Philipps-University Marburg
Department of Technology and Innovation Management

Discussion Papers on Strategy and Innovation

Discussion Papers on Strategy and Innovation 08-01

Michael Stephan
Martin Schneider

Schutzstrategien zur Aufdeckung und Abwehr von (Produkt-)Piraterie

Konzeptionelle Grundlagen zur wirksamen Bekämpfung der Produkt- und Markenpiraterie

Discussion Papers on Strategy and Innovation

Michael Stephan[☠]
Martin Schneider[☠☠]

Schutzstrategien zur Aufdeckung und Abwehr von (Produkt-)Piraterie

Konzeptionelle Grundlagen zur wirksamen Bekämpfung der Produkt- und Markenpiraterie

Discussion Paper 08-01
Marburg, Februar 2008
ISSN 1864-2039

☠ Prof. Dr. Michael Stephan, Contact: Department of Technology and Innovation Management (TIM), Philipps-University Marburg, Am Plan 2, D-35037 Marburg, E-mail: michael.stephan@wiwi.uni-marburg.de.

☠☠ Dipl. oec. Martin Schneider, Contact: Department of Technology and Innovation Management (TIM), Philipps-University Marburg, Am Plan 2, D-35037 Marburg, E-mail: martin.schneider@wiwi.uni-marburg.de.

Abstract

China gilt neben Russland als Hauptakteur bei der Verletzung von geistigem Eigentum. Als Hauptprobleme werden die Nichteinhaltung internationaler Verträge, das Fehlen von rechtlichen Durchsetzungsmöglichkeiten sowie die eingeschränkte Freiheit der Medien in der Berichterstattung genannt. Auch die zunehmende Verflechtung der Märkte und der Abbau von Handelshemmnissen begünstigen die illegale Imitation und den Vertrieb von Nachbauten. Die Verschmelzung von technologischen Wissenschaftsgebieten, die Dezentralisierung von Wissen und die Eskalation der Innovationskosten in Verbindung mit kürzeren Innovationszyklen verstärken das Schutzbedürfnis zusätzlich.

Die EU – Kommission beziffert den weltweiten Schaden durch Produkt- und Markenpiraterie in zurückhaltenden Schätzungen auf 129 Milliarden Euro und in Schätzungen welche auch die Dunkelziffern miteinbeziehen auf 370 Milliarden Euro pro Jahr. Die Internationale Handelskammer (ICC) rechnet mit einem Volumen von fünf bis sieben Prozent des Welthandels. Die Weltorganisation für Geistiges Eigentum (WIPO) beziffert den Schaden auf 450 Milliarden US-Dollar (circa fünf Prozent des Welthandels) und der Aktionskreis Deutsche Wirtschaft gegen Produktpiraterie e.V. (APM) gibt fünf bis acht Prozent an. Wird von einem Welthandelsvolumen von knapp 10.000 Milliarden US-Dollar im Jahr 2005 ausgegangen, so ergibt sich bei einer Annahme von fünf Prozent ein Schadensvolumen von 500 Milliarden US-Dollar. Exakte Schätzungen der Schadenssumme durch Produktpiraterie sind nur schwer möglich und alle Institutionen gehen von einer hohen Dunkelziffer aus. Auch wenn sich die einzelnen Prognosen unterscheiden, so wird dennoch deutlich, dass Fälschungen einen nicht zu unterschätzenden und weiter wachsenden Schadensfaktor insbesondere für deutsche Unternehmen und die deutsche Volkswirtschaft darstellen.

In diesem Diskussionspapier erfolgt die Herleitung von konzeptionellen Grundlagen zur Gestaltung eines Schutzsystems. Schutzsysteme zur Bekämpfung von (Produkt-) Piraterie müssen über eine passende schutzstrategische Grundhaltung in das strategische Technologie- und Innovationsmanagement integriert sein. Aus der entsprechenden schutzstrategischen Grundhaltung lassen sich dann konkrete juristische, technische, geheimhaltungsbezogene sowie flankierende betriebswirtschaftliche und politische Maßnahmen zur Gestaltung eines unternehmensspezifischen Schutzsystems ableiten. Darüber hinaus empfiehlt sich zur Lösung des Informationsproblems die Gestaltung eines Competitive Intelligence Systems.

Schlüsselwörter:

Competitive Intelligence, Intellectual Property Management, Konzept-, Marken- und Produktpiraterie, strategisches Management, alternative Schutzinstrumente.

Inhaltsverzeichnis

1. Problem und Phänomen der Produktpiraterie

Die EU – Kommission beziffert den weltweiten Schaden durch Produkt- und Markenpiraterie auf 129 – 370 Milliarden Euro pro Jahr.[1] Von den im Jahr 2005 im Wert von 215 Millionen Euro beschlagnahmten Waren an der deutschen Grenze stammen mehr als ein Drittel aus China. Die Zahl der Grenzbeschlagnahmungsfälle für Konsumgüter durch die Zollbehörde hat sich in den letzten zehn Jahren mehr als verdoppelt.[2] Die Internationale Handelskammer (ICC) rechnet mit einem Volumen von fünf bis sieben Prozent des Welthandels.[3] Die Weltorganisation für Geistiges Eigentum (WIPO) beziffert den Schaden auf 450 Milliarden US-Dollar (ca. fünf Prozent des Welthandels) und der Aktionskreis Deutsche Wirtschaft gegen Produktpiraterie e.V. (APM) gibt fünf bis acht Prozent an.[4] Wird von einem Welthandelsvolumen von knapp 10.000 Milliarden US-Dollar im Jahr 2005 ausgegangen, so ergibt sich bei einer Annahme von fünf Prozent ein Schadensvolumen von 500 Milliarden US-Dollar.[5] Exakte Schätzungen der Schadenssumme durch Produktpiraterie sind nur schwer möglich und alle Institutionen gehen von einer hohen Dunkelziffer aus. Auch wenn sich die einzelnen Prognosen unterscheiden, so wird dennoch deutlich, dass Fälschungen einen nicht zu unterschätzenden und weiter wachsenden Schadensfaktor insbesondere für deutsche Unternehmen und auch die deutsche Volkswirtschaft darstellen.[6]

China gilt neben Russland als Hauptakteur bei der Verletzung von geistigem Eigentum.[7] Als Hauptprobleme werden die Nichteinhaltung internationaler Verträge, das Fehlen von rechtlichen Durchsetzungsmöglichkeiten sowie die eingeschränkte Freiheit der Medien in der Berichterstattung genannt. Auch die zunehmende Verflechtung der Märkte und der Abbau von Handelshemmnissen begünstigen die illegale Imitation und den Vertrieb von Nachbauten. Die Konvergenz bzw. Verschmelzung von technologischen Wissenschaftsgebieten, die Dezentralisierung von Wissen und die Eskalation der Innovationskosten in Verbindung mit kürzeren Innovationszyklen verstärken das Schutzbedürfnis zusätzlich.

Mittlerweile können sich immer weniger Branchen der Produktpiraterie entziehen, auch Produkte aus dem Maschinenbau, der Elektro-, Automobil-(zulieferer-) und Pharmaindustrie sind

---

1 Vgl. Deutscher Bundestag (2006), S. 4f.
2 Vgl. Zollbehörde (2005).
3 Vgl. ICC (2007).
4 Vgl. Wildemann et al. (2007), S. 2.
5 Vgl. WTO (2006); WTO (2006b).
6 Vgl. Wildemann (2007).
7 Vgl. ICC (2007), S. 3, 12.

zunehmend betroffen. Darüber hinaus zeigt eine Studie des VDMA vom März 2006 auf, dass zwei Drittel der befragten Unternehmen der Investitionsgüterindustrie bereits von Produktpiraterie betroffen sind und 77 Prozent einen Anstieg der Produktpiraterie erwarten.[8] Insbesondere für die international und innovationsorientiert agierenden deutschen Unternehmen wiegt dieser Befund schwer. Angesichts der Bedrohung durch Produktpiraterie laufen deutsche Unternehmen Gefahr, ihren Technologie- und Wettbewerbsvorsprung zu verlieren.[9]

Schutzsysteme zur Bekämpfung von (Produkt-) Piraterie müssen über eine passende schutzstrategische Grundhaltung in das strategische Technologie- und Innovationsmanagement integriert sein. Schutzstrategische Grundhaltungen leiten sich aus übergeordneten Überlegungen zur Technologie- bzw. Innovationsstrategie ab und reichen von einer passiven Duldungsstrategie bis hin zu einer offensiven Bekämpfungs- bzw. Verfolgungsstrategie. Aus der schutzstrategischen Grundhaltung lassen sich dann konkrete juristische, technische, geheimhaltungsbezogene sowie flankierende betriebswirtschaftliche und politische Maßnahmen zur Gestaltung eines unternehmensspezifischen Schutzsystems ableiten.

Zur Lösung des Problems der Erkennung und Aufklärung der Bedrohung durch (Produkt-) Piraterie ist die Einrichtung eines Systems zur sogenannten ‚Competitive Intelligence' (nachfolgend auch CI) erforderlich.[10] CI stellt (u. a.) Methoden und Instrumente zur Aufdeckung und Abwehr von Fälschungen bereit. Ganz allgemein wird unter CI

> *„der systematische Prozess der Informationserhebung und –analyse bezeichnet, durch den aus fragmentierten (Roh-) Informationen über Märkte, Wettbewerber und Technologien den Entscheidern ein plastisches Verhältnis für ihr Unternehmensumfeld und damit eine Entscheidungsgrundlage geliefert wird".*[11]

Auf Grundlage der Informationsbereitstellung durch CI kann eine Unterstützung von Schutzstrategien und Maßnahmen für Unternehmen zur Abwehr von Produktpiraterie erfolgen.

Ziel des vorliegenden Diskussionspapiers ist es, einen konzeptionellen Bezugsrahmen zum wirksamen Umgang bzw. zur Bekämpfung von Produktpiraterie aus dem übergeordneten Theoriegebäude des strategischen Technologie- und Innovationsmanagements abzuleiten. Der Bezugsrahmen thematisiert zunächst die strategische Verankerung eines solchen Schutzsystems, beinhaltet aber auch eine konkrete Maßnahmenplanung sowie den Einsatz von CI zur Aufdeckung und Abwehr von Fälschungen. Der Aufbau des Diskussionspapiers

---

8 Nach Wildemann (2007), S. 3f.
9 Vgl. Burr/Stephan et al. (2007), S. 276.
10 Vgl. Michaeli (2006), S. 21.
11 Michaeli (2006), S. 3.

orientiert sich am idealtypischen Ablauf der Formulierung von Strategien und Maßnahmen im Kontext des strategischen Managements. In Teil 2 werden zunächst Formen der Piraterie und diese begünstigende Faktoren vorgestellt. Im Sinne einer strategisch orientierten Gegenwarts- und Zukunftsbeurteilung wird das Konzept der CI herausgearbeitet. Aufbauend auf der Informationsbereitstellung durch CI wird schließlich eine grundlegende strategische Stoßrichtung bzgl. der schutzstrategischen Grundhaltung festgelegt, welche die Basis für die Planung der konkreten Maßnahmen darstellt. Teil 3 stellt verschiedene Instrumente und konkrete Maßnahmenkataloge zur Abwehr bzw. Bekämpfung von (Produkt-)Piraterie vor. Das Diskussionspapier endet mit einem konzeptionellen Fazit und Ausblick auf zukünftige Forschungsarbeiten.

2. Grundlagen eines konzeptionellen Bezugsrahmens zum wirksamen Umgang mit und Schutz vor (Produkt-)Piraterie

2.1 Erscheinungsformen und Ursachen von Fälschungen

Bei der Behandlung der Fälschungsthematik wird eine Vielzahl an Bezeichnungen verwendet. Die folgenden Begriffe sind voneinander zu unterscheiden:

- **Produktpiraterie (im engeren Sinne):** Unter dem Begriff der Produktpiraterie wird die illegale Nachahmung und Vervielfältigung von Waren, für die der rechtmäßige Hersteller Erfindungs-, Design- oder Verfahrensrechte besitzt, verstanden.
- **Markenpiraterie:** Die Bezeichnung Markenpiraterie beinhaltet die illegale Verwendung von geschützten Zeichen, Namen und Logos (Marken) sowie geschäftlichen Bezeichnungen, die von Markenherstellern zur Kennzeichnung der eigenen Produkte im Handel eingesetzt werden.
- **Konzeptpiraterie:** Im Gegensatz zur Produkt- und Markenpiraterie bezieht sich die Konzeptpiraterie auf von Herstellern und Dienstleistern entwickelte Prozesse. Nachahmer übernehmen ein definiertes Konzept und generieren das gleiche Konzept unter einem anderen Branding.
- **Plagiat:** Plagiate bezeichnen Verletzungen des Designs nach dem Urheberrecht und Geschmacksmuster. Der Plagiator verletzt diese Rechte bewusst, indem er fremdes Ideengut (Geistesgut) als sein eigenes ausgibt.
- **Falsifikat:** Eine Fälschung wird als Falsifikat bezeichnet. Der Fälscher verletzt bewusst bestehende Schutzrechte der Rechtsinhaber. Im Gegensatz zum Plagiat entwendet er

nicht die Idee, sondern produziert bspw. einen Gegenstand und kennzeichnet ihn mit einer Marke, an der er keine Rechte besitzt.

- **Counterfeiting:** Der aus dem englischsprachigen Raum kommende Begriff bedeutet in der deutschen Sprache schlicht „Fälschung“ und wird dort synonym mit Produkt- und Markenpiraterie verwendet. Die EU-Kommission erarbeitet derzeit eine geeignete Definition für Produkt-, Marken- und Dienstleistungspiraterie.
- **Sklavische Nachahmung:** Bei einem Plagiat steht die Nachahmung eines Produkts zur wirtschaftlichen Ausbeutung im Zentrum. Es kann entweder sklavisch exakt oder mit kleineren Änderungen nachgebaut werden.[12]

Wie zu erkennen ist, wird Produkt- und Markenpiraterie von Nachahmern verwendet, um die Bekanntheit eines Produkts oder eine Marke zu nutzen und über die tatsächliche Herkunft und Qualität hinwegzutäuschen. Die Konzeptpiraterie steht dagegen für die analoge Nachahmung eines Basiskonzepts, im Sinne der Übertragung oder Adaption eines Geschäfts-, Produkt- oder Prozessmodells. Im Folgenden wird die Definition von *Wildemann et al. (2007)* verwendet, der zufolge

> *„bei Produktpiraterie eine Ware nachgeahmt [wird], für welche der Orginalhersteller Verfahrens-, Erfindungs- oder Designrechte besitzt, er also Patentinhaber oder Urheber ist, oder ein gebrauchs- beziehungsweise geschmacksmusterrechtlicher Schutz besteht.“*[13]

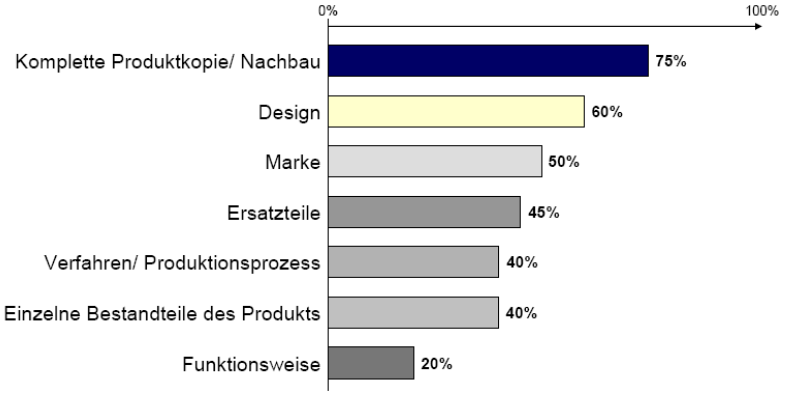
In der Praxis treten die verschiedenen Piraterieformen nicht in Rein-, sondern in Mischform auf. Eine einheitliche Definition für Piraterie hat sich noch nicht herausgebildet, weshalb im Folgenden auch auf Markenpiraterie eingegangen wird. Vereinfachend wird von (Produkt-) Piraterie, Nachahmungen oder Fälschungen gesprochen und bei Bedarf auf Unterschiede in den Piraterieformen eingegangen. Abb. 1 zeigt die Verteilung der Pirateriefälle.

---

[12] Vgl. Sokianos (2006), S. 20f.

[13] Wildemann et al. (2007), S. 1.

Abb. 1: Betroffenheit durch Piraterie (in Prozent der befragten Unternehmen)



Quelle: *Wildemann et al. (2007), S. 4.*

Zur Anwendung von Strategien zum Schutz der Innovation ist die Kenntnis potenzieller Ursachen bzw. Quellen von Fälschungen notwendig:

1) Eine Ursache stellt der *Geheimnisverrat durch eigene Mitarbeiter* dar. Motive für deren Handlungen können finanzielle Not, Geldgier, Rache oder Profilierungswünsche sein. Während finanzielle Not und Geldgier relativ einfach durch Unterstützung von Unternehmensseite aus oder der Androhung rechtlicher Konsequenzen begegnet werden kann, sind Racheabsichten und Profilierungsabsichten schwieriger festzustellen.[14]
2) Als weitere Quelle für Produktpiraterie sind *Unternehmensdokumentationen* aller Art, vor allem aber die technische Produktdokumentation zu nennen. Beispiele sind Lasten- und Pflichtenhefte, Entwürfe, technische Zeichnungen, Schalt- und Arbeitspläne, Ersatzteillisten und Betriebsanleitungen. Über die technischen Produktdokumentationen erhalten Produktpiraten Zugriff auf Zeichnungen und Stücklisten und verringern auf diesem Weg den Nachahmungsaufwand. Vereinfacht wird dies durch die zunehmenden Downloadgelegenheiten auf Internetseiten der Hersteller. Ein weiteres Problem ist, dass eine Dokumentation kopiert werden kann und Pirateriewaren damit eine höhere Authentizität erhält.[15]
3) Sowohl in der *Beschaffung* als auch im *Vertrieb* kann die Gefahr des Wissensabflusses an Fälscher auftreten. Auf Zuliefererseite werden Rohstoffe oder Vorprodukte der Originalteile von Piraten eingekauft, entwendet oder über die Einschleusung von Mitarbeitern kopiert. Diese Vorgehensweise wird durch Intransparenz und Mangel an objektiven Einkaufsführern begünstigt. Gefahren auf Vertriebsseite bestehen in der Bestechung von

[14] Vgl. Pütz/ Rundstedt (2006), S. 56ff.; Levin et al. (1987), S. 806f.
[15] Vgl. u. a. Helbig (2006), S. 150ff.

Vertriebsmitarbeitern, dem Verlust von Produkten auf undurchsichtigen Vertriebswegen oder der Unterstützung der Fälscher beim Vertrieb der Pirateriewaren.[16]

4) Die *Fertigung* selbst ist ebenfalls eine Quelle für Produktpiraterie. Der unkontrollierte Zugang zu Bauplänen, Materialien oder Maschinenspezifikationen ermöglicht den Diebstahl von Dokumenten, Komponenten oder fertigen Endprodukten. Die unkontrollierte Entsorgung von Ausschussteilen kann von Fälschern in gleichem Maße zur Erlangung der benötigten Informationen verwendet werden.[17]
5) Auch die *Lizenzierung der Konkurrenztechnologie* ist als Ursache zu sehen. Indem Unternehmen Teile einer Technologie lizenzieren erhalten sie umfassenden Einblick und können Rückschlüsse für die eigene Imitation ableiten. Analog können auch aus der *Offenlegung von Patentschriften* Informationen an Konkurrenten abfließen.[18]
6) Eine effektive Methode zur Nachahmung der Originalprodukte ohne die Kenntnis der genauen Produktdokumentation kann durch *Reverse Engineering* erfolgen. Dabei wird das Originalprodukt Stück für Stück demontiert, so dass die genauen Produktspezifika messbar gemacht werden.[19]
7) Im Rahmen von *Outsourcing* vergeben Unternehmen einzelne Projekte oder ganze Unternehmensfunktionen, wie bspw. IT-Abteilungen, an Fremdunternehmen. Oftmals werden sogar Entwicklungen von Zulieferern vorgenommen, so dass das originäre Wissen nicht mehr beim Hersteller verbleibt. Mit Outsourcing erhöht sich die Gefahr des Informationsabflusses, die Piraterie wird erleichtert.[20]
8) *Kooperationen zwischen Unternehmen* können ebenfalls eine Ursache für Know-how Abfluss sein. Eine wichtige Aufgabe innerhalb einer Kooperation ist demnach die Überprüfung der Haltung zum Schutz geistigen Eigentums beim Kooperationspartner.[21] In vielen Ländern ist der Marktzugang nur über Kooperationen möglich. So ist bspw. die chinesische Regierung bestrebt, ausländische Unternehmen zu einer engen Zusammenarbeit mit chinesischen Unternehmen und staatlichen Stellen zu bewegen. In einigen Branchen, wie im Automobil- oder Schienenfahrzeugbau, sind Joint-Ventures als Eintrittsvoraussetzung in den Markt zwingend vorgeschrieben. Bei der Ausschreibung von öffentlichen Aufträgen müssen ausländische Unternehmen bis zu 80 Prozent lokale Fertigung nachweisen. Die Erbringung dieses Anteils ist aber nicht durch Tochtergesellschaften möglich, sondern

---

16 Vgl. u. a. Fuchs et al. (2006) 220f., 248f.
17 Vgl. u. a. Fuchs et al. (2006), S. 239.
18 Vgl. Burr/Stephan et al. (2007), S. 108f.
19 Vgl. u. a. Levin et al. (1987), S. 805ff.
20 Vgl. Levin et al. (1987), S. 805; Lfv (2004), S. 16f.
21 Vgl. Bremicker (2006), S. 68.

muss in Kooperation mit chinesischen Partnern erbracht werden. Im Maschinen- und Anlagenbau wird eine weit reichende technologische Zusammenarbeit mit chinesischen Designinstituten bis hin zur Weitergabe von technischen Dokumentationen oder der Ausbildung chinesischer Fachkräfte eingefordert. Für viele Produkte besteht eine Zertifizierungspflicht durch entsprechende chinesische Stellen.[22]

9) Eine sehr häufig vorkommende Ursache für Piraterie ist der Besuch von entsprechenden *Fach- und Publikumsmessen*. Auf diesen können auf der einen Seite Produkte, die für eine Nachahmung interessant sein könnten, genauer untersucht werden und auf der anderen Seite bereits hergestellte Pirateriewaren auf ihre Marktfähigkeit getestet werden, bevor sie in Serie produziert wird.[23]

Zwischen der Produktpiraterie und dem Phänomen der Wirtschaftsspionage besteht eine enge, fließende Verbindung. Infolge der Verbreitung IT-gestützter Informationssysteme in Unternehmen können Angriffe auf Computer (z. B. durch Hacking, Einschleusung von Viren, Trojanern und Würmern), Lauschangriffe auf Gebäude und Telekommunikationssysteme sowie Diebstahl von Hardwarekomponenten (z. B. Laptop, Organizer und Speichermedien) zur Unterstützung der Produktpiraterie beitragen. Ein in vielen Fällen vernachlässigter Faktor kann die auf Sicherheitsprobleme ungeprüfte Anstellung von Doktoranden, Diplomanden oder Praktikanten sein.[24] Wirtschafsspionage setzt vor allem in der F&E an, um u. a. frühzeitig auf potenzielle Produkte zur Nachahmung aufmerksam zu werden.

Die Folgen von Piraterie sind unmittelbar oder erst mittelbar auf längere Frist erkennbar. Unmittelbare Folgen sind Umsatz- und Gewinnverluste oder Zusatzkosten für Schutzmaßnahmen. Direkte Umsatz- und Gewinnverluste entstehen durch die Produktpiraten als zusätzliche Marktteilnehmer. Originale werden durch Piraterieprodukte substituiert. Zusatzkosten entstehen den von Piraterie bedrohten oder betroffenen Unternehmen durch die Anmeldung, Verfolgung und Durchsetzung von Schutzrechten sowie der Verwendung zusätzlicher Schutzmaßnahmen. Abb. 2 zeigt, dass die Kosten für Marktbeobachtung, Verfolgung und technische Schutzmaßnahmen knapp ein Viertel des unmittelbaren Schadens ausmachen.

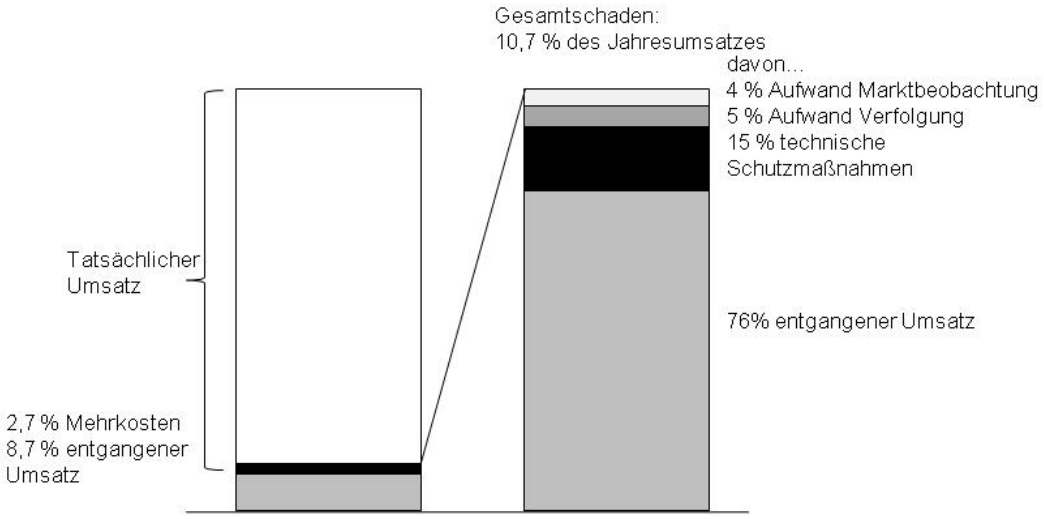
---

[22] Vgl. APA (2006), S. 1f.

[23] Vgl. Wildemann et al. (2007), S. 15.

[24] Vgl. LfV (2004), S. 14ff.

Abb. 2: Kostenzusammensetzung im Pirateriefall



Quelle: Eigene Darstellung in Anlehnung an *Wildemann et al. (2007), S. 6.*

Neben unmittelbar auftretenden Ertragsminderungen sind im Pirateriefall auch längerfristige Folgen zu erwarten. Infolge der Positionierung zu geringeren Preisen am Markt wächst der Preisdruck auf die Hersteller der Originalprodukte zur Aufrechterhaltung des eigenen Marktanteils, so dass die Gefahr einer dauerhaften Senkung des Preisniveaus besteht.[25]

Die Qualität der Piraterieprodukte erreichen selten die Qualitätsstufen der Originalprodukte. Käufer halten diese Nachahmungen allerdings oftmals für Originale oder nehmen mit gefälschten Marken versehene Plagiate nicht als solche wahr, so dass Negativerfahrungen über das gefälschte Produkt auf die Marke und die Originalprodukte übertragen werden. Marken- und Produktpiraterie führen, in Kombination mit einer verminderten Exklusivität der Marke durch ein erhöhtes Angebot, zu einer Verwässerung der Marke und Reputationsschäden, aus welchen wiederum Umsatzverluste resultieren können. Aufgrund von fehlerhaften oder qualitativ minderwertigeren Piraterieprodukten können Unfälle mit Sach- und Personenschaden auftreten. Unter Umständen wird der Originalhersteller von der geschädigten Partei haftbar gemacht und hat zu beweisen, dass er nicht für den Schaden verantwortlich ist und nicht mit der Nutzung von Piraterieware im Zusammenhang steht. Die Verfahrenskosten und der Reputationsschaden in der Öffentlichkeit können für den Hersteller hoch sein. Sollten schuldhafte Handlungen nachgewiesen werden, steigen die Kosten weiter an.[26]

---

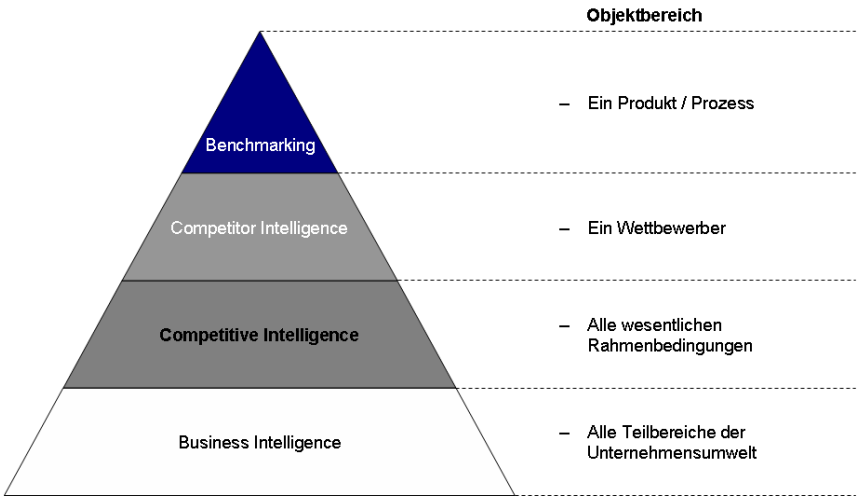
[25] Vgl. Wildemann et al. (2007) 4ff.

[26] Vgl. Wildemann et al. (2007) 5ff; Fuchs et al. (2006) 43ff.

2.2 Zum Konzept einer Competitive Intelligence

Der erste Arbeitsschritt in einem System des wirksamen Umgangs mit bzw. der effektiven Bekämpfung von Produktpiraterie beinhaltet eine strategisch orientierte Gegenwarts- und Zukunftsbeurteilung zur Erkennung und Aufklärung der Bedrohung durch (Produkt-) Piraterie. Das notwendige Instrumentarium hierzu wird durch eine sogenannte ‚Competitive Intelligence' bereitgestellt. Eine Möglichkeit zur Abgrenzung des Konzepts der CI von anderen, z. T. eng verwandten Begriffen, wie Business Intelligence, Competitor Intelligence oder Benchmarking, bildet der durch die Analyse abgedeckte Objektbereich. Es wird nach den in die Analyse einbezogenen Teilsegmenten differenziert (vgl. Abb. 3).[27]

Abb. 3: Abgrenzung der verschiedenen ‚Intelligence'-Begriffe;



Quelle: Eigene Darstellung in Anlehnung an *Kunze (2005), S. 66.*

Einen sehr weit gefassten Objektbereich deckt die ‚Business Intelligence' (BI) ab. Die Suche nach Informationen umfasst dabei (potenzielle) Märkte, neue Technologien, (potenzielle) Wettbewerber sowie allgemeine gesellschaftliche Entwicklungen.[28] In der Analyse werden keine Einschränkungen auf Teilsegmente vorgenommen, da die gesamte Umwelt als Untersuchungsgegenstand dienen kann, solange die Informationen entscheidungsrelevant sind.[29]

---

[27] Vgl. Kunze (2000), S. 64.
[28] Vgl. Ghoshal (1986), S. 49.
[29] Vgl. Gilad/Gilad (1988), S. vii.

In Anlehnung an die in dieser Arbeit verwendete Definition wird der Objektbereich dagegen enger gefasst – Gegenstand der Informationsgewinnung im Rahmen der Competitive Intelligence sind Märkte, Technologien und Wettbewerber. CI soll die Antizipation sich verändernder Branchenstrukturen und eine möglichst frühzeitige Anpassung der Unternehmensstrategie ermöglichen. Die Identifizierung und Analyse breiter sozialer Trends ist im Gegensatz zur BI kein elementarer Untersuchungsbestandteil.[30] Der Untersuchungsbereich von CI ist somit vergleichbar mit der Branchenanalyse nach Porter.[31] ‚Competitor Intelligence' ist enger gefasst und bezieht sich auf die Sammlung von Aktivitäten, Eigenheiten und Strategien von Wettbewerbern.[32] Somit kann Competitor Intelligence als Element von CI betrachtet werden.

Neben dem Interesse an einer Darstellung von Branchen und Wettbewerbern sind Informationen zur Analyse von betrieblichen Schwachstellen wichtig für Unternehmen. In einem solchen Fall kann die Notwendigkeit entstehen, ‚Benchmarking' zu betreiben und unternehmenseigene Strukturen und Prozesse mit Wettbewerbern bzw. Best-Practice-Unternehmen zu vergleichen. Benchmarking ist somit Teilelement der Competitor Intelligence.

Der Begriff ‚Intelligence' ist ursprünglich auf den militärischen Sprachgebrauch zurückzuführen und wird mit (Früh- bzw. Feind-)Aufklärung übersetzt (siehe z. B. die Bezeichnungen ‚Luft- und Panzeraufklärung'). Im Kontext der Notwendigkeit von Unternehmen, sich durch die Beschaffung und Auswertung von Informationen über Märkte, Wettbewerber, Kunden und Technologien selbst zu positionieren, wird die Entscheidungsfindung und zeitlich optimale Umsetzung in Wettbewerbsstrategien analog zur militärischen Erklärung gesehen. Die wettbewerbsorientierte Ausrichtung der Tätigkeiten führt zu dem ergänzenden Begriff ‚Competitive'.[33] CI hat seinen Ursprung in staatlichen Nachrichten (Intelligence-) Diensten. Im Management sind heute CI relevante Themen überwiegend im Feld der Strategieformulierung bzw. im Kontext von Wettbewerbsanalysen zu finden. Zwischen der traditionellen Marktforschung und CI existieren Zusammenhänge insbesondere bei der Erforschung von Kundenpräferenzen und der Verwendung von Analyseverfahren (z. B. Marktsegmentierung), so dass sich diese Disziplinen komplementär verwenden lassen.[34]

Das vage formulierte Ziel von Competitive Intelligence-Aktivitäten, nämlich aus fragmentierten (Roh-)Informationen über Märkte, Wettbewerber und Technologien den Entscheidern ein

---

[30] Vgl. Babbar/Rai (1993); Kunze (2000), S. 65.
[31] Vgl. Porter (1980) 4ff.; Porter (1985).
[32] Vgl. Sammon (1984), S. 62.
[33] Vgl. Michaeli (2006), S. 3.
[34] Vgl. Michaeli (2006), S. 32ff.

plastisches Verständnis über ihr Unternehmensumfeld und damit eine Entscheidungsgrundlage zu liefern, bedingt eine große Heterogenität der Anforderungen an CI-Analysen. Unterschiede können bei den Inhalten, der zeitlichen Stabilität und Fristigkeit der Ergebnisse, der Analyserhytmik und –frequenz, der Analysetiefe sowie der jeweiligen Zielgruppen auftreten.[35] Abbildung 4 stellt Kriterien, Ausprägungen und Beispiele der CI dar.

Abb. 4: Kriterien, Ausprägungen und Beispiele der CI

Kriterium	Ausprägung	Beispiele für CI
Inhalte	Markt-, wettbewerbs-, technologie- und umfeldorientierte Analysen	▸ Analyse der Konsequenzen neuer Substitutionsprodukte, der Produktpolitik eines Wettbewerbers oder von Patentdaten zur Identifikation technischer Trends ▸ Beobachtung politischer Entwicklungen in einem Zielmarkt
Zeitliche Stabilität und Fristigkeit	Von unmittelbarer bis langfristiger Gültigkeit	▸ Bereitstellung von Aktienkursdaten der Wettbewerber ▸ Analyse demographischer Entwicklungen im Zielgruppensegment
Analyserhythmik	Einmalig, wiederholt oder regelmäßig	▸ Analyse von Handlungsoptionen in Krisensituationen ▸ Marktanalyse zur Neuproduktentwicklung ▸ Benchmarking von Wettbewerbern
Analysefrequenz	Jährlich bis mehrmals täglich	▸ Benchmarking der Jahresabschlussdaten ▸ Bereitstellung von Daten zur Preispolitik von Wettbewerbern
Analysetiefe	Keine Datenaufbereitung bis komplexe Analyse erforderlich	▸ Bereitstellung von Daten zu Aktienkursen ▸ Analyse einer großen Zahl an Nachrichtenmeldungen zu Wettbewerbern
Zielgruppen	Marketing, Planung, F&E Strategisches, taktisches und operatives Management	▸ Analyse von Marktanteilen ▸ Szenariobasierte Analyse des Werbemittelbudgets ▸ Identifikation bspw. von potenziell disruptiven Technologien oder Best Practises ▸ SWOT-Analyse zur Strategieentwicklung ▸ Marktanalysen für Produktmanager

Quelle: *Kemper (2006), S. 17*.

Hinsichtlich der Analysefrequenz lassen sich zwei grundsätzliche Formen von CI-Aktivitäten unterscheiden: CI-Aktivitäten können im Rahmen eines befristeten Projektes, d. h. temporär begrenzt oder aber institutionalisiert und auf Dauer angelegt sein. Die Institutionalisierung von CI in der Organisation erfordert die Implementierung einer professionellen CI-Abteilung oder eines CI-Centers.[36] Die zu schaffende CI-Einheit sollte an vorhandene Organisationsstrukturen, wie bspw. an die Konzernplanung angegliedert werden. Dauerhafte CI-Aufgaben lassen sich in Scanning- und Monitoring-Aktivitäten gliedern. Ähnlich wie bei projektbezogenen Aktivitäten liegt der Schwerpunkt beim Scanning auf der Identifikation (potenziell) rele-

[35] Vgl. Lux (2002), S. 61f.
[36] Vgl. Michaeli (2006), S. 443f.

vanter Analyse- bzw. Beobachtungsobjekte (‚Identifikationszielsetzung'). Genauer betrachtet befasst sich Scanning mit der Identifikation von Veränderungen im Unternehmensumfeld, welche potenzielle Chancen oder Gefahren für die Strategie oder das Unternehmen selbst darstellen. Sind die Chancen oder Gefahren identifiziert, werden sie in CI-Projekten genauer untersucht. Monitoring richtet sich auf die kontinuierliche Beobachtung bereits bekannter Analyseobjekte bzw. bekannter Recherchegegenstände (z. B. Websites, Frühwarnindikatoren, Patentdatenbanken, etc.).[37] Ein spezifische Variante des Monitoring bildet bspw. die Observation von Wettbewerberaktivitäten. Die Observation beinhaltet alle direkten und indirekten audiovisuellen Maßnahmen zur Erfassung von Wettbewerberaktivitäten. Zum Observationsgegenstand zählen Personen, Anlagen und Gebäude, Materialflüsse, Messe- und Konferenzauftritte.[38] Während beim Monitoring der Recherchegegenstand bzw. der Analysefokus, d. h. die Einheit, über die Wissen erlangt werden soll, bereits bekannt sind, ist der Analyse- bzw. Recherchefokus beim Scanning noch unbestimmt. Beispiele für Recherchegenstände sind Unternehmen (Wettbewerber), Produkte, Personen oder einzelne Sachverhalte.

2.3 CI-Bestandteile und Analyseverfahren

Grundvoraussetzung für genauere Einblicke in die verschiedenen Analyseebenen von CI-Aktivitäten ist die Kenntnis der verschiedenen CI-Bestandteile bzw. Komponenten. Elementare Grundlage von CI-Aktivitäten bilden (Roh-)Daten und schwache Signale (z. B. Gerüchte oder subjektive Eindrücke). Sowohl (Roh-) Daten als auch schwache Signale liefern im Rahmen von Scanning-Aktivitäten erste Hinweise zu relevanten Recherche- bzw. Analysegegenständen. Diese Daten bzw. Signale werden durch Aufbereitung, Evaluierung, Interpretation und Integration zu Informationen, welche Entscheidungen beeinflussen können. So lassen sich Rohdaten durch entsprechende Überprüfung der Inhalts- und Konstruktvalidität zu Indikatoren für bestimmte entscheidungsrelevante Sachverhalte aufwerten. Indikatoren kündigen demzufolge einen spezifischen Sachverhalt (bzw. das Eintreten sowie das Nichteintreten dieses Sachverhalts) an. (Competitive) Intelligence stellt aufbereitete und in einen Entscheidungskontext eingebrachte Information dar. Dies beinhaltet die Aufbereitung und Anreicherung von Informationen zu Hypothesen (Kausalzusammenhänge im Kontext des Recherchegegenstandes), welche durch die Herbeiführung von Indizien und Fakten getestet bzw. überprüft werden müssen.[39]

---

[37] Vgl. Michaeli (2006), S. 118.

[38] Zu einer ausführlichen Vorstellung der Observation siehe Michaeli (2006) 178ff.

[39] Vgl. Michaeli (2006), S. 27f.

Je nach erforderlicher Analysetiefe kann sich die Entscheidungsunterstützung durch CI auf die Reduzierung von Informationen auf entscheidungsrelevante Inhalte, der Nutzenabschätzung einer Information, der Unterbindung subjektiver Wahrnehmungsfehler beim Entscheider, der Definition von neutralen Projektabbruchsgrenzen, Risikoeinschätzungen, der Einordnung von Intelligence in den Entscheidungskontext sowie auf die Erfahrungssteigerung der Entscheider beziehen.[40] Zur Effizienzsteigerung und Schaffung von Transparenz ist eine klare Strukturierung von CI-Aktivitäten sinnvoll. Abb. 5 illustriert eine solche Strukturierung für projektbezogene CI am Beispiel des sogenannten ‚Competitive Intelligence-Zyklus'.

Abb. 5: Der Competitive Intelligence Zyklus

Quelle: In Anlehnung an *Michaeli (2006), S. 117* sowie *Ashton/Klavans (1997).*

Im CI-Zyklus folgt auf die Bedarfsermittlung, d. h. nach der Präzisierung des Analyseobjektes, die Phase der Planung, in der die Vorgehensweise für CI festgelegt wird. Aufgabe der CI-Planung ist es, ein „kritisches Informationsvolumen" sicherzustellen, auf dessen Basis die spätere Analyse zur Intelligence-Bildung erfolgen kann. Eine wichtige Aufgabe im Kontext der CI-Planung ist demnach die Identifikation und Verwaltung von Datenquellen. In der Datenerhebung erfolgt die (Roh-)Datensammlung gemäß den Planungsvorgaben. In dieser Phase erfolgt die eigentliche Datenrecherche nach den Regeln des Erhebungsplans. Prinzipiell können Daten und Informationen aus Primär- und Sekundärquellen gewonnen werden. Der Schwerpunkt der CI-Datenerhebung beruht jedoch auf Primärquellen, da diese einen

[40] Vgl. Michaeli (2006), S. 110.

höheren Wert für CI aufweisen. Quellen für Primärrecherchen sind Informationsnetzwerke, Human Intelligence und Wettbewerbsbeobachtungen. Sekundärquellen sind alle vom oder über das Analyseobjekt verfassten Publikationen. Dies können Geschäftsberichte, Jahrbücher, (Fach-)Artikel aus (Fach-)Zeitschriften und Magazinen, Zeitungen, Gerichtsprotokollen, Patentinformationen sowie akademische Veröffentlichungen sein. Auch das Internet sowie die Nutzung von (Online-) Datenbanken sind zu den Sekundärrecherchen zu zählen.[41]

Im Rahmen der Daten- und Informationsaufbereitung erfolgt die Transformation der fragmentierten, eventuell unvollständigen und unbearbeiteten Rohdaten unterschiedlichster Formate in einen einheitlichen, auswertbaren Zustand, welcher die Datenbasis für die anschließende Analyse darstellt. Folgende Aufgaben sind im Rahmen der Aufbereitung zu beachten:

- Prüfung der Glaubwürdigkeit, Plausibilität und Zuverlässigkeit der Quellen;
- Berücksichtigung subjektiver Bewertungen infolge von Wahrnehmungsfehlern;
- Schließung von Datenlücken durch Extrapolation, Interpolation, Deduktion oder Induktion;
- Ausfilterung von falschen Informationen.

Im Anschluss an die Datenaufbereitung erfolgt die Interpretation bzw. Analyse der aufbereiteten Informationen mit Blick auf die Aufgabenstellung. In dieser Projektphase erfolgt die Transformation von Information zu Intelligence.[42] Zur Analyse unterschiedlicher Informationen werden Analyseverfahren verwendet, welche die Informationen strukturieren und aussagekräftig modellieren, so dass sie für die Beantwortung der Recherchefragestellung verwendet werden können. Die Analysen und deren Ergebnisse sind zusammen mit deren Annahmen und der verwendeten Verfahren zu dokumentieren und schließlich in eine Präsentation der Ergebnisse zu überführen (Reporting). Nach der Berichterstellung der Analyseergebnisse schließt sich die Umsetzung in konkrete Entscheidungen durch das Management und die Bewertung der Leistung des CI Teams oder der Competitive Intelligence-Abteilung an. Veränderte Rahmenbedingungen durch Umsetzung der Managemententscheidungen können ein erneutes Durchlaufen des CI-Zyklus erforderlich machen.[43]

Für die Unterstützung der Aufgaben im CI-Zyklus sind zahlreiche Instrumente einsetzbar, welche in Abb. 6 im Überblick dargestellt sind. Die Haupt- und Nebenanwendungen der Verfahren sind den einzelnen Phasen des Zyklus zugeordnet und jeweils schwarz (Hauptanwendung) bzw. grau (Nebenanwendung) hinterlegt. Die Verfahren können in Basisverfahren,

---

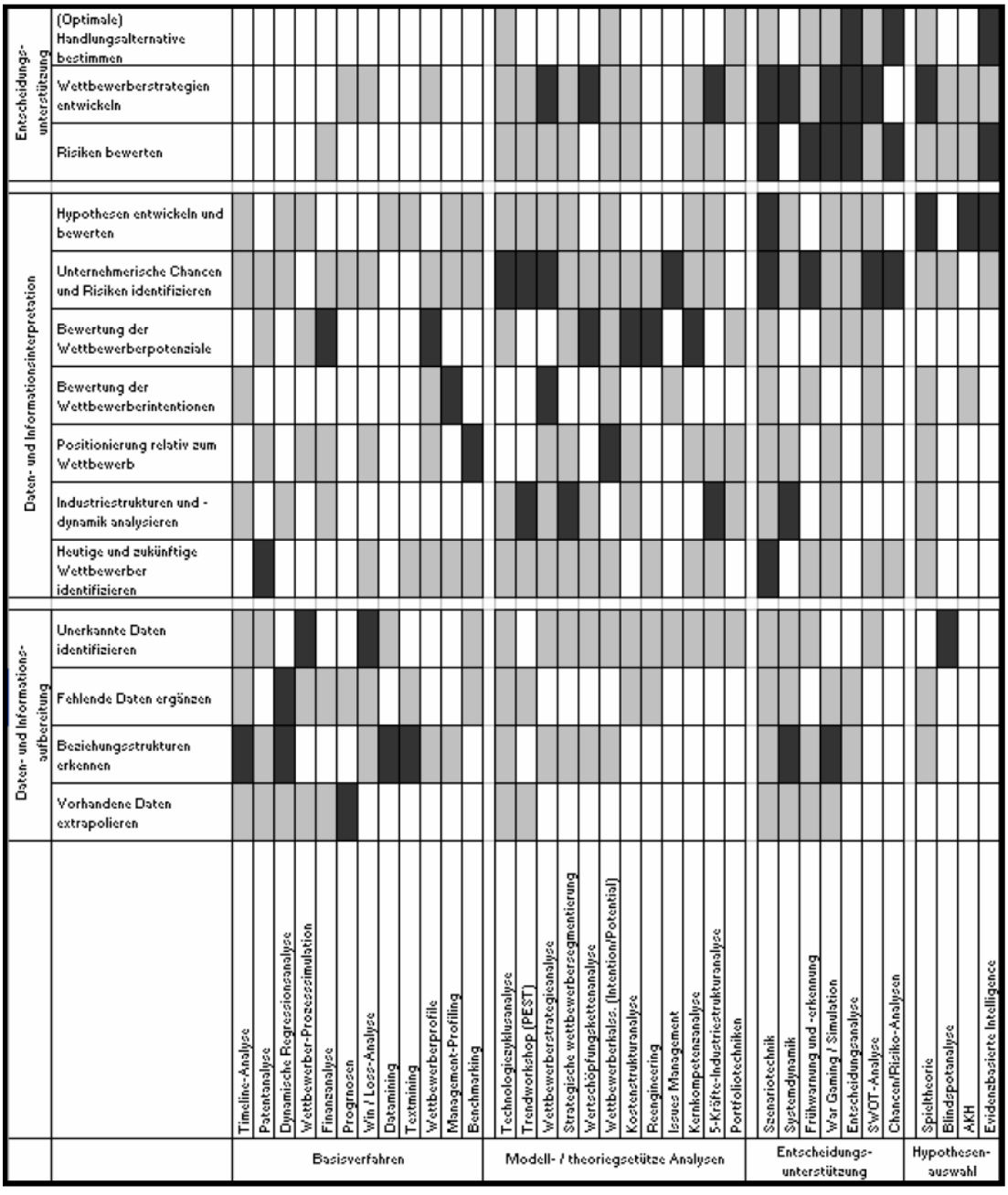
41 Vgl. Kunze (2000), S. 76.

42 Vgl. Kunze (2000), S. 90.

43 Zu einer sehr ausführlichen Darstellung der CI-Zyklusphasen vgl. Michaeli (2006), S. 117ff.

modell-/theoriegestützte Verfahren, sowie in Verfahren zur Entscheidungsunterstützung und Hypothesenauswahl gegliedert werden.

Abb. 6: Analyseverfahren im Rahmen des CI-Zyklus



Quelle: *Michaeli (2006), S. 237.*

Basisverfahren finden zumeist in der Daten- und Informationsaufbereitung Verwendung. Die Instrumente dienen der Datenextrapolation, der Erkennung von Beziehungsstrukturen, der

Ergänzung fehlender Daten und der Identifizierung unerkannter Daten.[44] *Modell- bzw. theoriegestützte Verfahren* basieren auf bestimmten Theorieansätzen. Vor der Anwendung dieser Modelle sind die Prämissen der jeweiligen Theorieansätze auf Konsistenz zum Anwendungsbezug zu prüfen. Modell- bzw. theoriegestützte Verfahren lassen sich vornehmlich in der Daten- bzw. Informationsinterpretation sowie vereinzelt auch in der Entscheidungsunterstützung einsetzen. Basisverfahren und modell- bzw. theoriegestützte Verfahren bilden zusammen die grundlegenden Analyseverfahren zur Erlangung von CI. *Verfahren zur Entscheidungsunterstützung* lassen sich mehr oder weniger universell einsetzen. Allerdings erfordert deren Auswahl und Einsatz entsprechende Methodenkompetenz und zeitigt einen hohen Modellierungsaufwand. Zu diesen Verfahren zählen u. a. die Risikobewertung, die Entwicklung von Wettbewerbsstrategien und die Bestimmung optimaler Handlungsalternativen.[45] *Verfahren zur Hypothesenauswahl* stellen schließlich die rationale Auswahl von Hypothesen sicher. Hierunter fallen u. a. spieltheoretische Ansätze sowie Blindspotanalysen. Die Verfahren zur Entscheidungsunterstützung und Hypothesenauswahl werden den fortgeschrittenen Analyseverfahren zugeordnet.[46]

2.4 Alternativen einer schutzstrategischen Stoßrichtung

Aufbauend auf der Informationsbereitstellung durch ein CI-System und der damit zusammenhängenden Offenlegung des Bedrohungspotenzials durch (Produkt-)Piraterie gilt es, eine grundlegende Stoßrichtung bzgl. der schutzstrategischen Grundhaltung festzulegen, welche die Basis für die Planung der konkreten Maßnahmen darstellt. Die strategische Stoßrichtung kann nach dem Verhalten des betroffenen Unternehmens in Prävention, Duldung, Kooperation und Sanktion gegliedert werden:

Die *Prävention* zielt auf die Vorbeugung gegenüber Piraterie ab. Bestandteile dieser Strategie sind die Konzentration auf Innovationen und ein besseres Timing am Markt. Dazu ist die Nutzung und Dokumentation von vorhandenem Wissen sowie die Arbeit in interdisziplinären Teams zu empfehlen. Zusätzlich sollten Schutz- und Markenrechte erworben werden. Die Marktbeobachtung zur Aufspürung von möglichen Nachahmern wird in diesem Kontext als wichtig angesehen. Des Weiteren können Produktkennzeichnungen, ein Kopierschutz oder besondere Verpackungen hilfreich sein. Der Vertriebsstrategie kommt dabei durch die Aufdeckung von Sicherheitslücken, der Auswahl und Überwachung von Vertriebswegen und der

---

[44] Vgl. Michaeli (2006), S. 235f.

[45] Eine Übersicht über unterschiedliche Managementinstrumente geben Fleisher/Bensoussan (2003).

[46] Vgl. Michaeli (2006), S. 369; Michaeli (2006), S. 419.

Durchführung von Schulungen eine wichtige Rolle zu. Werden Logistikdienstleistungen an externe Unternehmen vergeben, ist eine Distributionslogistik gezielt auszuwählen. Darüber hinaus fördert Personalmanagement die Loyalität der Mitarbeiter. Das Technologiemanagement kann zur Know-how Absicherung Informationen über Technologien zurückhalten oder durch bewusste Falschinformation Gegner verwirren. Die verwendeten Maßnahmen sind nach Kosten und Nutzen zu bewerten.[47]

Bei einer *Duldung* von Produktpiraterie werden für einen bestimmten Zeitraum oder eine bestimmte Zielgruppe keine Schutzmaßnahmen angewendet. Eine Duldung von Schutzrechtsverletzungen kann in Fällen von Vorteil sein, in denen sie Bestandteil der Unternehmenspolitik ist.[48] Es sind auch Konstellationen denkbar, in denen sich Produktpiraterie positiv auf den Unternehmenserfolg auswirkt. So konnten *Nia* und *Zaichkowsky (2000)* für den Fall von Luxusgütern (z. B. Cartier- und Rolex-Uhren, Gianni Versaci-Anzüge oder Prada-Mode) nachweisen, dass der Wert der Originale, die Kundenzufriedenheit der Käufer der Originale sowie die Reputation der Originalprodukte nicht negativ durch die Existenz von Pirateriewaren beeinflusst werden.[49] Hinsichtlich der Reputationswirkung ist in diesen Fällen eher von einem positiven Zusammenhang auszugehen. Erklärt werden kann dieses Phänomen durch eine duale Marktstruktur – das Segment für die originalen Luxusgüter ist vollkommen isoliert vom Segment der Imitate. Infolge der z. T. enormen Preisdifferenzen und klar getrennten Vertriebs- und Distributionskanälen, sind „versehentliche“ Käufe infolge von Täuschung selten.[50] Die verschiedenen Kundenschichten wechseln nicht zwischen den Segmenten.

Kooperationen können sich sowohl auf ebenfalls betroffene Unternehmen oder die Nachahmer selbst beziehen. In Kooperation mit betroffenen Unternehmen kann gemeinsam Aufklärungsarbeit zum Thema Produktpiraterie geleistet werden. Durch einen Erfahrungsaustausch gelangen die Kooperationspartner zu neuen Erkenntnissen. Interessengemeinschaften, wie bspw. der ‚Aktionskreis Deutsche Wirtschaft gegen Produkt- und Markenpiraterie e.V.‘ leisten Öffentlichkeitsarbeit, Aufklärung, Ermittlungen, Informationssammlung und Weitergabe sowie Lobbyarbeit. Individuelle außergerichtliche Lösungen können teilweise von Vorteil sein, wenn die Marktchancen die Verluste übertreffen. Im Bezug auf die Nachahmer können Partnerschaften mit oder gar die Akquisition von Piraten in Betracht gezogen werden. *Sanktionen*

---

47 Vgl. Sokianos (2006), S. 44f.

48 Vgl. Sokianos (2006), S. 45.

49 Vgl. Nia/Zaichkovsky (2000), S. 485.

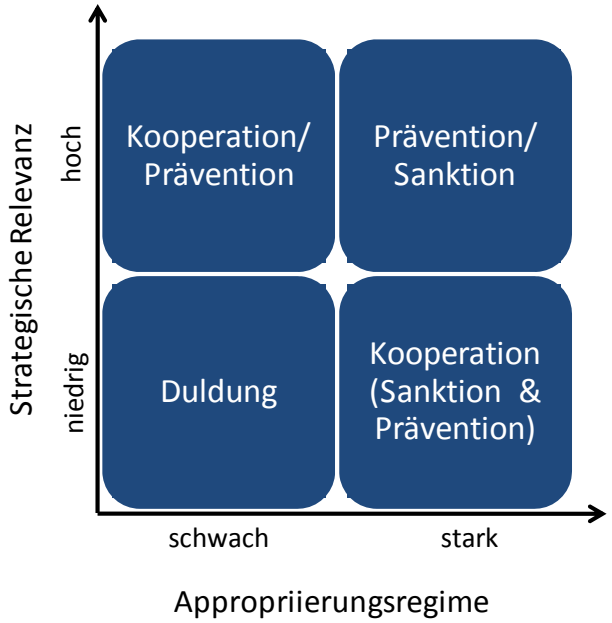
50 Vgl. zu dieser Thematik Grossmann/Shapiro (1988), S. 79 ff.

schließlich beziehen sich auf die Beendigung der Piraterieaktivitäten. Bestandteil dieser Vorgehensweise sind insbesondere juristische Schutzmaßnahmen.[51]

2.5 Konzeptionelle Überlegungen zur Auswahl der geeigneten schutzstrategischen Grundhaltung

Wird mittels des CI-Systems ein entsprechendes Bedrohungspotenzial durch (Produkt-)Piraterie offengelegt bzw. transparent gemacht, dann gilt es, in Abhängigkeit der übergeordneten Rahmenbedingungen aus dem strategischen Technologie- und Innovationsmanagement eine geeignete schutzstrategische Grundhaltung auszuwählen, welche dann die Basis für die Planung der konkreten Schutzmaßnahmen bildet. Zwei wesentliche Determinanten, welche sich aus dem Technologie- und Innovationsmanagement ableiten, stellen zum einen die strategische Relevanz der betreffenden Technologie bzw. Innovation für das Unternehmen und zum anderen die Stärke des Appropriierungsregimes dar. Abb. 7 visualisiert die beiden zentralen Einflussgrößen auf die Wahl der geeigneten schutzstrategischen Grundhaltung.

Abb. 7: Determinanten der schutzstrategischen Grundhaltung



Unter einem Appropriierungsregime versteht *Teece (1986)*:

> *„...the environmental factors, excluding firm and market structure, that govern an innovator´s ability to capture the profits generated by an innovation"*

[51] Vgl. Sokianos (2006), S. 46.

Die Stärke eines Appropriierungsregimes, oder in anderen Worten die Möglichkeiten, mit denen ein Innovator sich die Erträge aus einer neuen Technologie/Innovation aneignen kann, variieren beträchtlich zwischen Produkten, Branchen und Ländern. Die Stärke wird im wesentlich durch zwei Elemente bestimmt:

1. die Art der Technologie (insbesondere ihren Anteil an implizitem Wissen, der die Imitierbarkeit der Technologie durch Wettbewerber bestimmt) und
2. die Verfügbarkeit von gesetzlichen Möglichkeiten zum Schutz der Technologie gegen Nachahmer (System intellektueller Eigentumsrechte: Patente, Copyright-Rechte etc.).

In starken Appropriierungsregimes können Innovatoren ihre Technologien bzw. Innovationen effektiv schützen und sich die Erträge aus einer Innovation aneignen (bspw. infolge gesetzlicher Schutzmöglichkeiten und deren Durchsetzbarkeit oder weil die Technologie per se schwer zu imitieren ist). In schwachen Appropriierungsregimes ist dies nicht möglich ist. Die strategische Relevanz kann für Technologien, Produkte oder Zielmärkte bestimmt werden. Kriterien hierfür können neben monetären Größen wie bspw. Umsatz, EBIT oder Deckungsbeitrag auch der Einfluss auf kritische Erfolgsfaktoren im jeweiligen Markt bzw. auf neue Produkte, die Bedeutung der Know-how Absicherung für das eigene Unternehmen vor Wissensabfluss oder das Wachstumspotenzial sein.[52]

Im Falle eines industrie- oder länderspezifisch schwachen Appropiierungsregimes und einer geringen strategischen Relevanz kann die Duldung von Produktpiraterie eine sinnvolle strategische Grundhaltung darstellen. Einerseits kann ein Unternehmen durch unwirksame oder nicht beim Unternehmen liegende Schutzrechte nicht aktiv gegen Imitatoren vorgehen und andererseits kommt dem betreffenden Fall eine geringe strategische Bedeutung zu, so dass auch die Notwendigkeit zur Verwendung von alternativen Schutzinstrumenten nicht gegeben ist. Über eine Duldung werden Unternehmensressourcen für Produkte mit höherer strategischer Priorität bzw. Relevanz und besseren Schutzmöglichkeiten frei gehalten und Managementkapazitäten in die entsprechende Richtung gelenkt.

Liegen schwache Appropriierungsbedingungen vor, aber genießt das untersuchte Objekt im Gegensatz zum ersten Fall eine hohe strategische Relevanz, erscheint die Duldung als ungeeignet. Eine Duldung ist allenfalls im oben beschriebenen Fall der segmentierten Käuferschichten (bei Luxusgütern) und bei positiven externen Effekten durch Piraterie sinnvoll. Problematisch in dieser Situation ist, dass aufgrund der unzureichenden rechtlichen Schutzmöglichkeiten und der geringen Rechtsdurchsetzung keine Sanktionsstrategie verfolgt werden kann. Trotzdem sollte auf die Anmeldung von Schutzrechten nicht verzichtet werden –

[52] Vgl. u. a. Gerybadze (2004) S. 173f.; Picot (1991).

soweit dies eben möglich ist. Unternehmen müssen darüberhinaus versuchen, jenseits von juristischen Maßnahmen (in Form von Schutzrechten), präventiven Schutz vor Piraterie durch alternative Schutzstrategien und –maßnahmen zu erwirken (vgl. Kapitel 3). Überdies kann auch eine Kooperationslösung angestrebt werden. Als Kooperationspartner können entweder die Fälscher selbst oder ebenfalls betroffene Unternehmen in Frage kommen.

Im Fall eines starken Appropriierungsregimes (Unternehmen verfügen über Schutzrechte, die Rechtsdurchsetzung ist gesichert etc.) bietet sich, insbesondere wenn die strategische Relevanz hoch ist, die Sanktion als probates Mittel an. Bei der Sanktion selbst sollte auf eine entschiedene Anmeldung, Verfolgung und Durchsetzung der Schutzrechte abgestellt werden, um den bestmöglichen Schutz zu erreichen. In dieser Konstellation eignen sich insbesondere auch alle präventiven Schutzstrategien. Der Prävention kommt die Rolle zu, Produkte entsprechend Ihrer strategischen Relevanz zu schützen und die Sanktionsstrategie zu unterstützen. Auch eine Kooperationslösung kann in Erwägung gezogen werden, wenn bspw. der Fälscher selbst eine spezifische Kompetenz einbringen kann, welche beim Schutzrechtsinhaber noch nicht vorhanden ist. Grundsätzlich dominieren jedoch Prävention und Sanktion.

Bei geringer strategischer Relevanz des betreffenden Objekts ist, auch bei einem starken Appropriierungsregime, der Einsatz der Sanktionsstrategie kritisch zu prüfen. Im Gegensatz zur Sanktion kann sich in dieser Konstellation auch eine Kooperation mit dem Fälscher als die sinnvollere strategische Grundhaltung erweisen. Denkbar ist, dass das betroffene Unternehmen im Austausch gegen einen Verzicht auf rechtliche Verfolgung von der Arbeit des Fälschers profitiert, bspw. von Folgeentwicklungen des Fälschers, durch Gratislieferungen oder geringen bzw. vergünstigten Lizenzzahlungen. In solchen Fällen der „kooperativen“ Duldung ist aber immer das Risiko durch drohende Reputationsverluste zu berücksichtigen. Jedoch erleichtert eine „kooperative“ Duldung auch die Einflussnahme auf die Tätigkeiten des Fälschers und somit auch die Beeinflussung der Pirateriequalität. Als Argument für den Einsatz von Sanktionsmechanismen und aggressiven Präventionsmaßnahmen auch bei einer geringen strategischen Relevanz kann die Reputationswirkung angeführt werden. Die nachdrückliche Verfolgung und Sanktionierung jedweder Form der Produktpiraterie, unabhängig von der strategischen Relevanz, stärkt die Reputation des Unternehmens in der Fälschungsbekämpfung und wirkt somit auf alle potenziellen Fälscher abschreckend, ist also mithin präventiver Natur.

3. Klassifikation von Schutzmaßnahmen

Schutzmaßnahmen zur Erlangung von Wettbewerbsvorteilen gegenüber Produktpiraten können in juristische, betriebswirtschaftliche, technische und politische Maßnahmen gegliedert werden, welche nachfolgend genauer dargestellt werden.[53] In diesem Zusammenhang ist vorab zu bemerken, dass einzelne Maßnahmen allein nicht ausreichend sind, sondern vielmehr Maßnahmenkombinationen anzuwenden sind.

3.1 Juristische Schutzmaßnahmen

Juristische Schutzstrategien beziehen sich auf den Schutz von Geistigem Eigentum (Intellectual Property, IP) durch formelle Schutzmaßnahmen, d. h. durch den Einsatz von Schutzrechten (Intellectual Property Rights, IPR). Geistige Schutz- bzw. Eigentumsrechte bilden die Grundlage für eine effektive Prävention und Bekämpfung der Produktpiraterie. Die Schutzrechte können nach dem Ergebnis geistigen Schaffens auf dem gewerblichen und dem kulturellen Gebiet differenziert werden. Auf gewerblicher Seite beinhalten IPR Patente, Gebrauchsmuster, Geschmacksmuster, Topographieschutzrechte, Sortenschutzrechte und Kennzeichenrechte. Im kulturellen Bereich kann Geistiges Eigentum über Urheberrechte geschützt werden. In Abbildung 8 sind die Schutzrechtsarten und deren jeweilige Schutzobjekt eingetragen. Zusätzlich sind Angaben über die Notwendigkeit eines Verfahrens zur Anmeldung des Rechts sowie dessen Prüfung und maximale Laufzeit enthalten. Eine vertiefende Darstellung der verschiedenen Schutzrechtsarten findet sich bei *Burr/Stephan et al.* (2007).

Bei Fällen der Nachahmung kann auch das Gesetz gegen den unlauteren Wettbewerb (UWG) eine Rolle spielen. Es greift dann, wenn kein Schutzrecht im juristischen Sinne besteht. Allerdings muss zur Anwendbarkeit des UWG eine Täuschung des Verbrauchers vorliegen.[54] Gegen das UWG handelt, wer Waren oder Dienstleistungen anbietet, die eine Nachahmung der Waren oder Dienstleistungen eines Mitbewerbers sind, wenn eine vermeidbare Täuschung der Abnehmer über die betriebliche Herkunft herbeigeführt wird, die Wertschätzung der nachgeahmten Ware oder Dienstleistung unangemessen ausnutzt oder beeinträchtigt wird, oder die für die Nachahmung erforderlichen Kenntnisse oder Unterlagen

---

[53] Gassmann (2006) unterscheidet in juristische und faktische Schutzmaßnahmen, wobei die faktischen Maßnahmen verschiedene Elemente aus den anderen Maßnahmen beinhalten.

[54] Vgl. Gillert (2006), S. 214.

unredlich erlangt worden sind, aber von einer Täuschung des Verbrauchers durch die Nachahmung auszugehen ist.[55]

Abb. 8: Schutzrechtsarten im deutschen Raum

Schutzrechtsart	Schutzobjekt	Erfordernis zur Anmeldung	Prüfung	Maximale Laufzeit
Patent	Technische Erfindung	Ja	Ja	20 Jahre
Gebrauchsmuster	Technische Erfindung (keine Verfahren)	Ja	Nein	10 Jahre
Geschmacksmuster	Gestaltung	Ja	Nein	25 Jahre
Topographie	Halbleitertopographie	Ja	Nein	10 Jahre
Kennzeichen	▸ Marke ▸ Geschäftliche Bezeichnung ▸ Herkunftsangabe	Ja Nein nein	Ja	Alle 10 Jahre verlängerbar
Sortenschutz	Pflanzensorte	Ja	Ja	25/30 Jahre
Urheberrecht	Werke der Literatur, Kunst, Wissenschaft, Software	Nein	Nein	Bis 70 Jahre nach Tod des Urhebers

Quelle: *Burr/Stephan et al. (2007), S. 3f.*

Aus der Anerkennung von Schutzrechten folgt die Möglichkeit, gegen Nachahmungen vorzugehen. Dem Schutzrechtsinhaber stehen Ansprüche auf Unterlassung, Auskunft, Schadensersatz oder Beseitigung zu. Der Anspruch auf *Unterlassung* richtet sich auf eine Handlung des Schutzrechtsverletzers. Der Anspruch besteht bereits bei der Gefahr, dass ein Schutzrecht verletzt werden könnte (sog. Erstbegehungsgefahr), der tatsächlichen Verletzung oder der Wiederholungsgefahr der verletzenden Handlung. Neben der Unterlassung steht dem Schutzrechtsinhaber der Anspruch auf *Auskunft* zu. Mit diesem lassen sich die Bezifferung der Schadensersatzforderung unterstützen und Zulieferer bzw. Abnehmer der Pirateriewaren ermitteln.[56] Der *Schadensersatz* deckt den Schaden ab, der dem Schutzrechtsinhaber durch die Schutzrechtsverletzung entstanden ist. Die Berechnung der konkreten Höhe stellt in der Praxis jedoch ein Problem dar, so dass in der Regel standardisierte Verfahren eingesetzt werden. Eine Möglichkeit bietet das Lizenzanalogiemethode. Die Höhe des Schadensersatzes richtet sich dabei nach einer fiktiven Lizenzgebühr, welche an den Inhaber zu zahlen gewesen wäre. Außerdem ist die Herausgabe des Verletzergewinns mög-

---

[55] §4 Nr. 9 UWG, in: http://www.gesetze-im-internet.de/uwg_2004/__4.html Abrufdatum 21. Mai 2007 in Verbindung mit §3 UWG, in: http://www.gesetze-im-internet.de/uwg_2004/__3.html Abrufdatum 21. Mai 2007.

[56] Vgl. Gillert (2006), S. 215f.

lich oder es wird der tatsächlich entstandene Schaden berechnet.[57] Schließlich hat der Schutzrechtsinhaber einen *Anspruch auf Beseitigung* des durch die Verletzung entstandenen rechtswidrigen Zustands, der von der Art und Weise der Verletzung abhängig ist. Ein Beispiel hierfür ist die Vernichtung der Piraterieware oder die Löschung eines widerrechtlich angemeldeten Schutzrechts.

Für die Durchsetzung der Ansprüche stehen mit der Sachverhaltsaufklärung, Berechtigungsanfrage, Abmahnung, einstweiliger Verfügung und Klageverfahren mehrere Instrumente zur Verfügung. Zur frühzeitigen Beschlagnahme von Piraterieware wird die Grenzbeschlagnahme eingesetzt. Die *Sachverhaltsaufklärung* kann in Pirateriefällen bspw. die Auskunft über gegenwärtige und zukünftige Verkaufszahlen umfassen. Eine weitere Möglichkeit ist die *Berechtigungsanfrage*. Diese beinhaltet den Hinweis auf die Schutzrechtsverletzung, ist aber nicht rechtlich bindend. Ein weiteres außergerichtliches Instrument ist die *Abmahnung*. Wie bei der Berechtigungsanfrage wird auf die Schutzrechtsverletzung hingewiesen. Im Gegensatz zur Berechtigungsanfrage wird bei der Abmahnung eine Aufforderung zur Unterlassung in Form eine strafbewährten Unterlassung- und Verpflichtungserklärung versandt. Wird diese nicht unterzeichnet, so wird eine gerichtliche Klage angedroht. Für die Bekämpfung der Produktpiraterie sind Abmahnungen nicht immer geeignet, weil Piraterieunternehmen nicht auf die Abmahnung eingehen und vorgewarnt werden, so dass sie Maßnahmen zur Unterbindung von gerichtlichen Verfahren einleiten können. Sind sich Unternehmen der Rechtsverletzung nicht bewusst, kann eine Abmahnung jedoch sehr wirkungsvoll sein.[58]

Während die vorangegangenen Verfahren außergerichtlich verwendet werden, basiert die *einstweilige Verfügung* auf einem abgekürzten gerichtlichen Verfahren. Sie wird eingesetzt, wenn eine Abmahnung nicht beantwortet worden ist oder keine Aussicht auf Erfolg hat. Für die Erlangungen einer solchen Verfügung reicht die glaubhafte Darlegung der Rechtsverletzung z.B. durch die Vorlage von Dokumenten aus. Inhalt der Verfügung kann die Unterlassung der Rechtsverletzung oder die Verwahrung der Waren durch einen Gerichtsvollzieher sein. Hat die einstweilige Verfügung keinen Erfolg, ist ein *Klageverfahren zur Anspruchsdurchsetzung* anzustreben. Damit können zwar alle Ansprüche durchgesetzt werden, aber bis zur Entscheidung der Klage kann ein langer Zeitraum verstreichen. *Die Grenzbeschlagnahme* besteht aus zwei zollrechtlichen Verfahren. Das gemeinschaftsrechtliche Grenzbeschlagnahmeverfahren der Europäischen Union erlaubt den nationalen Zollbehörden auf den Verdacht des Schutzrechtsinhabers hin, die vermutliche Piraterieware zu kontrollieren, so

---

[57] Vgl. Gillert (2006), S. 216ff.

[58] Vgl. Gillert (2006), S. 218f.

dass der Schutzrechtsinhaber gegebenenfalls die Vernichtung verlangen oder ein gerichtliches Verfahren anstreben kann. Im Unterschied dazu muss bei der Grenzbeschlagnahme nach nationalem Recht eine offensichtliche Schutzrechtsverletzung gegeben sein, um die Vernichtung oder gerichtliche Klage zu begründen. In beiden Fällen werden die Behörden nur auf Antrag des Rechtsinhabers tätig. Aus diesem Grund ist zu empfehlen, dass der Rechtsinhaber immer Anträge für beide Verfahren stellt, um den handelnden Behörden vor Ort einen größeren Spielraum zu ermöglichen.[59]

3.2 Geheimhaltung als Schutzmaßnahme

Anstelle der Anmeldung von gewerblichen Schutzrechten (und damit zusammenhängend der Offenlegung des zugrunde liegenden Wissens) kann sich das Unternehmen auch zur Geheimhaltung des technologischen bzw. innovationsbezogenen Wissens entschließen. An die Stelle formeller Schutzrechte treten in diesem Fall Betriebs- und Geschäftsgeheimnisse als faktische Schutzinstrumente (‚Trade Secrets').[60] Trotz des Fehlens einer Legaldefinition hat sich für Betriebs- und Geschäftsgeheimnisse eine gängige und allgemein akzeptierte Begriffsfassung herausgebildet, die sich an der Rechtsprechung zu §17 des Gesetzes gegen unlauteren Wettbewerb (UWG) orientiert.[61] Als Betriebs- und Geschäftsgeheimnisse werden demzufolge alle auf ein Unternehmen bezogenen Wissensbestände und Informationen über Tatsachen, Gegenstände, Begebenheiten, Vorgänge etc. verstanden, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Geheimhaltung ein berechtigtes Interesse besteht.[62] Betriebsgeheimnisse richten sich dabei primär auf technologisches Wissen, während Geschäftsgeheimnisse vornehmlich betriebswirtschaftliche Informationen betreffen (bspw. Umsätze, Umsatzprognosen, Gewinne, Kundenlisten, Strategiepapiere, Bezugs- und Lieferquellen, Bezugskonditionen, Kalkulationsunterlagen etc.). Voraussetzung für das Vorliegen eines im Sinne des §17 UWG geschützten Geschäfts- bzw. Betriebsgeheimnisses sind demzufolge drei Merkmale:

(1) Die betreffenden Informationen dürfen nur einem begrenzten Personenkreis bekannt, d. h. nicht offenkundig und nicht ohne weiteres zugänglich sein.

(2) Die Information muss in einem gewerblichen Bezug, d. h. in einer Beziehung zu einem Geschäftsbetrieb stehen.

---

[59] Vgl. Gillert (2006), S. 219ff.

[60] Vgl. Burr/Stephan et al. (2007), S. 257ff.

[61] Vgl. Hartung (2006), S. 24.

[62] Vgl. Köhler (2004), §17, Rndnr. 4.

(3) Der herrschenden Begriffsauffassung zufolge hängt das Vorliegen eines Geschäftsgeheimnisses auch davon ab, ob das Management den Willen zur Geheimhaltung jedem Mitwissenden gegenüber erkennen lässt.

Insbesondere in jenen Technologiefeldern, in denen sich formelle Schutzrechte bzw. der Patentschutz als schwach und damit als ineffektiv erweisen, Wettbewerber bzw. Produktpiraten von Schutzrechtsverletzungen abzuhalten (bspw. bei Prozesstechnologien), tendieren Unternehmen zu Geheimhaltungsstrategien. Voraussetzung für diese Schutzstrategie ist jedoch, dass die Innovation auch erfolgreich geheim gehalten werden kann.[63] Entscheiden sich Unternehmen für die Geheimhaltungsstrategie als faktisches Schutzinstrument, so ist diese durch flankierende personalpolitische, juristische und organisatorische Maßnahmen zu untermauern.

Die personalpolitische Flankierung umfasst im Wesentlichen folgende Instrumente:

(1) *Personalbeschaffung/-auswahl:* Bei der Selektion neuer Mitarbeiter sind neben der fachlichen Eignung speziell Einstellungen, Werthaltungen und bisheriges Verhalten zu überprüfen. Wichtige Faktoren sind die Loyalität des Mitarbeiters über das bestehende Arbeitsverhältnis hinaus, ethische Werte wie Gewissen und Moral, die Vereinbarung von eigenen und Unternehmensinteressen, die Wahrung von Vertraulichkeit, Zuverlässigkeit sowie Engagement und Fairness.

(2) *Personalentwicklungsmaßnahmen:* Mitarbeiter des Unternehmens müssen über die Geheimhaltungsstrategie und daraus abgeleitete Richtlinien und Verhaltenskodizes informiert werden. Über die reine Information hinaus müssen auch Verhaltensweisen und Kommunikationsformen der Mitarbeiter zur Geheimhaltung trainiert werden:

> „All employees should be trained on the practical aspects of information protection, including marking all trade secret materials with a clear and noticeable proprietary legend ('confidential')."[64]

Überdies muss das Unternehmen den betroffenen Personenkreis deutlich vor Missbrauch bzw. Fehlverhalten warnen und die etwaigen Sanktions- bzw. Strafverfolgungsmaßnahmen konkret benennen. Letzteres gilt insbesondere für Mitarbeiter, die zu (potenziellen) Konkurrenten wechseln. In der Beurteilung und Förderung von Mitarbeitern liegt ein großes Potenzial für die Verursachung von Unzufriedenheit in einem Unternehmen. Vor diesem Hintergrund müssen Personalentwicklungsmaßnahmen eng mit entsprechenden Personalanreiz und -vergütungssystemen gekoppelt werden.

---

[63] Vgl. Burr/Stephan et al. (2007), S. 257f.

[64] Hemphill (2004), S. 288.

(3) *Personalanreiz- und Vergütungssysteme:* Die Leistung eines Mitarbeiters ist entsprechend eines transparenten Verfahrens zu würdigen. Die Erwartungshaltung des beurteilenden Gremiums bezüglich Eigenschaften, Verhaltensdimensionen und Fähigkeiten muss transparent kommuniziert werden. Entwicklungsschritte und Fördermaßnahmen wie bspw. Seminare, externe Trainings, Training-on-the-job, Coaching, Intervision, Mediation, internes Mentoring und Job Rotation müssen nach klaren Vorgaben vergeben werden. Wichtige Aufgabe des Personalmanagements ist es in diesem Zusammenhang auch, die Loyalität der Mitarbeiter auszubauen, da loyale und zufriedene Mitarbeiter eine geringere Motivation zur Unterstützung von Piraterie haben. Dabei sind neben finanziellen Anreizen auch langfristig wirkende weiche Faktoren zu beachten. Schließlich können Unternehmen im Rahmen einer Risikoanalyse die Stellen und Positionen sowie Schlüsselpersonen mit hoher Relevanz für die Sicherung der Wettbewerbsfähigkeit identifizieren. Diese werden dann in einer anonymen Befragung zu ihrer Motivation im Bezug auf pirateriebezogene Aspekte befragt, wobei auch Mitarbeiter, die kurz vor der Beendigung des Arbeitsverhältnisses stehen bzw. das Unternehmen bereits verlassen haben, eingeschlossen werden sollten. Auf Basis der Ergebnisse sind dann Maßnahmen zur Erhöhung der Motivation zu erarbeiten und in nachfolgenden Befragungen auf ihre Wirkung hin zu überwachen.[65]

(4) *Personalfreisetzung:* Die Trennung von Mitarbeitern wird in vielen Fällen mittels einer großzügigen Abfindung erleichtert. Diese Maßnahme wirkt jedoch nur kurzfristig, wenn ein neues Arbeitsverhältnis nicht gefunden werden kann. Um die Belastung für den ehemaligen Mitarbeiter und dessen Vorgesetzen zu verringern, ist ein professionelles Vorgehen in Form von Trennungsgesprächen zur Würdigung des Mitarbeiters, der Auflösung des Arbeitsverhältnisses, aber auch zum Hinweis auf das Verbot zur Geheimnisweitergabe zu empfehlen.[66]

Die juristischen Maßnahmen betreffen im Kern die vertraglichen Vereinbarungen mit Mitarbeitern des eigenen Unternehmens und mit externen Kooperationspartnern. Über die oben beschriebene reine Informationsfunktion hinaus sind in den Fällen, in denen Mitarbeiter des Unternehmens in besonders sensiblen Bereichen tätig sind (z. B. in der F&E-Abteilung) oder externe Partner eingebunden werden, gesonderte vertragliche Vereinbarungen zur Geheimhaltung – typischerweise Vertraulichkeitsvereinbarungen – erforderlich. Gängige alternative Bezeichnungen für diese Vertragsgattung in der Unternehmenspraxis sind:

---

[65] Vgl. dazu u. a. Burr/Stephan et al. (2007), S. 258f. sowie Pütz/Rundstedt (2006), S. 60ff.

[66] Vgl. Pütz/ Rundstedt (2006), S. 60ff.

- Geheimhaltungsvereinbarung
- Geheimhaltungsverpflichtung
- Confidential Disclosure Agreement (CDA)
- Confidentiality Agreement
- Nondisclosure Agreement (NDA).[67]

Vertraulichkeitsvereinbarungen enthalten in der Regel mehrere Verpflichtungen. Ein Hauptbestandteil ist natürlich zunächst die vertragliche Verpflichtung des Empfängers, vertrauliche Informationen des Unternehmens Dritten nicht zugänglich zu machen. Mindestens ebenso wichtig ist in vielen Fällen aber auch ein für den Empfänger geltendes Verwendungs- oder Verwertungsverbot, d. h. der Empfänger darf die erhaltenen Informationen auch nicht für seine eigenen Zwecke benutzen.[68]

Ergänzend zu den personalpolitischen und juristischen Maßnahmen sollten auch organisatorische Vorkehrungen zur effektiven Durchsetzung der Geheimhaltungsstrategie getroffen werden. So sind zunächst der Schutz und die Kontrolle des physischen und elektronischen Datenzugangs sicherzustellen. Der physische Zugang zu Orten, an denen Geschäftsgeheimnisse in gebündelter Form im Unternehmen zu finden sind, bspw. in Forschungslabors, sollte mit entsprechenden Restriktionen belegt und mittels Kontrollen gesichert werden *(Zugangssicherung)*. Sensible Betriebsbereiche sind von außen und innen zu sichern. Zur äußeren Überwachung zählen Sensoren, Magnetkontakte, Überwachungskameras für Türen, Fenster, Glasflächen und Öffnungen sonstiger Art. Zugang zu solchen Sicherheits- oder Sperrzonen sollte nur Schlüsselpersonen gewährt werden, mit denen zuvor Vertraulichkeitsvereinbarungen abgeschlossen wurden (vgl. vorhergehender Absatz).[69] Dokumente, die Geschäfts- bzw. Betriebsgeheimnisse zum Inhalt haben, sollten nur in sehr begrenzter Zahl kopiert sowie ausschließlich nummeriert (eindeutig gekennzeichnet) und mit konkreten Rückgabefristen bzw. Sperrvermerken ausgegeben werden *(Dokumentensicherung)*. Besonderes Augenmerk erfordert auch die Sicherung des Zugangs zu elektronisch gespeicherten Daten (*Elektronische Datensicherheit*). So sollten bspw. der allgemeine Intranet-Zugang vermieden und entsprechende Passwörter oder Verschlüsselungstechnologien eingesetzt werden.

Neben den F&E-Abteilungen sind auch weitere kritische betriebliche Funktionsbereiche mit einem besonderen ‚Sicherungsvermerk' zu belegen. Zur Sicherung des Know-how Abflusses in der Fertigung sind u. a. die sich im Produktionsprozess befindlichen Teile sowie Aus-

---

[67] Vgl. Kurz (2004), S. 2.
[68] Vgl. Kurz (2004), S. 4.
[69] Vgl. Burr/Stephan et al. (2007), S. 259f.; Ronde (2001), S. 391 ff.

schussware permanent zu überwachen. Kritisch ist insbesondere der Umstand zu erachten, wenn dritten Personen, bspw. von Zulieferunternehmen oder Spediteuren, Zugang zur Fertigung einzuräumen ist (wenn bspw. Dritte Wertschöpfungsleistungen in der Montage übernehmen). Der Zugang zu kritischen Bereichen ist grundsätzlich zu reglementieren. Besonders in Nachtschichten sind vertrauenswürdige Mitarbeiter einzusetzen, Qualitätskontrollen durchzuführen und Stillstandszeiten zu protokollieren. Auch kann über eine entsprechende Aufteilung der Fertigung erreicht werden, dass nur einzelne Bestandteile kopiert werden können. Dabei müssen verschieden Produktionsstandorte und Zulieferer eingesetzt werden.

3.3 Technische Schutzmaßnahmen

Technische Schutzmaßnahmen bilden, neben den formalen Schutzrechten, einen weiteren wichtigen Ansatzpunkt für die Prävention der Produktpiraterie. Eine mögliche Einteilung liefern *Fuchs et al. (2006)*, die Schutztechnologien in sichtbare, unsichtbare und maschinengestützte Technologien untergliedern. Sichtbare Schutzmaßnahmen werden direkt auf dem Produkt oder der Verpackung angebracht und können ohne weitere Hilfsmittel erkannt werden. Dazu sind Hologramme, optisch variable Elemente, Folien, Sicherheitsetiketten bzw. -siegel, Sicherheitstinten sowie Sicherheitspapier und -druck zu zählen. Unsichtbare Technologien sind nur durch den Einsatz spezialisierter Geräte zu erkennen. Wichtige Technologien in diesem Bereich stellen Mikrofarbstoffe, DNA und DNA-Computing, Nanotechnologie, Nanobiotechnologie, Isotope und Chromogene Systeme dar. Maschinengestützte Technologien basieren bei der Planung und Steuerung auf Daten, die mit speziellen Geräten eingelesen werden müssen. Beispiele hierfür bilden RFID (Radio Frequency Identification) Chips, Barcodes, Chipkarten, OCR (Optical Character Recognition), Biometrie, Klebestreifen als Datenträger, Internet Monitoring, Digital Rights Management Systeme (DRMS), digitale Wasserzeichen, intelligente Verpackungen, chemische Marker und Selbstzerstörungsmechanismen. Kombinationen bestehen aus Sicherheitslabels, Certificates of Authenticity oder Track and Trace Technologien.[70] Insbesondere RFID und DRM werden als vielversprechende und zukunftsträchtige Schutzinstrumente angesehen.[71] RFID-Chips sind Transponder, die mit Sensoren und Antennen ausgestattet sind. RFID-Chips besitzen eine eindeutige Kennnummer. Diese Kennnummern ermöglichen jederzeit die eindeutige Identifikation der Chips bzw. der mit diesen Chips etikettierten Produkte.[72] Digital Rights Management (DRM) Systeme sind

---

[70] Vgl. Fuchs et al. (2006), S. 261f.

[71] Vgl. Burr/Stephan et al. (2007), S. 280.

[72] Vgl. Burr/Stephan (2006), S. 55f.

technische Mittel, die digitale Inhalte gegen unbefugten Zugriff schützen sollen und/oder deren Gebrauch überwachen bzw. der Durchsetzung von Einschränkungen der eingeräumten Nutzerrechte dienen. Im Kern stellen DRM-Systeme eine Form des technischen Kopierschutzes für digitale Inhalte wie Musik oder Filme dar.[73]

Zur Beurteilung technischer Schutzmaßnahmen existieren unterschiedliche Standpunkte. Auf der einen Seite wird festgestellt, dass Schutztechnologien an Bedeutung gewinnen, da sie ausgereift sind, hohe Barrieren für Fälscher aufbauen und kostengünstig eingesetzt werden können. Barrieren können insbesondere über technische Maßnahmen im Herstellungsprozess und der Kombination verschiedener technischer Schutzmaßnahmen aufgebaut werden, da Fälscher erst entsprechendes Produktionswissen und –ausrüstung erlangen müssen. Der kostengünstigen Bereitstellung technischer Schutzmaßnahmen steht entgegen, dass diese den Aufwand und die Kosten in der Produktion erhöhen, ohne langfristige Schutzmöglichkeiten bereitzustellen. Grund hier ist die Problematik, dass technische Schutzstrategien, genau wie die Produkte selbst, nachgeahmt werden können. Sie können aber dafür genutzt werden, Schwachstellen in der eigenen Lieferkette zu identifizieren und Fälschungen von Originalen zu unterscheiden.[74]

3.4 Flankierende betriebswirtschaftliche Schutzstrategien

Ergänzend zu den oben diskutierten Schutzmaßnahmen können Unternehmen auch durch ihre strategische Ausrichtung die Gefahren infolge von Produktpiraterie eindämmen. So bewirken bspw. offensiv eingesetzte und kommunizierte Schutzrechtsstrategien eine Abschreckung gegenüber potenziellen Produktpiraten. Unternehmen, die in bestimmten Technologiefeldern gehäuft Patente anmelden und damit ihre technologische Leistungsfähigkeit sowie ihr besonderes Interesse an diesem Technologiefeld signalisieren, schrecken dadurch indirekt auch potenzielle Produktpiraten ab. Wenn Unternehmen dazu begleitend spezifische Investitionen (z. B. Bau neuer Fabriken für die Herstellung der Produkte, Start aufwändiger Werbekampagnen zur Ankündigung der Markteinführung) tätigen, so kann damit ein glaubhaftes Interesse an der betreffenden Technologie signalisiert und Produktpiraten von einem eventuellen Markteintritt abgehalten werden. Auch die Mitarbeit in Interessengruppen zur Rechtsentwicklung kann diese offensive Grundhaltung zusätzlich verstärken (vgl. dazu auch den

---

[73] Vgl. Arlt (2006), S. 12.

[74] Vgl. Brenner (2006), S. 284.

nachfolgenden Abschnitt).[75] Ziel letztendlich ist es, eine Reputation der aktiven und offensiven Rechtsdurchsetzung zu etablieren.

Ergänzend zu diesem Reputationsaufbau stehen Unternehmen auf der strategischen Ebene natürlich auch alle faktischen Schutzinstrumente zur Verfügung, um innovative Produkte und Dienstleistungen sowie Prozessinnovationen gegen Imitation durch Konkurrenten bzw. Produktpiraten zu schützen. *Burr* und *Stephan et al.* (2007) nennen folgende Ansatzpunkte:

- *Fast Pace Strategien:* Bei Fast Pace-Strategien versucht das innovierende Unternehmen, immer neue Innovationen hervorzubringen und zwar schneller als seine Konkurrenten die bisherigen Innovationen imitieren können. Zielsetzung einer Fast Pace-Strategie ist, beständig einen Innovationsvorsprung vor Konkurrenten bzw. Produktpiraten zu erhalten.
- *Ausschöpfung von Skalen- und Lernkurvenvorteilen:* Die Erzielung von Kostenvorteilen kann ein weiterer Ansatzpunkt zum Schutz von Innovationen gegen Imitation sein. Skalenvorteile (z. B. im Automobilbau, in der Stahlindustrie) beruhen auf großen jährlichen Ausbringungsmengen, was zu geringeren Stückkosten führt. Lernkurvenvorteile beruhen auf einer über die Zeit kumulierten Ausbringungsmenge, die dem Unternehmen und seinen Mitarbeitern das Sammeln entsprechender Erfahrungen (z. B. bei der Optimierung des Produkts und des Herstellungsprozesses, bei der routinemäßigen Erfüllung bestimmter Arbeitsschritte) ermöglicht, was zu über die Zeit sinkenden Herstellkosten führt. Lernkurvenvorteile sind typisch für Industrien mit komplexen Herstellungsprozessen (z. B. Autobau, Flugzeugbau).[76] Solche Kostenvorteile ermöglichen dem Innovator, Wettbewerbsvorteile gegenüber Imitatoren zu erzielen, die auf niedrigeren Stückkosten beruhen. Selbst wenn Imitatoren das Produkt des Innovators nachahmen können, so hat der Innovator dennoch gute Chancen aufgrund seiner Kostenvorteile, die auf seinem frühzeitigen Marktstart beruhen, Gewinne aus seinen Innovationen zu erzielen und die Marktanteile der Imitatoren zu begrenzen.
- *Kontrolle komplementärer Ressourcen:* Selbst wenn der Konkurrent durch Patente nicht an der Imitation der Produkte und Produktionsprozesse des Innovators gehindert werden kann, kann der Innovator dennoch durch Kontrolle komplementärer Ressourcen einen gewissen Schutz vor Imitation erreichen. Komplementäre Ressourcen sind oftmals erforderlich zur Kommerzialisierung einer Innovation. Sie sind typischerweise auf nachgelagerten Stufen der Wertschöpfungskette angesiedelt. Zu den wichtigsten komplementären

---

[75] Vgl. Burr/Stephan et al. (2007), S. 94f. Für weitere Strategieoptionen vgl. Burr/Stephan et al. (2007), S. 101ff.

[76] Vgl. dazu Burr et al. (2005), S. 294 f.

Ressourcen zählt die Kontrolle über Markennamen, Vertriebskanäle und Produktionskapazitäten. Gelingt es dem Innovator, wichtige Vertriebskanäle (z. B. Einzelhandelsketten mit großem Marktanteil oder Fachgeschäfte in 1a-Innenstadtlagen) an sich zu binden, so behindert dies den Imitator bzw. Produktpiraten bei der Marktdurchdringung. Ebenso kann der Innovator durch Aufbau eines bekannten Markennamens für das Produkt und eine entsprechende Anbieterreputation (z. B. als Technologieführer der Branche) Imitatoren das Image eines Plagiators anheften und sie bei der Marktdurchdringung behindern.

- *Komplexe, schwer imitierbare Systemlösungen:* Eine weitere Möglichkeit für den Innovator, Imitatoren trotz fehlender Schutzrechte am Markteintritt zu hindern, ist in der Entwicklung und dem Angebot komplexer Systemlösungen zu sehen. Zu den komplexen Systemlösungen zählen beispielsweise Komplettlösungen aus einer Hand, die eine Vielzahl von Einzelleistungen zu einem abgestimmten und optimierten Gesamtpaket integrieren. Zu nennen wären hier beispielsweise Komplett-Outsourcing Lösungen im IT-Bereich oder im Facility Management, bei denen ein Unternehmen die komplette Bewirtschaftung der gesamten Unternehmens-EDV oder aller Gebäude des Unternehmens an einen spezialisierten Dienstleister überträgt. Solche komplexen Systemlösungen sind oftmals schwerer als Einzeldienstleistungen oder als einzelne, isolierte Produkte zu imitieren. Komplexe Gesamtlösungen sind für den Konkurrenten bzw. Produktpiraten schwer imitierbar, wenn für diesen das komplexe Zusammenspiel der Einzelleistungen kaum verständlich ist und der Innovator dem Kunden keine Einzelleistungen mit Einzelpreisen offeriert, sondern nur Paketlösungen mit einem Paketpreis. Dies zwingt den Imitator bzw. Piraten zur Nachahmung der kompletten Lösung und erschwert es ihm, durch Imitation einer Einzelleistung in die Geschäftsbeziehung zwischen Innovator und Kunden einzubrechen, um diese Geschäftsbeziehung später durch weitere Dienstleistungsangebote schrittweise auszubauen.
- *Entwicklung langfristiger Geschäftsbeziehungen mit Kunden und Lieferanten*: Eine weitere Möglichkeit des Innovators, Imitatoren bzw. Piraten den Markteintritt zu erschweren, liegt in der Entwicklung langfristiger Geschäftsbeziehungen mit wichtigen Marktpartnern (z. B. Kunden und Lieferanten). Gelingt es dem Innovator, Kunden oder wichtige Zulieferer mit langfristigen Verträgen und einer über die Jahre hinweg guten und vertrauensvollen Zusammenarbeit an sich zu binden, so wird der Markteintritt für den Imitator erschwert. Problematisch ist an dieser Vorgehensweise allerdings, dass nicht alle Lieferanten zur exklusiven Belieferung des Innovators bereit sein werden, weil sie sich dadurch die Möglichkeit zusätzlichen Geschäftsvolumens mit den Imitatoren nehmen. Ebenfalls sind nicht alle Kunden bereit, sich langfristig an den Innovator zu binden, wenn Imitatoren in der Zukunft signifikant niedrigere Preise offerieren könnten und der Kunde davon durch einen Anbieterwechsel zu geringen Wechselkosten profitieren könnte.

3.5 Flankierende politische Schutzmaßnahmen

Das (volks-) wirtschaftliche Problem durch Produktpiraterie hat sich in den vergangenen Jahren zu einem populären bzw. öffentlich diskutierten Phänomen entwickelt und ist für politische Handlungsträger auf nationaler, regionaler sowie supranationaler Ebene zu einem brisanten Thema und Handlungsfeld geworden. Unternehmen können hier verstärkt auf die Unterstützung der politischen Akteure zählen und aktiv Lobbyismusarbeit sowohl auf unternehmensindividueller Ebene als auch indirekt über die Verbandsebene betrieben. Internationale Lobbyarbeit bzw. „diplomatische Anstrengungen" wurden bisher weitestgehend unterschätzt. Aber gerade in Fälscherländern, wie bspw. China, sollten Unternehmen direkt oder zumindest über Verbände verstärkt Lobbyismusarbeit und Aufklärungsarbeit gegen Produktpiraterie betreiben, um die Effektivität ihrer Anstrengungen zu erhöhen.

Neben den Unternehmen selbst haben in den letzten Jahren auch nationale politische Institutionen (bspw. Bundes- oder Landesministerien) und Verbände (bspw. die Spitzenverbände der deutschen Wirtschaft oder die Industrie- und Handelskammern) vermehrt eigeninitiativ Programme zur Aufklärung und zur Unterstützung von Unternehmen im Kampf gegen die internationale Produktpiraterie lanciert.[77] Die Maßnahmen der politischen Institutionen betreffen neben der Verschärfung der Gesetzgebung auch das Angebot von wirtschaftspolitischen Dialogplattformen (z. B. der deutsch chinesische Rechtsstaatsdialog), Symposien und Arbeitskreisen. Auch hat die öffentliche Hand in Deutschland in den vergangenen Jahren gezielt Forschungsprojekte zu Maßnahmen gegen Produktpiraterie initiiert und gefördert. Verbandsbezogene Maßnahmen umfassen u. a. die Bildung von themenspezifischen Arbeitskreisen und eigenen Verbänden. Hier sind beispielhaft der Aktionskreis ‚Deutsche Wirtschaft gegen Produkt- und Markenpiraterie e.V. (APM)' sowie die Arbeit des Deutschen Innungs- und Handelskammertags (DIHK) zu nennen. Ihre Aufgabe liegt in der Informationsbereitstellung und Unterstützung für Mitgliedsunternehmen, einer gezielten Öffentlichkeitsarbeit und der Beratung von politischen Akteuren durch Lobbyarbeit. Auch Messeberatung oder rechtliche Beratung und Seminare runden das Angebot ab.[78]

Internationale Maßnahmen werden vor allem durch die WTO, die Weltzollorganisation (WCO), die Weltorganisation für geistiges Eigentum (WIPO), die internationale kriminalpolizeiliche Organisation (Interpol) und die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) gefördert. Hierzu zählen insbesondere die Verwaltung und Kontrolle

[77] Vgl. z. B. BDI (2007).
[78] Vgl. BMWi (2007).

von Abkommen wie das Übereinkommen über handelsbezogene Aspekte der Rechte des geistigen Eigentums (TRIPS), breite Seminar- und Weiterbildungsangebote und die Erstellung von Analysen und Berichten über Brennpunkte der Produktpiraterie. Auch die Gruppe der G8-Staaten[79] tritt für eine Stärkung von Schutzrechten und den Kampf gegen die Produktpiraterie ein. Auf europäischer Ebene wird der Schutz geistigen Eigentums durch die Richtlinie 2004/48/EG zur Durchsetzung der Rechte des geistigen Eigentums und der Verordnung (EG) Nr. 1383/2003 gestützt. Darin ist das Vorgehen der Zollbehörden zur Bekämpfung von Schutzrechtsverletzungen wie bspw. die Grenzbeschlagnahme geregelt. Des Weiteren wird die Durchsetzung von Rechten des geistigen Eigentums in Drittstaaten mittels eines verstärkten politischen Dialogs (bspw. dem Dialogforum mit China), technischer Unterstützung und Zusammenarbeit (z. B. im Rahmen der EU–U. S. Action Strategy for the Enforcement of Intellectual Property Rights), unterstützt. Überdies wird an einem Aktionsplan zur Intensivierung der Zollarbeit gearbeitet.

4. Fazit: Gestaltung von integrierten Schutzsystemen zur Bekämpfung von (Produkt-) Piraterie

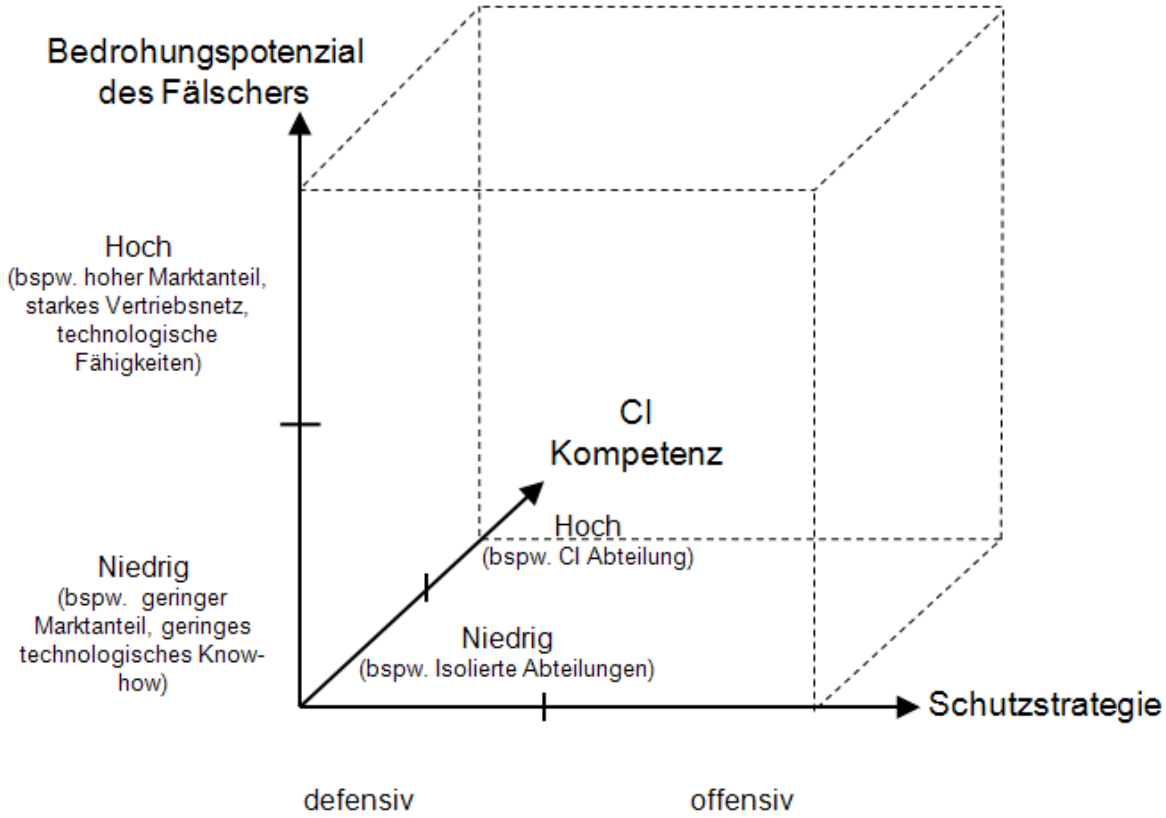
Aus der Betrachtung der konzeptionellen Grundlagen lassen sich zahlreiche Herausforderungen für die Gestaltung von integrierten Schutzsystemen in Unternehmen ableiten. Bei der Konfiguration eines Schutzsystems sind vor allem die Informationsgewinnung und -verarbeitung, die Strategieformulierung sowie die Instrumentenauswahl von besonderer Bedeutung. Im Kontext der Gestaltung eines umfassenden Schutzsystems für ein Unternehmen ist in einem ersten Schritt die strategische Ausrichtung in der Bekämpfung von Fälschern vor dem Eintritt eines Pirateriefalls als Teil der Unternehmensstrategie zu bestimmen bzw. aus dieser abzuleiten. Allgemein können die unterschiedlichen Strategien den Feldern Prävention, Sanktion, Duldung und Kooperation zugeordnet werden. Innerhalb und zwischen diesen ist die Bestimmung der hierfür notwendigen zusätzlichen Schutzinstrumente zu untersuchen. Sowohl für die Strategieformulierung als auch für die Instrumentenauswahl ist mittels CI ein kritisches Informationsvolumen zu generieren.

Insbesondere vor dem Hintergrund begrenzter Ressourcenverfügbarkeit und der Notwendigkeit zur gezielten Gestaltung und Abstimmung des Schutzsystems sind CI Instrumente und Schutzmaßnahmen im Bezug auf das Gefährdungspotenzial eines Fälschers zu konfigurieren. Der Gestaltungs- und Handlungsbedarf für Unternehmen ergibt dabei sich aus der eige-

[79] Deutschland, Frankreich, Großbritannien, Italien, Japan, Kanada, Russland und die USA.

nen bereits, vorhandenen CI-Kompetenz und der Grundausrichtung der bisherigen Schutzstrategie. Eine hohe CI-Kompetenz ist bspw. gegeben, wenn das Unternehmen bereits über eine spezialisierte, funktions- und produktübergreifende CI-Funktion (etwa in Gestalt eines zentralen Service Centers) verfügt, welche in koordinierender Weise oder als zentral verantwortliche Instanz die CI-relevanten Aktivitäten steuert und abstimmt. Eine geringe CI-Kompetenz liegt dagegen vor, wenn die mit CI verbundenen Aktivitäten über mehrere Funktionsbereiche oder Geschäftsbereiche zerstreut sind und überdies nicht primär mit CI-Aufgabe betraut (CI in der Nebentätigkeit). Bei der strategischen Grundhaltung im Umgang mit und Einsatz von Schutzmaßnahmen kann nach *Burr/Stephan et al. (2007)* zwischen einer offensiven und einer defensiven Schutzstrategie unterschieden werden. Defensive Strategien bleiben im Wesentlichen auf den Einsatz von formalen Schutzrechten beschränkt. Im Mittelpunkt von defensiven Schutz(rechts)strategien stehen Bemühungen des Unternehmens, eigene Innovationen mit Hilfe von juristischen Maßnahmen wie Patent- und Markenanmeldungen gegen Imitation abzusichern. Im Extremfall bleibt die defensive „Strategie“ auf die Anmeldung sowie „Verwaltung“ des Schutzrechtsportfolios beschränkt und schließt allenfalls die sporadische Überprüfung von Schutzrechtsverletzungen ein. Offensive Schutzstrategien richten sich dagegen nicht nur auf die Anmeldung (und Verwaltung) formaler Schutzrechte. Unternehmen mit offensiven Schutzrechtsstrategien bedienen sich des gesamten Portfolios juristischer und präventiver Instrumente einschließlich der flankierenden betriebswirtschaftlichen und politischen Maßnahmen. Eine offensive Schutzstrategie ist ferner bewusst gegen aktuelle und potenzielle Konkurrenten (und Piraten) des Unternehmens gerichtet und prinzipiell an der vorbeugenden Abschreckung der „feindlichen“ Akteure und der Reduzierung ihrer Handlungsspielräume interessiert. Abb. 9 visualisiert die Zusammenhänge.

Abb. 9: Abstimmung des Schutzsystems



Ausgehend von Abbildung 9 ergeben sich unterschiedliche Implikationen für die Konfiguration eines integrierten Schutzsystems. Im Falle einer niedrigen CI-Kompetenz und defensiv ausgerichteter Schutzstrategie bei gleichzeitig niedrigem Bedrohungspotenzial scheint auf den ersten Blick kein Handlungsbedarf gegeben zu sein. Allerdings muss hier zwischen dem wahrgenommenem und dem tatsächlich bestehenden Bedrohungspotenzial unterschieden werden. Es besteht nämlich die Gefahr, dass das Unternehmen trotz bestehender Bedrohung keine Gefahr erkennt (was in Anbetracht der geringen CI-Kompetenz nicht unwahrscheinlich ist). So sollte zumindest als grundlegender Schritt die CI-Kompetenz gesteigert werden, um Bedrohungspotenziale besser erkennen und einschätzen zu können. Ist im Unternehmen eine entsprechende CI-Kompetenz vorhanden, so können mit Hilfe einer permanenten Umfeldanalyse Gefahren frühzeitig und zuverlässig erkannt werden. Verfolgen Unternehmen bei geringer CI-Kompetenz eine offensive Schutzstrategie, so lassen sich zwar Markteintrittsbarrieren für Fälscher bzw. Wettbewerber aufbauen, es besteht jedoch die Gefahr, dass ohne Intelligence die falschen Instrumente ausgewählt werden. Zur Effektivitätssteigerung der präventiven und abschreckenden Maßnahmen sollte eine offensive Schutzrechtsstrategie durch eine entsprechende CI-Kompetenz gestützt sein. Bei einer über längere Zeit niedrigen Bedrohung durch Piraterie besteht der Anreiz, Ressourcen aus der Compe-

titive Intelligence-Funktion abzuziehen. Dieser Schritt will jedoch wohl überlegt sein, da ein erneuter Kompetenzaufbau unter Umständen nur durch einen überproportional hohen Ressourceneinsatz erfolgen kann.

Wird ein hohes Bedrohungspotenzial durch Fälscher oder Fälschungen festgestellt und sind gleichzeitig nur niedrige CI-Kompetenzen vorhanden, so ist externe Hilfe in Anspruch zu nehmen. Der „autodidaktische“ CI-Kompetenzaufbau und erforderliche Reorganisationen nehmen viel Zeit in Anspruch. Als Kooperationspartner kommen spezialisierte CI-Dienstleister, Patentanwaltskanzleien mit entsprechender Expertise oder horizontale bzw. vertikale Wertschöpfungspartner in Betracht. Diese Kooperationen mit externen Partnern sollten mittelfristig natürlich auch dazu genutzt werden, die entsprechenden Kompetenzen in das Unternehmen einzulagern. Bereits vorhandene CI-Kompetenzen im Unternehmen sollten bei einer primär defensiv ausgerichteten Schutzstrategie, in Anbetracht eines Bedrohungspotenzials, dazu genutzt werden, eine offensivere Ausrichtung anzustreben und ein breiteres Abwehrpotenzial zu aktivieren. Vergleichbar ist die Situation bei einer offensiven Schutzstrategie aber gleichzeitig geringer CI-Kompetenz. Hier wird zwar versucht, ein breites Spektrum an Schutzmaßnahmen zur Abwehr von Piraterie einzusetzen, aber es besteht die Gefahr, dass das Potenzial der Schutzinstrumente nicht vollständig ausgeschöpft bzw. in eine falsche Richtung gelenkt wird. Im Fall eines hohen Bedrohungspotenzials muss eine offensive Schutzstrategie durch entsprechende CI-Aktivitäten bzw. -Kompetenzen ergänzt werden et vice versa.

Im nachfolgenden Discussion Paper 08-02 werden die im vorliegenden Beitrag konzeptionell skizzierten Gestaltungsparameter und vorgestellten Handlungsempfehlungen zum Aufbau eines effektiven, integrierten Schutzsystems zur Aufdeckung und Abwehr von Produktpiraterie anhand von konkreten Beispielen aus der Unternehmens- und Pirateriepraxis illustriert. Primär am Beispiel von Erfahrungen deutscher Unternehmen in China werden Erfolgs- und vor allem Misserfolgsfaktoren im Umgang mit (Produkt-)Piraterie herausgearbeitet.

Literaturverzeichnis

APA - Asien-Pazifik Ausschuss der deutschen Wirtschaft (2006): Technologietransfer nach China: Leitfaden für Unternehmen, Berlin 2006.

Arlt, C. (2006): Digital Rights Management Systeme - Der Einsatz technischer Maßnahmen zum Schutz digitaler Inhalte, München 2006.

Ashton, W. B./Klavans, R. A. (1997): Keeping Abreast of Science and Technology: Technical Intelligence for Business, Columbus 1997.

Babbar, S./Rai, R. (1993): Competitive Intelligence for International Business, in: Long Range Planning, Jg. 26., Heft 3, S. 103-113.

BDI - Bundesverband der Deutschen Industrie e. V. (2007): Produkt- und Markenpiraterie verhindern - Präventionsstrategien der deutschen Wirtschaft, BDI-Drucksache Nr. 393, Berlin 2007, in: http://www.bdi-online.de/Dokumente/Recht-Wettbewerb-Versicherungen /Produktpiraterie.pdf, Abrufdatum 13. April 2007.

BMWi - Bundesministerium für Wirtschaft und Technologie (2007): Maßnahmen gegen Produktpiraterie und andere Schutzrechtsverletzungen, in: http://www.bmwi.de/BMWi/Navigation/aussenwirtschaft,did=184990,render=renderPrint.html, Abrufdatum 03. April 2007.

Brenner, C. (2006): Schutzmaßnahmen gegen Produktpiraterie in der Praxis, in: Sokianos, N. P. (Hrsg.): Produkt- und Konzeptpiraterie – erkennen, vorbeugen, abwehren, nutzen, dulden, Wiesbaden 2006, S. 275-290.

Burr, W./Stephan, M./Soppe, B./Weisheit, S. (2007): Patentmanagement: Strategischer Einsatz und ökonomische Bewertung von technologischen Schutzrechten, Stuttgart 2007.

Burr, W./Stephan, M. (2006): Dienstleistungsmanagement: Innovative Wertschöpfungskonzepte im Dienstleistungssektor, Stuttgart 2006.

Burr, W./Musil, A./Stephan, M./Werkmeister, C. (2005): Unternehmensführung, München 2005.

Deutscher Bundestag (2006): Auswirkungen chinesischer Produktpiraterie für deutsche Unternehmen, Drucksache 16/3566, Berlin 2006, in: http://dip.bundestag.de/btd/16/035/1603566.pdf, Abrufdatum 12. April 2007.

DIHK - Deutscher Industrie- und Handelskammertag (2006): Export und Import 2006/2007. DIHK – Umfrage bei den deutschen Außenhandelskammern – Herbst 2006, Berlin 2006.

Fleisher, C. S./Bensoussan, B. E. (2003): Strategic and competitive analysis: Methods and techniques for analyzing business competition, New Jersey 2003.

Fuchs, H. J./Kammerer, J./Ma, X./Rehn, I. M. (2006): Piraten, Fälscher und Kopierer. Strategien und Instrumente zum Schutz geistigen Eigentums in der Volksrepublik China, Wiesbaden 2006.

Gassmann, O./Bader, M. A. (2006): Patentmanagement. Innovationen erfolgreich nutzen und schützen, Berlin 2006.

Gerybadze, A. (2004): Technologie und Innovationsmanagement. Strategie, Organisation und Implementierung, München 2004.

Ghoshal, S./Kim, S. K. (1986): Building effective intelligence systems for competitive advantage, in: Sloan Management Review, Jg. 28, Heft 1, S. 49-58.

Gilad, B./Gilad T. (1988): The business intelligence system: A new tool for competitor advantage, New York 1988.

Gillert, O. (2006): Juristische Gesichtspunkte der Produkt- und Konzeptpiraterie, in: Sokianos, N. P. (Hrsg.): Produkt- und Konzeptpiraterie - erkennen, vorbeugen, abwehren, nutzen, dulden, Wiesbaden 2006, S. 205-222.

Grossman, G.M./Shapiro, C. (1988): Foreign counterfeiting of status goods, in: The Quarterly Journal of Economics, Heft Februar, S. 79-100.

Hartung, A. (2006): Geheimnisschutz und Whistleblowing im deutschen und englischen Recht, Saarbrücken 2006.

Helbig, V. (2006): Anforderungen an die Produktdokumentation und Schutz vor Missbrauch, in: Sokianos, N. P. (Hrsg.): Produkt- und Konzeptpiraterie – erkennen, vorbeugen, abwehren, nutzen, dulden, Wiesbaden 2006, S. 149-168.

Hemphill, T. A. (2004): The Strategic Management of Trade Secrets in Technology-based Firms, in: Technology Analysis & Strategic Management, Jg. 16, Heft 4, S. 479-494.

Holtbrügge, D./Puck, J.F. (2005): Geschäftserfolg in China – Strategien für den größten Markt der Welt, Berlin 2005

ICC - International Chamber of Commerce (2007): Global Survey on Counterfeiting and Piracy - Survey Findings Report 2007, in: http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Survey%20findings%20report.pdf, Abrufdatum 12. April 2007.

Kemper, H. G./Baars, H. (2006): Business & Competitive Intelligence. IT-basierte Managementunterstützung und markt-/wettbewerbsorientierte Anwendungen, in: HDM-Praxis der Wirtschaftsinformatik, Heft 247, S. 7-20.

Kunze, C. W. (2000): Competitive Intelligence - Ein ressourcenorientierter Ansatz strategischer Frühaufklärung, Aachen 2000.

Köhler, H. (2004): §§ 1-4, §§ 17-22 UWG, in: Baumbach, A./Hefermehl, W./Köhler, H. (Hrsg.): Wettbewerbsrecht: Gesetz gegen unlauteren Wettbewerb, Zugabeverordnung, Rabattgesetz und Nebengesetze: Kommentar, Bd. 13a, 23. Auflage, München 2004.

Kurz, P. (2004): Vertraulichkeitsvereinbarungen, Köln 2004.

LfV - Landesamt für Verfassungsschutz Baden-Württemberg (2004): Know-how Schutz. Handlungsempfehlungen für die gewerbliche Wirtschaft, in: http://www.verfassungsschutz.bw.de/downloads/publikationen/spio/know_how_schutz_2004.pdf, Abrufdatum 20. Mai 2007.

Lux, C./Peske, T. (2002): Competitive Intelligence und Wirtschaftsspionage – Analyse, Praxis, Strategie, Wiesbaden 2002.

Michaeli, R. (2006): Competitive Intelligence. Strategische Wettbewerbsvorteile erzielen durch systematische Konkurrenz-, Markt- und Technologieanalyse, Berlin 2006.

Nia, A. /Zaichkowsky, J. L. (2000): Do counterfeits devalue the ownership of luxury brands?, in: Journal of Product & Brand Management, Jg. 9, Heft 7, S. 485-498.

Picot, A. (1991): Ein neuer Ansatz zur Strukturierung der Leistungstiefe, in: Zeitschrift für betriebswirtschaftliche Forschung, Jg. 43, Heft 4, S. 336-357.

Porter, M. E. (1980): Competitive Strategy - Techniques for analyzing industries and competitors, New York 1980.

Porter, M. E. (1985): Competitive Advantage. Creating and sustaining superior performance, New York 1985.

Pütz, T./von Rundstedt, E. (2006): Personalpolitik und Technologieschutz: Zufriedenheit ist entscheidend, in: Sokianos, N. P. (Hrsg.): Produkt- und Konzeptpiraterie - erkennen, vorbeugen, abwehren, nutzen, dulden, Wiesbaden 2006, S. 55–66.

Ronde, T. (2001): Trade secrets and information sharing, in: Journal of Economics & Management Strategy, Jg. 10, S. 391–417.

Sammon, W. L. (1984): Competitor Intelligence: An organizational framework for business, in: Sammon, W. L./Kurland, M. A./Spitalnic, R., (Hrsg.): Business Competitor Intelligence - Methods for collecting, organizing and using information, New York 1984, S. 61-89.

Sokianos, N. P. (2006): Produkt- und Konzeptpiraterie: Herausforderungen im erweiterten Unternehmensnetzwerk, in: Sokianos, N. P. (Hrsg.): Produkt- und Konzeptpiraterie - erkennen, vorbeugen, abwehren, nutzen, dulden, Wiesbaden 2006, S. 15-54.

Teece, D. J. (2000): Strategies for managing knowledge assets: the role of firm structure and industrial context, in: Long Range Planning, Jg. 33, S. 35-54.

Teece, D. J. (1986): Profiting from Technological Innovation, in: Research Policy, Jg. 15, Heft 6, S. 285-305.

Wildemann, H. (2007): Produktpiraten auf dem Vormarsch, in: IHK Ostwürttemberg (Hrsg.): Wirtschaft in Ostwürttemberg, Februar 2007, S. 8-10.

Wildemann, H./.Ann C./Broy M./Günthner, W./Lindemann A U. (2007): Plagiatsschutz – Handlungsspielräume der produzierenden Industrie gegen Produktpiraterie, München 2007.

Williamson, O. E. (1975): Markets and Hierarchies: Analysis and Antitrust Implications: A Study in the Economics of Internal Organization, New York 1975.

WTO - World Trade Organization (2006): World Trade Developments in 2005, in: http:/ /www .wto.org/english/res_e/statis_e/its2006_e/its06_general_overview_e.pdf, Abrufdatum 20. Mai 2007.

WTO - World Trade Organization (2006b): Network of world merchandise trade by region, 2003-05, in: http://www.wto.org/english/res_e/statis_e/its2006_e/appendix_e/a02.xls, Abrufdatum 20. Mai 2007.

Zollbehörde (2005): Statistik 2005, in: http://www.zoll.de/b0_zoll_und_steuern/d0_verbote _und_beschraenkungen/f0_gew_rechtsschutz/a0_marken_piraterie/d0_statistik/index.html, Abrufdatum 11. April 2007.

Herausgeber Michael Stephan

Department of Technology and
Innovation Management

Philipps-University Marburg
Am Plan 2
35037 Marburg

Erscheinungsort Marburg, Deutschland

ISSN 1864-2039