschaftsschutzes leider nicht dienlich. Unternehmen befürchten, dass hierdurch das Medieninteresse geweckt wird und ein Reputationsschaden einhergeht.

Der Fokus der Wirtschaftsspionage liegt auf der Steigerung und Verbesserung der Wirtschaftskraft bzw. des wirtschaftlichen Potentials der eigenen Volkswirtschaft. Hier unterscheiden sich oftmals die angewandten Methoden bezüglich der Vorgehensweise bei der direkten Spionagetätigkeit sowie bei der Handhabung der durch Spionage erlangten Informationen: Während aufstrebende Volkswirtschaften („Emerging Markets“) die durch Spionage generierten Informationen – ähnlich der reinen Werksspionage – zur unmittelbaren Verwertung in Unternehmen und der dadurch ermöglichten Stärkung der Wettbewerbsfähigkeit verwenden, setzen hoch entwickelte Industrieländer andere Methoden aufgrund der generierten Informationen ein. Sie profitieren oftmals mehr von verhinderten Geschäftsvorgängen anderer Unternehmen. Der Schwerpunkt liegt deshalb auf der Förderung der eigenen Wirtschaft bei der Vertragsvergabe. So werden z. B. Informationen

---

20 Bundesamt für Verfassungsschutz (2009), S. 28.

21 Anmerkung: Entsprechend der hL ist hier „Ausland“ als „EU-Ausland“ zu lesen. siehe hierzu OGH 19.08.2009, 15 Os 67/09f.

22 EBRV StRÄG 1965,9,L/St § 124 Rz1.

gezielt gestreut, die andere (ausländische) Unternehmen diskreditieren. Das soll den potentiellen Vertragspartner zu Gunsten eigener Unternehmen beeinflussen.

Wirtschafts- und Industriespionage unterscheiden sich somit hinsichtlich der Täter, aber nicht anhand der Unternehmen, die als Opfer ausgewählt werden.<sup>23</sup> Bei der Wirtschaftsspionage sind es staatliche oder staatlich gelenkte wirtschaftliche Unternehmen, welche als Akteure agieren. Bei der Industriespionage sind es (privat) wirtschaftliche Akteure, die mit dem Opfer in unmittelbarem oder mittelbarem Wettbewerb stehen. Obgleich unterschiedliche Strukturen von Volkswirtschaften und Unternehmen von Wirtschafts- oder Industriespionage profitieren, so sind die tatsächlich ausführenden Akteure immer Menschen.

| UNTERSCHIEDUNGSMERKMAL             | WIRTSCHAFTSSPIONAGE                                                                                                                                                                                                                    | INDUSTRIESPIONAGE                                                                                         |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Herkunft des Angreifers            | Staatlich gelenkte Nachrichtendienste                                                                                                                                                                                                  | Konkurrenzunternehmen                                                                                     |
| Ziel des Angriffs                  | Angriff erfolgt aufgrund national-ökonomischer Interessen gegen Wirtschafts- und Wissenschaftsunternehmen oder Industriebereiche anderer Länder und ist meist auf über einzelne Unternehmen hinausgehende Interessensgebiete gerichtet | Betriebs- und Geschäftsgeheimnisse zur Stärkung der Konkurrenzfähigkeit                                   |
| Zeitliche Ausrichtung des Angriffs | Ist oft auf langfristige Perspektiven (bis zu 20 Jahre) angelegt und darauf ausgerichtet, wirtschaftliche oder wissenschaftliche Defizite auf breiter Basis auszugleichen                                                              | Konzentriert sich meist auf zeitlich absehbare wirtschaftliche Vorteile                                   |
| Modus Operandi                     | Langfristig angelegte, professionelle Durchführung; Einsatz von nachrichtendienstlichen Mitteln; verdecktes Nutzen von Mitarbeitern                                                                                                    | Zeitlich absehbar, Einsatz von z.B. Privatdetektiven, Wissenshändlern, OK usw.; Abwerben von Mitarbeitern |
| Folgen/Geschädigte                 | Mittelbarer volkswirtschaftlicher Schaden, Schadenshöhe nur schwer abschätzbar                                                                                                                                                         | Unmittelbarer wirtschaftlicher Schaden für Einzelunternehmen                                              |
| Aufwand des Einsatzes              | Der betriebene Aufwand kann weit höher sein als dies rational erklärbar ist                                                                                                                                                            | Der betriebene Aufwand steht meist in einem materiellen Verhältnis zu dem angestrebten Ziel               |

**Abb. 10** Unterscheidung Wirtschafts- und Industriespionage

© Eigene Darstellung: In Anlehnung an WKÖ/FHCW/BVT (2011), S. 16

23 Siehe hierzu: Abbildung 9.

Klar ist, dass es aus Sicht des einzelnen Unternehmers nur von zweitrangiger Bedeutung ist, ob es sich um eine staatlich oder durch ein Konkurrenzunternehmen gelenkte Aktion handelt. Der Schaden bleibt der gleiche. Wichtig sind die Unterscheidung nach zivilrechtlichen und strafrechtlichen Normen sowie die Frage der Beweislast. Bei der Beweislast<sup>24</sup> müssen die damit allfällig verbundenen Kosten berücksichtigt werden, die auch zur Existenzbedrohung für das Unternehmen führen können. Von Interesse für Unternehmen sind daher in erster Linie der entstandene Schaden – und die bestehenden bzw. nicht bestehenden rechtlichen Möglichkeiten zu Schadenminimierung und -wiedergutmachung.

Zahlreiche Beispiele verdeutlichen, dass eine repressive Vorgehensweise oftmals zu spät ist, zu kurz greift und den Schaden sogar vergrößern kann. Aktiver Wirtschaftsschutz im Bereich Wirtschafts- und Industriespionage bzw. zum Schutz des unternehmensinternen Know-hows darf sich daher nicht auf die Frage reduzieren, inwiefern strafbare Handlungen gesetzt werden können bzw. gesetzt wurden. Entscheidend ist es, adäquaten Schutz für relevantes Wissen im Unternehmen zu entwickeln. Erfolgreicher Schutz vor Wirtschafts- und Industriespionage beginnt beim Denken und Handeln des Managements.

## Literatur

- Bundesamt für Verfassungsschutz (2009) – Glossar der Verfassungsschutzbehörden (12/2009), Deutschland.
- Fantapié Altobelli, Claudia (2011): Marktforschung. Methoden – Anwendungen – Praxisbeispiele.; Auflage: 2. überarb. u. erw. Aufl, UTB, Stuttgart.
- Koch, Jörg (2012): Marktforschung; Grundlagen und praktische Anwendungen, 6. Auflage, Oldenbourg Verlag, München.
- Lux, Christian; Peske, Thorsten (2002): Competitive Intelligence und Wirtschaftsspionage. Analyse, Praxis, Strategie. Gabler Verlag. Berlin.
- Michaeli, Rainer (2006). Competitive Intelligence: Strategische Wettbewerbsvorteile erzielen durch systematische Konkurrenz-, Markt- und Technologieanalysen. Berlin: Springer Verlag.
- Schaaf, Christian (2009): Industriespionage: Der große Angriff auf den Mittelstand. Boorberg. München.
- Wassermann Dr., Martin (1931): Werkspionage und Vorschläge zu ihrer Bekämpfung. Verlag Dr. Walther Rothschild, Berlin-Grunewald.
- WKÖ/FHCW/BVT (2011): Wirtschafts- und Industriespionage Handbuch Know-How-Schutz für die österreichische Wirtschaft. WKÖ. Wien.

---

24 Anmerkung: z. B. bei einem Privatanklagedelikt (§ 122 StGB).

## **Rechtstexte und Normen**

EBRV StRÄG 1965,9,L/St § 124 Rz1  
OGH 28.08.2012 12 Os 38/12y  
ÖNORM S 2430:2011

Wirtschafts- und Industriespionage

Informationsgewinnung – Management – Kompetenz

Hofer, A.; Weiß, M.

2016, XIV, 131 S. 25 Abb. in Farbe., Softcover

ISBN: 978-3-658-09232-0