Carsten Fussan (Hrsg.)

Managementmaßnahmen gegen Produktpiraterie und Industriespionage

RESEARCH

Carsten Fussan (Hrsg.)

Managementmaßnahmen gegen Produktpiraterie und Industriespionage

GABLER RESEARCH

Carsten Fussan (Hrsg.)

Managementmaßnahmen gegen Produktpiraterie und Industriespionage

GABLER RESEARCH

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Die Finanzierung des Projektes und dieser Veröffentlichung erfolgte durch Fördermittel der STAEDTLER-Stiftung Nürnberg.

1. Auflage 2010

Alle Rechte vorbehalten
© Gabler Verlag | Springer Fachmedien Wiesbaden GmbH 2010

Lektorat: Ute Wrasmann | Anita Wilke

Gabler Verlag ist eine Marke von Springer Fachmedien.
Springer Fachmedien ist Teil der Fachverlagsgruppe Springer Science+Business Media.
www.gabler.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlags unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Umschlaggestaltung: KünkelLopka Medienentwicklung, Heidelberg
Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier
Printed in Germany

ISBN 978-3-8349-2097-3

Vorwort

Wissen und Kompetenz sind die zentralen Quellen für Entwicklung, Fortschritt sowie Wohlstand – nicht nur für individuelle menschliche Entwicklung, sondern auch für die Wettbewerbspositionierung von Unternehmen. Wissenstransfers zwischen Personen sind sowohl individuell-entwicklungssoziologisch als auch volkswirtschaftlich essentiell für Wohlstandsgenerierung und werden daher nicht nur an Schulen und Hochschulen, sondern auch in Unternehmen systematisch betrieben. Auf Bildungsidealen – also auf historisch gewachsenen Kulturen des Wissenstransfers – basieren moderne Ethik, Demokratie, technische Innovationen und volkswirtschaftlicher Wohlstand aller.

Wissenstransfers zwischen Unternehmen sind hingegen sensibel. Sofern wettbewerbsrelevante Informationen nicht zwischen Partnerunternehmen, sondern zwischen Konkurrenten diffundieren, gefährden sie Beschäftigung, Wohlstand und hart erarbeitete Marktpositionen. Wissen ist Innovation. Und Innovation ist Umsatz. Besonders für innovative Unternehmenslandschaften wie die bundesdeutsche stellen illegale Kompetenztransfers an die internationale Konkurrenz bedrohliche Umsatz- und Wohlstandsgefahren dar. Der Schutz wettbewerbsrelevanten Wissens ist für die betroffenen Unternehmen daher essentiell. Die Methoden nicht erwünschten Wissenstransfers zwischen Konkurrenzunternehmen sind Produktpiraterie und Industriespionage. Es sind dies die beiden weltweit am weitesten verbreiteten Spielarten von Wirtschaftskriminalität. Mit steigender Tendenz. Der Umgang mit Produktpiraterie und Industriespionage muss daher auch im Zentrum betriebswirtschaftlicher Aufmerksamkeit und Forschung stehen.

Produktpiraterie wird hierbei verstanden als Nachahmung von Produktelementen, Designs, Warenzeichen, technischen Komponenten oder Materialien von Produkten, welche bereits auf dem Markt sind. Produkt-Know-how von noch nicht markteingeführten Produkten oder wettbewerbsrelevantes Prozess-Know-how, welches die Grenzen des Unternehmens nicht verlässt, wird hingegen durch Industriespionage ausgespäht.

Die besondere Bedeutung, welche der betriebswirtschaftlichen Analyse von Know-how-Schutz zuzumessen ist, hat zur Initiierung eines internationalen Forschungsprojektes zu Produktpiraterie und Industriespionage geführt, welches ich an der Ohm-Hochschule Nürnberg durchgeführt habe. Die Studien zu diesem Projekt wurden in zwei grundlegenden analytischen Komplexen bearbeitet: einem empirischen For-

schungsteil, welcher in eine neue Interpretation von Produktpiraterie und Industriespionage im Rahmen betriebswirtschaftlicher Methodik mündete, und einem ergänzenden Forschungsteil, welcher die wirtschaftskriminellen Phänomene „Produktpiraterie“ und „Industriespionage“ generell einordnet und sie aus Perspektive der beiden wichtigen Funktionsbereiche Marketing und Logistik einer besonderen Analyse zuführt. Der vorliegende Herausgeberband bündelt die Erkenntnisse aus dem zweiten, ergänzenden Forschungsteil und steht somit in direktem gedanklichen Zusammenhang zur Veröffentlichung der empirischen Studie und wissenschaftlichen Einordnung (Fussan 2010: „Unternehmerisches Handeln, Wirtschaftskriminalität und Terrorismus – Erfolgsstrategien am Beispiel von Produktpiraterie und organisierter Kriminalität“, Gabler Verlag).

Im vorliegenden Band wird nach einer zusammenfassenden betriebswirtschaftlichen Interpretation des Problems und der Einzelbeiträge (Carsten Fussan) eine analytische Synopse mit Handlungsempfehlungen zu Produktpiraterie (Christina Witte) und Industriespionage (Gundula Warnecke) vorgenommen. Möglichkeiten betrieblichen Know-how-Schutzes werden zudem aus den funktionalen Perspektiven Marketing (Selina Rehn) und Logistik (Marion Fricke) erörtert. Ich danke allen Co-Autorinnen dieses Herausgeberbandes sehr herzlich für ihre Beiträge.

Unternehmen können durch eine Know-how-bezogene prozessanalytische Bestandsaufnahme und durch Umsetzung am Einzelfall orientierter betriebswirtschaftlicher Abwehrmaßnahmen gegen Produktpiraterie und Industriespionage das Risiko und die Folgen illegalen Know-how-Transfers entscheidend verringern. Durch Veränderung der internen Strukturen können so Hürden gegen Produktpiraterie und Industriespionage aufgebaut werden. Es ist dies die zentrale Botschaft dieses Herausgeberbandes. Unternehmen sollten diese Möglichkeiten aktiv nutzen und umsetzen.

Das Forschungsprojekt zu Produktpiraterie und Industriespionage sowie die vorliegende Veröffentlichung wäre ohne die engagierte und umfangreiche Förderung durch die STAEDTLER-Stiftung nie in dieser Form realisiert worden. Ich danke daher in besonderem Maße den Vorsitzenden der STAEDTLER-Stiftung, Herrn Dr. jur. Werner Grandi und Herrn Dieter Schoch, für die Gewährung der Förderung sowie Herrn Herbert Hofmann für seine geduldige Begleitung des Projektes auf administrativer Ebene.

Das Forschungsprojekt wurde an der Ohm-Hochschule Nürnberg durchgeführt. Die Hochschule hat dem Projektteam dabei über die gesamte Projektlaufzeit sehr engagiert

generelle, infrastrukturelle und personell-rechnungsmäßige Unterstützung gewährleistet, wofür ich insbesondere dem Rektor der Ohm-Hochschule, Herrn Prof. Dr. Michael Braun, und dem Kanzler der Ohm-Hochschule, Herrn Achim Hoffmann, äußerst dankbar bin.

Wichtig für die Analyserichtung des Projektes war die sehr intensive und impulsgebende betriebswirtschaftliche Diskussion mit Frau Christina Witte in der Konzeptphase des Forschungsprojektes, wofür ich ihr besonders danke. Für das tägliche große Engagement im Rahmen der Durchführung des Projektes bedanke ich mich sehr intensiv bei allen Projektmitarbeiterinnen und Projektmitarbeitern, besonders jedoch bei Frau Gundula Warnecke, Frau Selina Rehn, Frau Antoaneta Hristova, Frau Christine Dressler und Frau Stefanie Rumpff. Ohne sie alle wäre eine so umfangreiche Studie, welche in zwei Veröffentlichungen mündete, nicht möglich gewesen.

Prof. Dr. Carsten Fussan

Inhaltsverzeichnis

Vorwort ..... **V**

Inhaltsverzeichnis ..... **IX**

A Bedeutung innerbetrieblicher Veränderungen für Know-how-Schutz in Unternehmen **1**
Prof. Dr. Carsten Fussan

1 Bedeutung innerbetrieblicher Veränderungen im Kontext des Unternehmensschutzes 5
2 Ansatzpunkte und Lösungsansätze zur Abwehr externer Sicherheitsrisiken 6
3 Neuausrichtung der Unternehmensidentität zur optimalen Realisierung der Sicherheitsanliegen 14
4 Eigenverantwortung der Unternehmen als wichtigste Komponente im Kampf gegen Produktpiraterie und Industriespionage 20

B Risikoeffizienz und Wirksamkeit betriebswirtschaftlicher Schutzmaßnahmen gegen Produktpiraterie **23**
Christina Maren Witte

1 Piraterieschutz als Kampf gegen Windmühlen? 27
2 Produkt- und Markenpiraterie in China 28
3 Strategien und Schutzmaßnahmen bei Produkt- und Markenpiraterie 39
4 Experteninterviews 77
5 Umdenken im China-Geschäft als entscheidende Maxime 98

C Schutzmaßnahmen gegen Produktpiraterie im Funktionalbereich Marketing 121
Selina C. W. Rehn

1 Produktpiraterie als Managementproblem 127
2 Grundlagen zur Produktpiraterie 128
3 Markteintrittsstrategie: Zeit als Wettbewerbsfaktor und Maßnahmen gegen Produktpiraterie 146
4 Maßnahmen aus dem Bereich Marketing und Vertrieb zur Bekämpfung von Produktpiraterie 153
5 Maßnahmenevaluation 172
6 Marketing als Teil eines unternehmensweiten Schutzkonzeptes 176

D Schutzmaßnahmen gegen Produktpiraterie im Funktionalbereich Logistik 183
Marion Fricke

1 Piraterie heute 187
2 Gegenstandsbereich und Hemmnisse bei der Bekämpfung von Produktpiraterie 187
3 Logistik als Angriffspunkt für Produktpiraten 192
4 Technische Schutzmaßnahmen in der Logistik 198
5 Betriebswirtschaftliche Schutzmaßnahmen in der Logistik 219
6 Managementempfehlungen 241

E Quellen illegalen Know-how-Abflusses aus Industrieunternehmen und Strategien gegen Industriespionage 249
Gundula Warnecke

1 Industriespionage als Reaktion auf den verschärften Wettbewerb 255
2 Grundlagen der Industriespionage 256
3 Information und Wissen als Wettbewerbsfaktor und Spionagegut 264
4 Quellen illegalen Know-how-Abflusses entlang der Wertkette 271
5 Strategien zur Vorbeugung und Abwehr von Industriespionage 294
6 Managementempfehlungen zur Spionageabwehr 318
7 Gefahren der Industriespionage weiterhin unterschätzt 320

Die Autoren 333

Prof. Dr. Carsten Fussan

A Bedeutung innerbetrieblicher Veränderungen für Know-how-Schutz in Unternehmen

Inhaltsverzeichnis

1 Bedeutung innerbetrieblicher Veränderungen im Kontext des Unternehmensschutzes 5

2 Ansatzpunkte und Lösungsansätze zur Abwehr externer Sicherheitsrisiken 6

2.1 Herangehensweise der Autoren 6

2.2 Funktionale Schwerpunktbereiche für Schutzmaßnahmen gegen Produktpiraterie und Industriespionage 7

2.2.1 Forschung und Entwicklung 7
2.2.2 Beschaffung 8
2.2.3 Produktion 9
2.2.4 Distribution 10
2.2.5 Kommunikation und Service 11

2.3 Grundproblem der kriminellen Herausforderungen 12

3 Neuausrichtung der Unternehmensidentität zur optimalen Realisierung der Sicherheitsanliegen 14

3.1 Kernkomponenten erfolgreichen Kriminalitätsmanagements 14

3.2 Adaptionsförderliche Strukturen zur Kriminalitätsbekämpfung 16

3.2.1 Management 16
3.2.2 Unternehmenskommunikation 17
3.2.3 Unternehmenskultur 19

4 Eigenverantwortung der Unternehmen als wichtigste Komponente im Kampf gegen Produktpiraterie und Industriespionage 20

Literaturverzeichnis 22

1 Bedeutung innerbetrieblicher Veränderungen im Kontext des Unternehmensschutzes

In hoch entwickelten Industrienationen wie Deutschland oder auch den USA gewinnen Innovationen als Basispfeiler internationaler Wettbewerbsfähigkeit für die Unternehmen immer mehr an Bedeutung. Es sind bereits seit langem nicht mehr nur Kostenvorteile der Produktion, welche langfristige Marktakzeptanz und Überlebensfähigkeit von Unternehmen sichern. Vielmehr erklären sich Handelsbilanzüberschüsse westlicher Volkswirtschaften zu einem signifikanten Teil durch eine Exzellenz des Wissens.

Wissen und Innovationen sind im Gegensatz zu beispielsweise mineralischen Rohstoffvorkommen immateriell und hierdurch auch leicht übertragbar und durchaus kopierbar. Eine Abhängigkeit vieler Unternehmen von diesen immateriellen Wirtschaftsgütern birgt daher durchaus Risiken. Internationale Produktpiraten und Industriespione haben sich auf diese sensiblen „Rohstoffe“ von Unternehmen spezialisiert und sind durch ihre kriminellen Handlungen durchaus in der Lage, die Wettbewerbspositionen der innovativen Unternehmen nachhaltig zu schwächen. Wissen und Innovationen bedürfen daher eines besonders hohen Schutzes gegen die kriminellen Energien von Produktpiraten und Industriespionen. Im Rahmen dieses Sammelbandes werden hierzu Strategien und Lösungsansätze auf unterschiedlichste Weise dargestellt, welche dem Unternehmensmanagement bei der Entwicklung effektiver Sicherheitskonzepte zur Verfügung stehen.

Der Beitrag der Autorin Witte befasst sich mit den Möglichkeiten eines präventiven Schutzes gegen Produktpiraterie aus betriebswirtschaftlicher Sicht; gewonnene Erkenntnisse werden praxisnah am Beispiel Chinas erläutert und anhand einer qualitativen Untersuchung auf ihre Wirksamkeit hin überprüft. Rehn und Fricke präsentieren in den nachfolgenden Beiträgen Strategien und Maßnahmen zur Bekämpfung von Produktpiraterie im Rahmen der Funktionalbereiche Marketing sowie Logistik. Erstgenannte bewertet dabei die von ihr vorgestellten Sicherheitsvorkehrungen entsprechend der Nachhaltigkeit und des Wirkungshorizonts. Die Autorin Warnecke beleuchtet abschließend pro- und reaktive Lösungsansätze in Hinblick auf die effiziente Abwehr von Industriespionage.

Es wird in allen Beiträgen deutlich, dass nur eine systematische Veränderung innerbetrieblicher Strukturen hin zu einem aktiven Sicherheitsmanagement die Bedrohung, welche von Produktpiraterie und Industriespionage ausgeht, verhindern oder ihre Wir-

kung zumindest abschwächen kann. Hierzu stellt bereits Witte heraus, dass die reaktive Haltung vieler Unternehmen „zu langwierig, ineffektiv und nicht effizient"[1] sei, und nur die gezielte Einbindung präventiver Maßnahmenpakete den Schutz der Unternehmen auf lange Sicht gewähren können.[2] Diese Ansicht wird auch von der Autorin Warnecke bezüglich der Bekämpfung spionagewirtschaftlicher Risiken vertreten: „Generell sind Vorkehrungen präventiver Natur effizienter als Abwehrmaßnahmen, die erst nach Bekanntwerden eines illegalen Informationsabflusses ergriffen werden."[3] Das Unternehmen muss aktiv werden und sich der wachsenden Gefahr stellen; Flexibilität und Anpassungsfähigkeit sind Grundvoraussetzung im Umgang mit Produktpiraterie und Industriespionage.

2 Ansatzpunkte und Lösungsansätze zur Abwehr externer Sicherheitsrisiken

2.1 Herangehensweise der Autoren

Auf welche Art eine zielgerichtete Umgestaltung interner Strukturen von Unternehmen am Sinnvollsten realisiert werden kann, veranschaulicht die similäre Herangehensweise der Autoren: Trotz unterschiedlicher Schwerpunkte liegt jedem Beitrag eine kritische Auseinandersetzung mit der Prozessorganisation der Unternehmen (Vgl. Abbildung 1) zugrunde. Das organisationale Design bildet den Dreh- und Angelpunkt für die systematische Analyse potenzieller Gefahrenquellen, auf deren Basis schließlich Managementempfehlungen zum Unternehmensschutz abgeleitet werden können.

Anders als die Autoren Witte und Warnecke, die in ihren Beiträgen Abwehrstrategien aus allen Funktionalbereichen erörtern, kombinieren die Autoren Rehn und Fricke aufbau- und ablauforganisatorische Perspektiven, indem sie die Schutzmöglichkeiten der Organisationseinheiten Logistik und Marketing den operativen Phasen des Wertschöpfungsprozesses zuordnen.

Diese horizontale Betrachtungsweise der durch die Autoren analysierten funktionalen Schwerpunktbereiche gestattet eine bessere Darstellung der Interdependenzen zwischen den Schutzmaßnahmen und ihrer prozessualen Wirkung. Ebenso werden zahlreiche Schnittstellen innerhalb der Unternehmung aufgedeckt und potentielle Gefah-

[1] Witte, S. 39.
[2] Vgl. Witte, S. 43.
[3] Warnecke, S. 294.

renherde auch außerhalb der Unternehmensgrenzen in die Sicherheitsüberlegungen einbezogen.

Die wesentlichen Erkenntnisse und Maßnahmen, die sich aus den Prozessanalysen der Autoren ergeben und die einen wirkungsvollen Schutz gegen Produktpiraterie und Industriespionage ermöglichen, werden nachfolgend in den verschiedenen Beiträgen umrissen.[4] Ziel der Autoren ist es, die Aufmerksamkeit auf wichtige Kernelemente komplexer Abwehrmaßnahmen gegen Produktpiraterie und Industriespionage zu lenken und die Vielfalt des gesamten Themas hierdurch zu reduzieren.

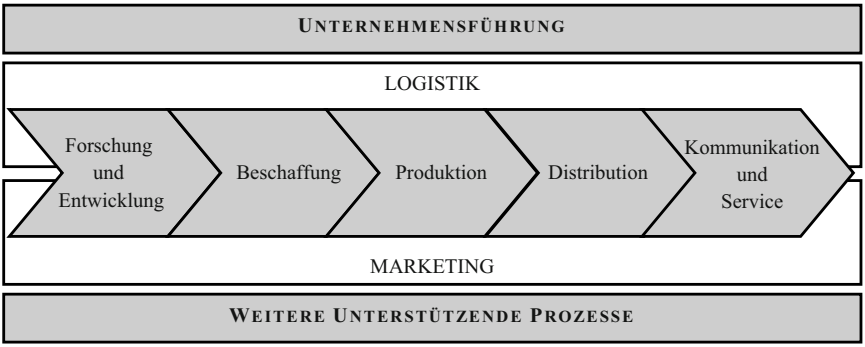


Abbildung 1: Maßnahmenbereiche gegen Produktpiraterie und Industriespionage
Quelle: eigene Darstellung.

2.2 Funktionale Schwerpunktbereiche für Schutzmaßnahmen gegen Produktpiraterie und Industriespionage

2.2.1 Forschung und Entwicklung

Eine der wirksamsten Strategien gegen Produkt- und Markenpiraterie beschreiben die Autoren Witte und Rehn mit der Verkürzung der Entwicklungszyklen.[5] Rehn argumentiert dabei, dass „durch ständige Innovation […] Märkte für Nachahmer blockiert werden“[6] können; die mit dem Innovationsstreben vieler Unternehmen einhergehende Marktforschung führe zu vergleichbaren Ergebnissen, da eine optimale Befriedigung

[4] Nachstehende Verweise auf Beiträge innerhalb dieses Bandes erheben keinen Anspruch auf vollständige Quellenwiedergabe. Es wird hierbei auf die jeweiligen Einzelbeiträge verwiesen.
[5] Vgl. Witte, S. 53; Rehn, S. 157.
[6] Rehn, S. 157.

der Konsumentenwünsche die Loyalität der Verbraucher fördere und ein Abwandern zu Konkurrenzprodukten mindern könne.[7]

Witte verweist in ihren Ausführungen darüber hinaus auf die Bedeutung von Komplementärprodukten: Werden ergänzende Komponenten dahingehend entwickelt, dass eine Nutzung nur mit Fabrikaten des Originalherstellers möglich ist, können Produktpiraten ihrer Existenzgrundlage beraubt werden.

Bei beiden Lösungsansätzen handelt es sich um Vorkehrungen, die im Rahmen der Forschungs- und Entwicklungsarbeit umgesetzt werden; es sind keine Konzepte, die dem physischen Schutz der Produktionsstätte dienen. Strategien, die von den Autoren Witte und Warnecke zur Sicherung des F&E-Bereichs selbst befürwortet werden, sind u.a. die zielgerichtete Abtrennung gefährdeter Abteilungen in Form von Zugangs- und Zutrittsbeschränkungen sowie die organisatorische und geografische Streuung der Forschungstätigkeit.[8] Auf juristischer Seite werden von allen Autoren gleichermaßen die klassischen Patent- und Markenanmeldungen sowie Geheimhaltungsvereinbarungen in ihrer Bedeutung unterstrichen.[9] Durch die reaktive Wirkung rechtlicher Maßnahmen auf bereits eingetroffene Störfälle sind sie jedoch als alleinstehende Sicherheitsvorkehrung in keinem Prozessabschnitt ausreichend.

2.2.2 Beschaffung

Der Vorgang der Beschaffung ist als Bindeglied zwischen Lieferant und Unternehmen besonders risikobehaftet, sodass Witte und Fricke eine sorgfältige Auswahl der Zulieferer als unentbehrlich erachten.[10] Neben quantitativen Leistungskriterien müsse der Auswahl- und Entwicklungsprozess von Zulieferern deshalb auch die persönliche Einstellung der Lieferanten bezüglich Produktpiraterie und Industriespionage berücksichtigen. Besondere Gefahrenquellen könnten sich beispielsweise bei Zusammenarbeit mit ausländischen Zulieferbetrieben sowie durch rechtlich und kulturell abweichende Rahmenbedingungen der Geschäftstätigkeit ergeben.

Gefahren, die durch Ausgliederungen vorgelagerter Produktionsabschnitte entstehen, rät Fricke mit der Vergabe von Teilaufträgen und der Bildung von Einkaufskooperationen zu begegnen. Speziell kleine und mittelständische Unternehmen könnten auf die-

[7] Vgl. Rehn, S. S. 156.
[8] Vgl. Witte, S. 52; Warnecke, S. 330.
[9] Vgl. Witte, S. 64ff.; Rehn, S. 154; Warnecke, S. 311ff.
[10] Vgl. Witte, S. 47f.; Fricke, S. 231.

se Weise ihre Macht gegenüber den Lieferanten stärken und Einfluss auf deren Sicherheitsbemühungen nehmen. Sie äußert außerdem, dass eine vertragliche Absicherung des Unternehmens in Form von Vertraulichkeitsvereinbarungen und Kontrollrechten unverzichtbar sei.

Alle Autoren betonen, eine genaue Überprüfung potentieller Lieferanten sowie die akkurate Gestaltung von Lieferverträgen genügten auf lange Sicht nicht, um ein konstantes Sicherheitsniveau zu garantieren. Unternehmen sollten dies stattdessen durch regelmäßige Wareneingangskontrollen ergänzen, da selbst bei zuverlässigen Lieferanten Unregelmäßigkeiten auf den Transportwegen auftreten können.[11] Nach erfolgreicher Abwicklung der Warenannahmen betont die Autorin Warnecke in ihren Ausführungen zusätzlich die bautechnische Absicherung des Wareneingangs, sodass nicht nur das Einschleusen illegaler Kopien, sondern auch der ungewollte Abgang firmeninternen Know-hows vermieden wird.

2.2.3 Produktion

Sicherheitsmaßnahmen, die von den Autoren Witte, Rehn und Fricke im Zuge der Produktion vorgeschlagen werden, befassen sich überwiegend mit der Markierung von Produkten und Produktteilen. Es gilt, die Originalware mit Eigenschaften zu versehen, „die schwer zu kopieren sind“[12] und später die Echtheit der Produkte zu verifizieren. Rehn bezieht sich dabei auf sichtbare und unsichtbare Technologien und betont die in diesem Sinne verkaufsfördernde Wirkung von Siegeln, Hologrammen, Folien sowie anderen offenen Merkmalen.[13] Bei ähnlicher Herangehensweise ergänzt Witte Rehns Systematisierung um die Klasse der maschinengestützten Produktkennzeichnungen, welche eine besondere Stellung bei der Rückverfolgbarkeit von Waren in der Distribution einnähmen.[14] Die Anwendung der verschiedenen Markierungsmöglichkeiten sowie deren Umfang müssen jedoch laut Fricke von der Art des Produkts, dessen Wert und dem Grad der Eigenfertigung bestimmt und beeinflusst werden.[15]

Im Rahmen der Logistikanalyse fasst Fricke außerdem die Möglichkeiten einer organisatorischen Sicherung des eigentlichen Produktionsprozesses zusammen und verdeutlicht, dass neben Überwachungsmaßnahmen und Zutrittsbeschränkungen auch der

[11] Vgl. Witte, S. 46; Fricke, S. 234.
[12] Fricke, S. 198.
[13] Vgl. Rehn, S. 159.
[14] Vgl. Witte, S. 75f.
[15] Vgl. Fricke, S. 213.

Aufbau der Lagerlogistik eine erhebliche Rolle bei der Abwehr von Plagiatoren spielt. Ist die von ihr präferierte Just-in-Time-Produktion nicht möglich, sollten Waren bei Stillstandzeiten entsprechend ihres Sicherheitsbedürfnisses in verschiedenen Lagersystemen aufbewahrt werden.[16]

Da im Rahmen der Forschung und Entwicklung generierte Wissensvorsprünge im Produktionsprozess weiterverarbeitet werden, sollten nach Ansicht von Warnecke die Sicherheitsüberlegungen des Managements auch konkrete Maßnahmen zur spionagewirtschaftlichen Gefahrenabwehr enthalten. Ziel müsse es sein, errungene Wettbewerbsvorteile nicht durch ungewollte Wissensabflüsse einzubüßen. Die Autorin merkt an, dass dazu die Ergreifung bautechnischer Vorkehrungen zur Sicherung des Fertigungsgeländes allein nicht ausreicht; vielmehr müsse es Aufgabe der Unternehmensführung sein, personellen Abgängen und damit einhergehenden Know-how-Verlusten durch eine aktive Förderung der Mitarbeiterzufriedenheit vorzubeugen.

2.2.4 Distribution

Der Distributionsprozess ist durch seine große Bedeutung für die Erschließung von Absatzmärkten besonders anfällig für kriminelle Aktivitäten. Schäden entstehen dabei weniger durch das unbemerkte Verwenden gefälschter Vorprodukte im eigenen Unternehmen, als vielmehr durch entgangene Verkaufserlöse und Imageverluste aufgrund im Markt befindlicher minderwertiger Plagiate. Die wichtigste Schutzmaßnahme dieses Bereichs sehen die Autoren Witte und Fricke daher in der richtigen Modellierung, Auswahl und Überwachung der Vertriebssysteme.[17]

Die Gefahr der Verbreitung illegaler Kopien in frühen Phasen der Markteinführung kann beispielsweise durch Straffung und Verkleinerung komplexer Vertriebsstrukturen erreicht werden. Diese auf den ersten Blick umsatzhemmende Vorgehensweise hat den Vorteil, dass die Anzahl der Schnittstellen zwischen Unternehmen und Kunden und somit auch die aus ihnen resultierenden Sicherheitsrisiken minimiert werden. Dies kann beispielsweise durch die horizontale sowie vertikale Verkürzung der Distributionskette in Form eines selektiven oder direkten Vertriebs erfolgen.[18] Die Vergabe von Lizenzen wird als weitere Variante einer sicherheitsbewussten Vertriebsgestaltung von der Autorin Witte zwar als „Zugeständnis gegenüber der Problematik der Produktpira-

[16] Vgl. Fricke, S. 225 und 235.
[17] Vgl. Witte, S. 57ff.; Fricke, S. 236.
[18] ebd.

terie“[19] kritisiert, gleichzeitig weist sie jedoch darauf hin, dass derartige Konzepte durch ihren offensiven Charakter gegebenenfalls einen äußerst wirksamen Schutz gewähren.

Unabhängig von der Art des Distributionskonzepts empfiehlt es sich, die vertragliche Absicherung des Unternehmens nicht ausschließlich auf die Einräumung von Kontroll- und Sanktionsrechten zu beschränken. Diese Auffassung vertritt auch Rehn und meint, dass die verbindliche Vereinbarung von Anreizen im Falle einer aktiven Teilnahme an den Sicherheitsvorhaben des Unternehmens ein weit effizienteres Maß an Schutz bietet.[20]

Fricke erklärt darüber hinaus, dass es bei längerfristigen Kooperationen im Verantwortungsbereich des Unternehmens liege, die Vertriebskanäle mit entsprechenden Lesegeräten und Know-how zur Identifikation von Original und Fälschung auszustatten.[21] Es müsse sowohl den Händlern, als auch gegebenenfalls den Kunden möglich sein, die in der Fertigung realisierten Markierungsmaßnahmen an Produkt und Verpackung auf ihrer Richtigkeit hin zu überprüfen. Zudem dürfe bei der sicheren Organisation der Vertriebssysteme und Händlerbeziehungen die Realisierung eines sicherheitsbewussten Transports der Ware vom Unternehmen zu den Händlern und Kunden nicht vernachlässigt werden. Fricke stellt dazu heraus, dass außer der sorgfältigen Auswahl des Transporteurs auch die verschiedenen methodischen Übermittlungsmöglichkeiten vom Management bedacht werden müssen. In Abhängigkeit von den jeweiligen Besonderheiten des zu transportierenden Guts bedarf es folglich einer genauen Abwägung der Vor- und Nachteilen, die eine Beförderung via Luft-, Schienen-, See- und Straßenverkehr zur Folge hat.[22]

2.2.5 Kommunikation und Service

Maßnahmen der Unternehmenskommunikation zielen maßgeblich auf die effektive Aufklärung von Mitarbeitern, Kooperationspartnern und Kunden über die steigenden Risiken, die fatalen Folgen sowie die durchgeführten Sicherheitsvorkehrungen gegen Produktpiraterie und Industriespionage ab. Die inhaltliche Ausgestaltung der jeweiligen Kommunikationsbotschaft wird dabei von der Art des Adressatenkreises bestimmt: So sollten Konsumenten, die mutwillig auf gefälschte Produkte zurückgreifen,

[19] Witte, S. 59.
[20] Vgl. Rehn, S. 164.
[21] Vgl. Fricke, S. 237ff.
[22] Vgl. Fricke, S. 226ff.

nach Aussage von Rehn über das Ausmaß der Schäden, die sie sich und anderen damit zufügen, informiert werden, während dem unwissentlichen Erwerb von Plagiaten durch Werbekampagnen mit Hinweis auf angewandte Sicherheitskennzeichnungen entgegengewirkt werden sollte.[23]

Rehn gibt des Weiteren zu bedenken, dass durch eine aktive Kundenbetreuung die Zufriedenheit der Konsumenten gesteigert werde und so langfristige Beziehungen aufgebaut werden könnten. Ein intensives After-Sales-Management in Form von Zusatzleistungen und Services sowie eine individualisierte Produktgestaltung kämen ebenfalls der Kundenloyalität zugute und erschwerten folglich den Marktzutritt für Produktpiraten.[24]

2.3 Grundproblem der kriminellen Herausforderungen

Die Beiträge der Autoren zeigen, dass Handlungsoptionen, welche dem Management zu einer wirksamen Absicherung der Unternehmenstätigkeit gegen kriminelle Einflüsse offen stehen, fast unbegrenzt vielfältig sind. In jeder spezifischen Situation können und sollten eine Reihe von Schutzmaßnahmen auf die Situation zugeschnitten und umgesetzt werden. Jedoch sind nicht nur die Handlungsoptionen vielfältig, sondern auch die Formen der kriminellen Bedrohung. Moderne Prozessketten der Produktion oder der Einsatz innovativen Know-hows in internationalen Produktionswertschöpfungsketten lassen an extrem vielen Stellen Ansatzpunkte für kriminelles Handeln zu. Die beschriebenen Phänomene der internationalen Produktpiraterie und der Industriespionage basieren im Kern also auf einer sehr großen Zahl von Gefährdungsoptionen durch Kriminelle und auf einer schier unbegrenzten Zahl von mehr oder weniger wirksamen Abwehrmöglichkeiten seitens der Unternehmen.

Dieses Phänomen kann als „Komplexität“ bezeichnet werden. Komplexität bezeichnet im Managementkontext die Vielfalt der einwirkenden Faktoren auf Situationen oder Organisationen und das Ausmaß der gegenseitigen Interdependenzen dieser Faktoren.[25] In Folge von Komplexität steigen die Probleme der Strukturierbarkeit von Entscheidungen. Sowohl die Analyse des Ist-Zustandes, als auch die Erarbeitung von Lösungsalternativen und die Bewertung dieser Handlungsoptionen fallen dem Management unter komplexen Bedingungen deutlich schwerer als in nicht komplexen Situati-

[23] Vgl. Rehn, S. 167f.
[24] Vgl. Rehn, S. 170; auch: Witte, S. 62.
[25] Vgl. Ulrich/Fluri (1992).

onen. Infolgedessen steigt die Wahrscheinlichkeit, Fehlentscheidungen oder suboptimale Entscheidungen zu treffen. Komplexität ist zwar ein ständiger Begleiter von Management, jedoch auch schwierig zu beherrschen. Je komplexer Managementsituationen sind, desto mehr Probleme bereiten sie und desto größer ist die Fehlerwahrscheinlichkeit.

Produktpiraterie und Industriespionage zeichnen sich durch die höchste Form der Informationsasymmetrie zwischen Akteuren aus. Unternehmen wissen nicht, wann, wo und in welcher Form die kriminellen Handlungen zu erwarten sind. Die Ergebnisse des illegalen Handelns lassen sich oft erst Monate später oder manchmal auch gar nicht erkennen. Die kriminellen Handlungen können überall auf der Kompetenz-Wertschöpfungskette des Unternehmens stattfinden, zu jeder Zeit und auf extrem vielfältige Weise. Die möglichen antizipativen und reaktiven Abwehrmaßnahmen sind ebenso vielfältig wie die kriminellen Handlungen und müssen dies auch sein, da mit Standardrezepten den oft sehr geschickten und einfallsreichen kriminellen Akteuren nicht beizukommen wäre. Im Ergebnis lässt sich feststellen, dass Produktpiraterie und Industriespionage sehr komplexe Herausforderungen modernen Managements sind. Aufgrund ihrer asymmetrischen Struktur und geringen Prognostizierbarkeit können diese kriminellen Phänomene sogar als vermutlich die komplexesten Herausforderungen modernen Managements begriffen werden.

Die Beiträge der Autoren in diesem Sammelband illustrieren die Komplexität der kriminellen Phänomene und zeigen Reaktionsmöglichkeiten des Managements auf. Wenngleich standardisierte Verfahren kein adäquates Mittel zur Bewältigung hoch komplexer Managementsituationen darstellen, sind die erläuterten Methoden doch Archetypen von möglichen Reaktionsmustern auf die kriminelle Bedrohungen, welche je nach Sachlage angepasst und verändert werden können und sollen. Das vorliegende Buch schärft insofern den Blick für eine sorgsame Analyse der beschriebenen Funktionalbereiche hinsichtlich ihrer kriminellen Exposition und bietet gleichermaßen mögliche Schutzmaßnahmen als Reaktion oder antizipativen Schutz an, welche an die jeweilige reale Situation situativ anzupassen sind.

3 Neuausrichtung der Unternehmensidentität zur optimalen Realisierung der Sicherheitsanliegen

3.1 Kernkomponenten erfolgreichen Kriminalitätsmanagements

Was unterscheidet nun erfolgreiche von nicht erfolgreichen Unternehmen in ihrem Kampf gegen kriminelle Handlungen im Bereich der internationalen Industriespionage und Produktpiraterie? Und wie können sich Unternehmen zu einem erfolgreichen Management dieser kriminellen Herausforderungen hin entwickeln?

Die Beantwortung dieser Frage nimmt Bezug auf Teilergebnisse einer europaweiten Studie zu Produktpiraterie und Industriespionage, welche in den Jahren 2007 bis 2009 unter Leitung des Herausgebers und unter freundlicher Finanzierung seitens der STAEDTLER-Stiftung stattfand.[26] In dieser Studie wurden zahlreiche Unternehmen zu ihren Mechanismen und Maßnahmen für die Abwehr von Produktpiraterie und Industriespionage befragt und die Ergebnisse empirisch ausgewertet. Ein wichtiges Ergebnis der empirischen Befragungen war der Umgang der Unternehmen mit dem Phänomen der Komplexität. Erfolgreiche Unternehmen wiesen Mechanismen auf, mit komplexen Themen wie Produktpiraterie und Industriespionage erfolgreicher umzugehen als andere Unternehmen. Diese Mechanismen können als „Adaption“ bezeichnet werden.

„Adaption“ bezeichnet hierbei die Fähigkeit des Managements und der operativ ausführenden Bereiche der Unternehmen, sich in ihrem Verhalten an externe Herausforderungen anzupassen, Lösungen für diese Herausforderungen zu entwickeln sowie diese schnell und in hoher Güte umzusetzen. Es ist evident, dass Unternehmen, welche adaptive Mechanismen besser beherrschen als andere Unternehmen, auch Komplexität besser beherrschen werden als ebendiese Konkurrenten.

Da Produktpiraterie und Industriespionage hoch komplexe Phänomene sind, haben adaptive Unternehmen gerade hier einen Vorteil: sie sind besser als ihre Konkurrenten in der Lage, die Bedrohungssituation richtig zu analysieren, sie entwickeln schneller als ihre Konkurrenz passende Abwehrkonzepte mit höherer Wirksamkeit und setzen diese Konzepte auch schneller um. Hierdurch verschaffen sie sich Wettbewerbsvorteile, welche sich in hart umkämpften Massenmärkten in höheren Margen gegenüber der Konkurrenz mittelfristig manifestieren.

[26] Vgl. Fussan (2010, in Erstellung).

Erfolgreiches Handeln gegen internationale Produktpiraterie und Industriespionage basiert letztlich auf internen Mechanismen der Adaption und des exzellenten Beherrschens aller Möglichkeiten von Schutzmaßnahmen. Die Beherrschung des „Werkzeugkastens" antizipativer und reaktiver Abwehrhandlungen ist Basisvoraussetzung für einen wirksamen Kampf gegen kriminelle Strukturen. Die Adaptionsfähigkeit des Unternehmens bestimmt jedoch den Erfolg der Maßnahmen insgesamt.

Management by Adaption
Komplexitätsbeherrschung
Exzellenz der Maßnahmenauswahl und Zukunftsentscheidungen
Geschwindigkeit des Entscheidungsprozesses
Qualität der Maßnahmenumsetzung
Geschwindigkeit der Maßnahmenumsetzung

Abbildung 2: Kernelemente Adaptionsmanagement
Quelle: eigene Darstellung.

Wenn nicht die richtige Einschätzung der kriminellen Bedrohung erfolgt, können auch nicht die wirksamsten Schutzmaßnahmen identifiziert werden. Wenn die Auswahl und die Konzeption der Schutzmaßnahmen nicht auf exzellentem Niveau erfolgen, werden diese Maßnahmen ihre maximale Wirksamkeit verfehlen. Wenn die Qualität der Umsetzung beschlossener Schutzmaßnahmen im Unternehmen mangelhaft durchgeführt wird, werden diese Maßnahmen ihren optimalen Effekt ebenso verfehlen. Wenn die Umsetzung der Maßnahmen zu langsam erfolgt, verschenken die Unternehmen wichtige Bekämpfungserfolge und frühe Aufdeckungseffekte. Sollte zudem bei allen diesen Aspekten adaptiven Kriminalitätsmanagements im Unternehmen die Konkurrenz schneller oder besser sein, so hat das betroffene Unternehmen konkrete Wettbewerbsnachteile.

„Management by Adaption" ist eine wichtige Grundlage erfolgreichen Kampfes gegen kriminelle Strukturen und in Kombination mit der profunden Kenntnis von Chancen und Möglichkeiten wirksamer Schutzmaßnahmen ursächlich für erfolgreiches Bekämpfen von Produktpiraterie und Industriespionage. Natürlich können Unternehmen sowohl Adaptionsmanagement als auch die Möglichkeiten des „Werkzeugkastens" gegen kriminelle Handlungen lernen und entwickeln. Das vorliegende Buch bietet in verschiedenen Beiträgen insbesondere die analytische Basis für erfolgreiche Krimina-

litätsbekämpfung, indem es die wichtigsten von krimineller Energie gefährdeten Funktionsbereiche analysiert und grundlegende Maßnahmen zur Vorbeugung und Bekämpfung nennt. Wichtige Aspekte von Adaptionsmanagement leiten diese Beschreibung des kriminalitätsanalytischen „Werkzeugkastens“ in den nachfolgenden Absätzen ein.

3.2 Adaptionsförderliche Strukturen zur Kriminalitätsbekämpfung

3.2.1 Management

Adaptionsmanagement ist kohärentes Einleiten von Maßnahmen auf allen hierarchischen Ebenen des Unternehmens. Die richtige Konzeption und Delegation von einem Set an sinnvollen Schutzmaßnahmen durch das Management reicht nicht aus für eine hohe Wirksamkeit der Maßnahmen. Insofern ist gerade bei kriminalitätsinduzierten Problemlagen die aktive und kluge Kooperation möglichst vieler Mitarbeiter im Unternehmen erforderlich. Eine aktive und konstruktive Beteiligung möglichst vieler Mitarbeiter im Unternehmen kann auch als „ganzheitliches Sicherheitssystem“ bezeichnet werden.

Beim Aufbau eines solchen ganzheitlichen Sicherheitssystems kann etwa die bewusste Integration des Personals in den Entscheidungsfindungsprozess des Managements einen positiven Effekt auf den Einsatzwillen der einzelnen Mitarbeiter haben. Da Fertigungsmitarbeiter im Allgemeinen über weit mehr produktionsspezifisches Know-how verfügen als administrative Angestellte, ist ihr Rat bei der Planung von technischen Sicherheitsmaßnahmen wichtig. Gleichzeitig begünstigt der Einbezug von Beschäftigten die Identifizierung mit dem Unternehmen und fördert die Detektion kriminellen Verhaltens in den Reihen der Mitarbeiter selbst.

Die Bekräftigung eines aktiven Miteinanders trägt indes zu einer offeneren Unternehmenskommunikation und einer Verkürzung der Kommunikationswege bei; auftretende Sicherheitsprobleme und Ungereimtheiten werden somit schneller aufgedeckt und an die zuständigen Stellen weitergegeben, sodass Abwehrmaßnahmen zeitnah und flexibel ergriffen werden können.

Die hinreichende Bereitstellung von finanziellen, personellen und zeitlichen Ressourcen ist Grundvoraussetzung für die effiziente Realisation der Sicherheitsanliegen. Unter personalpolitischen Gesichtspunkten beginnt die Verantwortlichkeit des Managements bei der sicherheitsorientierten Durchführung des Personalauswahlverfahrens, erstreckt sich über die schriftliche Fixierung individueller Sicherheitsanforderungen, die

kontinuierliche Beobachtung und Betreuung der Mitarbeiter in allen Sicherheitsfragen, und endet erst mit der risikoreduzierenden Umsetzung von Personalfreisetzungen in Verdachtsfällen. Die Einführung eines Anreizsystems, mit dem sicherheitsbewusstes Verhalten belohnt und risikovolles Handeln bestraft wird, sollte ebenso Bestandteil der personellen Sicherheitsvorkehrungen sein.

Das Handeln gegenüber anderen Marktteilnehmern und Kunden sollte widerspruchsfrei zu diesen firmeninternen Verhaltensweisen sein. Im Kontext der Unternehmenssicherheit fallen hierunter speziell die bereits angesprochenen Aktivitäten in den Bereichen Distribution und Kundenservice. Unternehmen, die ein besonderes Interesse an der Sicherheit ihrer Kunden propagieren, müssen diesen auch die Möglichkeiten geben, erworbene Produkte im Verdachtsfall auf ihrer Echtheit hin überprüfen zu lassen, sodass zum Beispiel gesundheitliche Gefahren, die von minderwertigen Plagiaten ausgehen, beseitigt werden können. Darüber hinaus verliert ein Unternehmen an Glaubwürdigkeit, wenn es intern alles zur Sicherung der eigenen Produkte und Dienstleistungen tut, seine Intention einer effizienten Piraterie- und Spionagebekämpfung aber nicht in Zusammenarbeit mit anderen Marktteilnehmern einhält. Besonders Produktionsbetriebe, die selbst als Zulieferer von Unternehmen am Markt agieren, sind dazu angehalten, sich an den Schutzbemühungen ihrer Abnehmer zu beteiligen. Dies hat den Vorteil, dass durch die Verknüpfung beider Sicherheitssysteme Synergien erzeugt werden können. Insgesamt gelingt es so, auch externe Partner des Unternehmens in die adaptiven Handlungsstrukturen gegen Produktpiraterie einzubinden.

3.2.2 Unternehmenskommunikation

Eine Änderung der Strukturen im Unternehmen zu mehr adaptivem Potential ist mit einer Steigerung der kollektiven Einsatzbereitschaft aller Mitarbeiter verbunden. Widerstände, Demotivation und mangelnde Einsatzfreude bzw. „Dienst nach Vorschrift" sind der Geschwindigkeit der Maßnahmenumsetzung gegen kriminelle Aktivitäten direkt abträglich. Positive Kooperation der Mitarbeiter beschleunigt hingegen unternehmerische Reaktions- und Anpassungsprozesse. Voraussetzung für eine Adaptionssteigerung mit kriminalitätsvermeidendem Fokus sind entsprechende Kommunikationsstrukturen im Unternehmen. Wenn Mitarbeiter nicht wissen, worauf sie achten sollen und an wen sie sich ggf. wenden können, entfalten Schutzmaßnahmen gegen Produktpiraterie und Industriespionage nicht ihre volle Wirkung.

Der internen Kommunikation kommt hierbei eine entscheidende Rolle zu. Im Innenverhältnis spielt hierbei die zweckmäßige Konfiguration der Kommunikationskultur eine übergeordnete Rolle. Grundsätzlich sollte für eine erfolgreiche Kriminalitätsbekämpfung ein gutes Betriebsklima im Interesse der Unternehmensleitung liegen, da nur ein offener Umgang untereinander einen optimalen Informationsaustausch zwischen den Mitarbeitern und Abteilungen gewährleisten kann. Dieser ermöglicht – wie bereits unter *3.2.1 Management* angedeutet – eine zügige Identifikation und Beseitigung von Schwachstellen in der Gefahrenabwehr. Mitarbeiter müssen die Gelegenheit haben, bei auftretenden Problemen aktiv zu werden und sich unter Umständen auch dezentral an eine Bezugsperson oder einen Sicherheitsbeauftragten zu wenden. Zur Steigerung der Motivation empfiehlt es sich, neben personalpolitischen Maßnahmen wie monetären Belohnungen auch kontinuierlich über Gefahren und Maßnahmen im Kampf gegen kriminelle Handlungen zu informieren. Dies kann bspw. über das Intranet oder über Artikel in Werkszeitschriften regelmäßig und sehr effizient erfolgen.

Der unternehmensexternen Kommunikation kommt in beiden Richtungen der Wertschöpfungskette eine wichtige Bedeutung bei der Abwehr krimineller Handlungen zu. Sowohl die Zulieferer als auch die Kunden müssen regelmäßig über Bedeutung und Möglichkeiten der Gefahrenabwehr unterrichtet werden. Im Falle privater Endkunden bietet es sich sogar an, in umfangreichen Werbekampagnen nicht nur auf die Vorzüge der Originalware, sondern auch auf die Risiken illegaler Plagiate direkt hinzuweisen. Indem Kunden und Partner auf der gesamten Distributionskette für Abwehrmethoden gegen Produktpiraterie und Industriespionage sensibilisiert werden, vermindern sich die Gefahren eines unbewussten Erwerbs von Plagiaten bzw. einer unwissentlichen Weitergabe von firmeninternem Know-how. Zusätzlich können Händler und Absatzmittler in die Lage versetzt werden, Kunden über verkaufsfördernde Maßnahmen hinaus beratend zur Seite zu stehen und Aufklärungsarbeit zu leisten. Eine erhöhte Distributionsnähe schafft prinzipiell ein besseres Verständnis und eine erhöhte Akzeptanz für die Notwendigkeit einer effizienten Piraterie- und Spionageabwehr mit höheren Reaktionsgeschwindigkeiten bei unbekannten Gefährdungslagen.

Mit einem kommunikationsfokussierten Maßnahmenpaket kann es so gelingen, die kriminalitätsbezogene Adaptionsfähigkeit von Unternehmen deutlich zu erhöhen. Der Effekt kommunikativer Maßnahmen wirkt mittelfristig, ist jedoch relativ günstig, da keine teuren Investitionen und nur vergleichsweise geringe laufende Kosten zu berücksichtigen sind.

3.2.3 Unternehmenskultur

Unternehmenskultur ist ein zentraler Baustein adaptionsfokussierter Unternehmensentwicklung. Unternehmenskultur als soziologischer Mechanismus der kollektiven Verhaltensnormierung kann als Unterstützung von kriminalitätsvermeidenden Strategien des Unternehmens sehr sinnvoll eingesetzt werden. Dieser Gedanke geht davon aus, dass die Kultur des internen Miteinanders der Unternehmensmitglieder in gewissen Grenzen aktiv steuerbar und beeinflussbar ist. Eine Kultur der Innovation, des gegenseitigen Ringens um die besten Ideen, der Vorsicht gegen illegale Ideendiffusion, der Geheimhaltung von Kernkompetenz-Know-how und der sozialen Kontrolle der Mitarbeiter untereinander zur Identifizierung von kriminellen Handlungen ist ein sehr effizientes Mittel gegen Produktpiraterie. Ohne eine solche Kultur würden auch viele Schutzmaßnahmen in ihrer Wirkung nur geringe Effekte zeigen. Der kollektive soziologische Wille der Unternehmensmitglieder zum Schutz ihrer Leistungen und Ideen ist eine ideale Grundlage für rasche Gefahrenabwehr und für eine schnelle und widerstandslose Einführung neuer Maßnahmen gegen Produktpiraterie und Industriespionage. Genau diese Geschwindigkeit und Konstruktivität der betroffenen Mitarbeiter führt zu höherer, kriminalitätsbezogener Adaptionsfähigkeit des Unternehmens.

Da die kulturellen Aspekte der Unternehmensidentität mehr oder weniger fest in den Köpfen der Organisationsmitglieder verankert sind, liegt es im Verantwortungsbereich der Unternehmensleitung, den Beschäftigten die Dringlichkeit eines aktiven Sicherheitsmanagements verständlich zu machen. Eine Beeinflussung der Unternehmenskultur gelingt nur durch Überzeugung der Mitarbeiter. Für eine dauerhafte Anpassung an die veränderten Marktbedingungen müssen sowohl Mitarbeiter als auch Führungskräfte begreifen, wie wichtig die Sicherung der eigenen Wettbewerbsvorteile für den nachhaltigen Unternehmenserfolg ist; nur durch den Erhalt seiner Einzigartigkeit kann ein Unternehmen gegen Wettbewerber am Markt bestehen. Je stärker die Mitarbeiter an diesen Grundsatz glauben, umso stärker ist die Unternehmenskultur und wahrscheinlicher deren Gelingen.

Die bloße Bekanntgabe eines neuen Unternehmenskurses mittels Schulungen und Führungsanweisungen allein führt noch zu keiner nachhaltigen Veränderung der Kultur. Nur wenn geplanten Neuerungen auch konkrete Handlungen in Form von technischen, juristischen sowie betriebswirtschaftlichen Maßnahmen folgen, kann sich das Unternehmen insgesamt entwickeln. Wiederum sind personalpolitische Maßnahmen der Motivation, der Belohnung der Mitarbeiter durch Bonuszahlungen oder durch andere

monetäre Anreize sinnvoll. Verhaltensvorschriften wie regelmäßige Sicherheitskonsultationen zwischen der Geschäftsführung und den OPE-Leitern manifestieren einen strategischen Kulturwechsel.

4 Eigenverantwortung der Unternehmen als wichtigste Komponente im Kampf gegen Produktpiraterie und Industriespionage

Unabhängig von der Art der Herangehensweise – sei es eine SWOT-Analyse der Ablauforganisation oder die Beurteilung von Chancen beim Aufbau der Corporate Identity – zeigen der vorangegangene, aber auch die kommenden Beiträge, dass es in den Händen der Unternehmen selbst liegt, in wieweit sie für die Gefahren der Produktpiraterie und Industriespionage angreifbar sind. Viele Unternehmen schützen sich auch heute noch unzureichend, da sie den Aufwand ihrer Bemühungen im Verhältnis zur den erwarteten Effekten als zu hoch erachten; sie sind sich oft nicht über das Ausmaß der Verluste bewusst, welche aus den Aktivitäten der Produktpiraten und Industriespione resultieren.

Besonders kleine und mittelständische Unternehmen müssen erkennen, dass die illegale Übertragung und Verwendung von Know-how nicht länger ausschließlich das Problem vom Großunternehmen ist; jeder Marktteilnehmer, der durch innovative Ideen Gewinne generiert, bildet ein potenzielles Ziel für Kriminelle. Auch die Einsicht, dass eine Lösung der Thematik weder einfach ist, noch dass es einen universellen Schutz gibt, sind Teil eines langen Lernprozesses. Durch die spezifischen Strukturen jeder unternehmerischen Wertschöpfungskette und den Besonderheiten der jeweiligen Marktumgebung kann – speziell in Zeiten der Globalisierung – keine einheitliche Antwort auf die Problematik der Kriminalitätsbekämpfung generiert werden. Jede Bedrohungslage ist speziell und mit anderen nur bedingt vergleichbar. Das Engagement und die gesetzlichen Handlungsoptionen staatlicher Organe für die Kriminalitätsbekämpfung sind wichtig, dienen aber letztlich nur als Basis eines effizienten Schutzkonzeptes. Einzig die Unternehmen selbst können ihre Stärken und Schwächen identifizieren und sind in der Lage, effiziente Abwehrmaßnahmen zu erdenken und umzusetzen. Keine juristische Maßnahme kann präventive betriebswirtschaftliche Maßnahmen in ihrer Wirksamkeit übertreffen. Eigenverantwortung und ein präventives Han-

deln von Unternehmen sind die wichtigsten Komponenten im Kampf gegen die Gefahren von Produktpiraterie und Industriespionage.

Die Möglichkeiten eines wirksamen Schutzes sind vielfältig und auch in wirtschaftlich schwierigeren Zeiten durchführbar; Know-how-Schutz und die Sicherung der eigenen Wettbewerbsvorteile sind im Ringen um Marktanteile wichtiger denn je. Es obliegt den Unternehmen, sich eine gute oder schlechte Ausgangsposition bei der Abwehr gegen illegale Tätigkeiten zu schaffen.

Literaturverzeichnis

Crijns, R./Thalheim, J. (Hrsg., 2006): Kooperation und Effizienz in der Unternehmenskommunikation. Inner- und außerbetriebliche Kommunikationsaspekte von Corporate Identity und Interkulturalität. 1. Auflage, Deutscher Universitäts-Verlag, Wiesbaden 2006.

Fuchs, H. J. (Hrsg., 2006): Piraten, Fälscher und Kopierer. Strategien und Instrumente zum Schutz gestiegen Eigentums in der Volksrepublik China. 1. Auflage, Gabler Verlag, Wiesbaden 2006.

Fussan, C. (2010, in Erstellung): Unternehmerisches Handeln, Wirtschaftskriminalität und Terrorismus. Erfolgsstrategien am Beispiel von Produktpiraterie und organisierter Kriminalität. 1. Auflage, Gabler Verlag, Wiesbaden 2010.

Herbst, D. (2003): Corporate Identity. Aufbau einer einzigartigen Unternehmensidentität. Leitbild und Unternehmenskultur. Image messen, gestalten und überprüfen. 2., völlig überarbeitete und erweiterte Auflage, Cornelsen Verlag, Berlin 2003.

OECD (Hrsg., 2008): Die wirtschaftlichen Folgen von Produkt- und Markenpiraterie. OECD Publications, Paris 2008.

Regenthal, G. (2009): Ganzheitliche Corporate Identity. Profilierung von Identität und Image. 2. Auflage, Gabler Verlag, Wiesbaden 2009.

Ulrich, P./Fluri, E. (1992): Management. Eine konzentrierte Einführung. 6. Auflage, UTB Haupt Verlag, Stuttgart 1992.

Christina Maren Witte

B Risikoeffizienz und Wirksamkeit betriebswirtschaftlicher Schutzmaßnahmen gegen Produktpiraterie

Inhaltsverzeichnis

1 Pirateriesschutz als Kampf gegen Windmühlen? 27

2 Produkt- und Markenpiraterie in China 28

2.1 Begriffserklärung und Einordung 28

2.2 Gründe für die Zunahme von Produkt- und Markenpiraterie 28

2.3 Ursachen der Produkt- und Markenpiraterie am Beispiel China 29

2.3.1 Wirtschaftliche Bedingungen 30

2.3.2 Politische Bedingungen 32

2.3.3 Rechtliche Bedingungen 34

2.3.4 Kulturelle Bedingungen 36

2.4 Ausgewählte Beispiele für Produktpiraterie 37

3 Strategien und Schutzmaßnahmen bei Produkt- und Markenpiraterie 39

3.1 Ziele und Anforderungen im Kampf gegen Produkt- und Markenpiraterie 40

3.2 Grundstrategien im Kampf gegen Produkt- und Markenpiraterie 41

3.3 Betriebswirtschaftliche Schutzmaßnahmen 43

3.3.1 Angriffspunkte und Schutzmaßnahmen bei Lieferanten 44

3.3.2 Angriffspunkte und Schutzmaßnahmen in der Beschaffung 46

3.3.3 Angriffspunkte und Schutzmaßnahmen beim Personal 47

3.3.4 Angriffspunkte und Schutzmaßnahmen in der F&E 52

3.3.5 Angriffspunkte und Schutzmaßnahmen in der Fertigung 53

3.3.6 Angriffspunkte und Schutzmaßnahmen im Aufbau der Infrastruktur 55

3.3.7 Angriffspunkte und Schutzmaßnahmen im Vertrieb 56

3.3.8 Angriffspunkte und Schutzmaßnahmen in der Distributionslogistik 60

3.3.9 Angriffspunkte und Schutzmaßnahmen durch Öffentlichkeitsarbeit und Marketing 61

3.3.10 Schutzmaßnahmen außerhalb der Lieferkette 63

3.4 Juristische Aspekte ... 64
3.4.1 Schutzrechte in China ... 64
3.4.2 Durchsetzung der Schutzrechte ... 67
3.5 Technische Schutzmaßnahmen ... 72
3.5.1 Sichtbare Technologien ... 72
3.5.2 Unsichtbare Technologien ... 74
3.5.3 Maschinengestützte Technologien ... 75
3.5.4 Kombinationen von Technologien ... 77
4 Experteninterviews ... 77
4.1 Methodologie ... 77
4.1.1 Erhebungsmethode ... 77
4.1.2 Datenerhebung und Durchführung ... 78
4.1.3 Auswertungsmethode ... 80
4.2 Auswertung und Interpretation der Experteninterviews ... 81
4.2.1 Firmenerfahrungen mit Produkt- und Markenpiraterie ... 81
4.2.2 Ausmaß der Fälschungsrisiken und -schäden ... 83
4.2.3 Erfahrungen mit Schutzmaßnahmen ... 85
4.2.4 Wirksamkeit und Durchführbarkeit der Schutzmaßnahmen ... 87
4.2.5 Hemmnisse bei der Durchführbarkeit von Schutzmaßnahmen ... 92
4.2.6 Fazit der Umfrage ... 93
4.3 Umsetzbarkeit im Management ... 95
5 Umdenken im China-Geschäft als entscheidende Maxime ... 98
Literaturverzeichnis ... 99
Anhang ... 105

1 Piraterieschutz als Kampf gegen Windmühlen?

November 2004 in Shanghai: Chinesische Ingenieure brechen nachts heimlich in die Wartungsstation des Transrapid ein und vermessen die Technologie, die die Magnetschwebebahn antreibt. Überwachungskameras filmen die Eindringlinge. Was sich liest wie ein Auszug aus einem Drehbuch für einen Krimi, ist ein Beispiel für intellektuellen Diebstahl. So würde ein deutscher Unternehmer diesen Vorfall beurteilen. Mitnichten, nur ein Forschungsprojekt, so die dreiste Antwort der von den deutschen Lizenzinhabern zur Rede gestellten Chinesen.[1]

Solche Vorfälle sind aktuell keine Seltenheit. Schlagzeilen wie „Das Ende des chinesischen Traums“[2], „Ausufernde Produktpiraterie – ein Mittelständler befürchtet existenzbedrohende Entwicklung“[3] oder „Kampf gegen Windmühlen“[4] zeigen die Brisanz der Gefahr, die durch Produkt- und Markenpiraterie entsteht. 50.000 Arbeitsplätze allein in Deutschland gehen durch die Fälschungen verloren[5], der Anteil der gefälschten Waren am Welthandel beträgt bis zu 9%.[6] Unternehmen leiden unter Umsatzeinbußen, Imageschäden und außerordentlichen Kosten zur Produkthaftung und Rechtsverfolgung. Produkt- und Markenpiraterie ist längst nicht mehr nur ein zu vernachlässigendes Risiko im China-Geschäft. In der gegenwärtigen Literatur wird das Phänomen der Produkt- und Markenpiraterie als eine Sicherheitskrise der Zukunft bezeichnet.[7] Diese zu durchleuchten bzw. ganzheitliche Strategien und einzelne Schutzmaßnahmen aufzuzeigen, mit denen man sich vor möglichen Übergriffen schützen kann, und diese erarbeiteten Maßnahmen im Rahmen einer abschließenden praktischen Studie zu untersuchen, ist Ziel dieses Beitrags. Folglich soll der vorliegende Beitrag mit Bezug auf die gegenwärtige wissenschaftliche Literatur für Unternehmen ein übersichtliches, praxisorientiertes Kompendium darstellen.

---

1 Vgl. Steingart (2006), S. 222.
2 Maas (2005), S. 15.
3 Rath (2001), S. 2.
4 Engelken (2005), S. 47.
5 Vgl. Bundesministerium der Finanzen (2006a).
6 Vgl. Bundesministerium der Justiz (2006a).
7 Vgl. Trauboth (2002), S. 19.

2 Produkt- und Markenpiraterie in China

2.1 Begriffserklärung und Einordnung

Eine uniforme Terminologie, die das Phänomen der vielfältigen Formen der Nachahmung genau differenziert, existiert auf nationaler wie internationaler Ebene nicht. Markenpiraterie wird als das „illegale Verwenden von Zeichen, Namen, Logos und geschäftlichen Bezeichnungen, die von den Markenherstellern zur Kennzeichnung ihrer Produkte im Handel eingesetzt werden“[8], definiert. Produktpiraterie ist dagegen das illegale Nachahmen und Vervielfältigen von Waren, für die der Originalhersteller eingetragene Schutzrechte besitzt.[9] Diese liegen ursprünglich im urheberrechtlichen und geschmacksmusterrechtlichen Bereich. Das Geschmacksmuster ist eng mit dem Urheberrecht verknüpft und bietet so „Schutz für die schöpferische Leistung und konzentriert sich auf die äußere Form.“[10] Die Marken- sowie die Produktfälscher verwenden die Bekanntheit einer Marke bzw. das technische Wissen, die der rechtmäßige Hersteller durch hohen finanziellen Aufwand und die Entwicklung von Qualitätsprodukten über viele Jahre erlangt hat.

2.2 Gründe für die Zunahme von Produkt- und Markenpiraterie

„Nachahmung ist biologisch bedingt und sie gehört zur Triebstruktur des Menschen.“[11] Der Mensch ist so konditioniert, dass er immer Verhalten nachahmt, das für ihn von Vorteil ist.[12] Erfolgreiche Handlungsweisen zu kopieren bzw. erfolgreiche Produkte nachzumachen, hat in der Evolution Weiterentwicklung und Differenzierung garantiert.

In diesem Kontext erscheint das Phänomen der hier besprochenen Marken- und Produktpiraterie erklärbar. Doch warum taucht das Phänomen der Marken- und Produktpiraterie in den letzten Jahren vermehrt auf? Die Gründe für die Zunahme sind vielfältig, ein entscheidender ist sicherlich die Globalisierung. Der Warenverkehr wurde in solchen Ausmaßen intensiviert, dass sich der Absatzmarkt der Produktpiraten deutlich vergrößert hat. Vor allem die Möglichkeit weltweiter Kommunikation durch das Internet ermöglicht den Warenverkauf an fast jedem Ort der Welt. Der Bedeutungszuwachs

[8] Bundesministerium der Finanzen (2006b), S. 6.
[9] Vgl. Bundesministerium der Finanzen (2006b), S. 6.
[10] Niggl (2006), S. 7.
[11] Blumenthal (2002), S. 39.
[12] Vgl. Blumenthal (2002), S. 39.

von Marken spielt bei der Zunahme von Markenpiraterie sicher eine wesentliche Rolle. Markenbewusstsein und fehlende finanzielle Mittel einer bestimmten Käuferschicht einerseits und hoher wirtschaftlicher Profit andererseits lassen das Geschäft mit den Markenfälschungen boomen. Ein großes Manko ist die Territorialität der Schutzrechte, welche die Durchsetzung eines internationalen Schutzes der Produkte und Marken erheblich erschwert. Die Schutzrechte gelten meist nur bis zur Landesgrenze und eine Harmonisierung der Rechtsgebiete ist noch immer in weiter Ferne.[13] Im europäischen Wirtschaftsraum gibt es jedoch einige Ansätze wie z.B. das Gemeinschaftsgeschmacksmuster, das im Juni 2002 eingeführt wurde. Dieses in einem europäischen Land eingetragene Geschmacksmuster garantiert auch in den anderen EU-Staaten Schutz.[14]

2.3 Ursachen der Produkt- und Markenpiraterie am Beispiel China

Im praktischen Teil dieses Beitrags, der seinen Schwerpunkt auf Produkt- und Markenpiraterie legt, ist die Region China, aus der die meisten Plagiate stammen, besonders zu beleuchten. Dass China den größten Anteil an nachgeahmten Produkten hat,[15] wird durch die Tabelle des Bundesministeriums der Finanzen bestätigt. Auch der Präsident des VDMA (Verband deutscher Maschinen- und Anlagenbau), Brucklacher, betont: „Das schwarze Schaf ist unveränderlich China."[16]

Tabelle 1: Beschlagnahmefälle nach Herkunftsländern (in Prozent der Aufgriffe)
Quelle: Bundesministerium der Finanzen (2006a), S. 17.

	2003	2004	2005
VR China	12,9	23,6	***35,8***
Thailand	24,9	23,5	10,2
Sonstige asiatische Länder (Hongkong, Malaysia u.a.)	12,3	9,0	11,5
Tschechien	11,4	3,6	1,0
Polen	10,0	3,6	0,6
Türkei	9,0	10,2	8,7
USA	3.8	8,5	11,2
Sonstige Länder	15,7	18,1	21,0

[13] Vgl. Harte-Bavendamm (2001), S. 6ff.
[14] Handelskammer Hamburg (2006).
[15] Vgl. o.V. (2005d), S. 43.
[16] Schäfer (2005).

2.3.1 Wirtschaftliche Bedingungen

„China ist die frohe Botschaft für die atemlose Weltwirtschaft."[17] Mit einem jährlichen Handelsvolumen von mehr als einer Billion USD ist China heute eine der größten Volkswirtschaften der Welt. Ausländische Investitionen betrugen allein im Jahre 2004 mehr als 60 Milliarden USD. Das chinesische Bruttosozialprodukt hat sich in den letzten 20 Jahren verdreifacht.[18]

Auch die Arbeitssituation hat sich verändert. Im Jahr 2005 waren 6,3 Millionen Menschen mehr beschäftigt als im Vorjahr. Der Jahreslohn eines Arbeiters oder Angestellten beträgt weiterhin nur 18.364 Yen (umgerechnet 1.829 EUR), was jedoch einen Anstieg gegenüber dem Vorjahr von 14,6% bedeutet.[19] Auch die Exporte sind rasant angewachsen. Allein die Importe nach Deutschland aus China sind in den letzten 10 Jahren um 500% auf 400 Milliarden EUR angestiegen.[20]

China hat großen Nutzen aus der Globalisierung gezogen und einen phänomenalen Aufschwung erlebt. Chinas Exporte von Modeartikeln bis hin zu High-Tech-Geräten sind weltführend.[21] Die meisten Investitionen deutscher Firmen kommen aus der Automobil-, Elektro- und Chemieindustrie sowie dem Maschinenbau. Überwiegend globale deutsche Unternehmen investieren in China, obwohl inzwischen auch der Anteil der mittelständischen Unternehmen rapide zunimmt. Mit der Bewilligung von Direktinvestitionen aus dem Ausland und der Genehmigung von Kooperationen zwischen chinesischen und ausländischen Partnern verfolgt die chinesische Regierung das Ziel, durch Know-how-Transfer ihre Exportindustrie noch weiter auszubauen. Dies wird besonders dadurch evident, dass gerade diejenigen Projekte, die mit einem Transfer von Technologien zusammenhängen, besonders begrüßt und stark unterstützt werden.[22]

Den Zwiespalt, der sich bei einer China-Investition ergibt, beschreibt der Siemens Aufsichtsratschef Heinrich von Pierer mit den Worten: „Das Risiko, in China nicht dabei zu sein, ist größter als das Risiko, dabei zu sein."[23] Auch Bernd Pieschetsrieder, ehemaliger Vorstandsvorsitzender der Volkswagen AG, betont, dass eine Investitions-

[17] Sieren (2005), S. 11.
[18] Vgl. Sieren (2005), S. 11ff.
[19] Vgl. o.V. (2006o).
[20] Vgl. o.V. (2006b), S. 8.
[21] Vgl. Sieren (2005), S. 11ff.
[22] Vgl. Holtbrügge/Puck (2005), S. 13.
[23] Wagner (2005), S. 96.

entscheidung in China überhaupt nicht zu diskutieren ist: „In vielen Ländern kann man investieren, aber in China muss man dabei sein.“[24]

Trotzdem müssen die Vor- und Nachteile einer China-Investition abgewogen werden. Einerseits sollten sich deutsche Firmen am Wirtschaftsboom in China beteiligen. Andererseits laufen sie dabei Gefahr, dass sie gezwungen werden, Joint Ventures mit chinesischen Unternehmen eingehen zu müssen, was einen erheblichen Technologietransfer voraussetzt. Ausländischen Unternehmen wird generell vorgeschrieben, wenn sie sich an Ausschreibungen in China beteiligen wollen, 80% der Produktion in China vorzunehmen. Dabei reicht es nicht aus, dass Tochterunternehmen aus den Herkunftsländern in China produzieren, sondern man verlangt beispielsweise auch, dass Unternehmen direkt mit einheimischen Design-Unternehmen zusammenarbeiten müssen.[25] Auch die Stuttgarter Zeitung vom 22. Mai 2006 berichtet über diese Bedingung der chinesischen Regierung. Darin steht, dass Betriebsgeheimnisse sowie genaue Bau- und Konstruktionsskizzen der chinesischen Regierung vorgelegt werden müssen, um überhaupt Investitionsmöglichkeiten zu bekommen.[26] Die Verbindung des Technologietransfers mit der Entwicklung einer leistungsfähigen Forschung kann China schon bald zum Technologieführer werden lassen. Nach Angaben der Frankfurter Allgemeinen Zeitung hat sich der Transfer von Spitzentechnologien in den letzten 10 Jahren vervierfacht.[27] Dass folglich das Phänomen der Produkt- und Markenpiraterie verstärkt auftritt, ist die logische Konsequenz. Wie schnell die Chinesen den deutschen Markt angreifen, zeigt das Beispiel des Transrapid. Inzwischen hat die China Aviation Industry Corporation eine eigene Magnetschwebebahn, die CM 1 Dolphin, entwickelt, die im Juli 2006 in Shanghai getestet wurde. Eine weitere Magnetschwebebahn für geringere Geschwindigkeiten wird außerdem in Nordchina getestet. Deutsche Kritiker führen an, dass die Technologie des von Siemens und Thyssen Krupp entwickelten Transrapid unzureichend geschützt wurde.[28]

Die Öffnung einer neuen Branche für chinesische und ausländische Unternehmen läuft meist nach einem bestimmten Muster ab: Zuerst erfolgt eine rasche Durchdringung des Marktes, doch bald schon herrscht ein Angebotsüberhang vor. Bei dem harten Wettbewerb um Kunden und die Neustrukturierung der Branche müssen häufig als erste die

[24] Sieren (2005), S.21.
[25] Vgl. o.V. (2006b), S. 8.
[26] Vgl. o.V. (2006d), S. 9.
[27] Vgl. o.V. (2006b), S. 8.
[28] Vgl. Sucher (2006).

ausländischen Investoren den Platz räumen.[29] Diese sind nach entsprechender legaler oder illegaler Technologieübernahme auch nicht mehr notwendig. Fehlt die entsprechende ausländische Lobby, können „neue" Produkte schneller marktreif werden. Zudem arbeiten chinesische Firmen effektiver, da der Wunsch der Chinesen zu arbeiten stärker ist, sodass längere Arbeitszeiten in Kauf genommen werden.

2.3.2 Politische Bedingungen

Im Jahre 1978 verabschiedete sich die chinesische Regierung von der damals praktizierten zentralen Planwirtschaft und ging zur sozialistischen Marktwirtschaft über. Ungeachtet der wirtschaftlichen Liberalisierung werden Teile der Volkswirtschaft immer noch zentral regiert. Liberalisierung ist nur insoweit gestattet, wie sie die politischen Ziele nicht gefährdet. Ein Grund für die Machthäufung der chinesischen Regierung liegt in der „engen Vermischung von politischen und wirtschaftlichen Entscheidungsträgern."[30] So sind staatliche Mitarbeiter häufig zusätzlich bei Wirtschaftsunternehmen angestellt. Staatliche Angelegenheiten werden daher zunehmend zwischen den einzelnen Parteien verhandelt, anstatt nach Vorschriften entschieden.[31] Das kann dazu führen, dass Produktpiraten mit guten Kontakten zur Regierung gedeckt werden.

Die Zentralregierung mit ihrem Einparteiensystem sowie der bereits erwähnte große Einfluss der Wirtschaft auf staatliche Angelegenheiten böten im Grunde eine gute Voraussetzung für den Kampf gegen die Produkt- und Markenpiraterie. Dennoch geht der Staat immer noch zu wenig gegen kriminelle Übergriffe vor. Trotz der Bemühungen europäischer Politiker – wie kürzlich von Bundeskanzlerin Merkel auf ihrer China-Reise und Versprechungen von Chinas Ministerpräsident Wen Jiabao, sich mehr für den Schutz des geistigen Eigentums einzusetzen – zeigt die chinesische Regierung wenig Interesse am Kampf gegen Marken- und Produktpiraterie.[32]

Eine weitere politische Besonderheit in China sind die Abhängigkeiten innerhalb der regionalen und lokalen Regierungen. Nicht nur die großen wirtschaftlichen Unterschiede der einzelnen Provinzen Chinas sind dafür verantwortlich, sondern gerade deren geographische Nähe. Der Grund dafür liegt in der Vorstellungswelt der Chinesen, westliche Autoren bezeichnen diese als "Klientelisierung". Dieser Begriff wurde nach

[29] Vgl. Fischer (2005), S. 13.
[30] Holtbrügge/Puck (2005), S. 15
[31] Vgl. Holtbrügge/Puck (2005), S. 15.
[32] Vgl. o.V. (2006c), S. 15; Maass (2006), S. 13.

dem lateinischen Wort *cliens*, was so viel wie Schützling oder Abhängiger bedeutet, gebildet und zeigt in unserer Begriffswelt, dass die chinesische Gesellschaft auf einem Beziehungsgeflecht Abhängiger von einer staatlichen Autorität aufgebaut ist. Die persönliche Beziehung zu den staatlichen Organen, was geographische Nähe leichter ermöglicht, verschafft den Provinzregierungen großen Einfluss.[33] Das sieht man deutlich am Beispiel von Putian, einer Stadt in der Provinz Fujian. Dort werden Markenprodukte im großen Stil kopiert und direkt in den Export weitergegeben. Nach Angaben des Markenschutzbeauftragten für Adidas in Hongkong, Ryan Tai, hat sich „die Stadt bewusst auf Raubkopierer eingestellt."[34] Seit Jahren dürfen die Unternehmen seitens der Behörden dort keine Kontrollen durchführen.[35]

Einen anderen Einblick in die chinesische Gesellschaft verschafft der Begriff „Guanxi", d.h. Lehre des Beziehungsaufbaus, der eine Lebensform bezeichnet, die auf einem Beziehungsgeflecht zwischen einzelnen Personen aufbaut. Dieses persönliche Netzwerk ist im Gegensatz zu staatlicher Autorität unerlässlich. Kaum eine Entscheidung in China bleibt von der Auswirkung durch Guanxi unbeeinflusst. Deswegen herrschen in der chinesischen Regierung immer noch informelle Einflüsse und Entscheidungsverfahren vor. Oft ist es nicht ersichtlich, wer in bestimmten Angelegenheiten überhaupt befugt ist.[36] Der spezielle Einfluss der Provinzen ist ein Nährboden für Produkt- und Markenpiraterie. Häufig fördern Regierungen sogar das Kopieren von Produkten und Marken. Gigantische Einkaufszentren, in denen man nur Plagiate kaufen kann, schaffen Arbeitsplätze und bringen der lokalen Regierung zusätzliche Steuereinnahmen.[37] Chinesen sind im Allgemeinen weniger politisch interessiert als Europäer. Ihre Ein- oder Unterordnung in die Gesellschaft ist den Chinesen näher als die Durchsetzung individueller Rechte. „Hierarchie, Autorität und die Unterordnung der Rechte und Interessen des einzelnen"[38] sind weit oben im Wertesystem der Chinesen verwurzelt, genauso wie Konfliktvermeidung. Der Kampf gegen Marken- und Produktpiraterie würde aber gerade Konfliktpotential in sich tragen. Das Phänomen einer autoritären Regierung hat zur Folge, dass langwierige Diskussionen unnötig sind und deswegen die Regierung schnell handeln kann, da die Entscheidung nur die internen Politi-

[33] Vgl. Holtbrügge/Puck (2005), S. 16.
[34] Maass (2006), S. 13.
[35] Vgl. Maass (2006), S. 13.
[36] Vgl. Holtbrügge/Puck (2005), S. 16.
[37] Vgl. Hüttemann (2006), S. 20.
[38] Kuhn (2006), S. 5.

ker der KPCh (Kommunistische Partei Chinas) mittragen müssen.[39] Die Vormachtstellung des Staates zeigt aber, dass die Regierung die Möglichkeit hätte, die Produkt- und Markenpiraterie in ihrem Land noch stärker zu unterbinden. Dass China theoretisch gerade durch seine zentralen Strukturen die Voraussetzung hätte, gegen Technologieklau in seinen Provinzen vorzugehen, betont auch Hartmut Schauerter, Staatsekretär im Bundesministerium für Wirtschaft.[40] Da aber wirtschaftspolitische Entscheidungen der Zentralregierung auf lokalpolitischer Ebene nicht ankommen oder ignoriert werden, sei ein effektives Durchgreifen schwierig.[41]

Absichtserklärungen der Regierung gibt es immer wieder, wie z. B. die Verlautbarung der stellvertretenden chinesischen Ministerpräsidentin Wu Yin im Februar 2006. Sie kündigte an, 50 Beschwerdezentren zum Schutz geistigen Eigentums in verschiedenen chinesischen Städten zu eröffnen. Sie appellierte dabei an die Kräfte der Gesellschaft, die aktiviert werden müssten, um diese Verletzungen zu ahnden[42], übersah aber offensichtlich, in wessen Interesse dieser unfreiwillige Technologietransfer ist.

2.3.3 Rechtliche Bedingungen

Für den vorliegenden Beitrag ist nur die so genannte „Rechtskultur" Chinas von Bedeutung. Deswegen wird auf die Einzelheiten der Verfassung Chinas nicht eingegangen. Eine Rechtskultur ist in China sehr schwach ausgeprägt. Nicht nur ist die Justiz mit der Legislative und Exekutive verbunden, sondern es fehlt die Möglichkeit, gegen staatliche Organe vorzugehen, weil es keine Verwaltungsgerichtsbarkeit gibt. Wie schon zuvor erwähnt, sind zwischenmenschliche Beziehungen in China sehr wichtig. Zusammenhängend damit hat die „Gesichtswahrung" eine der höchsten Prioritäten in der chinesischen Kultur. Bei rechtsstaatlichem Vorgehen provoziert man jedoch einen Gesichtsverlust des Angeklagten, was der Wertschätzung der Guanxi zuwiderläuft. Dagegen betrachten chinesische Geschäftspartner es als Schwäche, wenn man Vertragsbrüche einfach ignoriert.[43] Unter den genannten Voraussetzungen ist eine gerichtliche Durchsetzung gegen Produkt- und Markenpiraterie noch problematischer. Deswegen werden Unstimmigkeiten oft außergerichtlich gelöst.

---

[39] Vgl. Kuhn (2006), S. 5.
[40] Vgl. Stratmann (2006), S. 2.
[41] Vgl. Holtbrügge/Puck (2005), S. 16.
[42] Vgl. o.V. (2006p).
[43] Vgl. Holtbrügge (2005), S. 18.

Die Volksrepublik China trat am 11. Dezember 2001 der World Trade Organization (WTO) bei. Dies sollte ein weiterer Schritt zur Liberalisierung des Außenhandels sein. China verpflichtete sich zur Öffnung weiterer Branchen und versprach gleichzeitig, geistiges Eigentum noch mehr zu schützen. Dieses Versprechen ist leider noch nicht vollständig in die Tat umgesetzt worden.[44] Auf dem Papier sind die rechtlichen Voraussetzungen gegeben. Die Schwierigkeit liegt vor allem in deren Durchsetzbarkeit.[45] Zwar wurden im Jahr 2005 5.336 Straftäter in China wegen Marken- und Produktpiraterie verurteilt, jedoch handelt es sich bei diesen meist nur um die Händler und nicht um die eigentlichen Auftraggeber. Der blinde Aktionismus, mit dem Dampfwalzen nachgemachte Produkte im chinesischen Fernsehen platt walzen, um ein öffentliches Zeichen zu setzen, kann nicht vom eigentlichen Vergehen ablenken.[46] Deswegen macht die deutsche Wirtschaft zusätzlichen Druck. „China braucht eine bessere Infrastruktur zur Durchsetzung seiner Gesetze."[47] Doch die Vorteile, die der illegale Technologietransfer garantiert, nämlich die „schnelle Möglichkeit, um mit den technisch fortgeschrittenen Konzernen aus dem Westen zu konkurrieren"[48], weil keine Kosten für Entwicklung und Forschung oder den Markteintritt entstehen, stoßen bei der chinesischen Regierung auf mehr Interesse.[49] Weil geistiges Eigentum in China nur unzureichend geschützt wird, verlagern Konzerne wie z.B. General Motors ihren F&E-Bereich eher nach Indien.[50] Auch Forrester Research bestätigt, dass bis zum Jahr 2015 etwa 3,3 Millionen amerikanische Arbeitsplätze, die Dienstleistung und Knowledge betreffen, ins Ausland verlagert werden, „davon 70% nach Indien."[51]

Es hat schon einige Verbesserungen bzw. Bemühungen seitens des obersten chinesischen Volksgerichts gegeben. So wurde beispielsweise am 22. Dezember 2004 eine „Ausführungsverordnung über die Anwendung des Strafrechts auf dem Gebiet des gewerblichen Rechtsschutzes" erlassen. Da Gesichtsverlust ein gefürchtetes Phänomen ist, kann bei wiederholten Straftaten davon ausgegangen werden, dass eben zur Vermeidung dieses Verlustes strafrechtlich gegen den Täter vorgegangen wird. Die strafrechtliche Verfolgung wird so erleichtert, die Regelungen bringen u.a. eine Verbesse-

[44] Vgl. Fischer (2005), S. 13.
[45] Vgl. Stratmann (2006), S. 2.
[46] Vgl. Maass (2006), S. 13.
[47] Hoffbauer (2006), S. 3.
[48] Maass (2006), S. 13.
[49] Vgl. Maass (2006), S. 13.
[50] Vgl. von Petersdorf (2006).
[51] Colteryahn/Davis (2006).

rung bei Verletzungen geistigen Eigentums, Fälschung von Patenten und im Fall von Beihilfe.[52] Auch zum Schutz gegen Marken- und Produktpiraterie auf Messen ist zum 1. März 2006 eine Richtlinie erlassen worden. Sie fordert, dass man für eine Messe, die länger als drei Tage dauert, ein Büro für die zuständigen Behörden einrichten muss, damit diese Piratenfällen sofort nachgehen und diese strafrechtlich verfolgen können. Aussteller, die wiederholt geistiges Eigentum anderer verletzen, bekommen ein Verbot für zukünftige Messeauftritte. Wie man sieht, wird einiges zum Kampf gegen die Marken- und Produktpiraterie unternommen, doch leider mangelt es noch immer an einer verlässlichen Umsetzung der Maßnahmen.[53]

2.3.4 Kulturelle Bedingungen

Kulturelle Bedingungen und Hintergründe spielen bei dieser Problematik eine große Rolle. Obwohl kulturelle Bedingungen schwer greifbar sind, sind ihre Einflüsse vor allem in China bedeutend und müssen erwähnt werden. Grundlage der chinesischen Kultur bilden philosophische Konzepte wie Konfuzianismus, Taoismus, Sun Tzu oder der Han Fei Tzu. Der Konfuzianismus ist noch immer stark in der chinesischen Kultur verankert. Er beruht auf der Basis von Pflicht, Loyalität, Ehrlichkeit und Respekt und drückt die „Verpflichtungen des Menschen gegenüber anderen in Abhängigkeit von den Beziehungen der Menschen untereinander“ aus.[54] Dieses daraus resultierende Klassendenken ist in China immer noch stark verwurzelt, ebenso wie die bereits beschriebene Bedeutung der mitmenschlichen Beziehungen, das Guanxi. Gerade in Bezug auf Produktpiraterie weist Holtbrügge/Puck auf Erfahrungen deutscher Unternehmern in China hin, bei denen chinesische Beschäftigte trotz deutlicher Anweisung der deutschen Vorgesetzten technologisches Wissen weitergegeben haben.[55] Diese Verfehlung aus unserer Sicht wird verständlich unter dem Einfluss der menschlichen Netzwerke wie Guanxi, welche dazu eingesetzt werden, die Weitergabe von Informationen zu unterstützen.

Ebenso wichtig für den Problembereich Produktpiraterie ist der Taoismus. Diese philosophische Denkweise beruht auf der Erkenntnis, dass es kein absolutes Wissen gibt, sondern es kommt darauf an, aus welcher Perspektive man Wissen betrachtet. „Das

[52] Vgl. Papageorgiou (2005), S. 82.
[53] Vgl. Häuslschmid (2006), S. 79.
[54] Holtbrügge/Puck (2005), S. 20.
[55] Vgl. Holtbrügge/Puck (2005), S. 24.

Kopieren hat in der chinesischen Kultur traditionelle Wurzeln."[56] Der Hintergrund liegt auch in der chinesischen Kunst, in der traditionellerweise zuerst der Meister perfekt nachgeahmt wird, bevor man eigene Ideen entwickelt.[57] „Das Kopieren ist daher ein wichtiger Schritt auf dem Weg zur Vervollkommnung der eigenen Kunst und der Entwicklung des persönlichen Stils."[58] Die Fälscher sehen sich nicht als Patentverletzer, sondern als „Chao-xi", was wörtlich übersetzt „nehmen" und „üben" bedeutet.[59] Bedingt durch den Taoismus ist auch die Harmoniebedürftigkeit der Chinesen. Die Menschen sind dazu angehalten, nach dem „natürlichen Lauf der Dinge"[60] zu leben und sich nicht aus der hierarchischen Ordnung zu lösen. Blinder Aktionismus wird abgelehnt; man versucht, nicht selbst Einfluss auf Geschehnisse zu nehmen. Singuläres Unrechtsbewusstsein bei geistigem Diebstahl ist in einer Gesellschaft, die nach Geert Hofstedes[61] Terminologie eher kollektivistisch geprägt ist, nicht üblich. In der chinesischen Gesellschaft mit hoher Machtdistanz des einzelnen ist Ungleichheit und hierarchische Abhängigkeit erwünscht. Eine kritische Durchdringung des eigenen Handelns ist in einer Gesellschaft, die nach Hofstede langfristig orientiert ist, d.h. Traditionen respektiert und ihr Gesicht wahrt, nicht zu erwarten.[62]

2.4 Ausgewählte Beispiele für Produktpiraterie

In den Anfängen der Produktpiraterie wurden konzentriert Luxusartikel und erst vereinzelt technische Produkte nachgeahmt.[63] Heutzutage bleibt keine Branche von illegalen Übergriffen verschont. Selbst alltägliche Konsumgüter wie Maggi-Saucen, Gilette-Rasierklingen und Evian-Mineralwasser werden im industriellen Stil gefälscht. Der VDMA berichtet, dass jedes zweite deutsche Maschinenbauunternehmen von Pirateriefällen in China betroffen sei.[64] Nicht nur Einzelteile, sondern ganze Großanlagen von beispielsweise 30 Metern werden komplett nachgebaut.[65] Zu den bisher betroffenen Produktbereichen wie Software, Bekleidung, Uhren und Parfüm kommen Produkte wie Fahrstühle, Autos und Flugzeugersatzteile, chemische Erzeugnisse und

[56] Scharrer (2001), S. 2.
[57] Vgl. Scharrer (2001), S. 2.
[58] Scharrer (2001), S. 2.
[59] Ramoser (2005), S. 26.
[60] Holtbrügge/Puck (2005), S. 21.
[61] Geert Hofstede: Niederländischer Experte für Kulturwissenschaften.
[62] Vgl. Holtbrügge/Puck (2005), S. 19ff.
[63] Vgl. Harte-Bavendamm (2005), S. 13.
[64] Vgl. o.V. (2005d), S. 42.
[65] Vgl. Maass (2006), S. 13.

Genussmittel. Die Palette der Produktpiraten geht sogar so weit, dass auf einem Markt in Handan in der Provinz Hebei ein gefälschtes Hühnerei entlarvt worden ist. Der Inhalt bestand aus Kalk und Gelatinefüllung. Die Fälschung war so gut, dass das Hühnerei sogar beim Kochen nicht von einem echten Hühnerei unterschieden werden konnte.[66]

Die Professionalität der Fälscher ist bis ins Unermessliche gestiegen. Sie verwenden die gleichen Materialien und kopieren Verpackung und Gebrauchsanweisung gleich mit.[67] So handeln die Fälscher mit Rolex-Uhren, die mit einem „fälschungssicheren" Hologramm versehen wurden, oder Levis-Jeans, die von der Qualität mit den echten vergleichbar sind.[68] Die Preispolitik der Fälscher wird immer ausgefeilter. So kosten die Fälschungen meist nur ein paar EUR weniger als das Originalprodukt, um dessen Echtheit vorzutäuschen.[69] Wienfried Krämer von der Zimmer AG berichtet, dass die Fälscher so gründlich vorgehen, dass sogar die Schweißnähte am Reaktor genau an derselben Stelle liegen wie beim Original.[70] Häufig wird die Fälschung weder vom Zoll noch vom Originalhersteller identifiziert. Entlarvt werden die Kopien dann erst bei anstehenden Reparaturen.[71]

Auch der Vertriebsweg nimmt immer neue Formen an. In Shanghai mieten Produktpiraten zunehmend Konferenzräume in Luxushotels, um dort ihre gefälschten Luxusartikel anzubieten. Touristen gehen davon aus, dass die gefälschten Rolex-Uhren echt sein müssen, wenn diese in solch einem Ambiente verkauft werden. Beim Versand, wo Label und Produkt getrennt voneinander verschickt werden, nehmen die Methoden schon fast die der Drogenschmuggler an.[72]

Produkt- und Markenpiraterie kann zunehmend mit organisierter Kriminalität in Verbindung gebracht werden. Man ist nicht mehr mit einzelnen Händlern konfrontiert, sondern mit organisierten, international verbreiteten Netzwerken mit modernsten Produktionsstätten. Moderne Techniken, wie Internet, Scanner und Digitalkameras, erleichtern den Fälschern ihre Arbeit enorm. Dabei wird diesen sogar vorgeworfen, mit ihren Gewinnen auch den internationalen Terrorismus mitzuorganisieren.[73]

---

66 Vgl. Schramm/Taube (2006).
67 Vgl. Maas (2006), S. 13.
68 Vgl. Eggert (2005), S. 41.
69 Vgl. Fuchs (2006), S. 39
70 Vgl. Wagner (2005), S. 96.
71 Vgl. o.V. (2005d), S. 42.
72 Vgl. Fuchs (2006), S. 38.
73 Vgl. Fuchs (2006), S. 40.

3 Strategien und Schutzmaßnahmen bei Produkt- und Markenpiraterie

"IPR[74] problems are simply a cost of doing business in China and little can be done."[75] Diese Einstellung teilen immer noch viele global agierende Unternehmen wegen der weiterhin entstehenden hohen Schäden durch Produkt- und Markenpiraterie. Sie reagieren aber erst dann, wenn ihre Produkte längst auf den Fälschermärkten zu finden sind. Diese Vorgehensweise ist nicht sinnvoll, da sie zu langwierig, ineffektiv und nicht effizient ist. Außerdem greifen die meisten Unternehmen bei der Auswahl der Schutzmaßnahmen immer noch ausschließlich auf juristische Mittel zurück. Diese fallen ebenfalls unter die Kategorie der reaktiven Schritte und „laufen der Entwicklung immer nur hinterher."[76] Erfolgreiche Unternehmen jedoch agieren statt nur zu reagieren. Sie schützen sich vor Übergriffen der Fälscher mit „strategisch untermauerte[n] intelligente[n] System[en] effektiver und effizienter Maßnahmen, die frühzeitig greifen und die sich auch auszahlen."[77] Marken- und Produktpiraterie auszulöschen wird schwer möglich sein. Es den Fälschern jedoch „so schwer wie möglich zu machen"[78] ist auch die Motivation von Martin Welker von der Firma Stiehl, die den Kampf gegen die Produktpiraten seit Jahren zunehmend erfolgreich aufnimmt. Das bedeutet, man kann das Kopieren eines Produktes oder einer Marke derart erschweren, dass ein Nachahmen für den Fälscher zu kostspielig, aufwendig und riskant wird, und er es von Anfang an unterlässt. Dazu muss ein umfassendes System aufgebaut werden, das es den Unternehmen gestattet, in allen Bereichen Widerstand zu leisten. Um solch ein System zu entwerfen, werden die betriebswirtschaftlichen, juristischen und technischen Bereiche untersucht. Erfolgreiche Unternehmen kombinieren heute zur Verfügung stehende Mittel so, dass sie sich ergänzen und ihre Wirkung dadurch intensiviert wird.[79] Auf Standardaktionen reagieren die Fälscher meist routiniert, wie z.B. nach Razzien, nach denen die Fälscher einfach ihr Versteck ändern. Auf komplexere Schutzmaßnahmen reagieren die Fälscher überrascht und resignieren schneller. Nicht die Reaktion der Fälscher ist von so großer Bedeutung wie die Nachhaltigkeit des

[74] Kurz für: Intellectual Property Rights.
[75] o.V. (2005c), S. 7.
[76] Fuchs (2006), S. 117.
[77] ebd.
[78] Lupp (2006).
[79] Fuchs (2006), S. 117.

Schutzes, die jedoch nur durch komplexe und wohl durchdachte Maßnahmensysteme erlangt werden kann.[80]

3.1 Ziele und Anforderungen im Kampf gegen Produkt- und Markenpiraterie

"Wenn du den Feind und dich selbst kennst, brauchst du den Ausgang von hundert Schlachten nicht zu fürchten. Wenn du dich selbst kennst, doch nicht den Feind, wirst du für jeden Sieg, den du erringst, eine Niederlage erleiden. Wenn du weder den Feind noch dich selbst kennst, wirst du in jeder Schlacht unterliegen."[81]

Diese Kampfstrategie von Sun Tsu verdeutlicht, wie existentiell notwendig ein ganzheitlich wirkendes Anti-Fälschungssystems wäre. Beim Kampf gegen Produkt- und Markenpiraterie „gewinnen […] westliche Unternehmen in China nur einzelne Schlachten, ohne den Krieg gegen die Fälscher zu gewinnen."[82] Ad-hoc-Reaktionen, beispielsweise Grenzbeschlagnahmungen, erlangen nie die Wirkung, die ganzheitliche Strategien mit einem zielorientierten Vorgehen haben. Wichtig ist, dass die Strategien zur Bekämpfung der Produkt- und Markenpiraterie nicht von den grundsätzlichen Zielen des Unternehmens abweichen. Eine solche Strategie sollte mittel- bis langfristig angelegt sein und ist von kurzfristig wirkenden Taktiken, wie oben beschrieben, zu unterscheiden. Strategien sind insofern auch effektiver, als sie pro-aktiv sind und somit den Fälschern von Anfang an den Wind aus den Segeln nehmen bzw. einen Wind erst gar nicht aufkommen lassen. Einzelne Maßnahmen müssen aufeinander abgestimmt sein, um deren Gesamtwirkung zu maximieren, und gleichzeitig flexibel genug, um sich an die Situation immer neu anzupassen. Laut Fuchs, Geschäftsführer von CHINABRAND Consulting, beeinflusst dieses Konzept u.a. entscheidend, ob ein Unternehmen in China „rentabel arbeitet und dort profitabel wachsen kann."[83] Effektiven Schutz bietet eine offensive Strategie gegenüber den Produktpiraten und „im Wirkungsbereich des Unternehmens ein integriertes System aus abgestimmten Schutzmaßnahmen."[84]

---

80 Fuchs (2006), S. 121.
81 Sunzi (2001), S. 35.
82 Fuchs (2006), S. 137.
83 Fuchs (2006), S. 141.
84 Ballhaus (2005), S. 40.

3.2 Grundstrategien im Kampf gegen Produkt- und Markenpiraterie

Gemäß Fuchs[85] sollte ein Unternehmen, bevor es sich mit den möglichen Schutzmaßnahmen aus den verschiedenen Bereichen beschäftigt, seine Grundstrategie festlegen, auf der die weiteren Maßnahmen aufbauen. Grundstrategien sind grundsätzliche Überlegungen eines Unternehmen, die festlegen, welche präventiven Maßnahmen getroffen werden müssen. Nur so kann im Fall eines Angriffs durch Produktpiraten schnellstmöglich gehandelt werden.

Als einfachste Strategie kann die *Do-nothing-Laisser-faire*-Strategie als eine Option betrachtet werden. Hierbei ignoriert man die Fälscher. Diese ist jedoch nur effektiv, wenn durch eine Kosten-Nutzen-Analyse bestätigt wird, dass der Umsatzverlust den potentiellen Aufwand für den Kampf gegen die Produktpiraten nicht überwiegt.

Um sich erst gar nicht mit der Bekämpfung der Produkt- und Markenpiraterie beschäftigen zu müssen, ist der *Verzicht auf Markteintritt* eine einfache Strategie. Leicht kopierbare Produkte und Technologien werden erst gar nicht in den chinesischen Markt eingeführt. Das Unternehmen, das diesen Weg einschlägt, nimmt dadurch allerdings entgangene Umsätze in Kauf.

Die *Duldungsstrategie* kommt für solche Unternehmen in Frage, die nicht über die Möglichkeit und finanziellen Mitteln verfügen, Schutzmaßnahmen zu treffen. Die Kernprodukte werden mit allen Mitteln verteidigt; bei anderen Produkten lässt man die Fälscher gewähren und akzeptiert damit bewusst Umsatzverluste.

Die *Kompensationsstrategie* ist eine Erweiterung der vorherigen Strategie. Das Unternehmen duldet die Fälscher, kompensiert jedoch die dadurch entgangenen Umsätze durch Verteuerung anderer Produkte bzw. kalkuliert den Verlust in den Verkaufspreis der restlichen Produkte ein.

Prinzipiell wäre auch möglich, dass sich ein Unternehmen für die *Kooperations- und Integrationsstrategie* entscheidet und mit den Produktpiraten zusammenarbeitet bzw. sie in ihre Produktion einbindet. Möglichkeiten wären dabei, dem Fälscher günstige Lizenzen anzubieten oder mit ihm zusammen sogar ein Joint Venture einzugehen, um ihn zu kontrollieren.

Unternehmen könnten auch von der Nachfrageseite an das Problem herangehen, indem sie *Einfluss auf Verbraucher und Politik* ausüben. Durch Aufklärungsarbeit könnte

[85] Fuchs (2006), S. 160ff.

man den Konsumentenmarkt für Fälschungen verkleinern. Kopieren ist nicht mehr attraktiv, wenn es keine Konsumenten für die Fälschungen gibt. Eine andere Möglichkeit wäre es, noch mehr Druck auf die chinesische Regierung auszuüben, sodass sie sich mehr für die Unterbindung von Fälschungen einsetzt.

Die meisten Unternehmen verfolgen eine *rechtliche Verteidigungsstrategie*, jedoch ist sie nicht immer effektiv und hält Produktpiraten auch nicht davon ab, trotzdem weiter zu kopieren. Rechtliche Schutzmaßnahmen wie Patente und Gebrauchsgeschmacksmuster werden im nächsten Abschnitt genauer erläutert.

Eine Option für ein Unternehmen wäre auch, erst dann zu handeln, wenn der Schaden schon eingetreten ist, d.h. auf eine *reaktive juristische Strategie* zurückzugreifen. Ein Beispiel sind Grenzbeschlagmaßnahmen, bei denen der Zoll die gefälschte Ware an der Landesgrenze abfängt oder die Polizei durch Hinweise die Produktionsstätten der Fälscher ausfindig macht und die Plagiate beschlagnahmt. Dieses Ad-hoc-Verfahren ist ineffektiv, da es nur die beschlagnahmten Waren betrifft, nicht aber das Problem an der Wurzel packt.

Eine der effektivsten Strategien, die *Innovationsstrategie***,** verkürzt den Produktlebenszyklus, indem ständig Innovationen erdacht werden. So ist man den Fälschern immer einen Schritt voraus. Eine direkte Auseinandersetzung mit den Produktpiraten entfällt. Alle finanziellen Mittel können eher in die Forschung und Entwicklung investieren werden anstatt in die Bekämpfung der Fälscher.

Eine sicher außergewöhnliche Strategie schlägt vor, ein „*Quasi-Plagiat*“ herzustellen, das man kostengünstiger als bewusste Alternative zum Originalprodukt herstellt. Damit schöpft man den Markt vollständig aus. Die Gefahr, dass das günstigere Produkt das Original verdrängt, muss mit einer genauen Abgrenzung der beiden Produkte abgefangen werden.

Durch Schaffung eines *starken Markensystems* kann man ebenso sein Produkt schützen. Dem Käufer werden Zusatzleistungen, wie man sie bei Produktpiraten nicht findet, angeboten, wie z.B. Garantieleistungen, Serviceverträge, Bringservice, Komplementärprodukte, Reparaturleistungen oder Beratungen. Diese Paketlösungen sind für den Konsumenten der effektivste Anreiz, eher das teurere Originalprodukt zu kaufen, als auf das billige Plagiat zurückzugreifen. Eine potentielle Käuferschicht, auf die sich viele Unternehmen noch einstellen müssen, ist die wachsende Mittelschicht in China,

die zunehmend großen Wert auf Markenprodukte legt. Durch Markenkäufe versucht sie, ihren Status zu definieren.

Zunehmend entscheiden sich immer mehr Unternehmen, präventive Maßnahmen einzuleiten, um nicht erst auf Fälschungen reagieren zu müssen, sondern sich pro-aktiv den Produktpiraten entgegenzustellen. Eine *umfassende Angriffsstrategie* ist wohl die effektivste Vorgehensweise für die Bekämpfung der Produkt- und Markenpiraterie. Wenn sich ein Unternehmen für diese Variante entscheidet, hat es die Möglichkeit, aus einem großen Portfolio von Schutzmaßnahmen zu wählen. Durch die Bündelung von Maßnahmen wirkt diese Strategie am langfristigsten und schreckt durch ihre Komplexität die Produktpiraten am ehesten vom Kopieren ab. Die Kombination der Strategien schafft ein ganzheitliches Schutzsystem. Diese umfassendste Strategie ist jedoch trotz großer Effektivität mit viel finanziellem wie auch personellem und zeitlichem Aufwand verbunden. Die einzelnen Schutzmaßnahmen und ihre Kombinationsmöglichkeiten werden im Folgenden genauer erklärt.

3.3 Betriebswirtschaftliche Schutzmaßnahmen

Produkt- und Markenpiraterie kann an allen Stellen der Wertschöpfungskette angreifen. Vom Rohstoff des Lieferanten bis zum Endverbraucher können Schwachstellen auftreten. Mit der Wertschöpfungskette als Grundlage werden im Folgenden die Angriffspunkte an den einzelnen Wertstufen erklärt und die jeweiligen präventiven Maßnahmen erläutert, welche das Risiko eines Übergriffes durch Fälscher mindern.

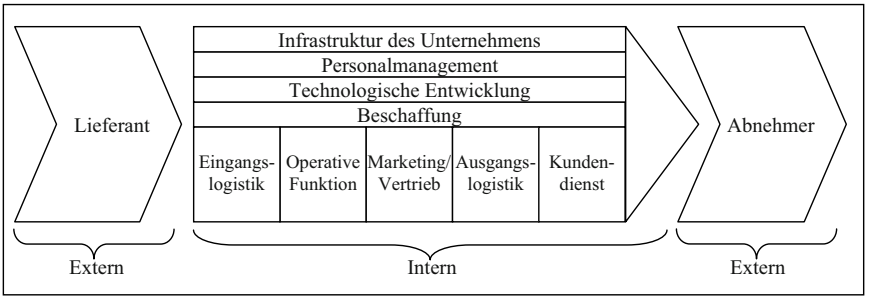


Abbildung 1: Wertekette eines Unternehmens mit vor- und nachgelagerten Aktivitäten
Quelle: in Anlehnung an Fuchs (2006), S. 219.

3.3.1 Angriffspunkte und Schutzmaßnahmen bei Lieferanten

Der erste potentielle Angriffspunkt einer Lieferkette tritt beim Lieferanten auf. Wenn dieser gefälschte Teile oder Komponenten liefert, beeinflussen diese natürlich auch das Endprodukt des Unternehmens. Das kann unbewusst passieren, wenn der Lieferant annimmt, der Produktpirat sei ein seriöser Hersteller, oder aber bewusst, wenn sich der Lieferant aus Kostengründen auf Produktpiraten einlässt. Da ein Unternehmen von der Vorleistung seiner Lieferanten entscheidend mit abhängt, müssen Schutzmaßnahmen bereits in der Wertschöpfungskette des Lieferanten ansetzen.

Jedes Unternehmen sollte vorab möglichst umfassende Kontrollrechte einrichten,[86] um z.B. so genannte *Lieferantenaudits* durchzuführen. Dadurch kann das Unternehmen, welches sich vor Produktpiraten schützen will, die Lieferanten in regelmäßigen Abständen überwachen und kontrollieren.[87] Lieferantenaudits dienen dazu, vor dem Auftrag abgesprochene Vorgaben und Prozesse zu überprüfen. In China erzeugen Lieferanten durch Einführung von Qualitätssiegeln und Kundenreferenzen einen verlässlichen Eindruck, doch sind selbst diese häufig gefälscht. Deshalb ist eine Kontrolle direkt vor Ort an den Produktionsstätten nötig.[88] Kontrollen können unter dem Vorwand durchgeführt werden, Schwachstellen zur Verbesserung der Effektivität aufzudecken. Ziel ist dabei vor allem die Qualitätsüberprüfung der gelieferten Komponenten. Eine Lösung ist auch, sich bei anderen schon etablierten Unternehmen in China über den einzelnen Lieferanten zu erkundigen und nur solche Lieferanten auszuwählen, die über vergleichbare Sicherheitsstandards wie das eigene Unternehmen verfügen. Es könnte eine Liste eingeführt werden, in der Firmen stehen, die den Schutz geistigen Eigentums garantieren. Damit könnte auf Unternehmen, die dies nicht vorzuweisen haben, enormer Druck ausgeübt werden. Auf dieser Grundlage könnte sich ein internationaler Investor von vorneherein ein Bild über das Geschäftsverhalten und die Reputation seines potentiellen Geschäftspartner machen.[89] Bisweilen erreicht man dieses Ziel am besten, wenn man die Lieferanten in das eigene Sicherheitssystem integriert oder das Sicherheitsniveau vertraglich bestimmt.[90] Eine weitere Möglichkeit besteht darin, chinesische Zulieferer von Anfang an in das Unternehmen einzubinden.[91] Als weiteres

[86] Vgl. Cremer (1991), S. 71; o.V. (2005c), S. 18.
[87] Vgl. o.V. (2005c), S. 18.
[88] Vgl. Fuchs (2006), S. 222.
[89] Vgl. o.V. (2005c), S. 18.
[90] Vgl. Fuchs (2006), S. 222.
[91] Vgl. Wenkel (2006).

effektives Instrument wird das Lieferantenportfolio angesehen. Es teilt Lieferanten „nach dem Fälschungsrisiko, das sie für Unternehmen darstellen, in verschiedene Risikokategorien“[92] ein. Lieferanten, die ein hohes Risiko für den Hersteller bedeuten, werden vermehrt und nachdrücklicher kontrolliert.[93] Somit steigt die Effizienz der Kontrolle und konsequenterweise verringert sich das Risiko der Produkt- und Markenpiraterie. Lieferantenaudits sollten nach Möglichkeit von unabhängigen Prüfern übernommen werden. Auch wenn diese Variante mit höheren Kosten verbunden ist, sind Untersuchungen durch neutrale Experten effektiver und im Falle einer Anklage auch vor Gericht aussagekräftiger.[94]

Nicht jede Kontrolle greift. Lieferanten, die mit gefälschten Waren handeln, können dieses auch unbewusst machen. Deswegen kann mit Hilfe von *Lieferantenschulungen und -beratungen*[95] das Fälschungsrisiko durch bewussteres Handeln und Wissen auf der Ebene der Lieferanten minimiert werden. Die Absicherung durch entsprechende Verträge verringert das Restrisiko.

Vertragsgestaltungen mit Lieferanten müssen so vereinbart werden, dass Lieferanten nicht nur Vorgaben haben, sondern selbst daran interessiert sind, in ihrem Unternehmen Produktpiraterie zu unterbinden. Der Lieferant verpflichtet sich dazu, nur Produkte aus Originalteilen herzustellen und anzuliefern. Kommt er dieser Verpflichtung nicht nach, muss er für den entstandenen Schaden aufkommen. Es kann z.B. vertraglich festgelegt werden, dass ein Lieferant Qualitätskontrollen durchführen muss und auch für die Arbeit der Sublieferanten verantwortlich ist bzw. durch eine Rückverfolgung der verwendeten Komponenten dem Unternehmen genau diesen Weg transparent machen muss.[96] Mit diesen Vereinbarungen können die Risiken durch Fälschungen auf den Lieferanten übertragen werden und minimieren so das Risiko des Unternehmens. Eine weitere Gefahr besteht darin, dass die Fertigungstiefe in der Industrie in den letzten Jahren immer deutlicher abgenommen hat. Deswegen haben Lieferanten zunehmend mehr Produktwissen des Originalherstellers, weil sie oft schon ganze Produktteile liefern. Diese Informationen müssen beim Lieferanten sicher aufbewahrt und dürfen

[92] Fuchs (2006), S. 226.
[93] Vgl. Fuchs (2006), S. 226.
[94] Vgl. The Economist (2005), S. 19.
[95] Vgl. Fuchs (2006), S. 226.
[96] Vgl. Fuchs (2006), S. 225.

nicht an Produktpiraten weitergetragen werden. Hierbei können wiederum Lieferverträge, die die Einhaltung der Schutzrechte garantieren, von großer Bedeutung sein.[97]

Im Kampf gegen Produkt- und Markenpiraterie ist es darüber hinaus von Vorteil, wenn die Lieferanten immer an den Produktionsstätten präsent sind. Auch EADS Vorstandsvorsitzender Enders sieht die „Internationalisierung [von] Zulieferindustrien"[98] als dringend notwendig. Dadurch können Strategien gegenüber potentiellen Fälschern häufiger und schneller geändert werden.[99] Durch Erhöhung der Flexibilität lässt sich das Risiko, von Produkt- und Markenpiraterie betroffen zu werden, auch hier durch eine ständige Anpassung drastisch verringern

Um sich nicht nur auf den Lieferanten und seine Arbeit zu verlassen, sollte eine strenge *Wareneingangskontrolle* durchgeführt werden, anhand derer Fälschungen entdeckt werden können. Die Korrektheit der Eingangsprüfungen muss Grundlage sein. Zwar fordert diese Maßnahme einen hohen Zeit- und Personalaufwand,[100] jedoch ist der Schaden in einem so frühen Stadium weit geringer, als wenn die Fälschung an den Endverbraucher gelangt ist, ohne entlarvt worden zu sein. Selbst wenn beim Lieferanten die Ware ordnungsgemäß das Haus verlassen hat, ist nicht gewährleistet, dass sie auch so beim Unternehmer ankommt. Auf dem Transportweg besteht wiederum das Risiko, dass die Ware gegen Fälschungen ausgetauscht werden kann. Aus diesem Grund sollten vor allem die Routen der Spediteure und Transportführer kontrolliert werden und nachvollziehbar sein.

3.3.2 Angriffspunkte und Schutzmaßnahmen in der Beschaffung

Der Schnittpunkt zwischen Lieferanten und dem Hersteller liegt in der Beschaffung. Die Einkäufer in den jeweiligen Unternehmen haben einen Großteil der Aufgabe im Kampf gegen Produkt- und Markenpiraterie übernommen. Nach einer Studie von A.T. Kearney wird bis in drei Jahren der Beschaffungsmarkt China von 72% der befragten Unternehmen genutzt werden.[101] Das bedeutet, dass heutzutage Einkäufer mehr gefordert sind als je zuvor, da sie einen intransparenten Markt wie China durchschauen und zuverlässige Informationen finden müssen. Die Lieferanten wie auch der Markt müs-

[97] Vgl. Fischer et al. (2002), S. 83.
[98] Wüpper (2006), S. 14.
[99] Vgl. Hüttemann (2006), S. 23.
[100] Vgl. Fuchs (2006), S. 228.
[101] Vgl. o.V. (2005i).

sen intensiv beobachtet werden, um Entwicklungen, die Hinweise auf Fälschungen geben, frühzeitig zu erkennen und diese sofort zu unterbinden. Gerade bei Roh-, Hilfs- und Betriebsstoffen sind Fälschungen wie z.B. chemische Zusatzstoffe schwer zu erkennen.[102]

Eine praktikable Lösung dafür sind *Einkaufskooperationen*. Dabei können alle nötigen Informationen gebündelt werden. Zusätzlich tritt man dem Lieferanten mit einer größeren Einkaufsmacht entgegen.[103] Nach einer intensiven Informationsanalyse minimiert man das Risiko, sich auf unseriöse Lieferanten einzulassen. Gewinnt ein Lieferant durch eine Einkaufskooperation einen Großauftrag, lässt er sich eher nicht auf Produktpiraten ein, aus Angst den Auftrag zu verlieren.

Ein weiteres Beispiel ist die *Mengenbeschränkung beim Einkauf von Sicherheitstechnologien*. Unabhängig davon, um welche Technologie es sich dabei handelt, darf es nicht passieren, dass z.B. Konfektionäre eine unbeschränkte Anzahl von Sicherheitsetiketten bestellen können. Auch an dieser Stelle müssen Kontrollen eingebaut werden, um das Risiko, dass Etiketten in Fälscherhände gelangen, nicht enorm zu erhöhen.[104]

Als Konsequenz muss folgender Schluss gezogen werden: Sicherheit nur möglich in „Verbindung [mit einem] optimalen Beschaffungsmanagements."[105]

3.3.3 Angriffspunkte und Schutzmaßnahmen beim Personal

Einer Studie von PricewaterhouseCoopers zufolge nahm die Wirtschaftskriminalität, zu der auch die Produkt- und Markenpiraterie zählt, von 2003 auf 2005 um 8% zu. In Deutschland setzen sich die 8% aus 5% Steigerung der Produktpiraterie und 3% Steigerung der Korruption zusammen. Das Beunruhigende dabei ist, dass etwa 50% der Wirtschaftstäter direkt aus dem Unternehmen kommen. Genau das schätzen die Unternehmen jedoch als unrealistisch ein. Entsprechend einer Studie von The Economist Corporate Network für KPMG befürchten nur 15% der befragten Firmen einen internen Übergriff, wogegen 85% der Meinung sind, die Übergriffe kämen von Externen.[106] Das Vertrauen zu einem Mitarbeiter wächst üblicherweise mit den Jahren, die der Mitarbeiter im Unternehmen angestellt ist. Entsprechend der PricewaterhouseCoo-

[102] Vgl. Fischer et al. (2002), S. 83.
[103] Vgl. Fuchs (2006), S. 221 ff.
[104] Vgl. Hüttemann (2006), S. 23.
[105] Hüttemann (2006), S. 23.
[106] Vgl. o.V. (2005c), S. 22.

pers-Studie nimmt das Kriminalitätsrisiko im Laufe der Zeit jedoch nicht ab, sondern zu. Weltweit kommen ein Viertel der Wirtschaftstäter aus dem Topmanagement; in Deutschland beträgt deren Anteil sogar 32%.[107] Die Wissensweitergabe durch Mitarbeiter ist wohl der sensibelste Punkt und stellt das größte Risiko im Kampf gegen Produktpiraten dar.

Nach Auffassung von Fuchs sind die meisten Sicherheitsverletzungen auf den Mensch zurückzuführen, da er derjenige ist, der die Schwachstellen des Unternehmens am besten erkennen kann. Das bedeutet, dass potentielle Schutzmaßnahmen „gezielt auf die Schwachstelle Mensch ausgerichtet sein sollten."[108] Die Erhöhung des Sicherheitsbewusstseins bei den Mitarbeitern ist ein wichtiges Ziel in diesem Prozess.

Am Anfang eines präventiven Schutzkonzepts sollte eine *solide Bestandsaufnahme* stehen. Dabei müssen auch „bisherige Personaleins[ätze], eingespielte Arbeitsroutinen und langjährig gepflegte Außenbeziehungen"[109] kritisch durchleuchtet werden. Die Schwierigkeit liegt wohl in der Balance zwischen den Hinterfragungen bisheriger Abläufe und deren Schutz. Ebenso müssen bestimmte Sicherheitsrisiken mit geringem Gefahrenpotential erkannt und akzeptiert werden.[110]

Da Mitarbeiter die häufigste Ursache für den Verlust von geistigem Eigentum sind, empfiehlt sich als Maßnahme eine *selektive Einstellung***,** d.h. schon bei der Personalauswahl muss genau auf die Schlüssigkeit der Unterlagen und den persönlichen Eindruck geachtet werden. Problematisch in China ist, dass selbst Zeugnisse und Referenzen nachgemacht sind, sodass zu einer Überprüfung spezielle Agenturen oder Wirtschaftsdetekteien hinzugezogen werden sollten. Weitere Vorsichtmaßnahmen sollten bei Praktikanten und Diplomanden getroffen werden bzw. sollten diese nicht uneingeschränkt in sensiblen Unternehmensbereichen eingesetzt werden.[111]

Entsprechend einer Roland Berger Studie zum Schutz geistigen Eigentums ist eine übliche Maßnahme von Unternehmen, auf technologische Top-Positionen keine lokalen Bewerber einzusetzen, sondern z.B. *Expatriates*[112], d.h. Mitarbeiter aus Deutschland, die nach China entsendet werden. Diese würden insofern das Risiko der Wis-

[107] Vgl. Busmann et al. (2005), S. 4.
[108] Fuchs (2006), S. 230.
[109] ebd.
[110] Vgl. Fuchs (2006), S. 230.
[111] Vgl. Fuchs (2006), S. 232.
[112] Vgl. Drinkuth et al. (2005), S. 27.

sensweitergabe reduzieren, als sie üblicherweise nicht zu einem chinesischen Netzwerk gehören, aber schon unternehmensinternes Wissen mitbringen.

Gefahr geht vor allem von Mitarbeitern aus, die mit dem Arbeitsklima oder den Arbeitsbedingungen des Unternehmens unzufrieden sind. Das Risiko, dass diese Mitarbeiter Informationen ausspähen, um diese Konkurrenten, zu denen auch Produktpiraten gehören, gegen Bezahlung zur Verfügung stellen, ist in diesem Fall sehr hoch. Dagegen hilft ein effektives *Fluktuationsmanagement*. Dies steht auch in direktem Zusammenhang mit der hohen Fluktuationsrate in China, die „weitere Risiken des Know-how-Verlusts in sich bergen."[113] Je enger die Mitarbeiter mit dem Unternehmen verbunden sind, umso geringer ist das Risiko der Spionage. Man unterscheidet hier zwischen langfristigen und kurzfristigen Maßnahmen. Kurzfristig kann die Weitergabe von Betriebsgeheimnissen durch persönliche finanzielle Vorteile vermieden werden wie einen Firmenwagen oder eine Wohnung, die bei Verlust des Arbeitsplatzes ebenfalls wegfallen.[114] Das bedeutet, der Ausstieg wird bei diesem Unternehmen „für einen Klienten teuer."[115] Langfristig sollen Mitarbeiter jedoch emotional an das Unternehmen gebunden werden. Dies bestätigt die Engagement Index Study[116] von der Gallup Organisation, die jedes Jahr die emotionale Bindung der Mitarbeiter in verschiedenen Ländern testet. Ein Beispiel dafür, wie emotionale Bindung die Fluktuationsrate sinken lässt, kann man im Anhang 1 betrachten. Das Risiko, dass bei einer hohen Fluktuationsrate internes Wissen leichter in die Hände von Produktfälschern gelangen kann, ist natürlich höher, heißt es doch „mit jedem Mitarbeiter verlässt ein Stück Wissen das Haus."[117] Wie man Mitarbeiter an Unternehmen emotional bindet, geht über diesen Beitrag hinaus, wäre jedoch eine besonders geeignete Maßnahme, um das Risiko von Wissenstransfers an Produktpiraten nachhaltig zu verringern. Die Verbindung zum Unternehmen schafft vor allem Aussicht auf Entwicklungsmöglichkeiten und Karrierechancen. Mitarbeitergespräche, die Lob und Anerkennung beinhalten, sind wichtige Bestandteile, um die Arbeitsatmosphäre deutlich zu verbessern. Zusammenfassend ist somit zu sagen, dass die Mitarbeiter, die eng mit ihrem Unternehmen verbunden sind, weniger ihre Arbeitsstelle wechseln, wodurch internes Wissen nicht immer wieder das

[113] Vgl. o.V. (2006e), S. 17; Fuchs (2006), S. 232.
[114] Vgl. Drinkuth (2005), S. 27; Fuchs (2006), S. 234.
[115] Anand/Galetovic (2006), S. 80.
[116] o.V. (2005e), S. 1-49.
[117] Fuchs (2006), S. 231.

Unternehmen verlässt. Auch so kann mehr Sicherheit gegen Produktpiraten garantiert werden.

Geheimhaltungsklauseln in Arbeitsverträgen sind die mögliche rechtliche Absicherung, damit Wissen nicht nach außen getragen wird.[118] Sie dienen eher der rechtlichen Grundlage im Konfliktfall als einer effektiven Abschreckung. Unternehmen sollten jedoch trotzdem darauf achten, den Bereich der Geheimhaltung genau zu definieren,[119] sodass vor Gericht diese Verträge auch Grundlage eines Verfahrens sein können. Einen Mitarbeiter, der internes Wissen ausspionieren will, wird die Geheimhaltungsklausel nicht von seinem Vorgehen abhalten können. Das Risiko, dass Wissen ständig nach außen sickert, wird aber verringert. Geheimhaltungsvereinbarungen müssen natürlich auch von Dritten unterzeichnet werden, falls das Produkt schon vor einer Anmeldung zur Ansicht vorgelegt werden muss.[120]

Das Risiko, dass Mitarbeiter Wissen an Dritte weitergeben, kann auch unbewusst entstehen. Eine Sensibilisierung hinsichtlich der Bedeutung von Wissenstransfer kann durch *Mitarbeiterschulungen* geschaffen werden. Mitarbeiter lernen, Schwachstellen im Sicherheitssystem selbst zu erkennen und ihnen präventiv entgegenzuwirken. Sicherheitsmaßnahmen nur zu befolgen, ohne über ihren Zweck aufgeklärt zu sein, ist ineffektiv – gerade „im kulturell sensiblen China."[121] Es ist davon auszugehen, dass die Belegschaft die größte Informationsquelle eines Unternehmens ist. Wenn in Schulungen gelehrt wird, wie man das Original von der Fälschung unterscheiden kann und welche Konsequenzen Produktpiraterie für die Wirtschaft und speziell ihre persönliche Arbeitsstelle hat, können Mitarbeiter schneller und zuverlässiger als Informanten für das Unternehmen fungieren. Möglich wäre es, Mitarbeiter, welche Fälschungen aufdecken oder wichtige Informationen liefern, finanziell zu belohnen.[122] Das schafft zusätzlichen Anreiz, Informationen preis zu geben. Diese Informationsquelle kann Fälle von Produktpiraterie häufiger aufzuspüren und trägt somit zur Risikominderung der Übergriffe von Produktpiraterie bei.

Job Rotation bedeutet der „systematische Wechsel von Arbeitsplätzen oder Aufgaben."[123] Der Vorteil bei dieser Maßnahme ist, dass Mitarbeiter ihren Arbeitsbereich

[118] Vgl. Fuchs (2006), S. 233.
[119] Vgl. Fuchs (2006), S. 233; Drinkuth (2005), S. 27.
[120] Vgl. Cremer (1991), S. 70.
[121] Fuchs (2006), S. 235.
[122] Vgl. Fuchs (2006), S. 235.
[123] Fuchs (2006), S. 237.

nur an der Oberfläche kennen lernen. So erhalten sie kein tiefergehendes Wissen von sensiblen Prozessen, welches dann an Produktpiraten weitergegeben werden könnte. Der Nachteil ist jedoch, dass die Mitarbeiter viele Stellen kennenlernen und so das Risiko der Wissensweitergabe an Dritte wiederum höher ist. Da in China der Aufbau von Beziehungen, auch zu Fälschergruppen, ein wichtiger Bestandteil des Geschäftslebens ist, unterbindet ein ständiger Jobwechsel diese Entwicklung.[124] Job Rotation kann ebenso verhindern, dass zu enge Beziehungen zu Lieferanten oder Abnehmern aufgebaut werden, die Ansätze für Bestechlichkeit bieten. Hier müssen die Vor- und Nachteile je nach Unternehmenssituation abgewogen werden.

Die Einführung von *Verhaltensregeln und Richtlinien* unter den Mitarbeitern ist bei der Bekämpfung der Produktpiraterie eine weitere wichtige Grundlage. Einige werden im Folgenden vorgestellt[125]:

- Beim „Vier-Augen-Prinzip“ muss eine zweite Stelle Verträge gegenzeichnen; sie fungiert so als Kontrolle.
- Beim „Need-to-know-Prinzip“ muss jeder Mitarbeiter nur das Minimum an Wissen und Zugang zu Informationen erhalten, die zur Durchführung seiner Aufgaben nötig sind. Sensibles Wissen sollte nur einem kleinen Kreis an Mitarbeitern bekannt sein, denn „expanding the sphere of people with access to a firm’s IPR[126] knowledge increases risk.”[127]
- Weitere Grundprinzipien sind die Funktionstrennung, eine transparente Buchführung sowie die vollständige Erfassung von Handlungen und Prozessen.

Durch diese Grundprinzipien kann das Risiko eines Übergriffs durch Produktpiraten schon von vornherein drastisch gesenkt werden. Zusammenfassend lässt sich sagen, dass es wichtig ist, so wenig Mitarbeitern wie möglich Zugang zu sensiblem internen Unternehmenswissen zu geben.[128]

[124] Vgl. Fuchs (2006), S. 237.
[125] Vgl. Fuchs (2006), S. 236.
[126] IPR kurz für: Intellectual Property Right, übersetzt: Recht an geistigem Eigentum.
[127] o.V. (2005c), S. 15.
[128] Vgl. o.V. (2005c), S. 15.

3.3.4 Angriffspunkte und Schutzmaßnahmen in der F&E

Forschung- und Entwicklungsbereiche, wo Ideen entstehen und zu machbaren Konzepten und Produkten umgearbeitet werden, werden als die sensibelsten Unternehmensbereiche bezeichnet. Wenn Produktpiraten in der Entwicklungsphase eines Produktes von dessen Idee und Umsetzung erfahren und womöglich das Produkt vor dem Originalhersteller in den Markt einführen, verliert der Originalhersteller seinen Wettbewerbsvorteil und die Folgen sind fatal. Fatal deshalb, weil die meist sehr hohen Entwicklungskosten dann nicht mehr durch den Verkauf der entwickelten Produkte amortisiert werden können, da der Umsatz der neuen Produkte durch die bereits bestehenden Plagiate zurückgehen wird. Dadurch wächst das „unternehmerische Risiko exponentiell."[129] Deshalb sollte „kritisches Know-how unter Verschluss gehalten"[130] werden. Gerade für deutsche Unternehmen ist dieser Angriff wohl der verhängnisvollste, da der Wettbewerbsvorteil, den deutsche Firmen immer noch gegenüber dem Ausland haben, aus ihrem Technologievorsprung hervorgeht.[131] Produktpiraterie ist deswegen so gewinnbringend, weil die Fälscher die notwendigen Investitionen in Forschung und Entwicklung sowie in Werbung und den Aufbau des Images nicht tätigen müssen.[132]

Organisatorisch sollte diese Abteilung klar vom restlichen Unternehmen abgetrennt sein. *Geheimhaltung* in der Forschung und Entwicklung hat oberste Priorität. Mitarbeitern von anderen Abteilungen sowie Externen, Praktikanten oder Diplomanden sollte der Zutritt verweigert werden bzw. nur eingeschränkt möglich sein. Nicht nur Mitarbeiter, sondern auch die internen Computernetzwerke sollten vom Gesamtnetzwerk – dem Intranet – sowie natürlich dem Internet, abgeschottet sein.

Eine weitere Schutzmaßnahme, um das *Gesamtwissen eines Produktes zu verschleiern*, wären einzelne Teams, die dezentral an unterschiedlichen Modulen des Gesamtsystems arbeiten.[133] Durch diese Streuung verringert sich das Risiko, dass der Gesamtplan des Produktes nach außen getragen werden kann.

Immer wieder wird berichtet, dass ausländische Unternehmen, um in China investieren zu können, Bauskizzen sowie Betriebsgeheimnisse offenbaren müssen.[134] Auf diese

[129] Vgl. Fuchs (2006), S. 237.
[130] Ballhaus (2005), S. 41.
[131] Vgl. Fuchs (2006), S. 237.
[132] Vgl. Hayers et al. (2005), S. 16.
[133] Vgl. Ballhaus (2005), S. 41.
[134] Vgl. o.V. (2006d), S. 9; o.V. (2006c), S. 15.

Forderung sollte sich kein Unternehmen einlassen. Die *Unterbindung des Technologietransfers* in allen Bereichen, jedoch vor allem in der Forschung und Entwicklung, minimiert das Risiko von Fälschern nachhaltig. Ebenso sollten neue Produkte schon vor der Zertifizierung der chinesischen Behörden patentiert sein. Fuchs schlägt ebenfalls vor, Gerichtsverfahren gegen Fälscher einzustellen oder erst gar nicht zu führen, sobald klar ist, dass technische Pläne als Beweis vorgelegt werden müssen.[135]

Eine weitere effektive Präventionsmaßnahme wäre, schon in der Forschung und Entwicklung grundsätzliche Überlegungen über mögliche *Komplementärprodukte* anzustellen, welche nur vom gleichen Hersteller zusammenpassen. Damit würden Fälscher, die nur einzelne Komponenten anbieten, eher aufgedeckt werden oder scheitern.[136]

Die Gefahr der Produktpiraterie könnte natürlich durch einen ständigen *Innovationsvorsprung* deutlich verkleinert werden. Dann wäre man ihnen „immer eine Nasenlänge voraus"[137], wie Siemens-Aufsichtsratsvorsitzender Heinrich von Pierer betont. Eine Schutzmaßnahme wäre also die Kürzung der Entwicklungszyklen. Diese Maßnahme würde das Risiko der Produktpiraterie fast völlig eindämmen, da die Fälscher durch ständige Erfindung neuer Produkte nicht mit dem Nachahmen Schritt halten könnten und sich dadurch wohl auch eher auf andere Produkte umstellen. Ob diese Maßnahme finanziell und personell durchführbar ist, muss im Einzelfall geklärt werden.

3.3.5 Angriffspunkte und Schutzmaßnahmen in der Fertigung

Wenn ein Produktpirat den kompletten Fertigungsprozess eines Produktes versteht, kann er das Produkt leicht nachbauen. Deshalb ist es im produzierenden Gewerbe besonders wichtig, Vorsichtsmaßnahmen innerhalb des Fertigungsprozesses zu treffen, da ein Großteil der Belegschaft in diesem Bereich beschäftigt ist und somit erhöhte Gefahr besteht, das Interna nach außen getragen werden. Angriffspunkte hier sind die verschiedenen Prozesse in den Fertigungsstufen und Unterlagen wie „Rezepturen, Pläne oder Maschinenspezifikationen."[138]

Um sich vor Übergriffen durch Produktpiraten zu schützen, sollten alle Dokumente über den Fertigungsprozess gut verschlossen aufbewahrt werden. *Geheimhaltung* ist hier die einfachste und wirksamste Lösung. So wurde z.B. die Zusammensetzung für

[135] Vgl. Fuchs (2006), S. 238.
[136] ebd.
[137] Michler (2006).
[138] Vgl. Fuchs (2006), S. 239.

das Produkt Coca-Cola trotz vieler Nachahmungsversuche nie aufgedeckt,[139] wodurch kein Konkurrenzprodukt wie das Original Coca-Cola schmeckt. Ein weiteres Beispiel für Geheimhaltung kommt aus Japan, wo ein Hersteller den Mitarbeitern zwar die richtige Mischung seiner Produkte verrät, jedoch nicht die einzelnen Bestandteile preisgibt.[140] Vor allem aber muss das Verschwinden von Teilkomponenten sofort aufgedeckt und untersucht werden, um möglichen Diebstahl auszuschließen. Aufmerksam darauf kann man werden, wenn man die Beschaffungsgröße kontinuierlich mit der Anzahl der gefertigten Teile vergleicht. Auch die Ausschussmenge sowie „Verpackungen, Bedienungsanleitungen oder Garantiekarten"[141] müssen kontrolliert entsorgt werden. Bei Schwund besteht der Verdacht, dass die Weitergabe an Fälscher erfolgt ist.[142] Nicht nur Lieferanten von Rohstoffen und Produktkomponenten müssen gut ausgesucht und kontrolliert werden; auch die Dienstleister, die sich mit dem Abfall oder dem Recycling beschäftigen, müssen garantieren können, Restbestände zuverlässig zu vernichten.[143] Dadurch wird das Risiko des Missbrauchs reduziert, indem man vermeidet, dass selbst diese noch ausgeschlachtet werden.

Durch *Stichproben und Qualitätskontrollen* müssen Fälschungen, die womöglich in den Produktionsprozess geschmuggelt oder schon vom Lieferanten eingeschleust wurden, aufgedeckt werden. Bei Roh- und Hilfsgütern wird dies besonders schwer, da Fälschungen hier äußerlich vom Original nicht zu unterscheiden sind.[144] Nicht vergessen sollte man auch, Stillstandzeiten genau zu protokollieren bzw. den Zugang zu den Fertigungshallen genau zu kontrollieren.[145] Dadurch kann das Risiko eines Übergriffs eingeschränkt bzw. im Falle eines Schadens der Täter leichter identifiziert werden.

Die *Streuung des Gesamtprozesses* auf mehre Produktionsstätten oder verschiedene Teams ist eine wirkungsvolle, risikomindernde Lösung.[146] Dadurch wird der Gesamtprozess verschleiert und ist nur schwer für Produktpiraten vollständig zu erfassen. Sensible Teile sollten nach Möglichkeit ausschließlich in Deutschland gefertigt werden, um geistiges Eigentum in dem Bereich besonders zu schützen.[147]

[139] Vgl. Anand/Galetovic (2005), S. 78.
[140] ebd.
[141] Fuchs (2006), S. 239.
[142] Vgl. Fuchs (2006), S. 239.
[143] Vgl. Harte-Bavendamm (2000), S. 45.
[144] Vgl. Weiser/Olsen (2004), S. 31.
[145] Vgl. Fuchs (2006), S. 240.
[146] Vgl. Ballhaus (2005), S. 41.
[147] Vgl. Drinkuth (2005), S. 26.

Im Endeffekt kristallisieren sich *zwei Grundstrategien aus der Sicht der Fertigung* heraus: Zum einen besteht die Möglichkeit, sich durch den Einsatz eines hoch komplexen Herstellungsverfahrens gegen Produktpiraterie zu schützen. Komplizierte Prozesse oder teure Maschinen und damit hohe Fixkosten schrecken Produktpiraten von Nachbildungen ab. Dies ist nach dem Prinzip der Economies of Scale und den geringen Lohnkosten in China eine wirkungsvolle Grundüberlegung. Zum anderen besteht die Möglichkeit, durch ein kostengünstiges Verfahren oder durch die Herstellung simpler Produkte in großer Stückanzahl das Geschäft der Fälscher finanziell unattraktiv zu machen.[148] Durch beide Grundüberlegungen wird das Risiko eines Übergriffs gesenkt.

Die Vergabe von Aufträgen an chinesische Fremdfirmen – *Outsourcing* – ist im Hinblick auf Produkt- und Markenpiraterie als sehr kritisch anzusehen. Auch hier ist die Streuung an mehrere Firmen unerlässlich, um die Kenntnisse des Gesamtprozesses zu verbergen.[149] Auch externe Spezialisten wie Unternehmensberater und Wirtschaftsprüfer bilden ein Risikopotential, da vor allem ihnen Einblicke in fast alle Unternehmensbereiche gewährt werden, weil die Firmen auf ihr Urteil angewiesen sind.[150] Aufträge an Dienstleister wie Übersetzungsbüros, EDV-Firmen oder Sicherheitskräfte sollten ebenfalls strikt untersucht werden. Dokumente können dort leicht kopiert, übermittelt oder ausspioniert werden, ein großes Risiko, das viele Unternehmen jedoch leichtfertig übersehen. Wenn ein Unternehmen Teile seiner Fertigung an andere Firmen vergibt, müssen Grundvoraussetzungen wie vergleichbare Sicherheitssysteme und abgeschlossene IT-Systeme übereinstimmen. Auch bei frühzeitiger Kündigung oder Erfüllung des Vertrags durch den Geschäftspartner müssen Kontrollen stattfinden, damit das Know-how nicht an Dritte weitergegeben wird.[151]

3.3.6 Angriffspunkte und Schutzmaßnahmen im Aufbau der Infrastruktur

Voraussetzung für den effektiven Schutz geistigen Eigentums sind die infrastrukturellen Rahmenbedingungen. Spionage wird Fälschern durch einfachen Zutritt von Mitarbeitern oder Externen in sensible Unternehmensbereiche oft zu einfach gemacht. Dem können Unternehmen mit zahlreichen Möglichkeiten begegnen.

[148] Vgl. Fuchs (2006), S. 238
[149] Vgl. Drinkuth (2005), S. 26.
[150] Vgl. Schöne (2000), S. 5.
[151] Vgl. Fuchs (2006) S. 240-241.

Zur Unternehmensinfrastruktur gehören auch die Informations- und Kommunikationsinstrumente, welche heutzutage immer mehr an Bedeutung gewinnen. Nach Fuchs sind sie das „primäre Ziel der Wirtschaftsspionage."[152] Vor allem wird versucht, extern auf die Computernetzwerke Zugriff zu bekommen bzw. durch Virenangriffe Schaden anzurichten oder durch Manipulation von Softwareprogrammen an Daten zu gelangen. Insbesondere Handys mit Kameras, PDAs, BlackBerrys usw. erleichtern es, Informationen aus der Firma zu schleusen.[153] Durch die Verbreitung von diesen oben genannten Technologien steigt das Risiko eines Übergriffs durch Fälscher drastisch.

Ein Sicherheitsdienst sowie „bauliche, mechanische und elektronische Absicherung"[154] der Gebäude und der einzelnen Bereiche sind unabdingbar. *Zutrittskontrollen* müssen eingerichtet werden, sodass keine Unbefugten das Gelände betreten dürfen. Dadurch kann man jederzeit nachvollziehen, wer wann wo war.[155] Starke Schutzsysteme dienen der Kontrolle und Überwachung, aber auch der Abschreckung, womit das Risiko eines Übergriffs durch Fälscher stark einschränkt wird. Bewegungsmelder, Alarmüberwachung und Kameras sollten beispielsweise zur Grundausstattung eines jeden Unternehmens gehören.

Das *Verbot der Nutzung von elektronischen Geräten* durch externe Besucher muss in sensiblen Unternehmensbereichen ausnahmslos durchgesetzt werden. Damit geht man kein Risiko ein, dass Fälscher Fotos oder betriebsinterne Informationen selbst erlangen können.

Gegenüber jeder elektronischen Anwendung gibt es mindestens eine Schutzmaßnahme. *Elektronische Schutzmaßnahmen* wie Passwörter, Verschlüsslungen, Signaturen, Virenprogramme und Firewall-Lösungen sind nur einige Beispiele, wie man sich vor externen Angriffen schützen kann.[156] Kosten und Arbeitsaufwand der Schutzmaßnahmen müssen gegenüber dem Risiko eines Übergriffs abgewogen werden.

3.3.7 Angriffspunkte und Schutzmaßnahmen im Vertrieb

Der volkswirtschaftliche Schaden durch Produktpiraterie beläuft sich auf 5 bis 9% des Welthandels. Dieser enorme Absatz von gefälschten Waren kann nicht nur auf Straßen

[152] Fuchs (2006), S. 245.
[153] Vgl. Fuchs (2006), S. 245.
[154] Fuchs (2006), S. 243.
[155] Vgl. Fuchs (2006), S. 244.
[156] Vgl. Fuchs (2006), S. 245-246.

und Hinterhöfen entstehen. Mit dem Anstieg der Plagiate steigt auch der Verkauf über offizielle Vertriebswege. Immer mehr Produktpiraten schmuggeln ihre Produkte in den Handel ein. Nach Aussage von Fuchs passiert dies häufig durch Bestechung der Vertriebsmitarbeiter. Um ihren Gewinn zu steigern, mischen chinesische Händler immer wieder Fälschungen unter das Originalsortiment. Mit dem Markenimage der westlichen Konzerne vertreiben sie an ahnungslose Kunden Plagiate und wirtschaften so am offiziellen Umsatz illegal vorbei.[157]

Um der oben genannten Korruption der Vertriebsmitarbeiter präventiv entgegenzuarbeiten, können *Verkaufsteams* gebildet werden, deren Mitarbeiter sich gegenseitig überprüfen. So vermeidet man, dass der Einzelne durch Bestechungsgeschenke beeinflussbar wird.[158]

Auch durch eine *Rotation der Vertriebsmitarbeiter* unterbindet man den engen Beziehungsaufbau zum Kunden und schafft so immer wieder die nötige Distanz, um nicht bestechlich zu werden. Doch auch hier muss man den Vorteil einer engen Kundenbindung, den man durch Rotation einbüßt, gegen den Nutzen einer solchen Maßnahme im Kampf gegen Produktpiraterie abwägen.[159]

Als weitere mögliche Maßnahme bietet es sich an, die Produkte schon beim Hersteller so zu verpacken, dass sie in *endkundengerechten Verbrauchseinheiten* verkauft werden können. Durch die fertig verpackten Einheiten reduziert sich die Gefahr der Beimischung von gefälschter Ware. Diese klare Deklarierung des Endprodukts und der Aufwand, diese individuell gekennzeichnete Verpackung neu umzupacken, stehen für Fälscher nicht im Verhältnis.[160]

Um sich präventiv gegen Produktpiraterie abzusichern, sollten die Originalprodukte je nach Relevanz des Fälschungsrisikos nur in *selektiven Verkaufsstellen* angeboten werden. Durch die Exklusivität der Geschäfte wird sofort ersichtlich, dass Produkte, die außerhalb dieses Systems verkauft werden, imitiert sein müssen.[161] Mit im Händlervertrag sollten Auflagen sein, wie die „Installation von Sicherheitstechnologien, […] oder die Schulung des Verkaufspersonals“[162], welche die Aufgaben der Bekämpfung der Fälscher auf die ausgesuchten Händler abwälzt.

[157] Vgl. Fuchs (2006), S. 248-250.
[158] Vgl. Fuchs (2006), S. 248.
[159] ebd.
[160] Vgl. Fuchs (2006), S. 249ff.
[161] Vgl. Fischer et al. (2002), S. 85.
[162] Fuchs (2006), S. 249.

Schulungen der Vertriebsmitarbeiter sowie deren Händler sind unverzichtbar. So lernen diese, Fälschungen leicht zu identifizieren. Darüber hinaus können sie ihre Mitarbeiter aufklären, welche straf- und zivilrechtlichen Konsequenzen zu befürchten sind, falls vorsätzlich gefälschte Waren durch ihre Vertriebswege in Umlauf gebracht werden.[163] Doch zahlt es sich nicht aus, seinen Händlern nur negativ gegenüberzustehen. Verkaufsteams sind meistens die ersten, die Signale über verdächtige Aktivitäten aufnehmen und sie sofort an den Hersteller weiterleiten können.[164] Die Mitarbeiter fungieren als „Frühwarnsystem", was das Risiko eines möglichen Angriffs durch Produktpiraten deutlich verringert.

Regelmäßige, am besten unangekündigte Kontrollen des Vertriebssystems sind unvermeidlich. Vor Ort sollten *Händleraudits* durchgeführt werden, die Schwachstellen aufdecken, um einen größeren Schaden abzuwenden. Unternehmen sollten nur mit zertifizierten Händlern zusammenarbeiten, d.h. Händler sollten nachweisen können, dass sie wirkungsvolle Sicherheitsbestimmungen getroffen haben und sich somit nachweislich mit am Kampf gegen Produktpiraterie beteiligen. Um die Kontrolle des Vertriebssystems zu gewährleisten, sollten chinesische Händler die genutzten Vertriebswege nachweislich aufzeigen können. Änderungen der Verkaufsbedingungen wie Rabatte und Sonderaktionen sollten dem Hersteller unverzüglich mitgeteilt werden, sodass die Kontrolle des Vertriebssystems stets in den Händen des Herstellers ist.[165]

Die folgende Schutzmaßnahme wird nicht zu vielen Vertriebsmodellen passen, soll aber trotzdem hier erwähnt werden: Die Firma DELL ist das typische Beispiel dafür, dass ein Unternehmen keinen Zwischenhändler mehr benötigt. Kunden können online ihren PC individuell zusammenstellen.[166] Der *Verzicht auf Zwischenhändler* verkürzt die Logistikkette um eine Komponente, was bedeutet, dass sich das Risiko eines Angriffs durch Produktpiraten um diese Möglichkeit verringert.

Eine kurze Versorgungskette ist natürlich leichter zu kontrollieren als eine sehr lange und verästelte. Deshalb ist eine Möglichkeit, auf chinesische Geschäftspartner zu verzichten und einen *Direktvertrieb* in China zu errichten.[167] Als Schutzmaßnahme ist dies sicherlich effektiv, doch ob sich die Kosten für den Aufbau eines eigenen Vertriebssystems auszahlen, ist fraglich. Gemäß einer Studie von The Economist wählen

[163] Vgl. Fischer et. al. (2002), S. 85.
[164] Vgl. o.V. (2005c), S. 15; Hartberg (2005), S. 12.
[165] Vgl. Fuchs (2006), S. 250ff.
[166] Vgl. o.V. (2005c), S. 16.
[167] Vgl. Ballhaus (2005), S. 41.

trotzdem immer mehr Unternehmen dieses Konzept, um die Kontrolle in eigenen Händen zu behalten und potentielle Konflikte zu vermeiden. Zu beachten ist dabei jedoch, dass es in China nicht in allen Bereichen erlaubt ist, nur vom Herstellerland allein kontrollierte Vertriebssysteme zu errichten.[168]

Lizenzen zu vergeben ist eine Art Zugeständnis gegenüber der Problematik der Produktpiraterie. Man gibt chinesischen Geschäftsleuten von Anfang an die Möglichkeit, von westlichem Know-how zu profitieren, indem man ihnen für einen bestimmten Zeitraum Lizenzen anbietet, sodass sie die Produkte legal produzieren oder verkaufen dürfen.[169] Das *Franchisingkonzept* bietet den Produktpiraten theoretisch kaum eine Angriffsfläche, da der Franchisegeber detailliert vorschreiben kann, wo und wann der Franchisenehmer bei welchem Lieferanten die Ware einzukaufen hat.[170] Ein großer Nachteil bietet das Franchisekonzept jedoch trotzdem. Auch wenn man den Franchisenehmer während des vertraglich bestimmten Zeitraums kontrollieren kann, besteht die Möglichkeit, dass er sich zu einem späteren Zeitpunkt durch das angeeignete technische Wissen zum Konkurrenten entwickelt. Auch läuft man Gefahr, dass der Lizenzpartner sein Wissen an Produktpiraten weitergibt. Um diesen Risiken entgegenzuwirken, kann man bei der Auswahl der Partner nicht sorgfältig genug die Zuverlässigkeit der Lizenzabnehmer prüfen. Kontrollen der Geschäftspartner und deren Standorte sind unerlässlich, ebenso die vertraglichen Verpflichtungen, keine Schutzrechte zu verletzen.[171] Nicht nur Prüfungen, sondern auch enge Beziehungen zueinander können das Risiko minimieren, dass der Franchisenehmer sich dazu entschließt, das Wissen extern weiterzugeben.[172] Der Studie von The Economist zufolge, ist es jedoch fast unmöglich „to get a former licensee to stop production once the licence runs out.“[173] Das große Risiko, dass hier langfristige Konkurrenten entstehen oder Technologiekonzepte nach außen gelangen, muss wohlüberlegt gegen den Vorteil einer Lizenzvergabe abgewogen werden.

[168] Vgl. o.V. (2005c), S. 14.
[169] Vgl. o.V. (2005c), S. 14.
[170] Vgl. Fischer et al. (2002), S. 85.
[171] Vgl. Fuchs (2006), S. 255.
[172] Vgl. o.V. (2005c), S. 18.
[173] o.V. (2005c), S. 15.

3.3.8 Angriffspunkte und Schutzmaßnahmen in der Distributionslogistik

Distributionsaufgaben wie „Lagerung, Kommissionierung, Verladung, Transport und Umschlag der Waren“[174] bergen wiederum Angriffspunkte für Produktpiraten, gegen die man sich schützen muss. Beispiele für die Schwachstellen in der Logistikkette sind unbewachte Zwischenlager, in denen Sendungen umgepackt und manipuliert werden, oder solche Fälle, bei denen Transportführer von der Route abkommen, um unbemerkt Originalteile gegen gefälschte umzuladen.[175] Zwischenlager sind hinsichtlich Produkt- und Markenpiraterie sehr gefährlich, da der Hersteller die Ware in diesem Stadium nur noch schwer kontrollieren kann.

Der *Lagerschutz* muss vom Distributionsdienstleister, der die Ware sicher von der Produktionsstätte zum Kunden bringt, gewährleistet sein. Damit man sicherstellt, dass die Logistikkette keine Schwachstellen aufweist, sollten Sicherheitsmaßnahmen wie abgeschlossene Räume, Zugangsprüfung und Videoüberwachung Standard in den ausgesuchten Lagern sein.[176] Jede Warenbewegung muss genau kontrolliert werden, um das Risiko des Austauschs von Originalwaren zu verhindern. Eck/Fischer und Richter weisen sogar in ihrem Artikel im Harvard Business Manager 1/2002 darauf hin, dass vertraglich abgestimmt werden muss, dass der Logistikdienstleister keine Aushilfsfahrer oder nicht im Vertrag vereinbarte Frachtführer einsetzen dürfen.[177] Hier minimiert Transparenz das Risiko des Angriffs durch Fälscher.

Sendungsverfolgungen (Track und Tracing) gelten als eine verlässliche Lösung, denn sie bieten die Möglichkeit zur Rückverfolgung einer Lieferung. Ein elektronisches System kann den genauen Sendungsverlauf verfolgen. Durch Mitarbeiter oder das Abscannen eines Barcodes, der am Produkt angebracht ist, kann der aktuelle Stand der Ware jederzeit abgefragt werden.[178] Durch solche Technologien entsteht eine gewisse Nachvollziehbarkeit, sodass Unstimmigkeiten in der Route sofort auffallen. Auch diese Kontrollmöglichkeit reduziert das Risiko, Opfer von Produktpiraten zu werden. Vertraglich sollten grundsätzlich Möglichkeiten zur Kontrolle und Stichproben abgestimmt sein.[179]

[174] Fischer et al. (2002), S. 85.
[175] Vgl. Fuchs (2006), S. 252.
[176] Vgl. Fuchs (2006), S. 253.
[177] Vgl. Fischer et al. (2002), S. 85.
[178] Vgl. Fuchs (2006), S. 253.
[179] Vgl. Fischer et al. (2002), S. 85.

Ähnlich wie beim Direktvertriebsbeispiel der Firma DELL versucht man auch bei folgender Schutzmaßnahme, Teile der Lieferkette zu kürzen, um das Risiko eines Angriffs durch Produktpiraten zu mindern: Bei der *Efficient Consumer Response* arbeiten die Händler mit den Herstellern eng zusammen und leiten die Kundenanfragen direkt an den Hersteller weiter. Durch Synergien der beiden Parteien und durch die Schaffung von Standards reduziert sich das Risiko eines Übergriffs drastisch, da „durch die Kooperation […] Potentiale aufgedeckt werden, die bei einer isolierten Betrachtung eines Unternehmens nicht möglich wären."[180] Durch eine Art Just-in-Time-Versorgung verzichtet man auf Zwischenlager und erzeugt so einen nicht unterbrochenen Warenfluss, was Produktpiraten deutlich einschränkt.

3.3.9 Angriffspunkte und Schutzmaßnahmen durch Öffentlichkeitsarbeit und Marketing

Für viele Unternehmen ist „das Thema Fälschung ein Tabu."[181] Der Grund liegt wohl darin, dass sie ihre Kunden nicht verunsichern wollen. Anstatt den Kunden die Problematik bewusst zu machen, schweigen sie aus Angst, die Kunden könnten bei negativen Schlagzeilen gleich auf die Konkurrenz umsteigen.[182] Dadurch erleichtern sie die Arbeit der Fälscher enorm. Dass nicht nur Fälschungen wie z.B. Gucci- oder Prada-Taschen auf der Straße in Urlaubsorten gehandelt werden, sondern auch alltägliche Konsumgüter und Medikamente gefälscht sind, ist vielen Kunden gar nicht bewusst. Indem Firmen diese Tatsachen verschweigen, erreichen sie jedoch oft das Gegenteil.

„There will always be counterfeiters if there is a market for them."[183] Die wohl einfachste Lösung der Problematik wäre der Wegfall des Marktes für Fälscher. Diese Vorstellung ist utopisch, solange Käufer aus diversen Gründen nach dem kostengünstigsten Produkt greifen. Trotzdem können *Werbekampagnen und Veranstaltungen*, in denen noch erheblicher Informationsbedarf gestillt wird, viel zum Kampf gegen die Produktpiraterie beitragen. Die Firma Stihl hat beispielsweise durch Werbekampagnen und offene Kommunikation das Problembewusstsein der Käufer geschärft. Durch diese aktiven Maßnahmen hat das Unternehmen heutzutage „in der Fälscherszene […]

[180] Fuchs (2006), S. 253.
[181] Maass (2006), S. 13.
[182] Vgl. Niggl (2006), S. 17.
[183] Drinkuth (2005), S. 6.

einen negativen Ruf“[184], was zu einer deutlichen Verringerung der Plagiate seiner Produkte geführt hat. Öffentlichkeitsarbeit macht den Kunden auf die Problematik aufmerksam und gibt den Kunden Tipps zur Identifizierung von Fälschungen. Die Zeitung InternetAgent gab im November 2005 Richtlinien heraus, wie man sich beim Kauf von CDs und DVDs aus dem Internet absichern kann.[185] Auch der Geschäftsführer Maximilian Burger-Scheidlin von der Wirtschaftskammer Österreichs erklärt, dass es wichtig sei, den Endverbrauchern zu erklären, dass es bei dem Thema Produktpiraterie nicht nur um den „vorhandenen Lizenzentgang geht, sondern auch darum, dass die Firmen weniger Geld für die Forschung haben.“[186] Mit solchen Einsichten ist vielleicht ein erster Schritt getan, dass sich der Markt für die Fälscher verengt. Auch Franz-Peter Falke, Präsident des deutschen Markenverbands, bestätigt das „mangelnde Unrechtsbewusstsein […] bei den Konsumenten, [welches] laut Umfragen […] besonders bei jungen Leuten kaum ausgeprägt [ist].“[187]

Ein etwas aggressiveres Auftreten sind öffentliche *Zerstörungen von Plagiaten*, bei denen die Fälschungen „planiert, farblich eingesprüht oder in Säure getaucht werden.“[188] Mit großem öffentlichen Interesse werden diese Aktionen verfolgt und dadurch die Bevölkerung sensibilisiert. Solche Handlungen haben eine klare Aussage: Das Unternehmen warnt alle potentiellen Fälscher, ihr geistiges Eigentum zu missbrauchen, und zeigt, dass es bewusst und aktiv gegen Produktpiraterie vorgeht.

Im Marketing kann eine *enge Kundenbindung*, die auf Qualität und Zuverlässigkeit beruht, dazu beitragen, dass sich der Fälschermarkt verkleinert. Da ein Unternehmen nicht auf der Kostenebene mit den Fälschern konkurrieren kann, sollte es den Schwerpunkt auf hochwertige Qualität und kundenspezifische Wünsche legen. Individuell angepasste Produkte z.B. bieten einen sicheren Schutz gegen Kopierer. Die Vorzüge für den Kauf eines Originalproduktes müssen ausreichend kommuniziert und es muss ein Anreiz durch Zusatzleistungen geschaffen werden. „Stil und Atmosphäre des Angebots machen Piraten nicht nach.“[189] Hier gibt es noch großes Potential im Kampf gegen Produktpiraten.

[184] Lupp (2006).
[185] o.V. (2005b), S. 3.
[186] Lorbeer (2005).
[187] Janke (2005), S. 22.
[188] Eggert (2005), S. 41.
[189] Sommer (2006).

Komplementäre Dienstleistungen wie ein Kundendienst sind unerlässlich im Kampf gegen Produktpiraterie. Garantieleistungen sind Angebote, die Fälscher nicht nachmachen können und auf welche viele Kunden großen Wert legen. Alle erdenklichen Zusatzleistungen, wie Schulungen, Hotlines, Beratungen oder Updates, die die Interaktion des Unternehmens mit dem Kunden verstärken, können dazu beitragen, dass der Kunde auf den Fälschungskauf verzichtet.

3.3.10 Schutzmaßnahmen außerhalb der Lieferkette

Einrichtungen und Institutionen wie der Aktionskreis Deutsche Wirtschaft gegen Produkt- und Markenpiraterie (APM e.V.) oder das Aktionsbündnis Plagiarius mit ihrer jährlichen Plagiarius Verleihung tragen dazu bei, das Thema Produktpiraterie noch mehr in das Bewusstsein der Menschen zu rücken und sie über die Ausmaße und Folgen der Problematik zu informieren. Der Plagiarius ist ein Negativpreis, der jährlich an die skrupellosesten Nachahmer verliehen wird und durch seine Medienpräsenz eine hohe öffentliche Wirkung erzielt.[190] Auch die Deutsche Messe hat sich der Problematik angenommen und einen Informationsstand „Messe Frankfurt against Copying" eingerichtet, an welchem sich Unternehmen, die kopiert werden, direkt auf der Messe über weitere Schritte informieren bzw. mit dem am Stand präsenten Zoll Sofortmaßnahmen einleiten können.[191] Neben unzähligen Verbänden[192] beschäftigt sich natürlich die Politik mit diesem Thema. Nicht nur Bundeskanzlerin Merkel setzte das Thema bei ihrer Chinareise auf ihre Prioritätenliste; auch die Europäische Kommission arbeitet eng mit dem Zoll zusammen, um den Schaden zu begrenzen. Auf der europäischen Ebene haben sich die Zollbehörden der Mitgliedsstaaten in der Operation „Codename Fake" untereinander vernetzt. Nach Angaben des Zolls ist die Rate der gefassten Fälscher stark gestiegen, was für eine effektive Schutzmaßnahme spricht.[193] Der Eintritt in internationale und chinesische Verbände sowie politische Maßnahmen der Unternehmen, wie der Beziehungsaufbau zu Regierungsbeamten oder enge Kontakte zu politischen Stellen, sollten im Kampf gegen Produktpiraten nicht fehlen. Ein diplomati-

[190] Lacroix (2006).
[191] Vögele-Ebering (2006) und o.V. (2006g).
[192] Wie beispielsweise die International Anti-Counterfeiting Coalition, die International Intellectual Property Alliance, The Anti-Counterfeiting Group etc.
[193] Fuchs (2006), S. 42.

sches Vorgehen verspricht in China eher Erfolg, da die Chinesen Konflikten lieber aus dem Weg gehen.[194]

Die Produktpiraterie hat ein solches Ausmaß und eine solche Professionalität angenommen, dass es für Unternehmen kaum möglich ist, allein gegen die Fälscher anzukämpfen. Deshalb haben sich *Zusammenschlüsse* von Unternehmen zum Informations- und Erfahrungsaustausch als sehr hilfreich erwiesen. Durch Koordination der einzelnen Maßnahmen werden diese deutlich effektiver.[195] Ein Beispiel ist der Fachausschuss BITKOM, ein Gremium aus internationalen Konzernen, das sich die Aufgabe stellt, Wirtschaft sowie Politik für das Thema Produktpiraterie zu sensibilisieren.[196] Auch das Fraunhofer Institut hat ein „Tekno-Pro Konsortial Projekt" gegründet, welches auf „strategische Maßnahmen, technologische Imitationsbarrieren sowie den gezielten Einsatz von Komplementärkompetenzen"[197] setzt. Synergien zu nutzen, ist in diesen Fällen unbedingt notwendig. Mit der Erfahrung des Fraunhofer Instituts als Basis und der inhaltlichen und finanziellen Unterstützung der Mitglieder sollen unüberwindbare Barrieren, sei es in marktseitiger oder technischer Hinsicht, für die Fälscher geschaffen werden.[198] Selbst Konkurrenten schließen sich beim Kampf gegen Fälscher zusammen. So koordinierten 30 Hersteller von Golfzubehör letztes Jahr zeitgleiche Razzien, wobei mehrere tausend Nachahmungen gefunden wurden.[199] Ein Konsortium hat den Vorteil, schlagkräftiger zu sein sowie finanzielle Mittel durch Synergieeffekte zu sparen, und verringert durch Informationsaustausch negative Erfahrungen.

3.4 Juristische Aspekte

3.4.1 Schutzrechte in China

Um sich mit den juristischen Schutzmaßnahmen zu beschäftigen, ist es sinnvoll, sich vorher mit den vorhandenen Schutzrechten auseinander zu setzen.

Die rasante Entwicklung der Globalisierung aller Wirtschaftszweige und -beziehungen bedingt eine internationale Antwort auf den Schutz des geistigen Eigentums. Nationale Regelungen sind zwar wichtig, reichen bei weitem aber nicht aus, das Problem der

[194] Ballhaus (2005), S.41.
[195] Vgl. Fuchs (2006), S. 299.
[196] o.V. (2005f).
[197] o.V. (2006f), S. 1-4.
[198] Vgl. o.V. (2006f), S. 1-4.
[199] Vgl. Fuchs (2006), S. 300.

Verletzung geistigen Eigentums zu lösen oder zumindest annähernd in den Griff zu bekommen. Einen weltweiten Ansatz bietet die Welthandelsorganisation WTO, die ihre Mitglieder verpflichtet, auf der Grundlage des so genannten TRIPS-Abkommens (Agreement on Trade Related Aspects of Intellectual Property Rights) Schutzrechte einzuführen und deren Verletzungen zu sanktionieren.

China ist der WTO im Jahre 2000 beigetreten und hat im Zuge der Beitrittsverhandlungen seine nationale Gesetzgebung an die Rahmenbedingungen des TRIPS-Abkommens angepasst.[200] Im Gesamtzusammenhang des Schutzes geistigen Eigentums in der VR China sind weitere Mitgliedschaften in internationalen Abkommen von großer Bedeutung. So ist die Volksrepublik China u.a. auch Mitglied in

- der Pariser Verbandsübereinkunft, ein Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens (Patent Corporation Treaty (PTC))[201],
- dem Madrider Markenabkommen (MMA)[202] mit dessen Protokoll[203],
- dem Nizza-Abkommen über die Internationale Klassifikation für die Eintragung der Waren- und Dienstleistungen für die Eintragung von Marken[204], sowie
- dem Straßburger Abkommen für die Internationale Patentklassifikation.[205]

Die nationalen Gesetze und Rechtsvorschriften wurden im Zusammenhang mit dem WTO-Beitritt den Rahmenbedingungen des TRIPS-Abkommens angeglichen. In Form des Subsidiaritätsprinzips haben die Vorschriften der internationalen Abkommen Vorrang vor abweichenden Bestimmungen des nationalen Rechts der VR China (z.B. Patent-, Marken-, Urheberrechtsgesetz oder Gesetz gegen unlauteren Wettbewerb). Voraussetzung für die Geltung der Schutzrechte insgesamt ist, abgesehen vom Urheberrechtsschutz, eine Registrierung in der VR China.[206]

Hinsichtlich des Registrierungsverfahrens und der Schutzdauer unterscheidet man zwischen Patentrechten (Erfindungspatenten, Gebrauchs- und Geschmacksmustern) und Markenrechten.

---

[200] Vgl. Fuchs (2006), S. 167.
[201] Patent Cooperation Treaty (PCT), BGBl. 1970 II, S. 649, 664 mit den Änderungen von BGBl. 1984 II, S. 799, vom 3. Februar 1984 BGBl. II, S. 975 und Änderungen von Art. 22, BGBl. 2002 II, S. 728.
[202] BGBl. 1970 II, S. 293, S. 418; BGBl. 1984 II, S. 799.
[203] Protokoll vom 27. Juni 1989, BGBl. 1995 II, S. 1017.
[204] vom 15. Juni 1957 in der in Genf am 13. Mail 1977 beschlossenen und am 2. Oktober 1979 geänderten Fassung BGBl. 1981 II, S. 358; 1984 II, S. 799.
[205] vom 24. März 1971, geändert am 2. Oktober 1979, BGBl. 1975 II, S. 283; 1984 II S. 799.
[206] Vgl. Fuchs (2006), S. 167ff.

Im Gegensatz zum deutschen Recht, das eigenständige Gesetze für Patente und Gebrauchs- und Geschmacksmuster beinhaltet, gibt es in China nur ein *Patentgesetz*, das jedoch wiederum die unterschiedlichen Patentarten unterschiedlich regelt.[207] So werden Erfindungspatente in China 20 Jahre, Gebrauchs- und Geschmacksmuster 10 Jahre, gerechnet ab Anmeldetag, geschützt.[208] Auch hinsichtlich der Prüfungsintensität wird zwischen dem Erfindungspatent (einer sachlich-materiellen und technischen Prüfung) und den Gebrauchs- und Geschmacksmustern (einer rein formalen Prüfung) differenziert. Die formellen und materiellen Voraussetzungen für eine erfolgreiche Patentanmeldung entsprechen internationalem Standard.[209] Wird einem Antragssteller das Patent zugesprochen und entsprechend eingetragen, so genießt er ein so genanntes Ausschließlichkeitsrecht, d.h. nur er darf das patentierte Erzeugnis herstellen, verkaufen oder ex- und importieren.[210] Dieses Recht verliert er nur bei Lizenzvergaben[211] oder wenn er die Jahresgebühren nicht bezahlt.[212]

Auch das *Markengesetz* der VR China wurde im Zuge des Beitritts Chinas in die WTO entsprechend überarbeitet. Dieses regelt u. a. die Eintragung einer Markenbezeichnung in China nach der Erstanmeldung im Ausland. Es beinhaltet auch, wie im TRIPS-Abkommen gefordert, eine Gleichbehandlung von In- und Ausländern.[213] Die Registrierung der Marke entwickelt ihre Schutzwirkung zunächst für 10 Jahre, kann jedoch jeweils um weitere 10 Jahre verlängert werden. Internationale Markennamen auf der Basis des Madrider Abkommen gelten auch in China, was eine große Zeitersparnis bedeutet.[214]

Ein weiteres Schutzgesetz stellt das *Gesetz gegen den unlauteren Wettbewerb* (UWG) dar.[215] Dieses Gesetz enthält Bestimmungen u.a. über irreführende Markennamen, Fälschung von Marken, Warenzeichen, Herkunftsort, Qualitätsangaben.[216] In Ergänzung zu diesem chinesischen UWG werden auch gesetzliche Bestimmungen zum Schutz des

[207] Vgl. Fuchs (2006), S. 168.
[208] Vgl. Sun (2004), S. 9.
[209] Vgl. Häuslschmid (2004), S. 7.
[210] Vgl. Sun (2004), S. 8.
[211] Vgl. Fuchs (2006), S. 169
[212] Vgl. Häuslschmid (2004), S. 6.
[213] Vgl. o.V. (2006m); Fuchs (2006), S. 170.
[214] Vgl. o.V. (2006n).
[215] Vgl. Häuslschmid (2004), S. 12.
[216] Vgl. Fuchs (2006), S. 179.

Betriebsgeheimnisses erlassen. Der Verletzende muss mit gerichtlichen oder verwaltungsrechtlichen Folgen rechnen.[217]

Einen weiteren Schutz erfahren Produkte und Marken indirekt durch *andere gesetzliche Regelungen* wie z. B. dem Produktqualitätsgesetz.[218] Die dort genannten Anforderungen, wie Produktbezeichnung, Hersteller, Menge und Inhalt sowie Herstellungs- und Ablaufdaten, erfüllen in der Regel gefälschte Waren nicht, sodass auch mit der Verletzung dieses Schutzes Produktpiraterie festgestellt bzw. bekämpft werden kann. Die Einhaltung diesbezüglicher Vorschriften wird von den lokalen Technical Supervision Bureaus überwacht.[219]

In der Praxis stark gemindert werden die Schutzrechte für Produkte und Marken durch die so genannte Erschöpfungswirkung bei *Paralleleinfuhren* von Produkten und Marken. Dies ist ein Verwirkungsrecht[220], wobei noch zwischen nationaler, regionaler und internationaler Erschöpfung unterschieden wird. Dieses im TRIPS-Abkommen nicht angesprochene und damit auch nicht gelöste Problem ist weiterhin Streitpunkt zwischen den Industrie- und Entwicklungsländern wegen der bisher noch unterschiedlichen Interessenlage. Die Industrieländer, die zum großen Teil Inhaber der Schutzrechte sind, plädieren verständlicherweise für eine Erschöpfungswirkung nur im nationalen Rahmen. In Bezug auf China geht es vor allem um die Frage, ob die mit Zustimmung des z. B. europäischen Schutzrechtsinhabers dort hergestellten und vertriebenen Produkte wieder in europäische Länder exportiert werden dürfen oder nicht. Die Frage der nationalen, regionalen oder internationalen Erschöpfungswirkung ist auf internationaler Ebene ungeklärt.[221]

3.4.2 Durchsetzung der Schutzrechte

a) Anmeldung und Eintragung der Schutzrechte

Eine weitere grundlegende Möglichkeit, die in China weit verbreitete Produkt- und Markenpiraterie zu bekämpfen, sind juristische Schutzmaßnahmen.

Voraussetzung für deren Durchsetzung ist es, sich zunächst ein internationales wie national gültiges und wirksames Schutzrecht zu verschaffen. Dafür ist die Registrie-

[217] Vgl. Häuslschmid (2004), S. 14.
[218] Produktqualitätsgesetz verabschiedet am 22.02.1993.
[219] Vgl. Fuchs (2006), S. 178.
[220] Verlust eines Rechts wegen verspäteter Geltendmachung.
[221] Vgl. Fuchs (2006), S. 180 ff.

rung in China erforderlich, die sich damit als entscheidende vorbeugende Maßnahme erweist.[222]

Dem Eintragungsverfahren ist ein Anmeldeverfahren vorgeschaltet, für das das First-to-File-Prinzip gilt, ein so genanntes „Windhundverfahren"; die erste Anmeldung ist relevant. Ausländer mit nicht ständigem Wohn- oder Geschäftssitz in China müssen sich zu ihrer Vertretung einer Patentvertretungsorganisation bedienen. Im anschließenden Eintragungsverfahren wird das angemeldete *Patent* einer Sachprüfung hinsichtlich Neuheit, Stand der Technik u.a. unterzogen. Nach positiver Prüfung wird über das Patent eine Urkunde ausgestellt, deren Inhalt im chinesischen Patentblatt veröffentlicht wird. Damit ist das Patent wirksam und damit auch geschützt.[223] Ein für Ausländer schnelleres und damit zunächst anzustrebendes Verfahren ist die so genannte *Patent Cooperation Treaty*(PCT)-Anmeldung, die für die dem Abkommen beigetretenen Mitgliedsstaaten – wie Deutschland und China – gilt.[224] Auch hier wird eine Sachprüfung vorgenommen, die in einen internationalen Recherchebericht mündet. Bei diesem PCT-Verfahren entstehen zwar zusätzliche Gebühren gegenüber dem Anmeldeverfahren direkt bei der nationalen Patentbehörde; bei einem anschließenden nationalen Verfahren werden die Gebühren jedoch angerechnet. Außerdem bietet das PCT-Verfahren eine Entscheidungshilfe für die Frage, in welchen Ländern ein nationales Registrierungsverfahren angeschlossen werden soll.[225]

Allgemein ist bei der Anmeldung von Patenten die Beantwortung der Frage entscheidend, worauf sich die Schutzwirkung der Registrierung beziehen soll – mehr auf die technischen Neuheiten oder mehr auf beispielsweise das Design.[226] Dabei ist auffällig, dass bei deutschen Anmeldeverfahren eher die Technik des Produktes im Vordergrund steht, während in China mehr Aussehen und Design, also ein *Geschmacksmusterschutz*, von Bedeutung und damit eintragungsrelevant ist. Nicht unproblematisch ist die Tatsache, dass durch das Anmelde- und Registrierungsverfahren wegen seiner Öffentlichkeitswirkung Konkurrenten, Mitbewerber oder potentielle Nachahmer auf Produkte und ihre Besonderheiten aufmerksam werden und eventuell deren eigene Vermarktung geradezu provozieren können.[227] Diese Gefahr muss erkannt und einkalku-

[222] Vgl. Fuchs (2006), S. 184.
[223] Vgl. Fuchs (2006), S. 185ff.
[224] Vgl. Häuslschmid (2004), S. 5.
[225] Vgl. Fuchs (2006), S. 189ff.
[226] Vgl. Häuslschmid (2004), S. 5.
[227] Vgl. Fuchs (2006), S. 192.

liert werden, kann jedoch kaum dazu führen, von einer Registrierung abzusehen, die die Grundlage weiterer juristischer Maßnahmen ist.

Bei der Anmeldung und Eintragung von *Marken* kommt dem Markennamen die entscheidende Bedeutung zu. Wegen der völlig unterschiedlichen Sprache und Begriffe führt eine bloße Übersetzung zu vollständiger Verwirrung und z. B. für die Werbung verheerenden Folgen, wenn korrekt übersetzte Begriffe im Chinesischen eine völlig andere Bedeutung haben.[228] Deswegen ist es für den Schutz eines bestimmten Markennamens unbedingt erforderlich, sich der Unterstützung professioneller Dolmetscher zu bedienen.[229] Um gegenüber potentiellen Markenpiraten Lücken im Markenschutz zu schließen, erscheint es auch aus strategischen Gründen angebracht, von den im Abkommen von Nizza unterschiedenen 42 Klassifizierungsklassen verwandte Klassen in die Markenregistrierung aufzunehmen. [230]

Wie beim PCT-Verfahren ist auch beim Anmelden von Marken nach dem Madrider Markenabkommen (MMA), dem China beigetreten ist, eine erste Anmeldung im Heimatland möglich.[231] Das Verfahren entspricht dem PCT-Verfahren. Deswegen kann darauf verwiesen werden.[232]

b) Verfahren bei Verletzungen der Schutzrechte

Falls die Schutzrechte verletzt und registrierte Produkte nachgemacht werden, muss die Durchsetzung der Schutzrechte erreicht werden. Sollten diese Maßnahmen erfolgreich sein, tragen sie damit zur Schadensminderung bei, indem die Fälschungen unterbunden werden und der Verletzende zur Rechenschaft gezogen werden kann.

Im chinesischen Rechtssystem, zumindest im Hinblick auf das hier interessierende Patent- und Markenschutzrecht, unterscheidet man zwischen gerichtlichen und verwaltungsbehördlichen Verfahren, die nebeneinander stehen.[233]

In dem 4-stufigen *zivilgerichtlichen Gerichtsaufbau* Chinas werden die Verletzungsverfahren gegen Schutzrechte grundsätzlich in der untersten Instanz, dem Basic Court, und die Patentstreitigkeiten wegen ihrer Komplexität im mittleren Gerichtszweig, dem

[228] Vgl. Fuchs (2006), S. 193.
[229] Vgl. Häuslschmid (2004), S. 8.
[230] Vgl. Fuchs (2006), S. 194-195.
[231] Vgl. Häuslschmid (2004), S. 8.
[232] Vgl. Fuchs (2006), S. 198.
[233] Vgl. Fuchs (2006), S. 199.

Intermediate Court, verhandelt.[234] Für das Verfahren zuständig ist der Ort, an dem die Schutzverletzung begangen wurde.[235]

Das *Verwaltungsverfahren* gegen Schutzrechtsverletzungen wird schneller und kostengünstiger abgewickelt, weil diese nicht an die Förmlichkeiten des Gerichtsverfahrens, z.B. die Einführung der Beweismittel, gebunden sind. Sie werden deswegen auch häufiger in Anspruch genommen, vor allem deswegen, weil die Chinesen die Öffentlichkeit der Gerichtsverfahren scheuen. Als Sanktionen können auch die Verwaltungsbehörden in dem Verfahren die Unterlassung der rechtsverletzenden Handlungen, den Entzug der Geschäftslizenz, die Vernichtung der Ware oder des aus dem Verkauf erzielten Gewinns anordnen. Rechtsinhaber wie Verletzender können gegen die Entscheidung ein Gerichtsverfahren einleiten. Das Verwaltungsverfahren leidet zum Teil an mangelnder Objektivität z. B. durch Lokalpatriotismus oder Korruption, d.h. es kann zu einer Interessenkollision innerhalb der Verwaltungsbehörde kommen.[236]

Der *einstweilige Rechtsschutz* der VR China ist zwar nicht deckungsgleich mit der einstweiligen Verfügung des deutschen Rechts, die dafür notwendigen rechtlichen Instrumente sind jedoch vergleichbar. Bei Dringlichkeit wegen Vermögensverlustes, irreparablen Schäden und Gefahr im Verzug kann das Gericht auf Antrag eine sofortige Einstellung der Schutzverletzung beim Antragsgegner anordnen.[237]

Vor jeder Einschaltung von Verwaltungsbehörden oder Gerichten sollte ein *informelles Verfahren* stehen, d.h. bei Feststellung einer Schutzverletzung sollte der Kontakt zum potentiellen Verletzenden hergestellt werden mit dem Ziel, eine einvernehmliche Lösung zu finden.[238] Mit dieser Alternative sind sicher viele förmliche Verfahren zu vermeiden.

Durch den Beitritt zum TRIPS-Abkommen war zwar China verpflichtet, für die Verletzung geistigen Eigentums *strafrechtliche Maßnahmen* vorzusehen. In der gerichtlichen Praxis sind diese Sanktionsmöglichkeiten trotz ausländischem Druck – viele Schutzrechteinhaber sehen darin die einzig wirksame Abschreckung – kaum angekommen. Die Verfahrenszahl ist zu vernachlässigen.[239]

[234] Vgl. Fuchs (2006), S. 200ff.
[235] Vgl. Häuslschmid (2004), S. 10.
[236] Vgl. Fuchs (2006), S. 202ff.
[237] Vgl. Häuslschmid (2004), S. 9f.
[238] Vgl. Fuchs (2006), S. 199.
[239] Vgl. Fuchs (2006), S. 207.

Eine verhältnismäßig neue Variante, Verfahren von Schutzrechten zu behandeln und zu erledigen, sind die *Schiedsgerichtverfahren*,[240] insbesondere vor der China International Economic and Trade Arbitration Commission (CIETAC). Solche Verfahren bieten sich dann an, wenn es dem Schutzrechtsinhaber weniger um die Verletzung eines einzelnen Schutzrechtes geht als darum, seine Stellung im gesamten chinesischen Markt nicht zu beschädigen.[241]

Eines der wichtigsten Verfahren gegen Schutzrechtsverletzungen ist das *Grenzbeschlagnahmeverfahren*, zu dessen Einführung die VR China auch wiederum durch das TRIPS-Abkommen verpflichtet ist. Zur Einleitung des Verfahrens ist die Registrierung des Schutzrechtes erforderlich, das in einem Zollzertifikat dokumentiert sein muss. Auf dieser Grundlage können Zöllner Ladungen inspizieren und vorübergehend zurückhalten. Gegen Sicherheitsleistung kann dann diese Ware beschlagnahmt werden.[242]

Tabelle 2: Entwicklung der Grenzbeschlagnahmeanträge und der Beschlagnahmefälle
Quelle: Bundesministerium der Finanzen (2006a), S. 31.

Jahr	1995	1996	1997	1998	1999	2000	2001	2002	2003	2004	2005
Anzahl	68	92	127	145	168	184	197	221	262	290	**352**
Fälle	506	973	1.368	2.013	2.188	3.178	2.427	3.427	3.461	8.564	**7.217**

Für alle rechtlichen Verfahren, ob Verwaltungsverfahren, zivilgerichtliche, strafrechtliche oder Grenzbeschlagnahmeverfahren mit entsprechendem einstweiligem Rechtsschutz, ist die Beweissicherung das größte Problem. Sie sollte jedoch möglichst frühzeitig nach Bekanntwerden der Schutzrechtsverletzung einsetzen. Zu deren Feststellung wird es notwendig sein, bei Ausstellungen, Messen und für Internetrecherchen Mitarbeiter einzusetzen, bis zur Verpflichtung professioneller Detekteien und Testkäufer, die den gesamten Markt der jeweiligen Branche beobachten. Sie können auch die Kontakte zu den lokalen Behörden herstellen, um die jeweiligen Schutzrechte durchzusetzen.[243]

Zusammenfassend lässt sich sagen: Die rechtlichen Grundlagen der VR China entsprechen internationalem Standard. Deren Durchsetzung ist jedoch aufgrund der dort herr-

[240] Schiedsverfahrensgesetz verabschiedet am 31.08.1994.
[241] Vgl. Fuchs (2006), S. 209.
[242] Vgl. Häuslschmid (2004), S. 12.
[243] Vgl. Fuchs (2006), S. 212ff.

schenden Verwaltungs- und Gerichtskultur problematisch. Lokalpatriotismus sowie Korruption sind weit verbreitet. Eventuell könnten Schadensersatzbestimmungen wie in den USA mit der Festsetzung von zig Millionen bis Milliarden Schadensersatzhöhen eine Abschreckungswirkung erzielen.[244] Dies erscheint jedoch zurzeit illusorisch. Die Prävention gegen Produkt- und Markenpiraterie in China erfordert sicher eine Gesamtstrategie aus juristischen, technischen, politischen, wie vor allem betriebswirtschaftlichen Maßnahmen. Aus juristischer Sicht ist unter dem Aspekt der Prävention eine rechtlich einwandfreie, umfassende, verwandte und Ersatzlösungen ausschließende Registrierung des jeweiligen Schutzrechts erforderlich. Im Falle einer hoffentlich rechtzeitig erkannten Schutzrechtsverletzung müsste unter Zuhilfenahme professioneller Detekteien oder Rechtsanwälten diese im Kontakt mit dem Verletzenden vorgerichtlich geklärt werden. Eine rechtliche Auseinandersetzung, ob im Verwaltungs- oder Gerichtsverfahren, sollte aber nicht ausgeschlossen werden.

3.5 Technische Schutzmaßnahmen

Das bestehende, weitreichende Angebot an sichtbaren, unsichtbaren und maschinengestützten Schutztechnologien ist ein wirksames Mittel gegen Produkt- und Markenpiraterie. Es reduziert das Risiko einer Fälschung beträchtlich, vermeidet Imageschäden und Produkthaftungsprozesse. So können auch im Ausland kostengünstig produzierte Waren gegenüber solchen, die nicht lizenziert gebaut wurden, gesichert werden. Die Bandbreite solcher Verfahren erstreckt sich von optischen und holographischen bis zu integrierten, nicht sichtbaren Verfahren. Da der Schwerpunkt des vorliegenden Beitrags aber auf den betriebswirtschaftlichen Schutzmaßnahmen liegt, sollen die technischen Möglichkeiten nur kurz angeschnitten werden.[245]

3.5.1 Sichtbare Technologien

Hologramme sind die am meisten verwendeten Schutztechnologien und erzielen immer wieder große Erfolge. Im Fall eines bekannten Whiskyherstellers sank der Absatz der Fälschungen nach Einführung eines Hologramms um 15%, wobei vom Originalwhisky 45% mehr verkauft wurde.[246] Hologramme gibt es in Form von Etiketten, La-

[244] Vgl. Fuchs (2006), S. 215.
[245] Mehr dazu in: Fuchs (2006), S. 261ff.; Harte-Bavendamm (2000), S. 35ff.
[246] Harte-Bavendamm (2000), S. 39.

bels, Stickern mit integrierten Selbstzerstörungsmechanismen, Wechselbildern oder Kippfarben. Auch die Hologrammarten sind zahlreich. Ein Standardmodell kostet ca. 8 bis 24 EUR-Cent, was sicherlich der Grund für deren weite Verbreitung ist. Außerdem vermitteln Hologramme dem Kunden das Gefühl von Authentizität. Hologramme erschweren Fälschern das Vorhaben, da sie für die Fälschung von Hologrammen zahlreiche Geräte und Ausrüstungen brauchen. In China jedoch fälschen Produktpiraten selbst Hologramme, das heißt, Sicherheit kann nur noch garantiert werden, wenn man Händlern sowie Kunden genau erklärt, wie das Hologramm des Originalproduktes auszusehen hat.[247]

Optically Variable Devices (OVDs) oder *Diffractive Optically Variable Image Devices* (DOVIDs) sind optisch veränderbare Elemente, die auf der Grundlage von Lichtbeugung wirken. Die Produktsicherung läuft so über Sicherheitslogos, die bei unterschiedlicher Betrachtungsweise die Farbe verändern[248] oder über speziell verzerrte Bilder, die nur mit einem passenden Decoder entschlüsselt werden können. Beliebt ist diese Technologie auch deshalb, weil sie nicht nur Schutz bietet, sondern auch imagefördernd eingesetzt werden kann. Um ein Produktdesign überhaupt nicht beeinträchtigen zu müssen, kann das entsprechende Produkt in Sicherheitsfolie eingehüllt werden, welche jedes unerlaubte Öffnen sofort sichtbar macht. Elemente wie Texte, Daten, Fotos sowie Produkt- oder Garantiecodes können gut lesbar bleiben und sind trotzdem vor Manipulation ausreichend geschützt. Die Prüfung der Folie erfolgt mit einem Handscanner.[249]

Etiketten und Siegel können unbemerktes Öffnen verhindern, indem sich beim Abziehen Muster lösen oder beim Abrubbeln eine Deckschicht beschädigt wird, die nicht wieder in den ursprünglichen Zustand zurückversetzt werden kann. Die Folienstruktur zerfällt und macht so auf die versuchte Manipulation aufmerksam. Auch die starke Haftung hinterlässt Spuren.[250]

Sicherheitstinten sind Flüssigkristalle, die reagieren, wenn versucht wird, gedruckte Angaben zu verändern oder zu löschen. Selbst ein Wechsel des Umfelds kann bei speziellen Tinten eine Reaktion hervorrufen. Sollte versucht werden, ein Duplikat zu erstellen, würde das Licht eines Scanners oder Druckers sofort die ursprüngliche Farbe

[247] Vgl. Fuchs (2006), S. 263-264.
[248] Krüger et al. (2004), S. 5.
[249] Vgl. Fuchs (2006), S. 264-265.
[250] Vgl. o.V. (2006h).

verändern.[251] Materialarten wie Papier, Plastik, Metall oder Glas können mit fluoreszierenden Tinten beträufelt und unter ultraviolettem Licht wieder erkannt werden.[252]

Sicherheitspapier und bestimmte Drucktechniken enthalten Farbkombinationen mit speziellen Schattierungen oder komplexen Wasserzeichen. 3D-Effekte sowie ineinanderfließende Farben und Streifen sind nur einige Besonderheiten dieser Technologie.[253]

3.5.2 Unsichtbare Technologien

„Wie sie sehen, sehen Sie nichts!“[254] Der Slogan des Produktsicherungssystems SECUTAG der Firma Simons Druck+Vertrieb GmbH beschreibt den Ansatzpunkt seines technologischen Schutzsystems gegen Produkt- und Markenpiraterie, welches auf der Basis von *Mikro-Farbcodes* arbeitet. Durch die Schichtung von kleinsten Farbcodepartikeln lassen sich mehrere Milliarden Farbcodekombinationen erstellen, welche nur einem bestimmten Hersteller zugeordnet werden. Vielseitig anwendbar, z.B. als Schutz für Produkte jeglicher Art und jeglichen Materials und sogar als Spezialtinte, gelten diese Farbcodes als absolut fälschungssicher. Zusätzlich kostet diese Sicherheitsmaßnahme nach Angaben des Herstellers nur ein Zehntel EUR-Cent.[255]

Bei einer Fälschungsschutztechnologie wird *Desoxyribonukleinsäure* (Desoxyribonucleid Acid, DNA), welche auch die menschlichen Erbinformationen bestimmt, künstlich erzeugt. Sie wirkt wie ein individueller Fingerabdruck.[256] Die Kettenmoleküle der DNA bieten unzählige Kombinationsmöglichkeiten. Mit einem Stift, welcher das eine DNA-Stück enthält, fährt man über das Etikett, welches das andere DNA-Stück enthält. Nur bei der richtigen Kombination leuchtet das System, da es zum Schloss (Etikett) nur einen einzigen Schlüssel (Stift) gibt.[257]

Die *Nanotechnologie* ist die Basis für immer kleinere Datenspeicher mit enormer Speicherkapazität, da ein Nanometer nur einem Milliardstel Meter entspricht. Von einem nanooptischen Siegel spricht man, wenn Materialien mit einem speziellen Metallcluster beschichtet sind, einem mehrschichtigen Spektralcode, der durch seine speziel-

[251] Vgl. Fuchs (2006), S. 267.
[252] Vgl. o.V. (2006i).
[253] Vgl. Fuchs (2006), S.268.
[254] o.V. (2004a).
[255] Vgl. o.V. (2004a).
[256] Vgl. o.V. (2006j).
[257] Vgl. Fuchs (2006), S. 271.

len Farbwechseleffekte zu identifizieren ist. Dieses Siegel ist gegen chemische, physikalische und Temperatureinflüsse geschützt.[258]

Die *Isotopenanalyse* kann verlässlich die Herkunft eines Produkts bestimmen, wenn dieses Isotope, d.h. verschiedene regional unterschiedliche Varianten eines Atoms, aufgenommen hat. Das Verhältnis der Atome eines Isotops ist an jedem Ort aufgrund der Umweltfaktoren anders zusammengesetzt. Die Technologie ist sozusagen ein Fingerabdruck des Ursprungslandes.[259]

Mit Hilfe chromogener, d.h. *farbstoffbildender Systeme* können Produkte ebenso fälschungssicher geschützt werden. Diese verändern sich optisch als Reaktion auf Umweltfaktoren, wie z. B. Temperatur, Licht, Druck oder Spannung.[260] Sicherheitspapier enthält eine Beschichtung, die mit Sicherheitsfeatures versehen ist und so durch einen Test eine farbliche Reaktion hervorruft. Sicherheitstinten funktionieren ähnlich. Kontakt mit Licht oder Wärme ruft eine farbliche Reaktion hervor, die es erlaubt, Originalware deutlich von Fälschungen zu unterscheiden. [261]

3.5.3 Maschinengestützte Technologien

Radio Frequency Identification System (RFDI) heißt übersetzt „Identifikation per Funk.“[262] Mittels Radiowellen können Daten durch einen Computerchip mit Antenne (Transponder), der am Produkt befestigt ist, übertragen werden. Ihren Bedeutungszuwachs hat die Technologie sicher aufgrund vieler Vorteile, wie berührungsloses Lesen, der Veränderung von Informationen infolge eines Identifikationsprozesses und dem gleichzeitigen Übertragen von mehreren Datenmengen ohne Sichtkontakt. Je nach Lesegerät können innerhalb einer Sekunde Paletten mit bis zu 50 Artikeln erfasst werden.[263] So können innerhalb kürzester Zeit Fälschungen aussortiert werden.

Intelligente elektronische Etiketten auf der Basis der oben beschriebenen RFID-Systeme wären weiter verbreitet, wären sie nicht so kostspielig. RFID-Technik mit Sensorfunktionalität kann z.B. Medikamentenpackungen nicht nur kennzeichnen, sodass das Produkt von Fälschungen zu unterscheiden ist, sondern sogar durch die Aufschrift „gut“ oder „schlecht“ alarmierend auf das Verfallsdatum hinweisen. Die Senso-

[258] Vgl. Bundesministerium für Bildung und Forschung (2006).
[259] Vgl. Fuchs (2006), S. 273.
[260] Vgl. Seeboth (2006)
[261] Vgl. Fuchs (2006), S. 274.
[262] Prahl (2006), S. 1.
[263] Vgl. Huber (2006), S. 1-2; Prahl (2006), S. 1-2.

ren bieten damit Produktsicherheit, da sie sogar mit Temperatursensoren erkennen können, wenn beispielsweise die Kühlkette unterbrochen wurde.[264]

Tesa-Klebestreifen werden als Datenträger genutzt, weil sie eine hohe Speicherkapazität aufweisen. Somit können Informationen direkt am Produkt angebracht werden. Eine Rolle des Tesafilms hat das Fassungsvermögen von 15 CD-ROMs.[265]

Die Identifikation von Produkten über *Barcodes* ist weit verbreitet. Ein Code wird aus Strichen und Lücken, die parallel nebeneinander liegen, erzeugt. Die Beschriftung mit den Codes gilt als preiswert und deshalb sind sie auf fast allen Alltagsprodukten vorhanden. Sie erfassen eine Speicherkapazität von mehr als 100 Bytes und können so klein sein, dass man sie weder spüren noch sehen kann.[266]

Die zunehmende Verbreitung von Produkt- und Markenpiraterie ist zum großen Teil auch auf die Expansion des Internets zurückzuführen. So genannte *Netz-Detektive* durchsuchen das Internet nach Schutzrechtsverletzungen und werden oft durch auffällige Preisspannen zum Originalprodukt und durch nicht autorisierte Händlern auf Plagiate aufmerksam. Digitale Auktionshäuser wie Ebay sind besonders gefährdet. Stößt die Software auf Unstimmigkeiten, schlägt sie Alarm und ein Mitarbeiter des Internet-Monitoring-Dienstleisters geht der Auffälligkeit nach.[267]

Bei der Technik, die *digitale Wasserzeichen* verwendet, werden Druckdaten unsichtbar verändert, sie sind aber trotzdem maschinenlesbar. Durch die Veränderung entsteht ein individuelles Bild, das vielfältige Informationen enthält und zum Kunden direkt zuzuordnen ist. Zur Überprüfung des Herstellers können Scanner oder Digitalkameras, die mit einer speziellen Software versehen sind, verwendet werden.[268]

Ein Schutz, der für den Fälscher zwar unsichtbar ist, das Produkt aber vor Nachahmung bewahrt, ist der *Selbstzerstörungsmechanismus*. Wenn der Fälscher versucht, ein so geschütztes Gerät auseinanderzubauen, zerstört es sich selbst oder zumindest wesentliche Komponenten, sodass es nicht mehr funktionsfähig ist. Der Nachteil dieser Technologie ist jedoch ihr Preis.[269]

[264] Vgl. Ebberg/Menges (2006), S. 31-33.
[265] Vgl. Link (1999), S. 44-46.
[266] Vgl. Fuchs (2006), S. 279.
[267] Vgl. Fuchs (2006), S. 283.
[268] Vgl. Fuchs (2006), S. 285-286.
[269] Vgl. Drinkuth (2005), S. 26.

3.5.4 Kombinationen von Technologien

Nachdem der Güter- und Warentransport heutzutage weltweit vernetzt ist, muss zur Optimierung, aber auch zur wirtschaftlichen und sicherheitstechnischen Überprüfung der Transport- und Handelsweg der Ware überwacht werden. Dazu hat man Überwachungstechnologien wie *Tracking und Tracing* entwickelt: Die Ware wird mit einem individuellen Code versehen, wodurch jeder Schritt zurückverfolgt werden kann. Diese Rückverfolgung in der Lieferkette kann durch viele der oben genannten Technologien wie einen Barcode oder durch ein RFID-Etikett und auch Global Positioning System(GPS)-Technologie erfolgen. Schutz vor Produktpiraterie wird dadurch geboten, dass Verzögerungen oder Umleitungen der Ware sofort erkannt werden. Der Status des Produktes wird hierbei ständig überwacht.[270]

Bei allen besprochenen Technologien muss in Betracht gezogen werden, dass die Kosten verhältnismäßig zum Ergebnis des Schutzes sind. Natürlich gilt: Je komplexer und größer die Kombinationen der genannten Schutztechnologien sind, desto höheren Schutz bieten sie und desto geringer ist das Risiko von Fälschungen. Bedeutend sind die Schutzmaßnahmen deshalb, weil sie zum einen präventiv Fälscher davon abhalten, Produkte nachzuahmen. Zum anderen können sie im Falle eines Produkthaftungsprozesses beweisen, dass das besagte Produkt gar nicht vom Originalhersteller stammt.

4 Experteninterviews

4.1 Methodologie

4.1.1 Erhebungsmethode

Um das Phänomen Produkt- und Markenpiraterie nicht nur theoretisch zu beschreiben, wird im Folgenden das untersuchte Thema mit praktischen Beispielen aus Unternehmensgesprächen beleuchtet. Dadurch werden die aufgestellten Schutzmaßnahmen abschließend durch eine kleine empirische Untersuchung auf ihre praktische Relevanz überprüft.

Der Schwerpunkt des vorliegenden Beitrags lag auf der Erarbeitung der wesentlichen Ursachen und betriebswirtschaftlichen Maßnahmen zur Abwehr von Produkt- und Markenpiraterie. Bedingt durch diesen vorgegebenen Rahmen wird keine große reprä-

[270] Vgl. Hoffknecht/Teichert (2006), S. 75.

sentative Studie zur Verifizierung durchgeführt, jedoch sollen durch Interviews erste Tendenzen und Trends aufgezeigt und interpretiert werden.

Der Einsatz der qualitativen Interviewtechnik bietet den Vorteil der offenen Befragung, um einen Einstieg in den Themenkomplex zu bekommen. Qualitative Verfahren sind neben quantitativen Verfahren eigenständige Methoden zur Datenerhebung und Datenauswertung. In der qualitativen Forschung geht man im Gegensatz zur quantitativen Methode, die eine große Zahl von Befragungen voraussetzt, von kleineren Stichproben aus. Die qualitative Befragungstechnik hat den Vorteil, inhaltliche Phänomene genauer zu erfassen, indem versucht wird, mit intensiven Einzelgesprächen komplexe Strukturen aufzudecken und somit stärker in die Tiefe zu gehen. Dabei stehen die subjektiven Einschätzungen der Interviewpartner im Vordergrund. Mit persönlichen Einzelinterviews wird eine vertraute Gesprächsatmosphäre erreicht, die den Abbau von Hemmschwellen fördert.[271] Diese Vorgehensweise garantiert eine gewisse Vertrauensbasis, bei der sich der Befragte nicht ausgehorcht fühlt. Außerdem kann der Interviewer im persönlichen Kontakt überprüfen, ob die Fragestellung richtig verstanden wurde, was wiederum zu exakteren und ehrlicheren Ergebnissen führt.[272] Aufgrund des kleinen Stichprobenumfangs in dieser Untersuchung führen die Ergebnisse zu keiner repräsentativen Aussage.

4.1.2 Datenerhebung und Durchführung

Untersucht wurden im vorliegenden Beitrag Unternehmen, die die unterschiedlichsten Erfahrungen mit Produkt- bzw. Markenpiraterie gemacht haben. Durch die relativ kleine Anzahl an Interviews können die Ergebnisse nicht die Einschätzung der gesamten Wirtschaft in Deutschland wiedergeben, sondern beleuchten eher einen kleinen Auszug. Die Varianz der Unternehmen erlaubt eine gewisse Bandbreite an Erfahrungen, um generelle Trends aufzuzeigen. Bei der Suche nach Unternehmen für die Befragung hat man sich auf das Auswahlkriterium „Industriegüter deutscher Unternehmen“ beschränkt. Bedingt durch ähnlich tiefe Wertschöpfungsketten bei Industriegütern sind die gewählten Unternehmen sehr gut zu vergleichen, auch wenn sie sich in Mitarbeiterzahl und Unternehmensumsätzen deutlich unterscheiden. Ein breites Portfolio an Unternehmen verschiedener Größenordnung wurde gewählt, um aufzeigen zu

[271] Diekmann (2000), S. 445.
[272] Vgl. Mayring (1993), S. 69.

können, dass sich Tendenzen zur Produkt- und Markenpiraterie nicht nur auf den Mittelstand oder die Großindustrie konzentrieren. Eine Beschränkung auf einen Industriezweig ist unabdingbar. Schutzmaßnahmen greifen in jedem Sektor unterschiedlich, daher sind allumfassende Aussagen nicht möglich.

In Internetrecherchen und durch diverse Anfragen an Organisationen, die sich mit diesem Thema beschäftigen, wurden 30 Unternehmen gefunden, die die oben genannten Kriterien erfüllen. Bedingt durch die Sensibilität des Themas gab es nur einen geringen Rücklauf auf die Anfragen. Manche Firmen erklärten offen, dass sie firmenfremden Personen keine Auskünfte zu diesem Thema gäben. Sechs Unternehmen erklärten sich letztendlich bereit, an der Befragung teilzunehmen, die in Tabelle 3 kurz vorgestellt werden. Zur Wahrung der Anonymität werden die Unternehmen mit 1 (U1) bis 6 (U6) bezeichnet.

Als Interviewtechnik wurden so genannte Experteninterviews gewählt. Als Experten bezeichnet man Menschen, die „über ein besonderes Wissen verfügen [bzw.] aufgrund ihrer Position über besondere Informationen verfügen“[273], die für die Befragung relevant sind. Da es die Aufgabe des Experteninterviews ist, dieses Wissen zu ermitteln, sind Einzelbefragungen zweckmäßig.[274]

Die Experten waren im vorliegenden Fall Leiter bzw. Referenten der Patentabteilung, ein geschäftsführender Gesellschafter, ein GM Asia-Pacific und ein Vertriebsleiter. Die Befragungen wurden in einstündigen persönlichen Gesprächen oder aus Entfernungsgründen am Telefon oder per E-Mail durchgeführt.

Gestützt werden die Interviews auf einen Fragebogen (Vgl. Anhang 3). Der Fragebogen dient als Hilfestellung, damit eine gewisse Vergleichbarkeit möglich ist.[275] Die Fragebogenkonzeption besteht aus zwei Teilen, einem Teil mit offenen, dem anderen mit geschlossenen Fragen, die in der traditionellen Interviewtechnik so nicht zusammen auftreten. Einige Autoren schätzen jedoch die Verbindung der quantitativen und qualitativen Methoden zur Verbesserung der Ergebnisse.[276] In dem hier vorliegenden Fragebogen enthält der eine Teil offene Fragen, bei denen während des Interviews nach der qualitativen Interviewtechnik die Formulierung sowie die Reihenfolge der Fragestellungen nicht verbindlich sind. Im Gespräch können auch Fragen, die nicht im

[273] Gläser/Laudel (2004), S. 9.
[274] Vgl. Gläser/Laudel (2004), S. 41.
[275] Vgl. Diekmann (2000), S. 446.
[276] Vgl. Oswald (1997), S. 71 ff.

Leitfaden vorkommen, gestellt werden, was zu neuen Erkenntnissen führen kann.[277] Im vorliegenden Fall werden mögliche Erfahrungen mit Produkt- und Markenpiraterie sowie Erfahrungen und Handhabungen angewendeter Schutzmaßnahmen erfragt.

Der zweite Teil beinhaltet geschlossene Fragen mit vorgegebenen Antwortmöglichkeiten, die die Experten je nach Einschätzung ankreuzen müssen. Zum einen muss eine Schätzung abgegeben werden, worauf sich potentielle Schäden durch Fälschungen verteilen. Der Schwerpunkt dieses Teils liegt auf der Untersuchung der erarbeiteten Schutzmaßnahmen nach den Parametern Wirksamkeit und Durchführbarkeit. Dort soll gezeigt werden, ob die einzelnen Schutzmaßnahmen auch in der Praxis realisierbar sind. Je nach Höhe der Wirksamkeit oder Durchführbarkeit müssen Noten von eins bis vier vergeben werden. Um zu verstehen, warum manche Schutzmaßnahmen nicht realisierbar sind, wurde in einer abrundenden Frage nach den Hemmnissen der Durchführbarkeit gefragt.

4.1.3 Auswertungsmethode

Da die auszuwertende Datenmenge nur sehr gering ist, ist eine Auswertung mit aufwendigen computergestützten Verfahren nicht nötig. Die Antworten der offenen Fragen werden zusammengefasst und mit dem vorgestellten Wissen kombiniert und interpretiert. Daraus werden nach jedem Abschnitt Handlungsempfehlungen formuliert. Von den Ergebnissen der geschlossenen Fragen wird der Durchschnitt der einzelnen Schutzmaßnahmen nach den Parametern Wirksamkeit und Durchführbarkeit gebildet. Diese Ergebnisse werden in einem Schaubild geordnet nach den Bereichen der Wertschöpfungskette dargestellt. Dies dient zur Erkennung grober Trends in den Teilbereichen der Wertschöpfungskette. Die auffälligsten Ergebnisse und Korrelationen werden in einem Text einheitlich verbalisiert:

- 1.0: sehr wirksam/sehr gut durchführbar;
- 1.0-2.5: eher wirksam, eher durchführbar;
- 2.5: mittelmäßig;
- 2.5-3.0: eher unwirksam/eher schlecht durchführbar;
- 3.0-4.0: unwirksam, nicht durchführbar.

Die Tabelle mit den genauen Werten befindet sich in der Tabelle in Anhang 2.

[277] Vgl. Gläser/Laudel (2004), S. 39.

4.2 Auswertung und Interpretation der Experteninterviews

Da die empirische Untersuchung nicht nur auf Unternehmen abzielt, die Erfahrungen mit Produkt- und Markenpiraterie gemacht haben, sind auch zwei Unternehmen in der Studie vertreten, die aufgrund von Nachahmungen in der Vergangenheit noch keine Schäden davon getragen haben. Erfahrungen einzelner Unternehmungen wurden bewusst nicht als Ausschlusskriterium angesetzt, da der Schwerpunkt der Befragung auf Basis der Einschätzungen der interviewten Personen liegt. Sie sollen als Experten aufgrund ihrer gesamten Erfahrungen und ihres Wissens zu diesem Thema dienen und nicht nur als Unternehmensvertreter in Bezug auf die Handlungsformen des Unternehmens fungieren. Eine anonymisierte Übersicht der Unternehmen gibt Einblick in die befragten Unternehmen:

Tabelle 3: Details der befragten Unternehmen – anonymisiert
Quelle: eigene Darstellung.

	(U1)	(U2)	(U3)
Produktbereich	Maschinenbau	Maschinenbau	Maschinenbau
Mitarbeiterzahl	90	300	800
Umsatz (in EUR)	30.000.000	k. A.	130.000.000
Tätigkeit in China	Fertigung nach wenigen Monaten geschlossen	Beschaffung	Vertrieb und Service
Position Befragter	Vertriebsleiter	Geschäftsführender Gesellschafter	GM Asia Pacific
	(U4)	**(U5)**	**(U6)**
Produktbereich	Maschinenbau	Maschinenbau	Kraftfahrzeug-, Industrie-, Gebäudetechnik, Gebrauchsgüter
Mitarbeiterzahl	3.800	7.000	251.000
Umsatz (in EUR)	380.000.000	750.000.000	41.500.000.000
Tätigkeit in China	Fertigung, Vertrieb und Service	Fertigung	Fertigung und Vertrieb
Position Befragter	Leiter Patente und Lizenzen	Leiter Revision und Patentabteilung	Referent, Corporate Intellectual Property-Trademarks

4.2.1 Firmenerfahrungen mit Produkt- und Markenpiraterie

Von den sechs befragten Unternehmen hatten zwei Unternehmen in der Vergangenheit noch keine, vier Unternehmen jedoch Probleme mit Produkt- und Markenpiraterie. Die Unternehmen, die schon mit Fälschungen zu kämpfen hatten, berichten über die ganze Palette der Produkt- und Markenpiraterie. Bei einigen wurde ihr Produkt kopiert und

als eigenes Produkt angeboten, bei anderen wurden Kopien mit dem Originalnamen vertrieben oder es wurde nur die Verpackung gefälscht und so neu entwickelte Produkte unter dem Namen des Originalherstellers verkauft.

Vor dem Hintergrund der vergangenen Erfahrungen werden in der gegenwärtigen Strategie wichtige Überlegungen zu dieser Problematik angestellt. Nach Meinung eines Unternehmensvertreters gibt es aktuell nur im Bereich des Markenrechts Chancen zur Bekämpfung. Dagegen sieht er aufgrund der chinesischen Regierung keine Handhabe bei Produktpiraterie, da diese immer zum Vorteil der eigenen Wirtschaft entscheiden würde, was die zuvor beschriebene Problematik bestätigt.[278] Ein Unternehmen hat gerade sein Joint Venture aufgelöst, da man ihm einen Spion in die Firma gesetzt hatte. Diese Entscheidung sei notwendig geworden, nachdem es auf Messen Nachbauten seiner Geräte gefunden habe. Es produziert wiederum nur noch in Deutschland.[279]

Gefragt nach der zukünftigen Bedeutung des China-Geschäftes ergab sich ein geschlossenes Bild: Alle Befragten sehen ihre Unternehmen überproportional gefährdet, da sie z.B. zunehmend Marktanteile gewinnen und somit für den Nachbau immer attraktiver werden.[280] Auch in der Zukunft steigt die Forderung nach China-Investitionen, dennoch müssen sich die Unternehmen „gedulden (min. 5 Jahre) bis die Chinesen es verstehen, dass mit Kopieren kein Vorteil erwirtschaftet werden kann."[281]

Die Frage nach konkreten Erfahrungen bzw. Einschätzungen hinsichtlich des Gefährdungspotenzials ergab nach Auswertung der Antworten zusammenfassend deutlich, dass der Schutz von Produktideen und Produktions-Know-how in der Vergangenheit eher niedriger bewertet wurde, in der gegenwärtigen China-Strategie jedoch eine immer größere Rolle spielt und insgesamt alle sechs Unternehmen die Nachahmproblematik in der Zukunft als überproportionales Risiko im China-Geschäft einschätzen. Selbst Unternehmen, die in der Vergangenheit noch nie mit Fälschungen konfrontiert waren, unterstreichen die Brisanz und haben eine Absicherung als festen Bestandteil in ihrer China-Strategie verankert bzw. vorgesehen.

Gefragt nach ihrer allgemeinen Einschätzung, ob das Sicherheitsrisiko in China oder der Nutzen einer Investition überwiege, antworteten alle Unternehmen, dass das The-

[278] U4: Leiter Patente und Lizenzen (23.10.2006).
[279] U1: Vertriebsleiter (30.10.2006).
[280] U3: GM Asia Pacific (24.10.2006).
[281] U4: Leiter Patente und Lizenzen (23.10.2006).

ma Produkt- und Markenpiraterie in China eine permanente bzw. zunehmende Bedrohung und damit im China-Geschäft immanent sei. Dies könne jedoch nach Aussagen der Mehrheit der Unternehmen nicht der Grund sein, nicht in China zu investieren. Durch die Globalisierung und dem daraus resultierenden stärkeren Wettbewerb sei der Gang nach China – sei es aus Produktions-, Vertriebs- oder Beschaffungsgründen – unabdingbar. Nur ein Unternehmensvertreter berichtete, dass sein Unternehmen seine Produktion in China nach 15 Monate schließen musste, weil seine Produkte gefälscht wurden. Dieses Unternehmen entschied sich lieber dafür, auf das Niedriglohnland China zu verzichten, anstatt weiteren Fälschern zum Opfer zu fallen.[282] Im Großen und Ganzen kommt die Ohnmacht der Unternehmen immer wieder zur Sprache, ein Interviewpartner, der seit zehn Jahren regelmäßig nach China kommt, äußerte, es sei „haarsträubend […], mit welcher Dreistigkeit kopiert wird."[283]

Im Folgenden werden die wichtigsten Erkenntnisse zusammengefasst und Handlungsvorschläge gemacht:

- Das Bewusstsein für das Gefährdungspotential hat zugenommen, muss aber noch weiter ausgebaut werden.
- Mit der Unternehmensexpansion steigt auch der Handlungsbedarf im Bereich der Schutzmaßnahmen.
- Eine fühlbare Ohnmacht der Unternehmen in China macht sich breit; dieser sollte entgegengewirkt werden.
- Die Forderung nach einer Änderung der chinesischen Grundeinstellung in Bezug auf Fälschungen wird deutlich.
- Die Vorteile und Nachteile (Kosten-Nutzen-Analyse) einer China-Investition müssen abgewogen werden.

4.2.2 Ausmaß der Fälschungsrisiken und -schäden

Auch wenn diese Ergebnisse nicht als repräsentativ auszuwerten sind, ist doch ein deutlicher Trend über den potentiellen Umfang der Risiken und Schäden zu spüren. Hier ist es wichtig, nur einen Industriezweig zu sehen, da diese potentiellen Schäden stark von der Branchenzugehörigkeit und dem Produkttyp abhängen. In der unten stehenden Abbildung kann man die Gesamtmeinung der befragten Unternehmen über die

[282] U1: Vertriebsleiter (30.10.2006).
[283] U3: GM Asia Pacific (24.10.2006).

Ausmaße der Risiken und Schäden ablesen. Dabei stehen in der Mitte des Netzes das Risiko bzw. der Schaden auf Null, die äußeren Ecken des Netzes stehen für ein sehr hohes Risiko bzw. einen sehr hohen Schaden.

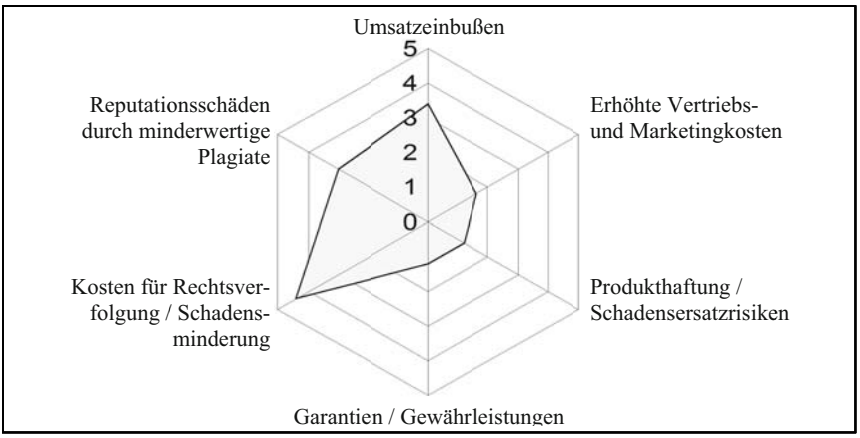


Abbildung 2: Ausmaß der Risiken und Schäden für das Unternehmen bei Fälschungen
Quelle: eigene Darstellung, in Anlehnung an: Fischer/Eck/Richter (2002).

Wie in der Abbildung 2 sichtbar sind die potentiellen Mehrkosten durch erhöhte bzw. zusätzlich notwendig gewordene Vertriebs- und Marketingmaßnahmen sowie Produkthaftungsansprüche und Garantieleistungen im unteren Bereich anzusiedeln. Dies lässt sich darauf zurückführen, dass die befragten Unternehmen ausschließlich aus dem Industriegüterzweig kommen. Die genannten Schäden bzw. Risiken sind wahrscheinlich eher im Konsumgüterbereich angesiedelt, da man die Reduzierung des Fälschungsschadens eher beim Endverbraucher durch Vertriebs- und Marketingmaßnahmen erreichen kann als in einer Business-to-Business(B2B)-Geschäftsbeziehung.

Der Schaden durch Umsatzeinbußen liegt im mittleren bis oberen Bereich. Eine Ursache hierfür könnte sein, dass nicht alle befragten Unternehmen Erfahrungen mit Fälschungen haben. Die Unternehmen, die hier einen geringen Schaden sehen, geben an, bis jetzt noch keine großen Umsatzverluste gemacht zu haben, deuten jedoch an, dass die Gefahr mit der steigenden Professionalität der Fälscher zunehmen werde.

Vergleichbar mit der Auswertung bei der Kategorie Umsatzeinbuße ist die Meinung über Reputationsschäden durch minderwertige Fälschungen. Verhältnismäßig hoch

sehen die Unternehmen hier das Risiko einer Imageverschlechterung durch Fälschungen. Im Industriegüterbereich fallen Nachahmungen jedoch schneller auf, da der Markt sehr viel kleiner ist als beispielsweise im Konsumgüterbereich. So kann mit der Bekämpfung schneller begonnen werden, was einen Zeitvorteil schafft.

Eindeutig ist, dass fast alle Unternehmen derzeit das größtmögliche Kostenrisiko in der Rechtsverfolgung bzw. der Schadensminderung sehen. Dies zeigt unter anderem die noch immer schlechte Durchsetzungsmöglichkeit der Schutzrechte bei den chinesischen Behörden und Gerichten. Auffällig ist, dass die Unternehmen, obwohl sie hier den größten potentiellen Schaden sehen, sich durch die beschriebenen Maßnahmen der Krisenprävention nur unzureichend absichern. Hier besteht immer noch massiver Aufklärungsbedarf über das Gefahrenpotential der Produkt- und Markenpiraterie. Das Bewusstsein der Unternehmen muss in diesem Punkt noch weiter geschärft werden.

4.2.3 Erfahrungen mit Schutzmaßnahmen

Nur einer der Interviewten gab an, dass in seiner Firma keinerlei Schutzmaßnahmen getroffen seien und es noch nie zu Vorfällen mit Fälschungen gekommen sei. Interessant ist, dass diese Firma im Vertrieb und Service in China tätig ist. Statt auf andere Schutzmaßnahmen setzt diese Firma auf hohe Innovationsgeschwindigkeit sowie Zusatzleistungen und erneuert alle zwei Jahre ihr Produktportfolio. Nach Meinung des Firmenvertreters sei dies die einzige Lösung, da man sich so „einen gewissen Abstand zu den Kopierern hält."[284] Die Gefahr, dass der Fälscher ein Auslaufmodell kopiert, ist immer da und kann evtl. auch dem Unternehmen langfristig schaden, wenn sich das Nachfolge- vom Vormodell nicht wesentlich unterscheidet.

Die anderen befragten Unternehmen haben alle juristischen Schutzmaßnahmen wie Patent-, Markenschutz-, und Gebrauchsmusterschutzanmeldungen in ihrer Strategie berücksichtigt. Zwei kleinere Unternehmen haben zwar den Markenschutz, nicht aber Patentanmeldungen der einzelnen Produkte, weil im Falle von Produktpiraterie die Patentanmeldungen meist nichts nützen, da die Durchsetzung der Schutzrechte in diesem Bereich in China – wie schon oben beschrieben – sehr dürftig ist.

Betriebswirtschaftliche Schutzmaßnahmen sowie Geheimhaltungsklauseln oder spezielle Vertragsgestaltungen sind in den meisten Unternehmen fester Bestandteil. Viele Vorschläge wie Qualitätskontrollen, selektive Einstellung oder Vertriebsmaßnahmen

[284] U3:GM Asia Pacific (24.10.2006).

zur Kundenbindung sind aus anderen betriebswirtschaftlichen Gründen, nicht aber speziell zur Bekämpfung von Produkt- und Markenpiraterie in den Unternehmen integriert. Deshalb ist hier eine genaue Abgrenzung sehr schwierig. Da die betriebswirtschaftlichen Schutzmaßnahmen gegenüber den juristischen ein eher neuer Ansatz sind, beginnen die Firmen sich erst jetzt mit dieser Art der Absicherung zu beschäftigen, bekunden aber großes Interesse und beabsichtigen zum Teil deren Umsetzung in naher Zukunft.

Bei der Absicherung durch technische Maßnahmen zeigt sich das Bild der Unternehmensvertreter weniger geschlossen: Drei der sechs befragten Unternehmen benutzen technische Hilfsmittel zur Sicherung ihrer Produkte gegen Fälscher. Den größten Teil an technischen Schutzmaßnahmen geben die Unternehmen für sichtbare Technologien aus. Das deutet darauf hin, dass die befragten Firmen diese eher aus Marketinggründen als aus Gründen der Rechtsverfolgung einsetzen. Sicherheitsetiketten auf dem Produkt oder integriert in die Verpackung dienen somit nicht nur zur Identifikation des Originalproduktes, sondern sollen durch das „Echtheitssiegel" die Qualität und somit das Image der Firma hervorheben. Unsichtbare Technologien haben keinen Einfluss auf den Kunden, sondern sind lediglich zur Identifikation bei Schadensersatzansprüchen, Grenzbeschlagmaßnahmen oder als Beweis vor Gericht notwendig. Laut einer VDMA-Umfrage[285] setzen nur 10% der Unternehmen im Maschinenbau technische Schutzmaßnahmen ein, ein deutlich geringerer Anteil als bei der Anmeldung juristischer Schutzrechte, was wiederum das Ergebnis der hier durchgeführten Befragung bestätigt. Als Grund geben die im Rahmen des Beitrages Befragten die finanziellen Aufwendungen an. In der Umfrage des VDMA wird das Fehlen geeigneter technischer Mittel speziell für den Maschinenbau angeführt.

Die Unternehmen geben außerdem an, dass sie die Einführung von Schutzmaßnahmen jeglicher Art entweder präventiv oder als Reaktion auf eingetretene Fälschungen unternommen haben. Mit rechtlichen Maßnahmen wie Patent- oder Markenschutzanmeldungen bereiten sich die meisten Unternehmen präventiv auf mögliche Übergriffe vor, also nicht speziell wegen eines potentiellen China-Geschäfts, sondern im Rahmen einer allgemeinen Anmeldung durch die Patentabteilung. Eine Gesamtstrategie von betriebswirtschaftlichen, juristischen und technischen Maßnahmen überlegen sich die wenigsten Unternehmen präventiv. Wie bereits erwähnt, reagierte eine Firma mit

[285] o.V. (2006k).

Schließung ihrer Produktion in China. Ob eine umfassende präventive Gesamtstrategie ein Unternehmen vor einem solchen Schritt bewahren könnte, muss jedoch von Fall zu Fall bewertet werden. Externe Hilfe nehmen die meisten Unternehmen an, dann jedoch meist in Form von Patentanwälten. Beratungen durch den Verfassungsschutz, Gremien wie das Sicherheitsforum Baden-Württemberg oder sämtliche Institutionen, Aktionskreise oder Verbände, die sich dem Thema Produkt- und Markenpiraterie angenommen haben, werden nur selten genutzt.

4.2.4 Wirksamkeit und Durchführbarkeit der Schutzmaßnahmen

Im zweiten Teil der Befragung wurden die zuvor beschriebenen Schutzmaßnahmen nach den Parametern „Wirksamkeit" und „Durchführbarkeit" gefragt. Da die Ergebnisse zu den technischen Maßnahmen zu dürftig für eine trendbestimmende Auswertung sind, wird im Folgenden nur auf die betriebswirtschaftlichen sowie juristischen Schutzmaßnahmen eingegangen.

Eine Studie des Sicherheitsforums Baden-Württemberg über den Know-how- und Informationsverlust in Baden-Württemberg ergab, dass die Aufwendungen für Schutzmaßnahmen ca. 0.1% des Unternehmensumsatzes betragen.[286] Die Ergebnisse der hier zugrunde liegenden Befragung können dieses Ergebnis nur verifizieren. Einige Unternehmen konnten die Frage zwar aufgrund ihres großen Produktportfolios nicht beantworten. Die Firmen, die Angaben dazu machen konnten, gaben Werte zwischen 0.002% und 1% ihres Gesamtumsatzes an. Grundsätzlich ist natürlich der Prozentanteil von Produkt zu Produkt unterschiedlich.

Im Bereich der *Beschaffung* ist ein deutlicher Trend erkennbar: Die Unternehmen können sich nur schwer vorstellen, hier wirksame Schutzmaßnahmen gegen Fälscher zu platzieren. Auffällig ist, dass Lieferantenschulungen und Kontrollen als unwirksam bzw. eher unwirksam eingestuft wurden, Wareneingangskontrollen und Vertragsgestaltungen dagegen eine mittelmäßige Bewertung bekamen. Daraus kann geschlossen werden, dass die Unternehmen sich eher auf sich selbst und ihre Wareneingangskontrollen als auf ihre Lieferanten verlassen. Bei den Lieferanten besteht ein besonderes Gefährdungspotential im Kampf gegen Produktpiraten, weil nicht alle Lieferungen genau spezifiziert werden können. Eine Einkaufskooperation als vorgeschlagene Maßnahme wird als unwirksam und eher schlecht durchführbar bewertet. Aus anderen be-

[286] Vgl. o.V. (2004b).

triebswirtschaftlichen Gründen kann es sein, dass Unternehmen auf solche Kooperationen verzichten, im Kampf gegen Fälscher können sich solche Zusammenschlüsse jedoch als sehr sinnvoll erweisen. Abgesehen vom Bereich Beschaffung haben auch Konsortien von Unternehmen bei gemeinsamen Aktionen und dem Austausch von Erfahrungen nur mittelmäßig abgeschnitten. Diese Ergebnisse sollten Unternehmen nachdenklich stimmen. Im Kampf gegen Produktpiraterie sollten westliche Unternehmen zusammenhalten und nicht jedes seinen eigenen Weg einschlagen. Dadurch wird kein kollektiver Druck aufgebaut. Konsortien wie z.B. vom Fraunhofer Institut sind gute Ansätze. Diese sollten unbedingt weiter ausgebaut werden.

Im Aufgabengebiet des *Personalmanagements* ist in der Auswertung eine etwas positivere Einschätzung erkennbar. Selektive Einstellungen werden als sehr gut durchführbar und sehr wirksam empfunden, ein effektives Fluktuationsmanagements dagegen als mittelmäßig wirksam und eher schlecht durchführbar. Dieser Ansatz sollte jedoch noch einmal überdacht werden. Ein intensives Auswahlverfahren mit genauer Betrachtung des bisherigen Lebenslaufs ist zwar ein wichtiger Bestandteil, um Schwachstellen zu schließen; das Risiko, dass ein enttäuschter oder unbefriedigter Mitarbeiter internes Wissen an einen Konkurrenten oder Fälscher weitergibt, ist jedoch sehr viel höher, als dass sich ein „Spion“ in das Unternehmen einschleusen lässt. Dass ein Personalchef schon bei der Auswahl abschätzen kann, ob ein Bewerber auf ein Angebot zur Spionage eingehen werde oder nicht, ist fraglich. Deshalb ist es wichtig, Fluktuation durch finanzielle oder soziale Anreize zu reduzieren. Gerade in China ist die Loyalität der Mitarbeiter sehr gering, was sich durch gezielt eingesetzte Anreize durchaus vergrößern ließe. Dass eine Job Rotation als eher unwirksam und schlecht durchführbares Mittel eingeschätzt wird, kann man durchaus nachvollziehen, da es in vielen Unternehmen wichtig ist, sich auf Spezialisten zu verlassen, was bei einem ständigen Funktionswechsel nicht möglich wäre. Die Einarbeitungszeit stände in den meisten Fällen in keinem Verhältnis zum erzielten Nutzen. Eine wichtige Erkenntnis ist, dass Geheimhaltungsklauseln, wie sie in jedem Unternehmen von Mitarbeitern unterschrieben werden müssen, in ihrer Wirksamkeit nur mittelmäßig eingeschätzt werden. Gerade in China liegt darin natürlich ein großes Problem, da Geheimhaltungsvereinbarungen zwar abgemacht werden, diese jedoch keinerlei Abschreckungseffekte haben und deswegen oft nicht eingehalten werden.

Im Bereich *Forschung und Entwicklung* liegt vermutlich das größte Gefährdungspotential. Den Technologietransfer zu unterbinden, wäre nach Aussagen der Befragten

zwar sehr wirksam, ist aufgrund der Haltung der chinesischen Regierung jedoch nur mittelmäßig durchführbar. Zertifizierungsstellen wie das China Compulsory Certification (CCC) machen es den Unternehmen sehr schwer. Die andere Möglichkeit, Know-how-Verluste zu vermeiden, indem man den Fälschern immer etwas voraus ist und ständig Innovationen anbietet, wird von einigen Unternehmen versucht. Hier sehen sie eine Lösung des Problems. Diese Maßnahme wird als eher wirksam eingestuft. Trotzdem muss man sich bewusst sein, dass auch eine Fälschung des Qualitätsproduktes aus dem Vorjahr zu erheblichen finanziellen Schäden führen kann. Die Maßnahme, das Gesamtwissen zu verschleiern, indem man verschiedene Forschungsteams bildet, wurde als unwirksam und nicht durchführbar angesehen. Da viele Forscher sehr spezialisiert sind und die Entwicklung eines Produktes das Verständnis des Gesamtkonzeptes voraussetzt, ist diese Maßnahme wohl eher zu vernachlässigen. Die Einführung von Komplementärprodukten wurde gleichermaßen schlecht bewertet, was vermutlich auf den befragten Industriezweig zurückzuführen ist.

Im Bereich der *Fertigung* jedoch schneidet die Verschleierung des Gesamtwissens durch Streuung der Prozesse deutlich besser ab als in der Forschung und Entwicklung. Dies wird sogar als sehr wirksam und mittelmäßig durchführbar bewertet. Der Unterschied zur Forschung und Entwicklung liegt sicher daran, dass zur Fertigung nicht das Gesamtwissen benötigt wird und das Produzieren einzelner Teile, die später zu einem Ganzen verbunden werden, die Durchführbarkeit nicht negativ beeinflusst. Als eine wirksame Schutzmaßnahme wird diese eingestuft, weil am Fertigungsprozess viele Mitarbeiter beteiligt sind und somit die Gefahr eines Informationsverlustes sehr viel höher ist. Deswegen kann eine Unterteilung diesen Informationsverlust wirksam verhindern. Auffällig ist, dass die Befragten die Maßnahme, sensible Teile in Deutschland herzustellen, nicht besonders hoch bewerten. Wahrscheinlich gehen sie davon aus, dass auch diese Gefahr laufen, später gefälscht zu werden.

Im Gegensatz zum Bereich Beschaffung werden im *Vertriebsnetz* Kontrollen bei und Schulungen für Händler als durchaus wirksamer gesehen. Kontrollen bei den Händlern sind sehr wichtig, da der Handel die letzte Stufe vor den Endkunden darstellt und deswegen nicht mehr zu beeinflussen ist. Außerdem sind Schulungen hier sehr effektiv, weil die Händler den engsten Kontakt zu den Kunden und zu anderen Händlern haben und so meist die ersten sind, die Informationen über Fälschungen erreichen. In den Schulungen lernen die Händler, wie sie mit solchen Informationen umgehen müssen bzw. diese interpretieren können. Der Verzicht auf Händler oder die Eingrenzung der

Verkaufsmöglichkeiten durch selektive Verkaufsstätten wurde zwar als eher wirksam, jedoch als eher nicht durchführbar erachtet. Ein Vertriebsmodell ohne Händler ist bei den meisten Firmen einfach nicht möglich. Selektive Verkaufsorte verringern das Vertriebsnetz und sind deshalb wohl eher nicht denkbar.

Auch bei den Vertriebsmodellen ergibt sich unter den sechs Unternehmen ein durchaus geschlossenes Bild. Der Direktvertrieb garantiert definitiv eine deutlich größere Absicherung, d.h. er wäre sehr wirksam und würde die Fälschungsgefahr stark reduzieren, ist aber aus Kostengründen eher schlecht durchführbar. Lizenzvergabe oder Franchising-Konzepte enthalten zwar ein größeres Risiko, sind aber aufgrund kleinerer Investitionen etwas leichter durchführbar. Auch hier muss vor dem Hintergrund der Gesamtstrategie des Unternehmens eine Entscheidung getroffen werden.

Überdurchschnittlich gut schneiden die Schutzmaßnahmen im *Marketing- und Öffentlichkeitsbereich* ab. Eine enge Kundenbindung sowie Anreize durch Zusatzleistungen werden als sehr wirksam und sehr gut durchführbar angesehen. Selbst Werbemaßnahmen oder Veranstaltungen zur Aufklärung über diese Problematik werden als sehr wirksam befunden, durchgeführt werden sie jedoch aus Kostengründen nur mittelmäßig. Zusatzleistungen, beispielsweise durch einen Kundenservice, oder Garantieleistungen bieten deswegen einen guten Schutz gegen Fälscher, die solche Leistungen nicht anbieten können.

Bei der Betrachtung der juristischen Aspekte, nämlich bei Patent- und Markenschutzanmeldungen, ergibt sich ein sehr widersprüchliches Bild. Bei den befragten Unternehmen haben alle entweder Produkte oder Marken angemeldet. Die Durchführbarkeit solcher Maßnahmen bewerten die Befragten mit 1.0, d.h. sehr gut durchführbar. Bei der Wirksamkeit ergibt sich jedoch ein unterer Wert von 3.25, wobei 4 als unwirksam gilt. Die Frage stellt sich, warum alle Firmen Patente und Markenrechte anmelden, wenn sie von deren Funktion nicht überzeugt sind. Dies mag an der fehlenden Flexibilität bzw. einer Fehleinschätzung hinsichtlich des chinesischen Marktes auf Seiten der Firmen liegen. Die Unternehmen haben bisher immer den Schutz geistigen Eigentums mit einer Schutzrechtsanmeldung versucht zu garantieren, was nun in China aufgrund der problematischen Durchsetzung der Schutzrechte wohl nicht funktioniert. Einige Unternehmen haben aufgrund dieser Problematik auch nur ihre Marke geschützt, auf Patentanmeldungen jedoch verzichtet. Wenn sich die rechtliche Durchsetzungsmöglichkeit in China nicht verbessert, muss hier ein Umdenken stattfinden.

Grenzbeschlagmaßnahmenverfahren werden hinsichtlich ihrer Durchführbarkeit sehr positiv bewertet, ihre langfristige Wirksamkeit aber nur mittelmäßig. Da beim Zoll zwar die eine entdeckte Ladung beschlagnahmt und vielleicht sogar vernichtet wird, trägt dieses Verfahren aber nur kurzfristig, jedoch nicht nachhaltig, zur Bekämpfung bei.

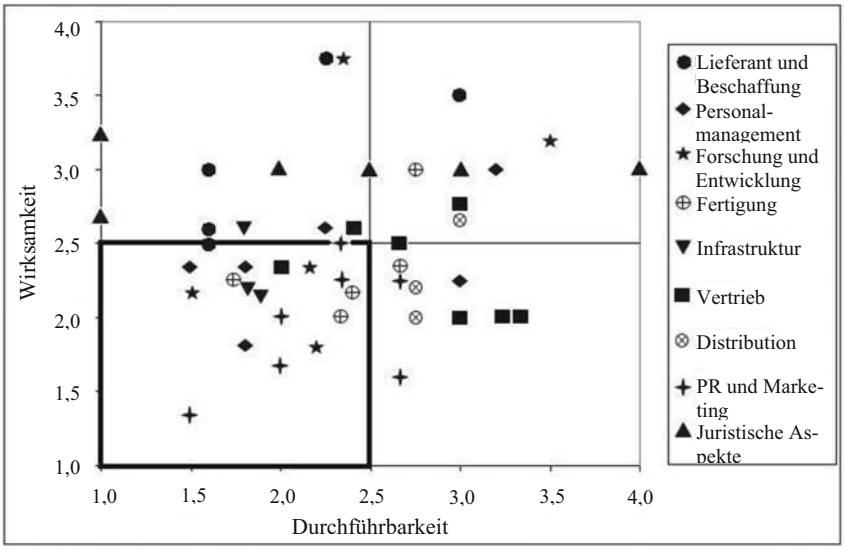


Abbildung 3: Anordnung der betriebswirtschaftlichen und juristischen Schutzmaßnahmen
Quelle: eigene Darstellung.

Zusammenfassend sieht man in Abbildung 3 die beschriebenen Schutzmaßnahmen nach den Parametern „Wirksamkeit“ und „Durchführbarkeit“ geordnet. Das Schaubild gliedert die Schutzmaßnahmen nach den Wertschöpfungsbereichen. Die genauen Ergebnisse der einzelnen Schutzmaßnahmen sind aus der Tabelle im Anhang 2 ersichtlich. Der umrahmte Teilbereich hat bei der Korrelation der zwei Parameter am besten abgeschnitten. Dabei kann man erkennen, dass man bei der Einführung von Schutzmaßnahmen im Bereich der Öffentlichkeitsarbeit, der Fertigung, des Personalmanagements, der Forschung und Entwicklung sowie der Infrastruktur ansetzen sollte, da in diesen Bereichen die Schutzmaßnahmen als überwiegend effektiv gelten und zugleich durchführbar sind. Vertriebsmaßnahmen hingegen gelten als zunehmend wirksam,

sind aber kaum durchsetzbar. Juristische Schutzmaßnahmen bieten das Gegenteil. Sie sind zum Teil sehr gut durchsetzbar, jedoch fehlt die entsprechende Wirksamkeit.

4.2.5 Hemmnisse bei der Durchführbarkeit von Schutzmaßnahmen

Auf die Frage, warum viele der Schutzmaßnahmen nicht durchführbar sind, wurde als Grund meist die geringe Verfügbarkeit finanzieller und personeller Ressourcen genannt. Gerade die kleineren Unternehmen haben oft nicht die Möglichkeit, sich teurer präventiver Schutzmaßnahmen zu bedienen. Eine Möglichkeit wäre zu untersuchen, ob die Schutzmaßnahmen nicht in das schon bestehende System eingebunden werden könnten, beispielsweise im Rahmen eines ohnehin durchgeführten Qualitätsmanagement in der Beschaffung oder in der Logistik, um die Absicherung gegen Fälscher in den Prozess mit zu integrieren. Dies wäre ein geringer Zusatzaufwand, aber die Nutzung eines Synergieeffekts.

Präventiv finanzielle und personelle Aufwendungen zu leisten, ist für viele Unternehmen ein zu großes Risiko, da immer die Möglichkeit besteht, auch ohne Schutzmaßnahmen davonzukommen. Das ist sicherlich ein Problem kurzfristigen Denkens und Planens in einem Unternehmen. Präventive Maßnahmen können sich oft erst in der weiteren Zukunft auszahlen. Immer noch zu häufig kommt es vor, dass das Management auf kurzfristige Gewinne aus ist und keine langfristigen Planungen vorfinanzieren will.

Fehlende Rechtsgrundlagen geben die Unternehmen als weiteren Grund dafür an, warum Schutzmaßnahmen nur in geringem Maße greifen. Diese Angabe stützt sich auf die Aussage, dass juristische Schutzmaßnahmen in China ineffektiv seien, da es keine rechtliche Grundlage dafür gebe. Interessanterweise herrscht bei der Durchsetzung der Schutzrechte eine sehr unterschiedliche Meinung unter den Unternehmen. Ein Unternehmen, das nach Aussagen seines Zuständigen äußerst defensiv geführt wird, legt seine Aufwendungen zu fast 100% in rechtliche Schutzmaßnahmen. Andere Unternehmen verzichten selbst auf die Patentanmeldungen, weil diese Investition für sie sinnlos erscheint. Auffällig dabei ist, dass zwei der mittelständischen Unternehmen, die große Probleme mit Fälschungen hatten, Schutzrechte als absolut nutzlos erachten. Bei großen Unternehmen sind Patent- und Markenschutzanmeldungen fest in ihren Investitionen vorgesehen. Entweder genießen die größeren Unternehmen eine größere Durchsetzungskraft bei den chinesischen Behörden oder sie sind nicht flexibel genug, neue

Wege zu gehen. Da Patentanmeldungen oft sehr kostenintensiv sind, könnte der Grund für die unterschiedliche Sichtweise auch darin bestehen, dass kleinere Unternehmen sich solche Investitionen nur leisten, wenn sie sicher sind, auch einen Nutzen davon zu haben. Da Patenanmeldungen aber keine Garantie dafür sind, Schutzrechte gegen potentielle Fälscher durchsetzen zu können, ist die Investition mit einem gewissen Risiko verbunden, weswegen sich kleinere Unternehmen eher dagegen entscheiden.

Auffällig war außerdem, dass Kommunikationsprobleme als häufig genanntes Hemmnis angegeben wurden. Die Unternehmensvertreter betonten immer wieder, dass die „chinesische Ethik ein anderes Grundverständnis besitzt“[287] als die deutschen Firmen. So kam es nach Erzählung eines Befragten in China zu einer Auseinandersetzung zwischen dem zuvor gekündigten chinesischen Mitarbeiter und dem Geschäftsführer, nachdem der chinesische Mitarbeiter sich geweigert hatte, den Firmenlaptop mit allen unternehmensinternen Informationen herauszugeben. Der von der Polizei beschlagnahmte Laptop wurde erst wieder freigegeben, nachdem der Geschäftsführer seine engen Beziehungen zum chinesischen Ministerpräsident betont hatte.[288] Auch der Verfassungsschutz[289] berichtet von einer chinesischen Praktikantin, die während ihres Praktikums bei einem französischen Automobilzulieferer immer wieder deswegen auffiel, weil sie ihren Laptop mit in das Unternehmen brachte. Bei einer polizeilichen Untersuchung wurden mehrere Laptops mit firmeninternen Daten in ihrer Wohnung gefunden. Sie war sich jedoch selbst nach ihrem Geständnis keiner Schuld bewusst, obwohl sie die Geheimhaltungsklauseln des Unternehmens unterschrieben hatte. Welche unterschiedlichen Erwartungen, bedingt durch kulturelle Unterschiede und Kommunikationsschwierigkeiten, das China-Geschäft beeinträchtigen kann, zeigen die beiden Beispiele.

4.2.6 Fazit der Umfrage

Nach Auswertung und Interpretation der Experteninterviews ergab sich zusammenfassend folgende Bilanz:

- Da juristische Schutzmaßnahmen speziell in China das Risiko der Produkt- und Markenpiraterie nur gering mindern können, müssen andere Alternativen in Betracht gezogen werden.

[287] U1: Vertriebsleiter (30.Oktober 2006).
[288] Vgl. U1: Vertriebsleiter (30.Oktober 2006).
[289] o.V. (2005a), S. 25ff.

- Betriebswirtschaftliche Schutzmaßnahmen können wichtige Komponenten im Gesamtkonzept der Fälschungsbekämpfung darstellen, müssen aufgrund ihrer Neuartigkeit jedoch erst im Bekämpfungsprozess der Unternehmen Akzeptanz finden.
- Betriebswirtschaftliche Schutzmaßnahmen können oft sehr leicht in bestehende Systeme integriert werden, so dass kein hoher Mehraufwand entsteht. Dies ist jedoch von den bestehenden Unternehmensprozessen und Konzepten abhängig und muss individuell gestaltet werden.
- Technische Schutzmaßnahmen werden aufgrund ihrer ständigen Entwicklung bald sehr viel ausgereifter und auch kostengünstiger werden und somit eher einsetzbar.
- Die Unternehmen sollten die beschriebenen Schutzmaßnahmen als Kompendium betrachten, aus denen sie diejenigen auswählen, die zu ihrer Gesamtstrategie und ihren unternehmensspezifischen Prozessen passen.
- Gerade im Industriegüterzweig – speziell hier im Maschinenbau – ist die Gefährdungssumme wegen der hohen Forschungs- und Produktionskosten sehr hoch. Bei Markteinführung der Produkte müssen die Anfangsinvestitionen getätigt werden. Treten Fälschungen auf, lassen diese die Investitionsplanung nicht mehr aufgehen. Da die Fälscher diese hohen Forschungskosten nicht aufbringen müssen und auch meist billige Materialien bei der Fertigung verwenden, entstehen große Preisunterschiede, gegen die der Originalhersteller machtlos ist.

Nach den Ergebnissen der Befragungen und den Erkenntnissen des Beitrages sind einige Handlungsmaxime ersichtlich. Es gibt zwar kein Patentrezept, das auf jedes Unternehmen anwendbar ist. Ein Grund ist, dass sich die Unternehmen noch immer unzureichend mit diesem Thema auseinandergesetzt haben. Diese Annahme wird durch die nicht ausdifferenzierten Ergebnisse (Tabelle 4) belegt. Zum anderen ist das Ergebnis sicher auf die Tatsache zurückzuführen, dass die Integration der Schutzmaßnahmen sehr vom ganzheitlichen System des Unternehmens abhängt. Somit funktionieren nur individuelle Lösungen, die u.a. der Grund für die Streuung der Ergebnisse sind. China als Markt stellt eine besonders Herausforderung dar, da sowohl im rechtlichen als auch im ethischen Bereich völlig anders agiert werden muss, weil eine gemeinsame verbindliche Basis fehlt. Daher sind neue Ansätze im Bereich der Schutzmaßnahmen dringend nötig. Es besteht Aufklärungsbedarf, wobei durch Informationsaustausch Unternehmen aus den negativen Erfahrungen anderer Unternehmen lernen können.

4.3 Umsetzbarkeit im Management

Im Nachfolgenden soll die praktische Umsetzung möglicher Präventivmaßnahmen strategisch mit den gewonnenen Ergebnissen der Befragung angewendet werden und in einer abschließenden Tabelle festgehalten werden:

Zunächst sollte jedes Unternehmen im Rahmen eines strategischen Risikomanagements die bestehenden Risiken identifizieren, analysieren und nach ihrem Gefährdungspotential für das Unternehmen bewerten. Da die Gefahr der Produkt- und Markenpiraterie allgegenwärtig ist und fast alle Produktbranchen und Unternehmenstypen betrifft, muss das Risikopotential eigentlich immer als besonders hoch eingestuft werden. Im Anschluss an die Risikoanalyse sollte eine umfassende Bestandsaufnahme der Sicherheitsvorkehrungen gegen Produkt- und Markenpiraterie erfolgen, um Schwachstellen zu entdecken. Darauf aufbauend wird anschließend eine ganzheitliche und individuelle Sicherheitsstrategie entwickelt, die alle Unternehmensbereiche umfasst. Dabei spielen auch die Grundstrategien aus Abschnitt 3.3 eine wichtige Rolle, um den grundsätzlichen Umgang mit dem Thema Produkt- und Markenpiraterie festzulegen. Die beschriebenen Schutzmaßnahmen sollen dabei als Kompendium dienen, aus denen die Unternehmen auf der Basis ihrer Unternehmensstrategie und -philosophie die passenden auswählen können. In Tabelle 4 sind dafür die einzelnen Schutzmaßnahmen der drei Bereiche (betriebswirtschaftlich, juristisch und technisch) nach der Zeitdauer ihrer Umsetzung eingeteilt. Bei der Kategorie „betriebswirtschaftliche Schutzmaßnahmen“ wurden nur die entsprechend der Befragung als am wirksamsten eingestuften Maßnahmen ausgewählt. Die betriebswirtschaftlichen Schutzmaßnahmen müssen in allen Bereichen der Wertschöpfungskette erarbeitet sowie juristische und technische Möglichkeiten geprüft und bewertet werden, um das Risiko der Produkt- und Markenpiraterie zu mindern. Da die betriebswirtschaftlichen Schutzmaßnahmen strategisch ausgerichtet sind, sind sie fast ausschließlich der Risikominderung zuzuordnen.

Falls sich das Risiko der Produkt- und Markenpiraterie doch realisiert und Schäden durch Fälschungen entstehen, müssen Schutzmaßnahmen zur Schadensminderung gewählt werden. Dabei helfen vor allem die reaktiven juristischen Maßnahmen, die sowohl spezial- als auch generalpräventiv wirken. Darüber hinaus helfen die zuvor eingeführten technischen Sicherungsmittel, um im Falle eines Rechtsstreits beweisen zu können, nicht für ein gefälschtes Produkt haften zu müssen.

Die vertraglichen Schutzmaßnahmen im betriebswirtschaftlichen Bereich sowie im technischen Bereich können als Risikominderung und als Schadensminderung fungieren. Als Risikominderung wirken sie wegen ihrer Abschreckungsfunktion für den Unterzeichnenden. Zur Schadensminderung können sie beitragen, da die Verursacher aufgrund der Geheimhaltungsklauseln oder Vertragsgestaltungen zur Rechenschaft gezogen werden können. Ob der Schaden durch Fälschungen dadurch jedoch weitgehend gemindert wird, ist fraglich.

Tabelle 4: Maßnahmenkatalog zum Schutz vor Produkt- und Markenpiraterie unter Berücksichtigung der Zeitkomponente
Quelle: eigene Darstellung.

	präventive Maßnahmen	**reaktive Maßnahmen**
Kurzfristige Wirkung		
betriebswirtschaftlich		
Beschaffung		
Personalmanagement	Mitarbeiterschulungen (2.3)	
Forschung und Entwicklung		
Fertigung	Stichproben/Qualitätskontrollen (2.25)	
Infrastruktur	elektronische Schutzmaßnahmen (2.17) Zutrittskontrollen (2.2)	
Vertrieb	Festlegung der Verkaufsquoten/ Besucherhäufigkeit (2.0) Händlerkontrollen (2.3)	
Distribution	Tracking & Tracing (2.2)	Tracking & Tracing (2.2)
Marketing/Öffentlichkeitsarbeit	Werbekampagnen und Veranstaltungen zur Aufklärung (1.6) aggressives Auftreten [z.B. Zerstörung von Plagiaten] (2.2)	
juristisch		
juristisch	Patent- und Markenschutzanmeldungen (3.25)	zivilrechtliche Durchsetzung (3.0) Verwaltungsverfahren (3.0) einstweiliger Rechtsschutz (3.0) informelle Verfahren (3.0) strafrechtliche Verfahren (3.0) Schiedsgerichtsverfahren (3.0) Grenzbeschlagnahmeverfahren (2.67)
technisch		

	präventive Maßnahmen	reaktive Maßnahmen
Mittelfristige Wirkung		
betriebswirtschaftlich		
Beschaffung	Vertragsgestaltung (2.5)	Vertragsgestaltung (2.5)
Personalmanagement	Geheimhaltungsklauseln (2.3)	Geheimhaltungsklauseln (2.3)
Forschung und Entwicklung	Unterbindung des Technologie-transfers (1.8)	
Fertigung	Kontrollen und Integration ins unternehmensinterne Sicherheits-system beim Outsourcing (2.3)	
Infrastruktur		
Vertrieb	Bildung von Verkaufsteams zur gegenseitigen Überprüfung (2.3) Rotation (2.3)	
Distribution	Lagerschutz (2.0)	
Marketing/Öffentlichkeitsarbeit	Schulungen/Hotlines/Updates (2.2)	
juristisch		
technisch		
technisch	technische Schutzmaßnahmen	technische Schutzmaßnahmen (als Beweis bei Produkthaftungs-fällen)
Langfristige Wirkung		
betriebswirtschaftlich		
Beschaffung		
Personalmanagement	Selektive Einstellung (1.8) Fluktuationsmanagement (2.25)	
Forschung und Entwicklung	Innovationsvorsprung (2.17) Trennung von der restlichen Infra-struktur (2.3)	
Fertigung	Fertigung sensibler Teile (2.17)	
Infrastruktur		
Vertrieb	enge Kundenbindung (1.3) Zusatzleistungen (1.33) individuelle Anpassungen (1.67) selektive Verkaufsstellen (2.0) Verzicht auf Händler (2.0)	
Distribution		
Marketing/Öffentlichkeitsarbeit		
außerhalb der Wertschöpfungs-kette	Konsortien (2.25)	
juristisch		
technisch		

5 Umdenken im China-Geschäft als entscheidende Maxime

Wissen, das früher von Generation zu Generation weiterentwickelt und vererbt wurde, wird heute von Kontinent zu Kontinent weitergereicht. Es ist die Tauschwährung, mit der sich der Westen seinen Eintritt auf dem chinesischen Markt erkauft hat.[290] Der Drang in China dabei zu sein, um kurzfristig erfolgreich zu werden auf dem Markt, auf dem man so billig produzieren und so hoch absetzen kann, lässt viele Unternehmen unvorsichtig werden. Schutzmaßnahmen zur Wahrung geistigen Eigentums werden oft erst eingefordert, nachdem entscheidendes Wissen als Vorleistung preisgegeben oder ehrgeizig abgekupfert wurde. Welche Gefahr diese Vorgehensweise in sich birgt, zeigen oft erst rückblickend die immensen Schäden und sogar die teilweise existenzbedrohenden Entwicklungen in Unternehmen.

Die Einführung eines Präventionsmanagement durch eine ganzheitliche Strategie aus den betriebswirtschaftlichen, juristischen und technischen Bereichen der Schutzmaßnahmen und folglich ein Umdenken im China-Geschäft ist die entscheidende Maxime, die als Erkenntnis dieses Beitrages abgeleitet werden muss, wenn die westliche Welt sich weiterhin in der schärferen Wettbewerbssituation behaupten will. Je nach Unternehmenssituation kann das Kompendium der Schutzstrategien in diesem Beitrag dazu Ideen liefern. Im Fazit der Umfrage werden erste Anwendungsmöglichkeiten kritisch betrachtet und praktische Umsetzungsbeispiele zur Risiko- bzw. Schadensminderung in Relation zu ihrer Umsetzungsdauer diskutiert. Zusammenfassend muss aber betont werden, dass gerade eine vorausschauende Gesamtstrategie, die Technologien und Produkte langfristig schützt, eine absolut lohnende Investition ist. Wird die Sensibilität für die Anwendung der existierenden Methoden und Instrumente für die Früherkennung geschärft, ist man dem Ziel, sich gegen Produkt- und Markenpiraterie präventiv zu schützen, ein gutes Stück näher gekommen.

Wenn eben diese Maßnahmen beachtet werden, wird hoffentlich die Äußerung von Philipp Vorndran, dem Chefstrategen der Credit Suisse, nicht Realität werden: „Die westlichen Industrienationen haben ihr Know-how zum großen Teil an China weitergegeben und damit ihre Aufgabe erfüllt. Sie werden bald nicht mehr gebraucht.“[291]

[290] Vgl. Steingart (2006), S. 219.
[291] Steingart (2006), S. 223.

Literaturverzeichnis

Anand, B./Galetovic, A. (2005): Stoppt die Ideendiebe. In: Harvard Business Manager. Ausgabe 05 (2005).

Ballhaus, J. (2005): Markenschutz. Gegen den Klau hilft nur Offensive. In: Absatzwirtschaft. Heft 05, Vol. 48 (2005), S. 40-41.

Blumenthal, C. (2002): Der strafrechtliche Schutz der Marke unter besonderer Berücksichtigung der Piraterie. Bern 2002.

Bundesgesetzblatt: Patent Coorporation Treaty. BGBl. 1970 II, S. 649, 664 mit den Änderungen von BGBl. 1984 II, S. 799, vom 3.Februar 1984 BGBl. II, S. 975 und Änderungen von Art. 22, BGBl. 2002 II, S. 728.

Bundesgesetzblatt: Madrider Markenabkommen. BGBl. 1970 II, S. 293, S. 418; BGBl. 1984 II, S. 799.

Bundesgesetzblatt: Protokoll des Madrider Abkommen. Protokoll vom 27.Juni 1989, BGBl. 1995 II, S. 1017.

Bundesgesetzblatt: Nizza-Abkommen. vom 15.Juni 1957 in der in Genf am 13.Mail 1977 beschlossenen und am 2.Oktober 1979 geänderten Fassung BGBl. 1981 II, S. 358; 1984 II, S. 799.

Bundesgesetzblatt: Straßburger Abkommen. vom 24.März 1971, geändert am 2.Oktober 1979, BGBl. 1975 II, S. 283; 1984 II S. 799.

Bundesministerium für Bildung und Forschung (2006): Nanotechnologie. Eine Zukunftstechnologie mit Visionen. URL: http://www.bmbf.de/de/nanotechnologie.php. (Stand: 2006, Zugriff: 08.10.2006).

Bundesministerium der Finanzen (2006a): Erfolgreiche Arbeit des Zolls im Jahre 2005. URL: http://www.bundesfinanzministerium.de/cln_01/nn_3792/DE/Aktuelles/Pressemitteilungen/2006/03/20061003__PM0035.html. (Stand: 2006, Zugriff: 20.07.2006).

Bundesministerium der Finanzen (2006b): Gewerblicher Rechtsschutz, Jahresbericht 2005, Berlin 2006.

Bundesministerium der Justiz (2006a): Produktpiraterie. Gefahr für den Wirtschaftsstandort Deutschland? URL: http://www.bmj.bund.de/enid/13a19ddbd9b658465bf291860710f8d0,0/Juli/_6__7_2__6_-_Produktpiraterie_y6.html. (Stand: 2006, Zugriff: 15. 09.2006).

Bundesministerium der Justiz (2006b): Es beginnt mit einer Idee. URL: http://www.bmj.de/enid/c816d7cb6822ced553a02d0e8349dee6,95c9817072657373656172746 96b656c5f6964092d0932343331093a096d795f79656172092d0932303036093a096d795f6d6f6e7468092d093034093a095f7472636964092d09333630/Presse/Pressemitteilungen_58.html. (Stand: 2006, Zugriff: 10.05.2006).

Busmann, K./Krieg, O./Nestler, C./Salvenmoser, S./Werle, S. (2005): Wirtschaftskriminalität 2005. Internationale und deutsche Ergebnisse, Pricewaterhouse Coopers (Hrsg.). Frankfurt am Main/ Halle 2005.

Colteryahn, K., Davis, P. (2004): Trends, die Sie kennen müssen. In: Training&Development. Januar (2004), S.1-15.

Cremer, R. (1991): Rote Karte für Plagiatoren – Bekämpfung der Produktpiraterie in der Praxis. In: Marketing Akademie (Hrsg.). Produktpiraterie. Köln 1991.

Diekmann, A. (2004): Empirische Sozialforschung. 12. Auflage, Reinbek bei Hamburg 1995.

Drinkuth, H./v. Keller, E./Wie, J. (2005): Intellectual Property Protection in China. Roland Berger (Hrsg.), Shanghai.

Ebberg, A./Menges, G. (2006): Intelligente Verpackung, In: W&S Handel und Logistik, Ausgabe 1-2 (2006), S.31-33.

Eggert, D. (2005): Piraten unter Beschuss. In: Absatzwirtschaft Marken 2005 (2006), S. 40-43.

Engelken, E. (2005): Kampf gegen Windmühlen. In: Handelsblatt, 02.11.2005, S. 47.

Europäische Kommission (2006): Antwort des Zolls auf jüngste Entwicklungen bei der Nachahmung von Waren und der Produktpiraterie. URL: http://europa.eu/scadplus/leg/de/lvb/l11016.htm. (Stand: 2006, Zugriff: 17.07.2006).

Fiege, S. (2006): Risikomanagement- und Überwachungssystem nach KonTraG. Wiesbaden 2006.

Fischer, D. (2005): Chinas sozialistische Marktwirtschaft, In: Informationen zur politischen Bildung, Vol. 289, S. 9-14.

Fischer, S./Eck, R./Richter H.-J. (2002): Was sich gegen Produkt- und Markenpiraterie tun lässt. In: Harvard Business Manager Vol. 1 (2002), S. 80-91.

Fuchs, H. J. (2006): Piraten, Fälscher und Kopierer. Wiesbaden 2006.

Gläser, J./Laudel, G. (2004): Experteninterviews und qualitative Inhaltsanalyse. Wiesbaden 2004.

Handelskammer Hamburg (2006): Fragen und Antworten über das Gemeinschaftsgeschmacksmuster. URL: http://www.hk24.de/produktmarken/innovation/innovations_patent_centrum/informationsdienstleistungen/geschmacksmuster/Gemeinschaftsgeschmacksmuster.jsp#nr1. (Stand: 2006, Zugriff: 08.11.2006).

Hartberg, A. (2005): Den Kampf gegen Produktpiraterie aufnehmen. DIHK – Sonderdienst „China“. Juli 2005, S. 10-12.

Harte-Bavendamm, H. (2000): Handbuch der Markenpiraterie in Europa. Bern 2000.

Häuslschmid, V. (2004): Strategien gegen Piraterie in China. 2. Auflage, VDMA Focus Recht (2004), S. 1-27.

Hayers, S./Lim, L./Petizon, L. (2005): Staying ahead of China‘s Counterfeiters. AT Kearney (Hrsg.), Chicago 2005.

Hoffbauer, A. (2006): Kanzlerin kündigt harten Kurs an. In: Handelsblatt 24.05.2006, S. 3.

Hoffknecht, A./Teichert, O. (2006): Nutzung der Nanotechnologie für sicherheitstechnische Anwendungen, Düsseldorf 2006.

Holtbrügge D./Puck J. (2005): Geschäftserfolg in China, Berlin/Heidelberg 2005.

Huber, A. (2006): Basiswissen RFID. Informationsforum RFID. Berlin 2006, S. 1-20.

Hüttemann, P. (2006): Überraschung nach dem ersten Waschgang. In: Sicherheitshalber. Zeitschrift für die Sicherheit in der Supply Chain des Handels. Ausgabe 1 (2006), S. 18-23.

Janke, K. (2005): Mehr PR für Marken. In: Horizont, 44 Jg. (2005), S. 22-24.

Krüger, R./Picard, J./Vorbrüggen, J., (2004): Digitales Sicherheitsmerkmal für fälschungssichere Verpackung. MediaSec Technologies GmbH, S. 1-11.

Kuhn, G. (2006): China und der Westen. Freiburg 2006.

Lacroix, C. (2006): Plagiarius Verleihung 2006. Pressemitteilung Februar 2006. Aktion Plagiarius e.V. (Hrsg.), Elchingen 2006.

Link, C. (1999): Harmonie zwischen Schönheit und Funktion. In: Verpackungsrundschau, Ausgabe 12 (1999), S. 34-46.

Lorbeer, K. (2005): Produktpiraterie: Es wird immer Ärger. In: Die Wirtschaft. URL: http://www.die-wirtschaft.at/ireds-7953-printurl-10643.html (Stand: 2005, Zugriff: 10.09.2006).

Lupp, J. (2006): Mit Wasserzeichen gegen Markenklau. In: Zweites Deutsches Fernsehen. URL: http://www.heute.de/ZDFheute/inhalt/0/0,3672,3899648,00.html (Stand: 2006, Zugriff: 24.08. 2006).

Maass, H. (2006): Auch der Fälschungsschutz fällt Fälschern zum Opfer. In: Stuttgarter Zeitung, 29.04.2006, S. 13.

Maass, H. (2005): Das Ende eines chinesischen Traums. In: Stuttgarter Zeitung, 9.08.2005, S. 15.

Mayring, P. (1993): Einführung in die qualitative Sozialforschung. 2. Auflage, Weinheim 1993.

Michler, I. (2006): Wir müssen immer eine Nasenlänge voraus sein. In: Die Welt. URL: http://www. welt.de/data/2006/02/17/847075.html [online] (Stand: 2006, Zugriff: 28.09.2006).

Niggl, P. (2006): Die Industrie mit der Augenklappe. In: Sicherheitshalber, Vol. 1 (2006), S. 6-17.

Oswald, H. (1997): Was heißt qualitativ forschen? In: Friebertshäuser, B. (1997): Handbuch qualitativer Forschungsmethoden in der Erziehungswissenschaft. München 1997.

o.V. (2004a): Große Halle für kleine Partikel. In: Wirtschaftsspiegel der Internationalen Handelskammer. URL: http://www.secutag.com/IHK-grosse-halle.htm (Stand: 2004, Zugriff: 27.03.2006).

o.V. (2004b): Mittelständische Wirtschaft in Baden-Württemberg. Große Schäden durch ungewollten Know-how Abfluss. Sicherheitsforum (Hrsg.), Stuttgart 2004.

o.V. (2005a): Mit Sicherheit erfolgreich. In: Sicherheitsforum Baden-Württemberg, Stuttgart 2005.

o.V. (2005b): Vorsicht beim Online Kauf von CDs und DVDs. In: InternetAgent (2005), S. 1-4.

o.V. (2005c): China Intellectual Property Rights. The Economist (Hrsg.), Hong Kong 2005.

o.V. (2005d): Anmerkung zur Sicherheitslage. Arbeitsgemeinschaft für Sicherheit der Wirtschaft, Berlin 2005.

o.V. (2005e): Vortrag A+A 2005. Gallup Organisation, Düsseldorf 2005.

o.V. (2005f): Fachausschuss Produktpiraterie. Bitkom. URL: http://www.bitkom.org/de/themen_gremien/17926.aspx (Stand: 2005, Zugirff: 10.11.2006).

o.V. (2005g): Oskar der Zitate-Klauer. In: Handelblatt Online 16.08.2005. URL: http://blog.handelsblatt.de/adhoc/eintrag.php?id=234. (Stand: 16.08.2005, Zugriff: 08.11.2006).

o.V. (2005h): Wirtschaftskrieger warnt Airbus vor China-Geschäft. In: Spiegel Online 12/2005. URL: http://www.spiegel.de/wirtschaft/0,1518,388796,00.html. (Stand: 2005, Zugriff: 08.10.2006).

o.V. (2005i): Global Procurement Study Finds Companies Unprepared to Manage Increased Sourcing from China and India Effectively. In: AT Kearney, Chicago 2005. URL: http://www.atkearney.com/main.taf?p=1,5,1,154. (Stand: 2005, Zugriff: 17.11.2006).

o.V. (2006a): China. Endlich mehr Pirateriеschutz auf Messen und Ausstellungen. In: VDMA Nachrichten Recht & Steuern, 5 Jg. (2006), S. 79.

o.V. (2006b): Merkel soll China wegen Technologiediebstahl rügen. In: Frankfurter Allgemeine Zeitung, 19.05.2006, S. 10.

o.V. (2006c): Merkel fordert China zum Schutz von Urheberrechten auf. In: Frankfurter Allgemeine Zeitung, 23.05.2006, S. 15.

o.V. (2006d): Abkommen gegen Produktpiraterie. In: Stuttgarter Zeitung, 22.05.2006, S. 9.

o.V. (2006e): Wirtschafts-/Industriespionage. Business Information Warefare, KDM Schriftenreihe, Frankfurt/Main 2006.

o.V. (2006f): Technology Know-how Protection Tekno Pro. Fraunhofer Institut, S. 1-6.

o.V. (2006g): Messe Frankfurt against copying. In: Messe Frankfurt GmbH. URL: http://heimtextil.messefrankfurt.com/frankfurt/de/aussteller-center_copying.html. (Stand: 2006, Zugriff: 30.03.2006)

o.V. (2006h): Software Patent. Methods and security label for applying confidential data on a carrier. URL: http://gauss.ffii.org/PatentView/EP1302921. (Stand: 2006, Zugriff: 12.10.2006).

o.V. (2006i): LINX Sicherheitstinte verhindert Produktfälschung. URL: www.bluhmsysteme.com/LINX-Sicherheitstinte_verhinde.317.0.html. (Stand: 2006, Zugriff: 08.10.2006).

o.V. (2006j): Vorsprung mit cleveren Produkten. URL: www.identif.de. (Stand: 2006, Zugriff: 19.10.2006)

o.V. (2006k): Kampf der Produktpiraten. Das Industrie Magazin. URL: www.maschinenmarkt.de/fachartikel/mm_fachartikel_linkservice_3373008.html (Stand: 2006, Zugriff: 16.06.2006).

o.V. (2006l): Neues chinesisches Zertifizierungssystem (CCC) birgt Sicherheitsrisiken. URL: http://www.sicherheitsforum-bw.de/berichte/berichte_ccc_china.htm (Stand: 2006, Zugriff: 11.10.2006)

o.V. (2006m): Gewerblicher Rechtsschutz in China. Rechtsanwälte Poppe (Hrsg.). URL: http://www.lawyerspoppe.de/publikationen_details.php?Kunde=405&Modul=13&Art=0&ID=296&GID=118 (Stand: 2006, Zugriff: 12.11.2006)

o.V. (2006n): Markenschutz in der VR China. URL: http://www.investinchina.de/OneArticle.aspx?ID=72. (Stand: 2006, Zugriff: 10.10.2006).

o.V. (2006o): Lohnniveau steigt in China. URL: www.german.china.org.cn/german/243332.htm. (Stand: 2006, Zugriff: 06.07.2006).

o.V. (jj) (2006): Wu Yin macht Zugeständnisse. URL: www.german.china.org.cn/german/243336.htm. (Stand: 2006, Zugriff: 08.07.2006)

Papageorgiou, E. (2006): China. Strafbarkeit von Piraten geändert. In: VDMA Nachrichten Recht& Steuern, 3. Jg. (2006), S. 82.

Prahl, D. (2006): RFID Grundlagen. Bluhmsysteme, S. 1-3.

Produktqualitätsgesetz der VR China. Verabschiedet am 22.02.1993 vom Ständigen Ausschuss des Nationalen Volkskongresses. Novelliert durch Beschluss des Ständigen Ausschusses des Nationalen Volkskongresses vom 8.07.2000, Neufassung in Kraft 1.09.2000. URL: http://lehrstuhl.jura.uni-goettingen.de/chinarecht/930222.htm. (Zugriff: 10.10.2006)

Ramoser, T. (2005): Chao-xi. In: Absatzwirtschaft, 5. Jg. (2005), S. 26.

Rath, V. (2001): Kress-Elektrik klagt über ausufernde Produktpiraterie. In: Schwarzwälder Boten, 31.07.2001, S. 2.

Schäfer, M. (2005): VDMA fordert Alternative zum Gemeinschaftspaten. URL: http://www.vdma.org/wps/portal/Home/de/Verband/VDMA_Presse/Pressemitteilungen/komm_20051201_Burghof_PI_Gemeinschaftspatent?WCM_GLOBAL_CONTEXT=/Home/de/Verband/VDMA_Presse/Pressemitteilungen/komm_20051201_Burghof_PI_Gemeinschaftspatent. (Stand: 2005, Zugriff: 11.07.2006).

Scharrer, B. (2001): Blickpunkt. Volksrepublik China. In: Newsletter Rödl & Partner, Juni Jg. (2001), S. 2-3.

Schiedsverfahrensgesetz der VR China. Verabschiedet vom Ständigen Ausschuss des Nationalen Volkskongresses am 31.8.1994, Deutsche Übersetzung. URL: www.jura.uni-goettingen.de/chinarecht/1994.zip. (Zugriff: 10.11.2006)

Schöne, B. (2000): Gefahr durch undichte Stellen im Netz der Berater. In: Die Welt, S. 5.

Schramm, M./Taube, M. (2006): China kopiert alles, das frustriert. In: Absatzwirtschaft. URL: http://www.absatzwirtschaft.de/psasw/fn/asw/sfn/buildpage/cn/cc_vt/artpage/3/SH/0/ID/36017/kid//page1/PAGE_1002979/page2/PAGE_1003000/aktelem/PAGE_1003205/s/0/index.html. (Stand 2006, Zugriff: 12.08.2006).

Seeboth, A. (2006): Thermochrome Polymerfolien und Kunststoffe. Frauenhofer Institut für angewandte Polymerforschung. URL: http://www.iap.fraunhofer.de. (Stand. 2006, Zugriff: 08.10.2006).

Sicherheitsforum Baden-Württemberg (2004): Mittelständische Wirtschaft in Baden-Württemberg. Große Schäden durch ungewollten Know-how Abfluss. Stuttgart 2004.

Sieren, F. (2005): Der China Code. Wie das boomende Reich der Mitte Deutschland verändert. Berlin 2005.

Sommer, T. (2006): Strategien? Marken- und Produktpiraterie in China. In: Markenbusiness. URL: http://www.markenbusiness.com/de/news.php?newsid=2956. (Stand: 2006, Zugriff: 08.07. 2006).

Steingart, G. (2006): Weltkrieg um Wohlstand. München 2006.

Stratmann, K. (2006): Angriff der Produktpiraten. In: Handelsblatt 11.05.2006, S. 2.

Sucher, J. (2006): Die Deutschen haben Fehler gemacht. In: Spiegel Online. URL: http://www.spiegel. de/wirtschaft/0,1518,401081,00.html. (Stand: 15.02.2005, Zugriff: 10.11.2006).

Sun, S. (2004): Patent und Markenschutz in China. German Industry & Commerce China, Shanghai 2004.

Sunzi (2001): Die Kunst des Krieges. In: Clavel, J. (Hrsg.): Die Kunst des Krieges. München 1988.

Trauboth, J. (2002): Krisenmanagement bei Unternehmensbedrohungen. Stuttgart et al. 2002.

Vögele-Ebering, T. (2006): Plagiatoren auf die Finger klopfen. In: Industrieanzeiger, 6ter Jg., S. 14-16. URL: http://www2.cav.de/cav/live/cav_infopol/ha_artikel/show.php3?id=30610074. (Stand: 2006, Zugriff: 15.08.2006).

Wenkel, R. (2006): Produktfälscher entdecken deutsche Maschinen. Deutsche Welle. (Stand: 2006, Zugriff: 05.04.2006).

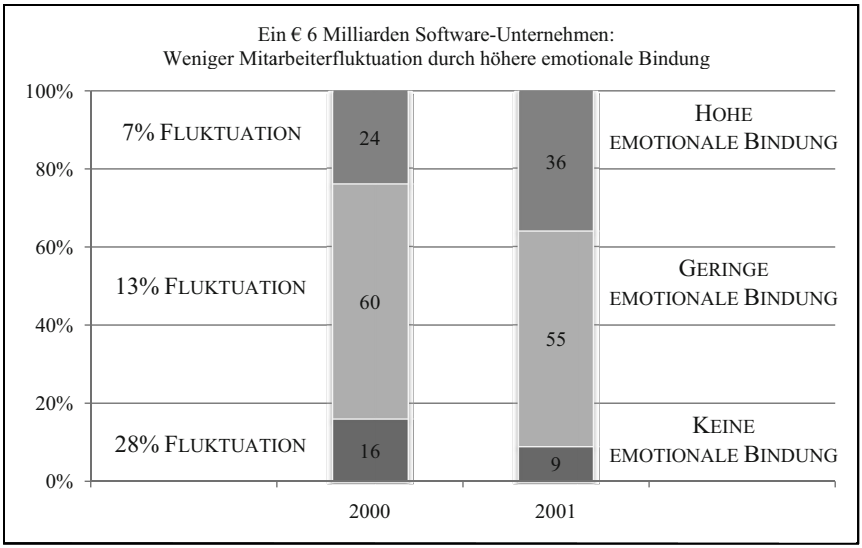
Wagner, W. (2005): Null Abweichung. In: Spiegel 7/2005.

Weiser, A./Olsen, G. (2004): Management von Markenpiraterie. Mannheim 2004.

Wüpper, T. (2006): In 30 Jahren werden China und Indien selbst große Flugzeuge fertigen. In: Stuttgarter Zeitung 27.04.2006, S. 14.

Anhang

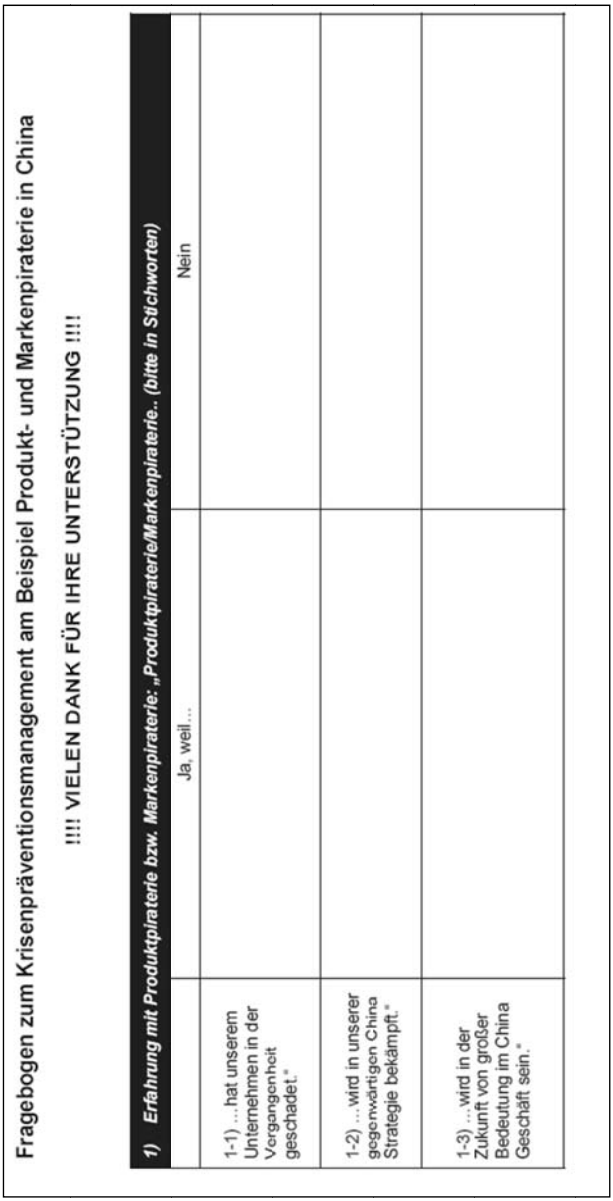
Anlage 1: Human Sigma™ Optimiert vs. Nicht-Optimiert.
Quelle: o.V. (2005e), S. 19.



Anlage 2: Ergebnisse der Interviews zu Frage 3 (Wirksamkeit und Durchführbarkeit der Schutzmaßnahmen). Quelle: eigene Darstellung.

Schutzmaßnahmen	Durchführbarkeit	Wirksamkeit
Einkaufskooperationen	3,00	3,50
Lieferantenaudit	1,60	3,00
Vertragsgestaltung	1,60	2,50
Lieferantenschulungen	2,25	3,75
Wareneingangskontrollen	1,60	2,60
Selektive Einstellung	1,80	1,80
Fluktuationsmanagement	3,00	2,25
Geheimhaltungsklauseln	1,50	2,33
Mitarbeiterschulungen	1,80	2,33
Job Rotation	3,20	3,00
Einführung von Richtlinien	2,25	2,60
Trennung von der restlichen Infrastruktur	2,17	2,33
Verschleierung des Gesamtwissen	3,50	3,20
Unterbindung von Technologietransfer	2,20	1,80
Einführung von Komplementärprodukten	2,33	3,75
Innovationsvorsprung	1,50	2,17
Geheimhaltung	2,33	2,00
Stichproben/Qualitätskontrollen	1,75	2,25
Streuung des Gesamtprozesses	2,75	3,00
Fertigung sensibler Teile in Deutschland	2,40	2,17
Outsourcing: Einführung zwingender Kontrollen und Sicherheitssysteme	2,67	2,33
Zutrittskontrollen und Schutzsysteme	1,80	2,20
Verbot von Verwendung elektronischer Geräte	1,80	2,60
Elektronische Schutzsysteme	1,83	2,17
Verkaufsteams zur gegenseitigen Überprüfung der Mitarbeiter	2,00	2,33
Rotation	2,00	2,33
Festlegung von Verkaufsquoten, Routen, Besucherhäufigkeit	3,00	2,00
Zusammenstellung endkundengerechter Verbrauchseinheiten beim Hersteller	2,67	2,50
Selektive Verkaufsstellen (Exklusivität)	3,33	2,00
Auflagen der Händler	3,00	2,75
Schulungen der Händler (zur Identifikation von Fälschungen, als Informationsquellen)	2,40	2,60
Händleraudit/Zertifizierung	2,33	2,33
Verzicht auf Händler (z.B. DELL)	3,25	2,00
Direktvertrieb	3,00	1,50
Franchising / Lizenzvergabe	2,75	2,00
Lagerschutz	2,75	2,00
Tracking&Tracing	2,75	2,20
Efficient Customer Response (bedingt Verkürzung der Lieferkette, Just in Time Versorgung)	3,00	2,67
Werbekampagnen und Veranstaltungen (z.B. Informationen über Gefahren)	2,67	1,60
Erklärungen zur Identifikation	2,00	2,00
Aggressives Auftreten (öffentliche Plagiatzerstörung)	2,67	2,25
Enge Kundenbindung	1,50	1,33
Individuelle Anpassung	2,00	1,67
Anreiz durch Zusatzleistungen	1,50	1,33
Garantieleistungen	2,33	2,50
Schulungen/Hotlines/Updates	2,33	2,25
Zusammenschlüsse von Unternehmen zum Informations- und Erfahrungsaustausch, zu gemeinsamen Aktionen (z.B. Razzien)	2,33	2,25
Joint Ventures	2,00	1,50
3-2-1) Anmeldung von Patent- und Markenrecht	1,00	3,25
3-2-2) Zivilgerichtliche Durchsetzung	2,00	3,00
3-2-3) Verwaltungsverfahren	2,50	3,00
3-2-4) Einstweiliger Rechtsschutz	4,00	3,00
3-2-5) Informelle Verfahren	3,00	3,00
3-2-6) Strafrechtliche Verfahren	2,00	3,00
3-2-7) Schiedsgerichtsverfahren	3,00	3,00
3-2-8) Grenzbeschlagnahmeverfahren	1,00	2,67

Anlage 3: Fragebogen für die Experteninterviews.
Quelle: eigene Konzeption.



Fragebogen zum Krisenpräventionsmanagement am Beispiel Produkt- und Markenpiraterie in China

!!!! VIELEN DANK FÜR IHRE UNTERSTÜTZUNG !!!!

1) *Erfahrung mit Produktpiraterie bzw. Markenpiraterie: „Produktpiraterie/Markenpiraterie.. (bitte in Stichworten)*		
	Ja, weil…	Nein
1-1) …hat unserem Unternehmen in der Vergangenheit geschadet."		
1-2) …wird in unserer gegenwärtigen China Strategie bekämpft."		
1-3) …wird in der Zukunft von großer Bedeutung im China Geschäft sein."		

Alle Angaben beruhen auf Schätzung und Erfahrungswerten der Interviewpartner.

2) *Ausmaß von Risiken und Schäden für das Unternehmen durch Fälschungen:*

(bitte ankreuzen: 1 = gering, 6 = hoch)

	1	2	3	4	5	6	Kommentar:
2-1) Umsatzeinbußen							
2-2) Erhöhte Vertriebs- und Marketingkosten							
2-3) Produkthaftung / Schadensersatzrisiken							
2-4) Garantien / Gewährleistungen							
2-5) Kosten für Rechtsverfolgung / Schadensminderung							
2-6) Reputationsschaden durch minderwertige Plagiate							

3) Wirksamkeit und Durchführbarkeit der Schutzmaßnahmen:

a) Wirksamkeit: Schätzen Sie die Höhe der Risikominimierung bei Einführung der jeweiligen Schutzmaßnahme ein:

b) Durchführbarkeit: Schätzen Sie die Durchführbarkeit der jeweiligen Schutzmaßnahmen ein:

Bitte ankreuzen: 1= sehr wirksam, 4=nicht wirksam 1= durchführbar, 4 = nicht durchführbar

3-1) Betriebswirtschaftliche Schutzmaßnahmen	a) Wirksamkeit				b) Durchführbarkeit			
	1	2	3	4	1	2	3	4
3-1-1) Beschaffung/Lieferanten/Wareneingangskontrolle								
Einkaufskooperationen								
Lieferantenaudit								
Vertragsgestaltung (z.B. Einführung von Qualitätsstandards, potentielle Rückverfolgung der verwendeten Rohstoffe/Komponenten)								
Lieferantenschulungen								
Wareneingangskontrollen								
3-1-2) Personal								
Selektive Einstellung (z.B. Pre-Employment Screening, Einsatz von Expatriates auf technologische Top Positionen)								
Fluktuationsmanagement (z.B. Bindung der Mitarbeiter an das Urternehmen, finanzielle Anreize oder emotionale Bindung [Lob, Anerkennung, Entwicklungschancen])								

	a) Wirksamkeit				b) Durchführbarkeit			
	1	2	3	4	1	2	3	4
Geheimhaltungsklauseln								
Mitarbeiterschulungen (z.B. Sensibilisierung für Fälschungsproblematik)								
Job Rotation (vermeidet tiefgehendes Wissen von sensiblen Prozessen)								
Einführung von Richtlinien (z.B. das „Vier Augen Prinzip", „Need to know Prinzip", Funktionstrennung, transparente Buchführung usw.)								

3-1-3) Forschung und Entwicklung

Trennung von der restlichen Infrastruktur								
Verschleierung des Gesamtwissen über ein Produkt durch Teambildung								
Unterbindung von Technologietransfer								
Einführung von Komplementärprodukten								
Innovationsvorsprung								

3-1-4) Fertigung

Geheimhaltung (z.B. Pläne, Rezepte, Maschinenspezifikationen)								
Stichproben/Qualitätskontrollen								
Streuung des Gesamtprozesses auf mehrere Teams oder Produktionsstätten								
Fertigung sensibler Teile in Deutschland								
Outsourcing: Einführung zwingender Kontrollen und vergleichbarer Sicherheitssysteme								

	a) Wirksamkeit				b) Durchführbarkeit			
	1	2	3	4	1	2	3	4
3-1-5) Infrastruktur								
Zutrittskontrollen und Schutzsysteme								
Verbot von Verwendung elektronischer Geräte (z.B. Handys, Digitalkamera, PDAs..)								
Elektronische Schutzsysteme (z.B. einmal verwendbare Passwörter, Verschlüsselungen, Firewalls, Signaturen..)								
3-1-6) Vertrieb								
Verkaufsteams zur gegenseitigen Überprüfung der Mitarbeiter								
Rotation								
Zusammenstellung endkundengerechter Verbrauchseinheiten beim Hersteller								
Selektive Verkaufsstellen (Exklusivität)								
Auflagen der Händler (z.B. Schulungen des Verkaufspersonals, Sicherheitstechnologien...)								
Schulungen der Händler (zur Identifikation von Fälschungen, als Informationsquellen)								
Händleraudit/Zertifizierung								
Verzicht auf Händler (z.B. DELL)								

	a) Wirksamkeit				b) Durchführbarkeit			
	1	2	3	4	1	2	3	4
3-1-7) Vertriebsmodelle								
Direktvertrieb								
Franchising / Lizenzvergabe								
3-1-8) Distributionslogistik								
Lagerschutz								
Tracking&Tracing								
Efficient Customer Response (bedingt Verkürzung der Lieferkette, Just in Time Versorgung)								
3-1-9) Öffentlichkeitsarbeit								
Werbekampagnen und Veranstaltungen (z.B. Informationen über Gefahren)								
Erklärungen zur Identifikation								
Aggressives Auftreten (öffentliche Plagiatzerstörung)								
3-1-10) Marketing								
Enge Kundenbindung								
Individuelle Anpassung								
Anreiz durch Zusatzleistungen								

	a) Wirksamkeit				b) Durchführbarkeit			
	1	2	3	4	1	2	3	4
3-1-11) Kundendienst								
Garantieleistungen								
Schulungen/Hotlines/Updates								
3-1-12) Konsortium								
Zusammenschlüsse von Unternehmen zum Informations- und Erfahrungsaustausch, zu gemeinsamen Aktionen (z.B. Razzien)								
3-1-13) Joint Ventures								
3-2) Juristische Schutzmaßnahmen								
3-2-1) Anmeldung von Patent- und Markenrecht								
3-2-2) Zivilgerichtliche Durchsetzung								
3-2-3) Verwaltungsverfahren								
3-2-4) Einstweiliger Rechtsschutz								
3-2-5) Informelle Verfahren								
3-2-6) Strafrechtliche Verfahren								
3-2-7) Schiedsgerichtsverfahren								
3-2-8) Grenzbeschlagnahmeverfahren								

3-3)Technische Schutzmaßnahmen (nur die ankreuzen, die Sie einschätzen können)	a) Wirksamkeit						b) Durchführbarkeit					
3-3-1) Sichtbare Technologien												
Hologramm												
OVD/DOVID												
Sicherheitsfolie												
Sicherheitsetikette												
Sicherheitstinte												
Sicherheitspapier/druck												
3-3-2) Unsichtbare Technologien												
Mikrofarbstoff												
DNA Computing												
Nanotechnologie												
Nanobiotechnologie												
Isotope												
Chromogene Systeme												

	a) Wirksamkeit				b) Durchführbarkeit			
	1	2	3	4	1	2	3	4
3-3-3) Maschinengestützte Technologien								
RFID								
Barcode								
Chipkarte								
OCR								
Biometrie								
Klebestreifen als Datenträger								
Internet Monitoring								
Digitales Wasserzeichen								
Intelligente Verpackung								
Chemischer Marker								
Selbstzerstörungsmechanismus								
3-3-4) Kombinierte Technologien								
Track&Trace Technologie								

4) Hemmnisse der Schutzmaßnahmen:

Aus welchen Gründen sind die oben mit Stufe 6 angegebenen Schutzmaßnahmen nicht durchführbar? Mögliche Hemmnisse: (bitte nur zutreffende ankreuzen)

Sachkosten ☐

Personalkosten: ☐

Rechtsgrundlage ☐

Mangelnde Flexibilität ☐

Kommunikationsprobleme: ☐

Eingeschränkte Transportmöglichkeiten ☐

Weitere Hemmnisse: _____

5) Erfahrung mit Schutzmaßnahmen:

5.1) Wie viel der Anschaffungs- und Herstellungskosten eines Produktes würden Sie in Schutzmaßnahmen investieren? _____%

5.2) Wie viel wären Sie bereit in Summe vom Unternehmensumsatz in Schutzmaßnahmen zu investieren? _____%

Juristisch:	☐ Ja ☐ Bisher nicht ☐ Nicht vorgesehen ☐ Beabsichtigt
Technisch:	☐ Ja ☐ Bisher nicht ☐ Nicht vorgesehen ☐ Beabsichtigt
Betriebswirtschaftlich:	☐ Ja ☐ Bisher nicht ☐ Nicht vorgesehen ☐ Beabsichtigt

6) Haben Sie die jeweiligen Schutzmaßnahmen präventiv oder als Reaktion auf Fälschungen eingeführt?	
Präventiv	Reaktiv

7) Nehmen Sie externe Hilfe beim Kampf gegen Produktpiraterie in Anspruch?	
Ja	Nein

8) Allgemeine Fragen zum Unternehmen	
Unternehmen	
Mitarbeiterzahl	
Branche	

Interviewpartner	Name	
	Position	
	Adresse	
	Telefon	
	E-Mail	

Fälschungsschwerpunkt		
	Produkte	
	Marke	

Umsatz in €	Total		Jahr	

Standorte	Standort der Hauptgeschäftsstelle	
	Tätigkeit in China	

Selina C.W. Rehn

C Schutzmaßnahmen gegen Produktpiraterie im Funktionalbereich Marketing

Inhaltsverzeichnis

1 Produktpiraterie als Managementproblem 127

2 Grundlagen zur Produktpiraterie..... 128

2.1 Aktueller Stand und Ausmaß der Produktpiraterie 128

2.1.1 Geschichtlicher Hintergrund..... 128
2.1.2 Entwicklung von Produktpiraterie – Gründe für die schnelle Ausbreitung..... 129
2.1.3 Betroffene Sektoren..... 130
2.1.4 Herkunftsländer..... 131

2.2 Produkt- und Markenpiraterie 132

2.2.1 Erklärungsansätze 132
2.2.2 Erscheinungsformen 133
2.2.3 Grad der externen Bedrohung..... 134

2.3 Gefahren, die durch Produktpiraterie entstehen 135

2.3.1 Gefahren für den Staat 135
2.3.1.1 Entgangene Steuern und Zölle..... 135
2.3.1.2 Sicherheit und Wettbewerbsfähigkeit der Staaten..... 136

2.3.2 Gefahren für Unternehmen..... 136
2.3.2.1 Umsatz- und Gewinneinbußen..... 136
2.3.2.2 Beeinträchtigung der Branchenattraktivität und Verlust von Marktanteilen..... 137
2.3.2.3 Entstehung von Kosten 137
2.3.2.4 Markenverwässerung und Preisbeeinträchtigung..... 138
2.3.2.5 Graue Märkte 139

2.3.3 Gefahren für Konsumenten..... 140
2.3.3.1 Gefahren für die Gesundheit der Konsumenten 140
2.3.3.2 Gefahren durch gefälschte Ersatzteile 141
2.3.3.3 Gefahren durch eigenes Verschulden..... 141

2.4 Käufertypen ... 142
2.4.1 Bewusster sowie unbewusster Erwerb von Pirateriewaren ... 142
2.4.2 Konsumgüterkunden ... 143
2.4.3 Industriegüterkunden ... 144
2.5 Zukunftsentwicklung ... 145

3 Markteintrittsstrategie: Zeit als Wettbewerbsfaktor und Maßnahmen gegen Produktpiraterie ... 146
3.1 Megatrends, Trends und Moden ... 146
3.2 Timing-Strategien ... 147
3.2.1 First-Mover-Strategie vs. Follower-Strategie ... 147
3.2.2 Wasserfall-Strategie vs. Sprinkler-Strategie ... 149

4 Maßnahmen aus dem Bereich Marketing und Vertrieb zur Bekämpfung von Produktpiraterie ... 153
4.1 Multi-Level-Strategie im Marketing ... 153
4.2 Umsetzung konkreter Maßnahmen im Marketing-Mix ... 154
4.2.1 Produkt ... 154
4.2.1.1 Entwicklung schutzfähiger Produkte ... 154
4.2.1.2 Unterscheidung durch Produktqualität und Individualisierung ... 155
4.2.1.3 Innovationsmanagement – Verkürzung der Zyklen ... 157
4.2.1.4 Technische Maßnahmen zur Produktkennzeichnung ... 158
4.2.1.5 Intelligente Verpackung ... 160
4.2.2 Preis ... 161
4.2.2.1 Preispolitik ... 161
4.2.2.2 Konditionspolitik ... 162
4.2.2.3 Target-Cost-Management ... 162
4.2.3 Distribution ... 163
4.2.3.1 Management des Vertriebs ... 163
4.2.3.2 Selektive Vertriebssysteme ... 164
4.2.3.3 Schutz der Vertriebskette durch ECR ... 165
4.2.3.4 Distributionslogistik ... 165

4.2.4 Kommunikation ... 166
4.2.4.1 Kommunikations-Mix ... 166
4.2.4.2 Öffentlichkeitsarbeit ... 169
4.2.4.3 Kommunikationspolitik im eigenen Unternehmen ... 170
4.2.5 Kundenbetreuung/-bindung ... 170
4.2.5.1 After-Sales-Management ... 170
4.2.5.2 Customer-Relationship-Management ... 171

5 Maßnahmenevaluation ... 172
5.1 Wirkungshorizont der Maßnahmen ... 172
5.2 Operativer Maßnahmenplan ... 173
5.3 Strategischer Maßnahmenplan ... 173
5.4 Managementmodell zur Maßnahmenplanung entlang des Produktlebenszyklus ... 174

6 Marketing als Teil eines unternehmensweiten Schutzkonzeptes ... 176

Literaturverzeichnis ... 179

1 Produktpiraterie als Managementproblem

In den letzten zehn Jahren wurde eine Reihe wissenschaftlicher Studien durchgeführt, die alle eine erschreckende Ausbreitung von Produktpiraterie aufzeigen. Die meisten dieser Studien befassen sich jedoch nur mit juristischen oder technischen Methoden, um geistiges Eigentum vor Nachahmern zu schützen. Es erweist sich als schwierig, gute wirtschaftswissenschaftliche Forschungsarbeiten zu finden, welche die Verbindungen zwischen strategischen sowie operativen Maßnahmen und einem daraus resultierenden Rückgang der Produktpiraterie aufzeigen. Infolgedessen wird Produkt- und Markenpiraterie oftmals als rechtliches und nicht als Managementproblem angesehen.[1]

Produktpiraten konzentrieren sich vorwiegend auf das Kopieren gewinnversprechender Waren. Ist ein Produkt am Markt erfolgreich, so erhoffen sich Piraten durch billige Fälschungen schnell Gewinne erzielen zu können. Allerdings beschränken sich Piraten schon lange nicht mehr nur auf das Fälschen von Designersonnenbrillen oder -uhren. Branchenübergreifend lassen sich Fälschungen jeglicher Art und Ausgestaltung wiederfinden. Vor allem der Industriegütersektor, der noch vor einigen Jahren von Produktpiraterie verschont wurde, hat heute mit der Ausbreitung der Produktpiraterie stark zu kämpfen.

Daher ist es auch nicht verwunderlich, dass das Thema Produktpiraterie fast täglich in vielen Zeitungen und Zeitschriften diskutiert wird. Weltweit bieten Organisationen Veranstaltungen zum Thema Produktpiraterie an. Ganz gleich ob es sich hierbei um die WTO, das ICC, die OECD, das WIPO oder die ACG handelt, um nur einige der vielen Organisationen zu nennen. Gemeinsam versuchen sie Aufklärungsarbeit zu leisten und stellen sich in Diskussionen der Frage, wie sich Produktpiraterie effektiv bekämpfen lässt.

In diesem Beitrag werden der Hintergrund, die Entwicklung und die Auswirkung von Produktpiraterie analysiert. Anschließend werden Strategien und Maßnahmen gegen Produktpiraterie anhand der „4Ps“ bzw. „5Ps“ im Marketing erarbeitet und bewertet. In einem Managementmodell werden schließlich die Maßnahmen je nach Wirkungshorizont entlang des Produktlebenszyklus eingeordnet.

[1] Vgl. Harte-Bavendamm (2000), S. 1.

2 Grundlagen zur Produktpiraterie

2.1 Aktueller Stand und Ausmaß der Produktpiraterie

2.1.1 Geschichtlicher Hintergrund

Produktfälschung ist keineswegs ein neues Phänomen, das durch die Öffnung vieler Handelsgrenzen sowie durch die immer schneller voranschreitende Globalisierung entsteht. Allerdings mag dies durchaus ein Grund für das rasante Wachstum sein, da Waren heutzutage weltweit einfach und schnell von A nach B transportiert werden können. Bemerkenswert ist jedoch, dass die Geschichte der Produktpiraterie bis ins Römische Reich nachverfolgt werden kann:

Das französische Institut „Union des Fabricants“[2], das sich in der Nähe von Paris befindet, stellt eine Wein-Amphora zur Besichtigung aus, die aus dem Jahre 27 v. Chr. stammt. Diese Amphora ist angeblich eine der ersten geschichtlich festgehaltenen Fälschungen. Zu dieser Zeit galt guter italienischer Wein als einer der besten Weine Europas. Er war qualitativ sehr hochwertig und daher teurer als andere Weine. Um die Echtheit dieser Weine zu garantieren, versiegelten die italienischen Winzer ihre Weinflaschen mit einem Tonstöpsel, der die Initialen des Winzers enthielt. Indem die Echtheit der Weine sichergestellt war, konnten die Winzer für ihre hochwertigen Weine höhere Preise verlangen und somit mehr Gewinn erzielen. Eines Tages jedoch hatte ein gallischer Winzer die hinterlistige Idee, diese Tonstöpsel für seine billigen Weine zu kopieren, um somit ebenfalls höhere Preise verlangen zu können. Seine Kunden würden glauben, einen guten italienischen Wein zu kaufen, wofür sie gerne bereit waren, den höheren Preis zu zahlen.[3]

Betrachtet man das Motiv des gallischen Winzers, den Tonstöpsel zu kopieren, um einen höheren Gewinn zu erzielen, so ist es nicht schwer, eine Verbindung zu den Motiven heutiger Produktpiraten zu erkennen. Während der letzten Dekade ist Produktpiraterie zu einem wesentlichen internationalen Problem mit einem beachtlichen Einfluss auf die Weltwirtschaft geworden.

---

[2] Das „Union des Fabricants“ ist ein französisches Institut, dessen Aufgabe darin besteht, den Schutz des geistigen Eigentums auf internationaler Ebene sicher zu stellen.

[3] Vgl. Phillips (2005), S. 7-8.

2.1.2 Entwicklung von Produktpiraterie – Gründe für die schnelle Ausbreitung

In den meisten Industrien kann eine Zunahme in der Anzahl und dem Umfang gefälschter Produkte wahrgenommen werden. Dennoch gibt es bislang keine allgemeingültige Methode, um das Ausmaß von Produktpiraterie und die Verletzung geistigen Eigentums zu messen.[4] Es gibt keine exakte Zahl, die die weltweit entstandenen Verluste durch Produktpiraterie beziffert. Da gefälschte Produkte illegal hergestellt und somit nicht von öffentlichen Instanzen kontrolliert werden, scheint es unmöglich, das gesamte Volumen von Pirateriewaren weltweit ausfindig zu machen. Trotzdem gibt es eine Reihe von Organisationen, die verschiedene Schätzungen aufstellen. Laut einer quantitativen Studie der OECD könnte das Volumen an gefälschten, international gehandelten materiellen Gütern einer Summe von 200 Mrd. USD entsprechen, wobei diese Zahl weder Fälschungen, die für den Eigenverbrauch hergestellt werden, noch gefälschte Waren, die über das Internet vertrieben werden, enthält.[5]

Die WCO schätzt den Wert der gehandelten Pirateriewaren auf 512 Mrd. USD, was 7% des gesamten Welthandels entspricht.[6] Andere Expertenschätzungen weisen darauf hin, dass Unternehmen aufgrund von Produktpiraterie weltweit jährlich mehr als 20 Mrd. USD Verlust erzeugen.[7] Weiterhin zeigt die Statistik der Europäischen Kommission aus dem Jahr 2006 einen beträchtlichen Anstieg der registrierten Fälle zwischen 1999 und 2006. Wurden 1999 weniger als 5.000 Fälle gefälschter Waren registriert, waren es 2006 bereits 37.000 (Vgl. Abbildung 1).[8]

Der Anstieg im Jahr 2006 machte sich in fast allen Sektoren bemerkbar. Die meisten konfiszierten Artikel waren wie auch in den Jahren zuvor Zigaretten, gefolgt von CDs, DVDs, Kleidung und Accessoires. Zudem konnte wieder ein Anstieg an gefälschten Luxusgütern und Markenkleidung verzeichnet werden.[9] Der deutsche Zoll konnte beispielsweise 2007 in Hamburg 117 Container mit Markenwaren – vorwiegend Sportschuhe – in Beschlag nehmen.[10]

---

4 Vgl. ICC Studie (2007).
5 Vgl. OECD Studie 2007), S. 15.
6 Vgl. Phillips (2005), S. 3.
7 Vgl. Johansson (2000), S. 381.
8 Vgl. European Commission (2006), S. 2.
9 Vgl. European Commission (2006), S. 3.
10 Vgl. Stockinger (2007), S. 208.

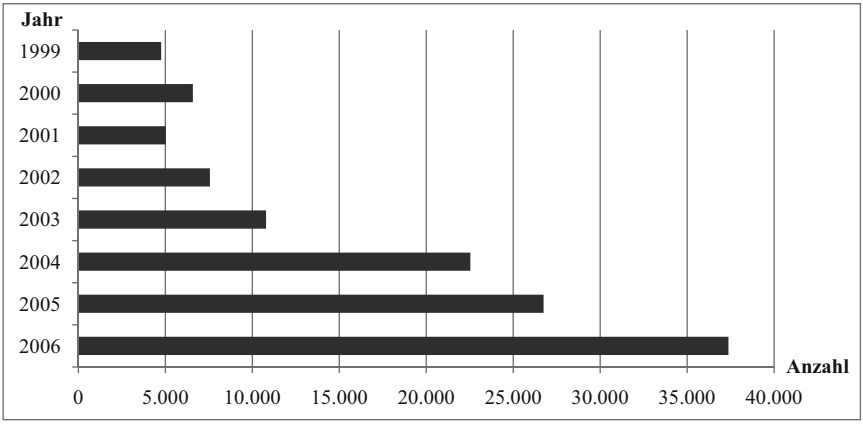


Abbildung 1: Anzahl registrierter Fälle 1999-2006
Quelle: European Commission (2006), S. 2.

Gründe für die schnelle Ausbreitung lassen sich auch in der andauernden Schnäppchenmentalität der westlichen Industrieländer wiederfinden.[11] Konsumenten versuchen heutzutage den möglichst günstigsten Preis zu zahlen und schrecken dabei immer weniger davor zurück, auf billige Pirateriewaren zurückzugreifen. Weiterhin steigt jährlich die Nachfrage nach Luxusartikeln. Konsumenten, die sich teure Originalwaren nicht leisten können, stillen ihr Verlangen oftmals durch billige Fälschungen und fördern somit das Pirateriegeschäft.

2.1.3 Betroffene Sektoren

Produktpiraterie betrifft schon lange nicht mehr ausschließlich die Konsumgüterindustrie oder globale Unternehmen mit starken Marken wie Adidas, Nike, Louis Vuitton oder Gucci, wie viele Konsumenten vermuten. Produktpiraterie hat einen alarmierend großen Einfluss auf grundsätzlich alle Industriebereiche: von Kleidung, Accessoires, Schmuck, Computer oder elektrischen Geräten bis hin zu Lebensmitteln, Spielzeug, Zigaretten, Alkohol, Maschinen und Software (Vgl. Abbildung 2).

Sogar komplette Unternehmenskonzepte werden nunmehr kopiert. Jedoch ist vor allem der Anstieg an gefälschten Arzneimitteln und Hygieneprodukten erschreckend. Ernsthafte gesundheitliche Risiken und Gefahren hinsichtlich der Sicherheit sind die Folge.

[11] Vgl. Fuchs (2006), S. 25.

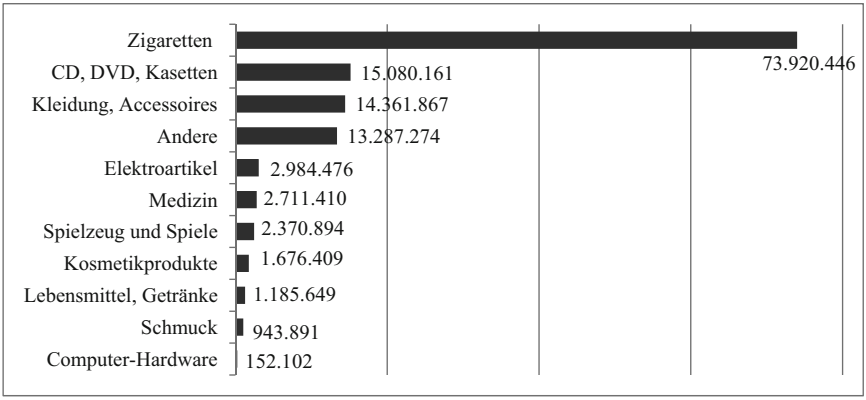


Abbildung 2: Betroffene Produktgruppen
Quelle: European Commission (2006), S. 3.

2.1.4 Herkunftsländer

Es ist festzustellen, dass gefälschte Produkte weltweit in allen Ländern hergestellt und vertrieben werden. Die OECD-Studie „The Economic Impact of Counterfeiting and Piracy 2007" zeigt, dass Asien sich als Nummer eins der Herkunftsgebiete abzeichnet, wobei China auch im Jahr 2007 das Hauptursprungsland bleibt.[12]

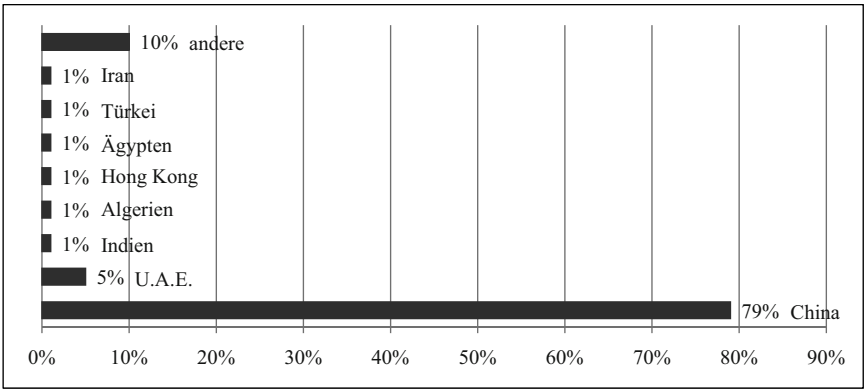


Abbildung 3: Herkunftsländer
Quelle: European Commission (2006), S. 4.

[12] Vgl. OECD Studie (2007), S. 13.

Die voranstehende Abbildung (Vgl. Abbildung 3) der Europäischen Kommission belegt ebenso, dass die meisten gefälschten Produkte vorwiegend aus China stammen. Neben China wird ein Großteil der Fälschungen in den Arabischen Emiraten hergestellt. Beachtlich ist, dass gerade einmal 10% der Pirateriewaren aus anderen Ländern wie z.B. den USA, Großbritannien oder auch Deutschland stammen. Dies zeigt deutlich, dass der asiatische Raum ein Ballungsgebiet für illegale Kopien ist.

2.2 Produkt- und Markenpiraterie

2.2.1 Erklärungsansätze

Hohe Absatz- und Gewinnchancen sind die Treiber für die steigende Attraktivität einer Branche. Die Produktpiraten handeln nach demselben wirtschaftlichen Muster wie der Originalhersteller: maximaler Output bei minimalem Input. Jedoch agieren sie nicht nach denselben Spielregeln. Indem sich Piraten ausschließlich auf das Kopieren erfolgreicher Produkte konzentrieren, geht für sie das Absatz- und Erfolgsrisiko gegen Null.

Piraten treten nur als frühe oder späte Folger auf Märkten auf. Durch das Ausnutzen fremden Know-hows sparen sich Piraten hohe Kosten für die Forschung und Entwicklung der Produkte.[13] Dies ermöglicht ihnen, trotz niedriger Preise hohe Margen durchzusetzen, schnell Marktanteile zu gewinnen und somit erhebliche Profite zu erzielen.

Hinzu kommt, dass die Gefahr der Rechtsverfolgung in den Herkunftsländern relativ gering ist und die westlichen Nationen ihre Möglichkeiten auf diesem Gebiet bei weitem nicht voll ausschöpfen.[14] Dies setzt allerdings auch voraus, dass Rechteinhaber die Märkte überwachen und gegebenenfalls ihre Rechte, wie z.B. Patent- oder Markenrechte, geltend machen.

Darüber hinaus profitieren Piraten oftmals vom Unwissen der Konsumenten. Liegt der Preis für die gefälschte Ware lediglich wenige EUR unter dem Verkaufspreis des Originals, greift der Käufer leicht zu gefälschter Ware, ohne dies zu bemerken.[15]

[13] Vgl. Wildemann (2007), S. 11.
[14] Vgl. Welser/González (2007), S. 22.
[15] Vgl. Fuchs (2006), S. 39.

2.2.2 Erscheinungsformen

Fälschung und Piraterie sind zwei Begriffe, die vorwiegend verwendet werden, wenn es darum geht, gesetzeswidrige Handlungen zu beschreiben, die in Verbindung mit der Verletzung geistigen Eigentums stehen.[16] Kopie, Knockoff, Imitat und Plagiat sind weitere Begriffe, die in Studien und in der Literatur oftmals als Synonyme verwendet werden.

Zusätzliche Formen von Produktpiraterie verstecken sich hinter Begriffen wie Reverse Engineering oder Bootlegging. Beim Reverse Engineering werden Originalprodukte umfassend analysiert und deren Lösungen unrechtmäßig zur Herstellung gefälschter Waren weiterverwendet. Bootlegging bezeichnet das geheime Mitschneiden und Vertreiben künstlerischer Leistungen.[17]

Weiterhin lassen sich Erscheinungsformen von Produktpiraterie nach Art der Rechtsverletzung unterscheiden, genau genommen nach Art der Verletzung des geistigen Eigentums: Patentverletzung, Gebrauchs- oder Geschmacksmusterverletzung, Markenverletzung oder auch Urheberrechtsverletzung.

Hans Joachim Fuchs unterscheidet Produktpiraterie nach folgenden vier Formen, die auch in kombinierter Weise auftreten können:

- Produkte aus gleichem Material, die unter gleichem oder ähnlichem Produktnamen angeboten werden,
- Produkte, die aus einfachem Material hergestellt werden und daher zu günstigeren Preisen verkauft werden,
- verwechselbare Produkte, die das positive Image des Originalherstellers ausnutzen, allerdings zu einem niedrigeren Preis angeboten werden. Hier handelt es sich vorwiegend um Markenpiraterie, und
- Produkte, die vom Original abweichen, jedoch durch die Verwendung einer ähnlichen Gesamterscheinung beim Kunden positive Assoziationen hervorrufen.[18]

Horst Wildemann fügt noch eine weitere Form hinzu:

- Produkte, die unter Verwendung fremden geistigen Eigentums hergestellt wurden, allerdings nicht mit dem Original verwechselt werden.[19]

[16] Vgl. OECD Studie (2007), S. 8.
[17] Vgl. Fuchs (2006), S. 30.
[18] Vgl. Fuchs (2006), S. 28.

2.2.3 Grad der externen Bedrohung

Eine weitere Möglichkeit, Formen von Produktpiraterie zu unterscheiden, ist nach Grad der externen Bedrohung, die Produktpiraten für Unternehmen darstellen (Vgl. Abbildung 4). Je nachdem, ob die Piraten das komplette Produktprogramm, einzelne Produkte oder nur Produktteile kopieren, können die Folgen für das Unternehmen sehr unterschiedlich sein.

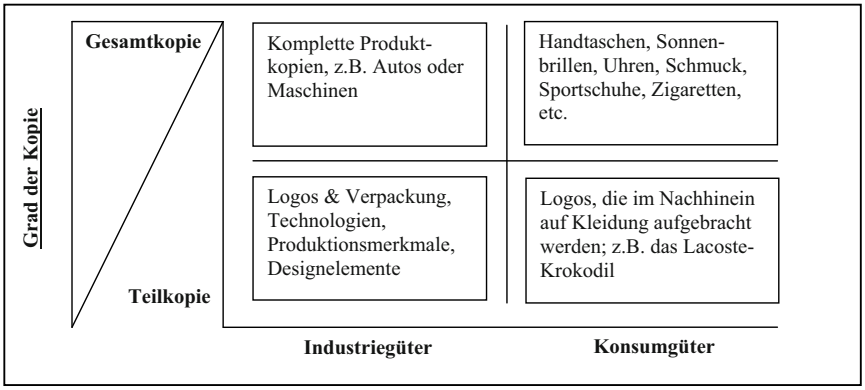


Abbildung 4: Grad der externen Bedrohung
Quelle: eigene Darstellung.

Produkte können in der Industrie- sowie Konsumgüterbranche als Gesamt- oder Teilkopien auftreten. Vor allem vollständige Produktkopien stellen eine große Bedrohung für Unternehmen dar. Sinken Absatzzahlen aufgrund kompletter Produktfälschungen, die zu günstigeren Preisen angeboten werden, so besteht die Gefahr, dass hohe Kosten, die für Forschung und Entwicklung neuer Produkte entstehen, sich nicht zeitgerecht amortisieren. Ferner stellen auch Teilkopien wie gefälschte Logos und Verpackungen, die für den Betrachter auf den ersten Blick oftmals nicht zu erkennen sind, eine Gefahr dar.

So lässt sich nicht leugnen, dass Konsumenten beim Anblick des Logos „Hongda“ eine sofortige Verbindung zum Markennamen „Honda“ herstellen. Der Konsument as-

[19] Vgl. Wildemann (2007), S. 20.

soziiert mit der Marke Honda eine bestimmte Qualität und überträgt diese auf das Plagiat.[20]

Ist das Produkt, welches unter dem ähnlichen Logo angeboten wird, womöglich viel günstiger als das Original, so wird der Konsument höchstwahrscheinlich aufgrund des erwarteten Preis-/Leistungsverhältnisses auf die Fälschung zurückgreifen. Somit gehen potentielle Kunden des Originalherstellers an Markenpiraten verloren.

2.3 Gefahren, die durch Produktpiraterie entstehen

2.3.1 Gefahren für den Staat

2.3.1.1 Entgangene Steuern und Zölle

Es ist nicht zu übersehen, dass Produktpiraterie immer gefährlicher für die Entwicklung der Weltwirtschaft wird. Indem Produktpiraten bei der Ein- und Ausfuhr von Waren Steuerzahlungen umgehen, gehen vielen Staaten immens hohe Forderungen aus Steuern und Zöllen verloren. Vor allem bei stark besteuerten Konsumgütern wie Zigaretten und Alkohol sind die Steuerausfälle beträchtlich.[21] Zusätzlich werden gefälschte Waren meist von Schwarzarbeitern gefertigt, die weder Einkommenssteuern zahlen, noch soziale Abgaben leisten.

In den exportabhängigen Industrienationen ist die Vernichtung rechtmäßiger Arbeitsplätze unter anderem ein Grund für die steigende Arbeitslosenquote. In Deutschland wird der jährlich entgangene Gewinn aufgrund von Produktpiraterie auf 30 Mrd. EUR geschätzt, was umgerechnet einem Verlust von 70.000 Arbeitsplätzen entspricht.[22] Die Vereinigung zur Bekämpfung von Produktpiraterie (VBP) schätzt den Verlust von Arbeitsplätzen sogar auf insgesamt 300.000 in Europa.[23] Durch den Verlust von Arbeitsplätzen steigen die staatlichen Sozialausgaben, da immer mehr Arbeitslose sozialhilfebedürftig werden.[24]

[20] Vgl. Fuchs (2006), S. 29.
[21] Vgl. OECD Studie (2007), S. 17.
[22] Vgl. o.V. (2007).
[23] Vgl. Vereinigung zur Bekämpfung von Produktpiraterie e.V. (2007).
[24] Vgl. Welser/González (2007), S. 54.

2.3.1.2 Sicherheit und Wettbewerbsfähigkeit der Staaten

Die Ausdehnung der Schwarzmärkte bringt meist auch eine Zunahme der Kriminalität mit sich, wodurch viele Staaten an Sicherheit verlieren. Dies führt wiederum zu einem Verlust des öffentlichen und wirtschaftlichen Vertrauens.

Heute wirft der Handel mit Pirateriewaren oftmals mehr Profit ab als der Handel der Drogenkartelle mit illegalen Drogen. Diese durch Produktpiraterie erzielten Gewinne werden häufig zur finanziellen Unterstützung anderer krimineller Handlungen verwendet. Daraus lässt sich schließen, dass Staaten mit einer höheren Pirateriequote meist auch eine höhere Kriminalitätsquote aufweisen. Relativ milde Strafen und ungenaue Kontrollen beim Zoll ermöglichen Kriminellen den einfachen und schnellen Aufbau eines weitreichenden Piraterienetzwerkes.[25] Staaten, die die Bekämpfung von Produktpiraterie nicht ernst nehmen und nicht genug dagegen tun, riskieren ihren guten internationalen Ruf. Die daraus folgenden Konsequenzen sind weniger ausländische Investitionen sowie der Verlust von Know-how.[26] Um das Risiko, von Produktpiraterie betroffen zu sein, zu minimieren, verzichten bereits heute einige Unternehmen auf die Expansion in asiatische Länder. Ferner kann auch dies die innovative Stärke und die Wettbewerbsfähigkeit eines Landes langfristig negativ beeinflussen.

2.3.2 Gefahren für Unternehmen

2.3.2.1 Umsatz- und Gewinneinbußen

In den betroffenen Industrien verursacht das Auftreten von Produktpiraterie für viele Unternehmen riesige Umsatz- und Gewinneinbußen. Eine Studie, die vom VDMA im März 2007 durchgeführt wurde, besagt, dass 67% der befragten Unternehmen in der Investitionsgüterindustrie bereits von Produktpiraterie betroffen sind. Im Vergleich zu 2006 stieg diese Zahl um 1% an. Weiterhin schätzen 18% der befragten Unternehmen ihre jährlichen Umsatzeinbußen auf 10%. Immerhin 4% der Unternehmen schätzen die Umsatzeinbußen auf 20%. Weitere 27% rechneten mit Umsatzeinbußen von 5%. Weit mehr als die Hälfte der befragten Unternehmen (78%) erwarten, dass Produktpiraterie langfristig ihre Wettbewerbsposition beeinflussen wird.[27] Piraten, die als neue Wettbewerber in Märkte eindringen oder Ersatzprodukte anbieten, sind der Grund, weshalb

[25] Vgl. OECD Studie (2007), S. 15.
[26] Vgl. Fuchs (2006), S. 54.
[27] Vgl. VDMA-Untersuchung (2007), S. 3.

die Nachfrage an Originalwaren zurückgeht. Somit verlieren Unternehmen wichtige Marktanteile an Produktpiraten. [28]

2.3.2.2 Beeinträchtigung der Branchenattraktivität und Verlust von Marktanteilen

Die Entwicklung einer Branche ist laut Porter von den fünf Wettbewerbskräften abhängig. Die so genannten „Five Forces" setzen sich zusammen aus: den vorhandenen Wettbewerbern, der Verhandlungsmacht der Lieferanten, der Verhandlungsmacht der Kunden, aus neuen Wettbewerbern sowie aus Substitutprodukten und -dienstleistungen. Wie stark diese Kräfte tatsächlich wirken, hängt vom jeweiligen Gewinnpotential einer Branche ab. Ist das Gewinnpotential einer Branche hoch, so herrscht meist ein vollkommener Wettbewerb, in dem jeder um die beste Marktposition kämpft.[29] Genau hier setzen auch Produktpiraten an. Da Produktpiraten nicht nach den üblichen Regeln des Wettbewerbs handeln, gestaltet sich das Eindringen in diese hart umkämpften Märkte für sie als recht einfach. Sie treten als neue Wettbewerber auf und verstärken somit den Wettbewerb dieser Branche. Das vergrößerte Angebot, womöglich zu günstigen Preisen, verschlechtert die Attraktivität der Branche und stärkt sogleich die Verhandlungsmacht der Lieferanten und Konsumenten.[30] Folglich verschlechtert sich die Marktsituation; es gehen Marktanteile verloren und langfristige Profite werden schwer realisierbar. Um herauszufinden, wo eine Branche anfällig für das Eindringen neuer Wettbewerber ist, sollten die einzelnen Kräfte einer Branche regelmäßig gründlich analysiert werden.[31] Dadurch kann einem Angriff durch Produktpiraten rechtzeitig entgegengewirkt werden.

2.3.2.3 Entstehung von Kosten

Die Auswirkungen von Produktpiraterie sind komplex und betreffen beide Seiten, zum einen die operative Dimension der Positionierung und den Marktanteil auf internationalen Märkten, zum anderen die strategische Perspektive von Unternehmen. Wie bereits erwähnt, verringert Piraterie die Attraktivität einer Branche und vernichtet Marktanteile, die in dieser operationalen Interpretation in Opportunitätskosten resultieren. Diese Opportunitätskosten lassen sich im Grunde genommen als entgangene Gewinne

[28] Vgl. Fuchs (2006), S. 47.
[29] Vgl. o.V. (2006), S. 7.
[30] Vgl. Wildemann (2007), S. 112.
[31] Vgl. o.V. (2006), S. 8.

für das Unternehmen interpretieren. Das weltweit geschätzte Volumen an Pirateriewaren beträgt jährlich 7% des gesamten Welthandels, was einem Gewinnverlust von weltweit 200 Mrd. USD ausmacht. Um die Kosten für Forschung und Entwicklung neuer Innovationen zu decken, müssen Gewinne in einem Mindestzeitraum generiert werden. Entgangene Gewinne zu Beginn einer Produkteinführung schlagen sich wiederum direkt in einer Verlängerung des Mindestzeitraums nieder.[32]

Weiterhin entstehen durch die Bekämpfung von Produktpiraterie Kosten für die Unternehmung. Es handelt sich hierbei zum Beispiel um Kosten für die Anmeldung von Patenten, Gebrauchs- und Geschmacksmustern, Marken, Kosten für die Überwachung von Märkten, für die Entwicklung und Anbringung technischer Schutzmaßnahmen oder auch Kosten, die durch die Errichtung unternehmensinterner Schutzabteilungen entstehen. Die wahrscheinlich folgenschwerste Konsequenz der Produktpiraterie ist der Verlust von Know-how. Wenn Know-how, das zur Entwicklung neuer innovativer Produkte verwendet wurde, abfließt, verliert das Produkt nicht nur seine Exklusivität und Einzigartigkeit, sondern es geht auch der Wettbewerbsvorteil des Unternehmens verloren.[33] Dieser strategische Einfluss erodiert langfristige Unternehmenserfolge.

2.3.2.4 Markenverwässerung und Preisbeeinträchtigung

Wenn Markenwaren – Originale sowie entsprechende Fälschungen – millionenfach angeboten werden, ist es sehr wahrscheinlich, dass das Markenimage an Bedeutung verliert. Folglich entsteht eine Verwässerung der Marke. Um eine starke Marke aufzubauen, die von Kunden wiedererkannt und unterstützt wird, investieren Originalhersteller hohe Summen. Daher ist es nicht schwer zu erkennen, wie ruinös die Vernichtung einer Marke für eine Unternehmung sein muss.[34] Marken sind immaterielle Wirtschaftsgüter, die einen bedeutenden Beitrag zum Unternehmenswert leisten.

Interbrand stellt jährlich ein Ranking der 100 erfolgreichsten globalen Marken auf. Im Jahr 2007 betrug der Markenwert von Louis Vuitton 20.231 Mio. USD, Nikes Markenwert lag bei 12.004 Mio. USD und der Markenwert von Rolex betrug 4.589 Mio. USD (Vgl. Tabelle 1).[35] Jede dieser Marken wird von Produktpiraten weltweit in großem Maße gefälscht. Markenwerte, die im zweistelligen Milliardenbereich liegen, ma-

[32] Vgl. Fussan (2007/2008).
[33] Vgl. Wildemann (2007), S. 7.
[34] Vgl. The Patent Office (2007), S. 4.
[35] Vgl. Interbrand (2007), S. 13, 14, 16.

chen deutlich, wie wichtig es für Unternehmen ist, ihre Marken vor einer Markenverwässerung zu schützen.

Laut Fuchs ist es nicht unwahrscheinlich, dass über einen Zeitraum von 10 Jahren ein Markenwert in bestimmten Teilmärkten um einen drei- bis vierstelligen Millionenbetrag reduziert werden kann. Dabei wird ein Erosionsfaktor von 10% unterstellt.[36] Da der Markenwert von Interbrand für alle Märkte global errechnet wird, lässt sich bei einigen Luxusmarken trotzdem ein Wachstum des Markenwertes zwischen 2001 und 2007 feststellen.

Tabelle 1: Markenwerte
Quelle: Interbrand (2001); Interbrand (2007).

2001			2007		
Rang	**Marke**	**Markenwert**	**Rang**	**Marke**	**Markenwert**
5	Nokia	35.040 Mio. USD	5	Nokia	33.696 Mio. USD
20	Sony	15.010 Mio. USD	25	Sony	12.907 Mio. USD
21	Honda	14.640 Mio. USD	19	Honda	17.998 Mio. USD
34	Nike	7.590 Mio. USD	29	Nike	12.004 Mio. USD
38	Louis Vuitton	7.050 Mio. USD	17	Louis Vuitton	20.321 Mio. USD
50	Gucci	5.360 Mio. USD	46	Gucci	7.697 Mio. USD
61	Chanel	4.470 Mio. USD	58	Chanel	5.830 Mio. USD
69	Rolex	3.70 Mio. USD	71	Rolex	4.589 Mio. USD
70	Adidas	3.650 Mio. USD	69	Adidas	4.767 Mio. USD

Eine weitere Bedrohung ist, dass ein Überangebot die Preiselastizität eines Produktes beeinflusst. Um ihre Marktposition zu verteidigen, sind Originalhersteller oftmals dazu gezwungen, ihre Preise an die niedrigen Preise der Fälschungen anzupassen.[37]

2.3.2.5 Graue Märkte

Nicht nur Schwarzmärkte wachsen in ihrer Größe und Anzahl. Auch graue Märkte werden zu einer immer größeren Gefahr für Unternehmen. Graumärkte entstehen, wenn Lizenznehmer so genannte „overruns“ produzieren. „Overruns“ kommen zu Stande, indem Lizenznehmer ihre Maschinen noch nach Produktionsschluss weiter laufen lassen und somit über das genehmigte Produktionsvolumen hinweg produzieren.[38] Waren, die aus der illegalen Überproduktion stammen, gelangen meist sogar

[36] Vgl. Fuchs (2006), S. 49.
[37] Vgl. Wildemann (2007), S. 6.
[38] Vgl. Fuchs (2006), S. 28.

über legale Distributionswege in den Handel. Da diese Produkte auf den gleichen Maschinen gefertigt werden wie die Originale, sind sie zumeist auch von selber Qualität.

Dennoch werden sie zu günstigeren Preisen angeboten, weshalb sie für Konsumenten eine attraktive Alternative zum Original darstellen. Durch illegale Parallelimporte und Fabrik-Overruns auf grauen Märkten verlieren Originalhersteller zunehmend Marktanteile. Laut einer KPMG-Studie verlieren IT-Unternehmen aufgrund unrechtmäßiger Überproduktion auf grauen Märkten jährlich bis zu 5 Mrd. USD.[39]

2.3.3 Gefahren für Konsumenten

2.3.3.1 Gefahren für die Gesundheit der Konsumenten

Experten schätzen, dass in der Volksrepublik China jedes Jahr 150.000 bis 200.000 Menschen aufgrund falscher Medikamente sterben.[40] Eine Studie der Europäischen Kommission zeigt, dass Indien an erster Stelle im Bereich gefälschter Medikamente steht, gefolgt von den Vereinigten Emiraten und China. Diese drei Länder sind verantwortlich für 80% aller gefälschten Medikamente weltweit.[41] Vor allem in Entwicklungsländern, in denen sich die Menschen aufgrund großer Armut die teuren Originalmedikamente nicht leisten können, tauchen massenhaft gefälschte Medikamente für tödliche Krankheiten wie Malaria, Tuberkulose oder Aids auf. Ganz im Gegensatz zu den reicheren Industrienationen: Hier konzentrieren sich Produktpiraten vor allem auf Lifestyle-Produkte wie Viagra oder Hormonpräparate. Aufgrund der steigenden Nachfrage und der relativ kostengünstigen Herstellung ist die Produktion gefälschter Medikamente für Produktpiraten besonders lukrativ und stellt somit eine große Bedrohung für Pharmaunternehmen dar.[42]

Laut WHO ist in den meisten entwickelten Ländern wie den USA, der EU, Australien, Kanada, Japan und Neuseeland der Anteil gefälschter Medikamente relativ gering. Er beträgt weniger als 1% des Marktvolumens. Jedoch wird sogar in diesen Ländern ein Anstieg erwartet. Den Kontrast hierzu bilden Entwicklungsländer wie Afrika, Teile Asiens und Teile Lateinamerikas: Hier beträgt der Anteil gefälschter Medikamente mehr als 30% des Marktvolumens. Andere Entwicklungsländer hingegen haben ledig-

[39] Vgl. Economist Corporate Network (2005), S. 10.
[40] Vgl. Fuchs (2006), S. 51.
[41] Vgl. European Commission (2006), S. 5.
[42] Vgl. Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (2005), S. 44.

lich einen Anteil von weniger als 10% des Gesamtmarktes. Vor allem der Erwerb günstiger Arzneimittel über das Internet kann für Konsumenten sehr gefährlich sein. Über 50% der Medikamente, die im Internet ohne Angabe einer realen Adresse gekauft werden, erweisen sich als Fälschung.[43]

Des Weiteren ist vergiftete Zahnpasta, die im Juli 2007 auf dem amerikanischen Markt entdeckt wurde[44], nur einer von vielen Fällen, die belegen, dass Produktpiraterie jeden Konsumenten tagtäglich betreffen kann. Gefälschtes Parfüm, Body Lotion und sogar Kleidung, die mit giftigen Farben gefärbt wurde, kann Hautirritationen und Allergien hervorrufen.[45]

2.3.3.2 Gefahren durch gefälschte Ersatzteile

Gefälschte Ersatzteile, die in Autos oder Flugzeugen eingebaut werden, stellen eine weitere große Gefahr für Konsumenten dar. Als Beispiel kann der Absturz des American-Airlines-Flugzeuges 587 im Jahre 2001, bei dem 265 Passagiere ihr Leben verloren, genannt werden. Die Ursache für das Unglück waren gefälschte Ersatzteile, die in das Flugzeug eingebaut wurden.[46]

Eine Studie, die 2007 vom VDMA durchgeführt wurde, belegt den Anstieg gefälschter Ersatzteile: 42% der befragten Unternehmen gaben an, von gefälschten Ersatzteilen betroffen zu sein – vergleichsweise waren 2006 lediglich 20% der befragten Unternehmen betroffen.[47] Vor allem die Automobilindustrie hat stark mit den Auswirkungen gefälschter Ersatzteile zu kämpfen. So gut wie jedes Teil wurde bereits kopiert: Bremsbeläge, Achsen, Windschutzscheiben, jegliche Metallteile und sogar Airbags. Diese gefälschten Ersatzteile sind meist von geringer Qualität, was sie zu einer sehr großen Gefahr für Konsumenten werden lässt.

2.3.3.3 Gefahren durch eigenes Verschulden

Konsumenten, die gewollt Pirateriewaren kaufen, riskieren es, verurteilt zu werden. Der Erwerb gefälschter Produkte stellt im Grunde genommen eine illegale Handlung dar. Vor allem italienische Behörden ergreifen drastische Maßnahmen, um gegen den

[43] Vgl. WHO (2006), S. 1.
[44] Vgl. Lachmann et al. (2007).
[45] Vgl. Welser/González (2007), S. 53.
[46] Vgl. Fuchs (2006), S. 50.
[47] Vgl. VDMA-Untersuchung (2007), S. 1.

Schwarzmarkt anzukämpfen. 2005 wurde eine dänische Touristin, die sich eine gefälschte Dior-Sonnenbrille zugelegt hatte, von der italienischen Polizei verhaftet und mit einem Bußgeld in Höhe von 10.000 EUR bestraft.[48] Obwohl noch nicht jedes Land vergleichbar harte Strafen durchsetzt, ist eine positive Entwicklung im Kampf gegen Produktpiraterie in fast allen europäischen Staaten zu erkennen.

Darüber hinaus können Konsumenten, die wissentlich oder unwissentlich gefälschte Waren erwerben, keine Garantieansprüche bei den Originalherstellern geltend machen. Geht zum Beispiel eine gefälschte Kamera kaputt, kann der Kunde nicht erwarten, dass er sie beim Originalhersteller kostenlos reparieren lassen kann.

2.4 Käufertypen

2.4.1 Bewusster sowie unbewusster Erwerb von Pirateriewaren

Es ist ebenfalls interessant, einen Blick auf die verschiedenen Käufertypen zu werfen, die gefälschte Waren erwerben. In seinem Buch „Counterfeiting Exposed" verwendet Hopkins eine so genannte „Harm Matrix", um den Grad der Täuschung sowie die von Produktpiraterie betroffenen Parteien darzustellen.

Täuschung		**Qualität**
hoch	Billige Produkte, die vom Original schwer zu unterscheiden sind.	Fälschungen von hoher Qualität, die vom Käufer in der Annahme, es handele sich um ein Original, erworben werden.
gering	Fälschungen, die leicht als Kopie zu erkennen sind und absichtlich erworben werden.	Overruns oder qualitativ hochwertige Produkte, die leicht als Fälschung zu erkennen sind, jedoch bewusst erworben werden.
	gering	hoch

Abbildung 5: Grad der Täuschung
Quelle: Hopkins (2003), S. 11.

Die Matrix (Vgl. Abbildung 5) zeigt, dass manche Kunden absichtlich Pirateriewaren erwerben, andere jedoch nicht. Ist der Grad der Täuschung hoch, bemerkt der Konsument selten, dass er eine Fälschung erworben hat. Ist der Täuschungsgrad hingegen

[48] Vgl. Fuchs (2006), S. 52.

niedrig, so handelt es sich in der Regel um bewusst getätigte Käufe, bei denen sich der Kunde über die Fälschung im Klaren ist.

2.4.2 Konsumgüterkunden

Bei Konsumgüterkunden lassen sich bewusste Käufe von unbewussten leicht nach Segmenten unterscheiden. Vor allem bei Luxusartikeln, die sich viele Konsumenten nicht leisten können, wird immer wieder bewusst auf billigere Fälschungen zurückgegriffen. Mit steigender Qualität der Fälschungen wächst jedoch auch die Nachfrage bei Kunden, die sich die Originalwaren leisten könnten. Es spielt keine Rolle mehr, ob es ein Original ist oder nicht. Bedeutend ist nur, ob das Produkt mit dem richtigen Etikett oder Logo versehen ist. Dies allein kann das Bedürfnis, eine bestimmte Ware besitzen zu wollen, stillen.

Eine Studie des Ledbury Research zeigte, dass im Jahr 2006 bereits 5% der britischen Bevölkerung mindestens einen gefälschten Luxusartikel erwarben. Interessanterweise stieg im selben Jahr auch der Verkauf von Originalen um 4%. Dies macht deutlich, dass weiterhin eine große Nachfrage nach Luxuswaren besteht, wodurch für Produktpiraten die Chance, ihre Marktanteile auszubauen, erhöht wird.[49]

Der stetige Anstieg gefälschter Luxusartikel zeigt, dass vielen Kunden die negativen Folgen, die die Käufe von Pirateriewaren mit sich bringen, nicht bewusst sind. Erst wenn sie selbst von den Folgen betroffen sind, werden Konsumenten aufmerksam.

Vorwiegend bei Medikamenten, die über das Internet bezogen werden, erwerben Käufer häufig ungewollt Fälschungen. Eine große Gefahr für den Kunden besteht dann, wenn die Täuschung hoch, die Qualität hingegen sehr gering ist, und es durch das Piraterieprodukt zu gesundheitlichen Schäden beim Käufer kommt.

Darüber hinaus lassen sich Käufer von Pirateriewaren im Segment der Konsumgüterkunden durch alle sozialen Käuferschichten hinweg wiederfinden. Es ist kaum möglich, den typischen Käufer von Pirateriewaren kategorisch zu bestimmen, da Käufer von Pirateriewaren zumeist auch Käufer von Originalwaren sind.[50]

[49] Vgl. Ledbury Research (2007), S. 5.
[50] Vgl. Ledbury Research (2007), S. 6.

2.4.3 Industriegüterkunden

Industriegüterkunden erwerben Pirateriewaren eher selten bewusst. Vorwiegend Fälschungen von niedriger Qualität und hohem Täuschungsgrad stellen eine große Bedrohung für Industriekunden dar. Gelangt zum Beispiel ein gefälschtes Modul durch einen Sublieferanten unerkannt in den Produktionsprozess, kann dies weitreichende Folgen für das Unternehmen haben. Das qualitativ minderwertige Bauteil verringert höchstwahrscheinlich die Qualität des Endproduktes, wodurch Probleme beim Kunden des Unternehmens auftreten können.

Darüber hinaus können durch die unerkannte Pirateriewaren hohe Kosten für das Unternehmen entstehen: Zum einen durch eine Rückrufaktion der bereits ausgelieferten Waren minderer Qualität, zum anderen durch einen erhöhten Ansturm im Kundenservice und einen möglichen Regressanspruch von Seiten des Kunden. Um die eigene Wertschöpfungskette vor Produktpiraterie zu schützen, werden Industriekunden gezwungen, die Ausgaben für Wareneingangskontrollen zu erhöhen.

Das Beispiel eines chinesischen Generatorbauers aus Taizhou zeigt deutlich, wie wichtig die Kontrolle von Eingangswaren heutzutage ist: Er erwarb von seinem Zulieferer einen gefälschten Generatorkern, der allerdings erst vom Endkunden entdeckt wurde. Haftbar für die Fälschung war jedoch der Generatorbauer selbst.[51]

Ein anders Beispiel aus der Druckerindustrie sind gefälschte Druckerpatronen oder Druckerpatronen, die mit billiger Tinte wieder aufgefüllt wurden. Das Problem entsteht, wenn große Unternehmen unwissend diese Fälschungen erwerben und daraufhin den Originalhersteller anrufen, um den Drucker, der durch den Gebrauch der falschen Patrone defekt geworden ist, reparieren zu lassen. Der Originalhersteller muss sich daraufhin entscheiden, ob er den Drucker repariert, obwohl der Schaden nicht auf ihn zurückzuführen ist, oder ob er die Reparatur verweigert und somit den Verlust eines großen Industriekunden riskiert.[52] Beide Beispiele zeigen deutlich, wie Produktpiraten in alle Bereiche der Wertschöpfungskette eingreifen.

[51] Vgl. Fuchs (2006), S. 219.
[52] Vgl. Economist Corporate Network (2005), S. 12.

2.5 Zukunftsentwicklung

Sollte sich Piraterie weiterhin so rasch ausbreiten, wie es in den letzten fünf Jahren der Fall war, so lässt sich ein erschreckendes Zukunftsszenario ausmalen. Folglich müsste damit gerechnet werden, dass das Gesamtvolumen an Pirateriewaren in den nächsten 5-10 Jahren von heute 7% der weltweit gehandelten Waren bis auf 15% oder gar 20% ansteigt.

Ganze Märkte oder Marktsegmente, die von Pirateriewaren überflutet werden, könnten zusammenbrechen. Durch den Verlust von Marktanteilen würden viele Unternehmen ihre Wettbewerbsfähigkeit verlieren und in Konkurs gehen. Das unerkannte Eindringen von Pirateriewaren in die Wertschöpfungskette hätte eine sinkende Produktivität zur Folge, wodurch Betriebe nicht mehr wirtschaftlich profitabel zu führen wären. Kooperationen mit anderen Partnern würden aus Angst des Know-how-Verlustes nicht mehr eingegangen und neue Vertriebswege, die zum Beispiel durch das Internet entstanden sind, müssten wieder aufgegeben werden. Die Folge wäre ein Rückschritt in der Entwicklung der Wirtschaft.

Durch eine rezessive Konjunktur würde sich die Arbeitsmarktsituation der Industrienationen verschlechtern, was wiederum zu einem Rückgang der Kaufkraft und somit zu einer wirtschaftlichen Abwärtsspirale führen würde. Unternehmen würden es vermeiden, ihre Waren in Piraterieländern anzubieten. Dadurch blieben ausländische Investitionen aus, was folglich die Innovationskraft und internationale Wettbewerbsfähigkeit vieler Staaten negativ beeinflussen würde.

Bedenkt man, dass viele Piraterieaktivitäten zur Finanzierung anderer krimineller Handlungen wie Prostitution, Menschenhandel, Rauschgifthandel oder Terrorismus dienen, hätte die Ausbreitung der Piraterie auch einen erheblichen Einfluss auf die allgemeine Sicherheit der Weltbevölkerung.

Um dieses „Worst-Case-Szenario“ zu vermeiden, werden Staaten, Industrien und Unternehmen dazu gezwungen sein, sich aktiv am Kampf gegen Produktpiraterie zu beteiligen.

Folgende Marktstrategien und Maßnahmen sollen einen profunden Überblick liefern, welche Möglichkeiten im Rahmen des Marketings bestehen, um gegen Produktpiraterie vorzugehen.

3 Markteintrittsstrategie: Zeit als Wettbewerbsfaktor und Maßnahmen gegen Produktpiraterie

3.1 Megatrends, Trends und Moden

Heutzutage wird dem Faktor Zeit eine immer bedeutendere Rolle beigemessen. Um in unserer schnelllebigen Gesellschaft, in der eine Innovation schon nach einigen Wochen oder sogar Tagen wieder durch eine andere ersetzt wird, zu überleben, bleibt einem Unternehmen keine andere Wahl, als sich der Geschwindigkeit des Fortschritts anzupassen oder im schnellen Treiben des Wettbewerbs unterzugehen. Ziel ist es, unbefriedigte Bedürfnisse und Trends in der Makroumwelt herauszufinden, um somit dem Wettbewerb einen Schritt voraus zu sein. Deshalb werden jährlich Millionenbeträge in die Marktforschung investiert. Schließlich gilt: Nur wer heute schon die Nachfragewünsche von morgen kennt, kann auf den stark umworbenen Märkten überleben.

Um eine Marktchance zu erkennen und richtig einzuschätzen, müssen Marktveränderungen sorgfältig analysiert werden. Es lassen sich drei Arten unterscheiden: Megatrend, Trend und Mode („fad“).[53]

Der *Megatrend* ist die langlebigste Form. Er bildet sich über Jahre hinweg und bewirkt eine Veränderung in vielerlei Hinsicht. Er beeinflusst die gesamte Gesellschaft und wirkt sich demnach auf Technologie, Politik, Wirtschaft und soziale Strukturen aus.[54]

Als *Trend* bezeichnet man eine Richtung oder eine Abfolge von verschiedenen Ereignissen, die von gewisser Dauerhaftigkeit sind und Veränderungskraft mit sich bringen. Ein Trend zeigt im Grunde genommen ein Stück der Zukunft. Beispielweise ist die steigende Anzahl weiblicher Arbeitskräfte in vielen Branchen ein Trend, der wiederum weitere Folgen mit sich bringt.[55]

Die kürzeste Form der Marktveränderung ist eine *Mode*, im Englischen auch „fad“ genannt. Ein „fad“ ist sehr kurzlebig, kaum vorhersehbar und hat keine langfristigen Auswirkungen auf das Makroumfeld der Unternehmung. So müssen Unternehmen, die an einer Mode verdienen wollen, besonders schnell reagieren, um die kurz anhaltende Nachfrage vor ihren Wettbewerbern zu bedienen.[56]

---

[53] Vgl. Kotler/Bliemel (2001), S. 280.
[54] ebd.
[55] ebd.
[56] ebd.

Vorwiegend spielt bei fads der Faktor Zeit (i.S.v. von Reaktionszeit) eine zentrale Rolle, da eine Nachfrage, so schnell wie sie aufkommt, auch wieder abflauen kann.

Ein Beispiel hierfür ist das Tamagotchi, ein aus Japan stammendes Elektronikspielzeug, das Ende der 90er weltweit Aufsehen erregte. Ein Tamagotchi ist ein virtuelles Küken, um das man sich, nachdem es zum Leben erweckt wurde, wie um ein echtes Haustier kümmern muss. Nachdem sich das Tamagotchi in Japan nach kürzester Zeit als Erfolg erwies, brachte der Originalhersteller Bandai das virtuelle Haustier auch auf den amerikanischen und europäischen Markt. Aufgrund der starken Nachfrage bildeten sich jedoch schnell Lieferengpässe, wodurch sich für Wettbewerber und vor allem für Produktpiraten die Chance auftat, rasch günstigere Ersatzprodukte und Plagiate mit weitaus mehr Funktionen auf den Markt zu bringen. Jedoch hielt der „Tamagotchi-Hype" nicht lange an, sodass der Lieferengpass für Bandai zur Hauptursache für entgangene Gewinne wurde.

Gelingt es einem Unternehmen jedoch, ein Produkt erfolgreich und ohne Vermarktungsfehler vor den Wettbewerbern auf den Markt zu bringen, besteht die Möglichkeit, den Markt abzuschöpfen bevor Konkurrenzprodukte, unter anderem Pirateriewaren, in den Markt treten. In dieser kurzen Monopolsituation lassen sich hohe Kosten für Forschung und Entwicklung durch große Umsätze meist schnell amortisieren. Dadurch können binnen kurzer Zeit hohe Gewinne realisiert werden.

3.2 Timing-Strategien

3.2.1 First-Mover-Strategie vs. Follower-Strategie

Eine Unternehmung muss sich überlegen, zu welchem Zeitpunkt sie in einen Markt eintritt. Es lassen sich zwei Strategien unterscheiden:

- die First-Mover-Strategie (auch Pionierstrategie genannt) und
- die Follower-Strategie (auch Folgerstrategie genannt).

Im Wesentlichen hängt die gewählte Strategie immer von dem Wettbewerber ab. Eine Unternehmung kann folglich langsamer oder schneller als der Wettbewerb in einen Markt eintreten.[57]

[57] Vgl. Kutschker/Schmid (2005), S. 958.

Bei der First-Mover-Strategie tritt ein Unternehmen als erstes in einen bestimmten Markt ein. Hierbei kann es sich um nationale, aber auch internationale Märkte handeln. Der Vorteil dieser Strategie liegt darin, dass sie dem Pionier ermöglicht, Markteintrittsbarrieren für Wettbewerber aufzubauen. Zu den Vorteilen zählen unter anderem auch: der Bekanntheits- und Imagevorsprung, der Aufbau guter Beziehungen zu Lieferanten, der frühzeitige Aufbau eines Netzwerkes, der Aufbau eines loyalen Kundenstammes, die Erzielung von Skaleneffekten vor den Wettbewerbern und monopolbedingte Gewinne.[58] Jedoch bringt diese Strategie auch Nachteile mit sich: So können der Unternehmung hohe Kosten für die Erschließung eines Marktes entstehen, die gegebenenfalls durch eine Fehleinschätzung der Nachfrage nicht gedeckt werden.[59]

Bei der Follower-Strategie handelt eine Unternehmung hingegen nach einem genau entgegengesetzten Vorgehensmodell. Sie tritt erst dann in einen Markt ein, wenn dieser bereits durch andere Konkurrenten erschlossen wurde. Auch diese Strategie birgt gewisse Vor- und Nachteile. Für den Folger ergibt sich der Vorteil, dass durch den First-Mover bereits Kenntnisse über den Markt bestehen. Diese ermöglichen es, den Pionier im Bereich seiner Produktpolitik anzugreifen und technisch weiterentwickelte Produkte anzubieten. Trotzdem darf hierbei nicht vergessen werden, dass der Folger den Vorsprung, den sich der Pionier bereits erwirtschaftet hat, aufholen muss. Zudem liegt ein Risiko dieser Strategie darin, dass auf dem Markt ein Wettbewerb herrscht, auf dem sich der Folger erst gegenüber seinen Konkurrenten behaupten muss.[60]

Da es sich bei Plagiaten ausschließlich um Kopien bereits existierender Produkte handelt, lässt sich nicht schwer erkennen, welche Strategie von den Piraten verfolgt wird. Piraten nutzen den so genannten „Free-Rider-Effekt“, bei dem der Folger von den Investitionen der Pioniere profitiert.[61]

Genau hier besteht die Möglichkeit gegen Piraterie vorzugehen. Gelingt es einer Unternehmung zahlreiche und effektive Markteintrittsbarrieren zu schaffen, so sinkt für die Wettbewerber – vorwiegend aber für Piraten – die Attraktivität, in diesen Markt einzudringen. Laut Koch wird die Markteintrittsbarriere für nachfolgende Wettbewer-

[58] Vgl. Kutschker/Schmid (2005), S. 959.
[59] Vgl. Kutschker/Schmid (2005), S. 960.
[60] Vgl. Koch (1999), S. 158.
[61] Vgl. Kutschker/Schmid (2005), S. 960.

ber umso größer, je stärker der Vorsprung in technologischer und organisatorischer Hinsicht ist.[62]

Handelt es sich außerdem um einen wie unter Abschnitt 3.1 beschriebenen fad, so ist es schwer für Piraten, ihre Plagiate auf den Markt zu bringen, bevor die Nachfrage bereits durch den Pionier gestillt ist.

3.2.2 Wasserfall-Strategie vs. Sprinkler-Strategie

Die First-Mover- bzw. Follower-Strategie bezieht sich lediglich auf den Eintritt in einen Markt. Üblicherweise treten internationale Unternehmen im Laufe der Zeit jedoch in mehrere Ländermärkte ein. Es gibt hier ebenfalls zwei Strategien, wie Unternehmen den optimalen Markteintrittszeitpunkt wählen und sich darüber hinaus noch bestmöglich vor Produktpiraterie schützen können.[63]

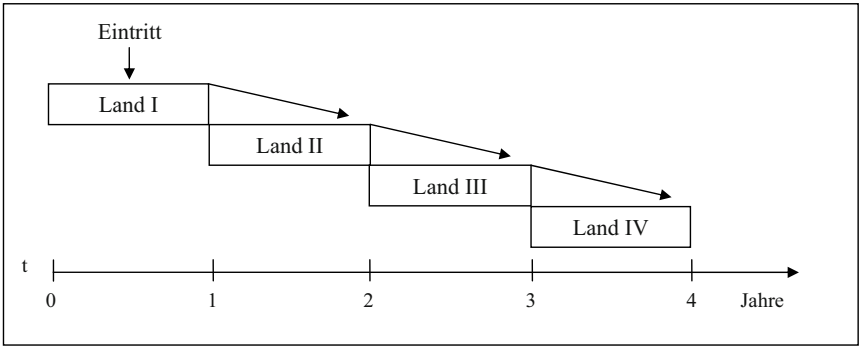


Abbildung 6: Die Wasserfall-Strategie
Quelle: Kutschker/Schmid (2005), S. 964.

Bei der Wasserfall-Strategie tritt das Unternehmen zuerst in einen Ländermarkt ein, bevor es anschließend Schritt für Schritt in weitere Länder vordringt (Vgl. Abbildung 6). Generell lässt sich feststellen, dass es sich bei der Wasserfall-Strategie anbietet, zuerst in Länder einzutreten, die dem Heimatmarkt ähnlich sind. Vertraute Marktgegebenheiten erleichtern hier den Eintritt. Von dort kann sich eine Unternehmung sukzessiv in andere Ländermärkte vorarbeiten. Eine Reihenfolge, wann in welches Land expandiert wird, lässt sich im Vorhinein schwer bestimmen, da ein Auslandsengagement

[62] Vgl. Koch (1999), S. 158.
[63] Vgl. Kutschker/Schmid (2005), S. 963.

von den internen und externen Rahmenbedingungen des Gastlandes abhängig ist, die sich über die Jahre hinweg verändern können.[64]

Es gibt viele Vorteile dieser Strategie. Zum einen wird der Bedarf an Ressourcen zeitlich versetzt, was besonders für kleine und mittelständische Unternehmen ausschlaggebend sein kann, da diese oftmals nur über begrenztes Kapital und limitierte Managementressourcen verfügen. Zum anderen können Länder, deren Markteintritt schon länger zurück liegt, den neuen Eintritt finanziell unterstützen. In diesem Zusammenhang lassen sich auch Produktlebenszyklen oder Technologiezyklen verlängern. Außerdem ermöglicht die Wasserfall-Strategie, sich den länderspezifischen Gegebenheiten genau anzupassen, was wiederum das Risiko des Scheiterns eingrenzt.[65]

Wenn es darum geht, das Unternehmen vor Produktpiraten zu schützen, setzen allerdings genau hier die Nachteile dieser Strategie an. Wird die Dauer bestimmter technologischer Lebenszyklen sowie Produktlebenszyklen ausgedehnt, so lohnt es sich für Piraten, sich das nötige Wissen für die Herstellung von Imitaten anzueignen und sich auf dem Markt mit günstigen Fälschungen auszubreiten.

Außerdem werden Wettbewerber im Grunde genommen vorzeitig gewarnt. Der Wettbewerb kann die Zeit, die zwischen dem einem und dem anderen Ländermarkteintritt liegt, dazu nutzen, das Produkt zu kopieren und selbst in den Markt einzutreten.[66] Die Wasserfall-Strategie bietet den Piraten genügend Angriffsmöglichkeiten und stellt somit nicht die beste Strategie für den Kampf gegen Produktpiraterie dar.

Die Sprinkler-Strategie (Vgl. Abbildung 7) zeichnet sich dadurch aus, dass ein Unternehmen zeitgleich bzw. in einer kurzen Zeitspanne in mehrere oder alle angestrebten Ländermärkte eintritt.[67]

Die Vorteile dieser Strategie liegen unter anderem im frühen Markteintritt in verschiedene Länder. Vor allem bei sehr schnelllebigen Produkten mit kurzem Lebenszyklus, die in allen Ländern ähnliche Bedürfnisse befriedigen, wie es z.B. bei PCs der Fall ist, erweist sich die Sprinkler-Strategie als sehr vorteilhaft.

---

[64] Vgl. Kutschker/Schmid (2005), S. 964.
[65] Vgl. Meffert/Pues (2002), In: Kutschker/Schmid (2005), S. 965.
[66] Vgl. Kutschker/Schmid (2005), S. 966.
[67] ebd.

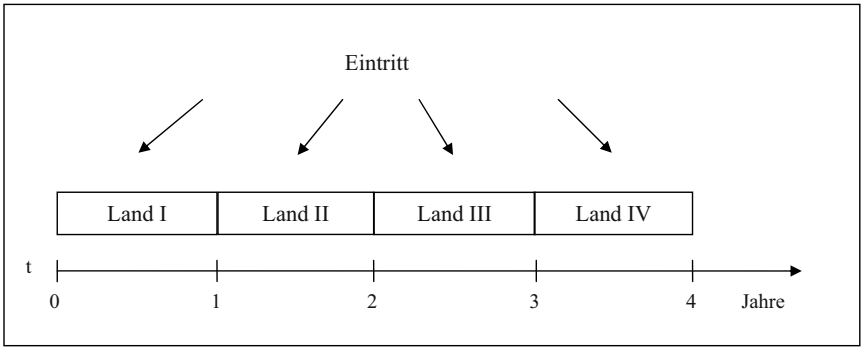


Abbildung 7: Die Sprinkler-Strategie
Quelle: Kutschker/Schmid (2005), S. 967.

Darüber hinaus greifen hier ebenfalls die oben genannten Vorteile der First-Mover-Strategie, da durch den frühen Markteintritt Barrieren für Wettbewerber aufgebaut werden können. Hohe Entwicklungs- und Produktionsfixkosten lassen sich verhältnismäßig schnell amortisieren, da in vielen Ländern gleichzeitig Cash Flows erzeugt werden. Dennoch liegt der größte Vorteil darin, dass der Wettbewerb regelrecht überrascht wird. Bei innovativen Produkten oder neuen Technologien kann der daraus resultierende Wettbewerbsvorsprung ausschlaggebend für die Gewinnung wichtiger Marktanteile sein. Es gilt, in dieser Zeit ein gutes und primär sicheres Netzwerk zwischen Lieferanten und Kunden aufzubauen. Außerdem kann ein Imagegewinn gegenüber den Kunden, aber auch gegenüber der Regierung entstehen, da die Unternehmung Engagement in den Gastländern zeigt.[68]

Die Kehrseite der Sprinkler-Strategie findet sich logischerweise in den Vorteilen der Wasserfall-Strategie wieder. Viele Ressourcen müssen zeitgleich zur Verfügung stehen. Hoher organisatorischer Aufwand sowie das Risiko, dass in einigen Ländern der Erfolg ausbleibt, stellen weitere Nachteile dar. Weiterhin lassen sich in manchen Branchen gewisse länderspezifische Anpassungen nicht umgehen.[69]

Interessanterweise können einige Nachteile, die in Verbindung mit dieser Strategie gesehen werden, im Bezug auf die Bekämpfung von Produktpiraterie sogar als vorteilhaft ausgelegt werden. Indem alle Länder gleichzeitig bearbeitet werden, scheint ein

[68] Vgl. Kutschker/Schmid (2005), S. 966/967.
[69] Vgl. Kutschker/Schmid (2005), S. 967.

Wissenstransfer unmöglich. Dies hat aber wiederum zur Folge, dass auch den Piraten der Zugang zu fremdem Wissen erschwert wird.

Um die Vorteile beider Strategien zu nutzen und sogleich wirksam gegen Produktpiraterie vorzugehen, bietet sich oftmals eine Kombination beider Strategien an: die kombinierte Wasserfall-Sprinkler-Strategie (Vgl. Abbildung 8).

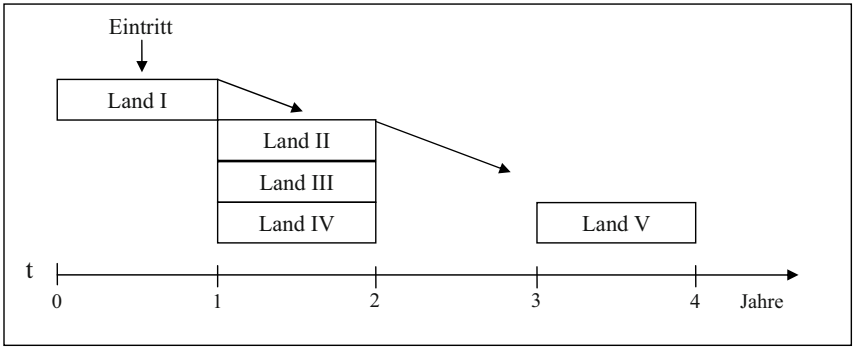


Abbildung 8: Die kombinierte Wasserfall-Sprinkler-Strategie
Quelle: Kutschker/Schmid (2005), S. 969.

Sind in einigen Ländern die Marktgegebenheiten sehr ähnlich, so werden diese Länder als Cluster zusammengefasst. Der Eintritt findet dann gleichzeitig statt. Länder, die nicht in die Cluster fallen, werden gemäß der Wasserfall-Strategie einzeln sowie zeitlich versetzt bearbeitet.[70] Die Kombination ermöglicht die Nachteile beider Strategien zu minimieren.

Außerdem ist ein Wissensaustausch unter angrenzenden Ländern wahrscheinlicher als ein Know-how-Transfer von beispielsweise Asien nach Südamerika. Geografisch nah beisammen liegende Regionen weisen oft homogene Nachfragestrukturen auf. Daher ergeben sich in diesen Ländern beim zeitgleichen Markteintritt Synergien, die zu einer Reduktion der Einführungskosten führen. Zusätzlich können in diesen Länderclustern gleichzeitig und im frühen Stadium der Markterschließung Barrieren gegen Produktpiraten geschaffen werden.

[70] Vgl. Kutschker/Schmid (2005), S. 969.

4 Maßnahmen aus dem Bereich Marketing und Vertrieb zur Bekämpfung von Produktpiraterie

4.1 Multi-Level-Strategie im Marketing

Im Allgemeinen lässt sich feststellen, dass Unternehmen nur kurzfristig auf Eingriffe durch Produktpiraterie reagieren. Es werden meist ad hoc-Maßnahmen ergriffen, wenn eine konkrete Bedrohung bevorsteht oder bereits eine Verletzung des geistigen Eigentums vorliegt.[71] Jedoch führt diese reaktive Haltung laut Harte-Bavendamm zu höheren Belastungen und Kosten für die Unternehmung als eine im Voraus erarbeitete und konsequent umgesetzte, intelligente Schutzstrategie.[72]

Eine zielgerichtete, ganzheitliche Strategie, welche auf die individuelle Unternehmenssituation abgestimmt werden muss, ist die Ausgangsbasis für ein erfolgreiches Anti-Counterfeiting-System.[73] Um die Gefahren und Folgen der Produktpiraterie zu minimieren und sie effektiv zu bekämpfen, zählt es zu den Aufgaben der Unternehmensleitung, eine langfristige Schutzstrategie zu erarbeiten und im Unternehmen umzusetzen. Es gilt, eine sinnvolle Kombination von Maßnahmen in die Schutzstrategie zu integrieren. Technische, juristische und betriebswirtschaftliche Maßnahmen müssen in allen Bereichen des Unternehmens genau aufeinander abgestimmt werden. Nur durch eine unternehmensweite Multi-Level-Strategie besteht eine Chance, erfolgreich gegen Piraterie vorzugehen und einen erwünschten Kosten-Nutzen-Effekt zu realisieren.

Die Möglichkeiten des Anti-Counterfeiting werden im betriebswirtschaftlichen Bereich bisweilen nicht genügend wahrgenommen. So bietet beispielsweise eine Multi-Level-Strategie auch im Marketing-Mix ein großes Spektrum an Maßnahmen, um proaktiv gegen Produktpiraterie vorzugehen. Der moderne Marketing-Mix umfasst die vier herkömmlichen Bereiche – Produktpolitik, Preispolitik, Distributionspolitik und Kommunikationspolitik – und kann um einen fünften Bereich – die Kundenbetreuung und -bindung – erweitert werden. Es gilt, Maßnahmen aus all diesen Bereichen bestmöglich aufeinander abzustimmen und im Unternehmen umzusetzen.

[71] Vgl. Harte-Bavendamm (2000), S. 31.
[72] Vgl. Harte-Bavendamm (2000), S. 32.
[73] Vgl. Fuchs (2006), S. 118.

4.2 Umsetzung konkreter Maßnahmen im Marketing-Mix

4.2.1 Produkt

4.2.1.1 Entwicklung schutzfähiger Produkte

Im Kampf gegen Produktpiraterie geht es im Bereich der Produktpolitik darum, dass Unternehmen rechtzeitig und vorausschauend handeln. Dies bedeutet, dass bereits in der frühen Phase der Forschung und Entwicklung an produktspezifische Schutzmaßnahmen gedacht werden muss.

Bei der Produktentwicklung sollte beachtet werden, dass nicht nur das Produkt in seiner bestehenden Form von technischen Schutzrechten erfasst werden kann, sondern auch ähnliche Lösungen und angrenzende Bereiche abgedeckt werden.[74]

Daher gilt es, *strategische* Patente anzustreben, die das Verfahren zur Herstellung der Produkte nicht konkretisieren und sich vornehmlich auf die kommerzielle Verwendung neuer Technologien konzentrieren. Der Patentschutz sollte auch benachbarte Felder einbeziehen. Dadurch wird es den Wettbewerbern und Nachahmern erschwert, Ersatzlösungen zu finden, die nicht die angrenzenden Patente verletzen. Neben dem Schutz des eigentlichen Produktes kann zudem ein entstandener Marktvorsprung vergrößert werden.[75]

Jedoch wird aus einem Artikel der Financial Times Deutschland deutlich, dass immer weniger Unternehmen ihre Erfindungen schützen lassen. Aus Angst, wichtige technische Daten und Informationen offen zu legen, die dann von chinesischen Wettbewerbern kopiert werden, verzichten viele Maschinenbauunternehmen auf eine Patentanmeldung. Der VDMA rät seinen Mitgliedern sogar, Patente nur anzumelden, wenn die Produkte ein fundiertes, technisches Wissen erfordern. Dennoch darf nicht vergessen werden, dass ohne Patent auch kein Schutz besteht. So können Produkte, die auf Messen ausgestellt werden, von jedem Konkurrenten nachgebaut werden. [76]

Neben dem Patentschutz gilt es durch rechtzeitige Markenanmeldung, Waren und Dienstleistung vor Piraterie zu schützen. In der Europäischen Union bietet sich hier

[74] Vgl. Harte-Bavendamm (2000), S. 43.
[75] ebd.
[76] Vgl. Bialdiga (2008), S. 3.

vor allem die Anmeldung einer Gemeinschaftsmarke an, die eine länderübergreifende Verfolgung der Rechtsverletzung ermöglicht.[77]

Des Weiteren sollte bei der Produktentwicklung auch das Produktdesign im Hinblick auf Piraterieschutz strategisch durchdacht werden. Das Produkt sowie ergänzende Produkte, wie beispielsweise Mobiltelefon und Akku, sollten so entwickelt werden, dass diese nur mit dem jeweiligen Original funktionieren. Zum einen ermöglicht dies leichtgläubigen Konsumenten, die Fälschung einfacher zu erkennen, zum anderen werden Verbraucher, die bereit sind, Fälschungen bewusst zu erwerben, davon abgehalten, diese zu verwenden.[78]

Ein kompliziertes Produktdesign, dessen Herstellung aufwendig ist und die Verwendung spezieller Werkzeuge und Maschinen benötigt, kann außerdem das Kopieren des Produktes für Piraten wirtschaftlich uninteressant machen.[79]

4.2.1.2 Unterscheidung durch Produktqualität und Individualisierung

Besondere Qualitätsmerkmale und hohe Qualitätsstandards erschweren die Produktion guter Produktkopien. Obwohl die Qualität von Pirateriewaren zunehmend steigt, gilt eine kontinuierliche Verbesserung der Produktqualität als wirksamer Schutz vor Piraterie.[80] Jedoch erfordert diese hohe Qualität auch einen erheblichen Aufwand von Seiten der Unternehmen, da die Auswahl und Verwendung hochwertiger Materialien i.d.R. sehr kosten-, zeit- und personalintensiv ist.

Zudem müssen ständig neue Methoden entwickelt werden, um den Piraten einen Schritt voraus zu sein. Eine Methode, die sich eignet, die Qualität der Produkte bereits bei der Phase der Entwicklung sicherzustellen, ist die *Fehler-Möglichkeits-* und *Einflussanalyse* (FMEA[81]). Sie ermöglicht, Fehler und deren Folgen frühzeitig zu erkennen, und erlaubt somit, den Zeitpunkt der technischen Reife der Produkte vor den Produktionsstart zu schieben. Die Verbesserung der Produktqualität sowie eine Verkürzung der Entwicklungszeit stellen zwei unverkennbare Chancen dar, Produktpiraterie zu verhindern.[82]

---

77 Vgl. Harte-Bavendamm (2000), S. 43.
78 ebd.
79 Vgl. Fuchs (2006), S. 238.
80 Vgl. Wildemann (2007), S. 44.
81 Abgeleitet aus dem Englischen „Failure-Mode- and Effects-Analysis".
82 Vgl. Wildemann (2007), S. 45.

Eine zweite Methode, die den Kunden in die Qualitätsbetrachtung mit einbezieht, ist die *Quality-Function-Deployment(QFD)-Methode*. Bei der Weiter- oder Neuentwicklung von Produkten soll mit dieser Methode herausgefunden werden, *was* genau von Kunden verlangt wird und *wie* dies konkret im Produkt umgesetzt werden kann.[83] Da der Originalhersteller somit ein Produkt auf den Markt bringt, das alle Kundenwünsche exakt erfüllt, ist der Konsument weniger geneigt, auf Alternativangebote und Kopien zurückzugreifen. Daher zeigt sich diese Methode bei der Vermeidung von Piraterie als sehr vorteilhaft. Zudem ist dieses kundenorientierte Produkt ein Grund für eine zunehmende Loyalität seitens der Verbraucher.

Sind die besonderen Qualitätsmerkmale den Konsumenten bewusst, so sind diese vielmals bereit, für die hohe Qualität erhöhte Kaufpreise zu zahlen.[84] Infolgedessen sind Investitionen, die sich in einer Verbesserung der Produktqualität niederschlagen, eine rentable Maßnahme, um Produktpiraten abzuschrecken.

Des Weiteren können aufwendige Details und Produkteigenschaften, die individuell auf den Kunden abgestimmt werden, das Nachahmen verhindern, da kundenindividuelle Produkte aufgrund kostenintensiver Herstellung für Piraten weniger interessant sind. Beispielweise bietet SAP seine Software nur in Kombination mit seinen Dienstleistungen an. Jedes Softwarepaket wird an die speziellen Bedürfnisse des Kunden angepasst. Durch diese Individualisierung ist die Software nur für den jeweiligen Kunden von Nutzen. SAP verhindert somit, dass die Software kopiert und widerrechtlich in einem anderen Unternehmen eingesetzt wird.

Das Produktprogramm, das alle Produktarten und -varianten umfasst, liefert zusätzliche Möglichkeiten zur Kundenindividualisierung.[85] Durch „add on"-Produkte, wie z.B. Zusatzsoftware und -hardware für das Apple ibook, kann der Kunde sein Produkt beliebig erweitern und personalisieren.

Außerdem eignen sich Module dazu, neue Technologien in Systeme zu integrieren. Der Verbraucher ist dadurch nicht gezwungen, ein Nachfolgeprodukt zu erwerben, sondern kann sein Produkt durch ein Upgrade auf das aktuelle Leistungsniveau bringen, wodurch für ihn die Lebensdauerkosten des Produktes sinken. Individuelle Produktlösungen bieten den Unternehmen einige Vorteile. Es entsteht eine gute Bindung zum Kunden, was eine Grundlage für eine langfristige Zusammenarbeit bieten kann.

[83] Vgl. Wildemann (2007), S. 45.
[84] Vgl. Wildemann (2007), S. 44.
[85] Vgl. Wildemann (2007), S. 40.

Zudem tun sich durch die daraus hervorgehenden Prozesse neue Geschäftsfelder auf, wie z.B. im Dienstleistungsbereich. Die Modularisierung von Produkten erschwert potentiellen Produktpiraten das Kopieren, da den Piraten lediglich das aktuelle Produkt zur Nachkonstruktion zur Verfügung steht. Kenntnisse über folgende Module bleiben Nachahmern verwehrt. Eine prospektive Planung wird daher für Produktpiraten erschwert.[86]

4.2.1.3 Innovationsmanagement – Verkürzung der Zyklen

Neben Maßnahmen, die sich direkt auf die Gestaltung des Produktes auswirken, können auch Strategien, die die Planung und Entwicklung neuer Produkte betreffen, genutzt werden, um Produktpiraterie zu vermeiden.[87] Durch ständige Innovation und Originalität können Märkte für Nachahmer blockiert werden. Vor allem bei technischen Produkten kann eine Beschleunigung der Innovationszyklen eine wirkungsvolle Maßnahme gegen Piraten sein, da die Forschung und Entwicklung hier auf eine fortlaufende Verbesserung der Produktvarianten abzielt.[88]

Werden Produkte kontinuierlich weiterentwickelt und neue Innovationen in sehr kurzen Zeitabständen auf den Markt gebracht, verkleinern sich für Piraten die Zyklen, in denen sie illegale Kopien anfertigen und auf den Markt bringen können. Zudem ermöglicht der Zeitvorsprung dem Marktführer den Markt abzuschöpfen, bevor Piraten mit ihren Kopien auf den Markt eintreten. Je kürzer also die Zeitabstände zwischen der Einführung neuer Produkte, desto geringer ist die Chance für Piraten, erfolgreich zu sein.[89] Die Verkürzung von Innovationszyklen macht Märkte für Nachahmer weniger attraktiv und hilft somit diese fernzuhalten.

Allerdings ist es auch für den Originalhersteller bzw. den Marktführer eine große Herausforderung, ständig neue Innovationen auf den Markt zu bringen, da gewisse Ressourcen auch Pionieren nicht unbegrenzt zur Verfügung stehen.[90] Zudem stellt sich der tatsächliche Innovationsgrad erst durch einen späteren Markterfolg heraus, weshalb jede neue Innovation auch ein gewisses Entwicklungsrisiko mit sich bringt.[91]

---

[86] Vgl. Wildemann (2007), S. 47.
[87] Vgl. Wildemann (2007), S. 32.
[88] Vgl. Welser/González (2007), S. 307.
[89] ebd.
[90] Vgl. Wildemann (2007), S. 113.
[91] Vgl. Wildemann (2007), S. 33.

Durch ein effizientes Änderungswesen, das die Überarbeitung bestehender Produkte vorsieht, können die Kosten der Entwicklung gering gehalten und somit das Erfolgsrisiko minimiert werden. Das Zielkostenmanagement erweist sich als geeignet, um die Zeit zwischen Produktidee und Markteinführung zu minimieren (time-to-market). Darüber hinaus werden die Ausgaben für Forschung und Entwicklung von Anfang an eingeschränkt. Beim Target-Costing wird im Grunde genommen rückwärts kalkuliert. Es wird nicht davon ausgegangen, wie viel ein Produkt kosten wird, sondern, je nach dem welcher Preis am Markt erzielt werden kann, wird festgelegt, was ein Produkt kosten darf.[92]

Durch den vorgegebenen Preis wird eine Reihe von Entscheidungen, wie beispielsweise über die Auswahl des Materials oder die Qualität des Produktes, vorweggenommen. Aufgabe des Zielkostenmanagements ist es, bei der Produktentwicklung keine Ressourcen zu verschwenden und sich auf ein kundennutzenoptimales Produkt zu konzentrieren. Ein ausgewogenes Preis-/Leistungsverhältnis verhindert, dass sich Piraten mit einem billigeren Produkt und gleichem Kundennutzen auf dem Markt ausbreiten können.[93]

4.2.1.4 Technische Maßnahmen zur Produktkennzeichnung

Maßnahmen der Produktkennzeichnung dienen vor allem zur Unterscheidbarkeit der Originalprodukte, zur Abschreckung von Nachahmern, aber auch zum Schutz der Verbraucher. Besonders bei Medikamenten, deren billige Kopien dem Konsumenten oftmals mehr schaden als helfen, kann dies bedeutsam sein. Durch die Kennzeichnung der Originalwaren kann sich der Kunden vergewissern, dass es sich nicht um eine Kopie handelt und das Medikament ohne jede Bedenken eingenommen werden kann. In der Literatur wird i.d.R. zwischen offenen (sichtbaren) und verdeckten (unsichtbaren) Technologien unterschieden.[94]

Offene Technologien sind für jedermann sichtbar und werden außen am Produkt angebracht. Die bekanntesten und am häufigsten verwendeten offenen Sicherungsmittel sind Hologramme. Im Kampf gegen Produktpiraterie haben sich die Präge- und die Polymerhologramme wegen ihrer geringen Größe bewährt. Als 3D-Abbildung werden

[92] Vgl. Homburg/Daum (1997), S. 108.
[93] Vgl. Wildemann (2007), S. 114.
[94] Vgl. Harte-Bavendamm (2000), S. 39; Wildemann (2007), S. 65; Welser/González (2007), S. 321.

sie in Form von Etiketten und Aufklebern auf dem Produkt oder auf CD-/DVD-Hüllen angebracht. Hologramme sind vom Kunden leicht zu erkennen. Sie verifizieren die Echtheit der Produkte und haben somit eine verkaufsfördernde Wirkung auf den Konsumenten. Zudem sind sie für Piraten schwer zu kopieren, da für ihre Herstellung eine Vielzahl von Geräten benötigt wird.[95]

Neben Hologrammen gibt es eine Reihe anderer offener Schutztechnologien, beispielweise optische Sicherungsmittel wie OVDs/DOVIDs[96], Siegel, Folien, Sicherheitspapiere und -tinte. Interessant bei den offenen Technologien ist, dass sie durch ihre Visualität zur Gestaltung des Produktdesigns beitragen und dadurch ein positives Erscheinungsbild des Produktes unterstützen können.[97]

Hingegen sind verdeckte Technologien nicht sichtbar und erfordern für ihre Erkennung besondere Geräte. Da Konsumenten meist nicht über diese Geräte verfügen, eignen sich unsichtbare Sicherungen insbesondere im B2B[98]-Bereich. Diese Technologien dienen vorwiegend zur Unterscheidung von Original und Fälschung[99], was im B2B-Bereich vor allem bei Zulieferteilen, die weiterverarbeitet werden, von besonderer Bedeutung sein kann (Vgl. Abschnitt 2.4.3).

Zu den verdeckten Produktkennzeichnungen zählen unter anderem Mikrofarbcodes, die Produkte mittels einzigartiger Farbpigmente kennzeichnen, DNA-Markierungen, Nanotechnologie, bei der spezielle Tinte verwendet wird, die nur unter UV-Licht lesbar ist, oder auch digitale Wasserzeichnen, die häufig für Softwareprodukte verwendet werden.[100]

Eine weitere Technologie zum Schutz vor Produktpiraterie ist die *Radio Frequency Identification* (RFID). Sie zählt zu den maschinenunterstützten Technologien[101] und wird vielfach im Logistikbereich zur Rationalisierung von Warenflüssen eingesetzt. RFID soll Waren rückverfolgbar machen und somit zur Fälschungssicherheit von Produkten beitragen.[102] Jedes Produkt erhält eine individuelle Codierung, z.B. in Form einer elektronischen Artikelnummer, über die Informationen gespeichert werden können. Auf diese Weise kann jeder Gegenstand von seiner Herstellung bis zur Abgabe an

[95] Vgl. Fuchs (2006), S. 263.
[96] Optically Variable Devices/Diffractive Optically Variable Image Devices.
[97] Vgl. Fuchs (2006), S. 265.
[98] Business-to-Business bezeichnet eine Handelsbeziehung zwischen zwei Unternehmen.
[99] Vgl. Welser/González (2007), S. 332.
[100] Vgl. Wildemann (2007), S. 66.
[101] Vgl. Fuchs (2006), S. 275.
[102] Vgl. o.V. (2008), S. 6.

den Verbraucher genauestens verfolgt werden.[103] Folglich wird es Fälschern erschwert, illegale Waren in die Logistikkette einzuschleusen oder Originale zu stehlen, die für ein Revers Engineering benötigt werden.

Darüber hinaus können Verbraucher beispielsweise durch RFID-Etiketten den Weg von Waren nachvollziehen. Aufgrund zahlreicher Skandale im Lebensmittelbereich wollen viele Kunden wissen, woher die Waren kommen. In Kanada soll bis 2008 durch RFID-Etiketten der Weg von 80% der Lebensmittel kontrolliert werden können.[104]

Viele dieser technischen Produktkennzeichnungsmaßnahmen erschweren den Fälschern das Geschäft erheblich, da sie schwer bis gar nicht zu fälschen sind. Sie besitzen eine Identitätsfunktion und erleichtern damit die Verfolgung von Produktfälschern. Durch die Echtheitsprüfung wird zudem das Produkthaftungsrisiko verringert.[105] Jedoch muss auch bedacht werden, dass viele Methoden mit vergleichsweise hohen Kosten verbunden sind und oftmals nur kurzfristigen Schutz bieten.[106] Daher sollten Unternehmen bei der Auswahl technischer Maßnahmen auf ihre Praktikabilität achten.

4.2.1.5 Intelligente Verpackung

Die Verpackung eines Produktes gilt oftmals als Kommunikationsschnittstelle zum Kunden. Sie soll nicht nur Produkte vor Beschädigung schützen, sondern ist Träger der Markenbotschaft und des Qualitätsversprechens des Herstellers[107] und bietet dem Kunden eine Informationsfunktion über den Inhalt. Da Piraten Verpackungen fälschen oder auch Originalverpackungen zur Tarnung ihrer illegalen Kopien verwenden, spielen intelligente Verpackungen bei der Prävention eine bedeutende Rolle.[108]

So lassen sich intelligente Verpackungen nicht nur zu Marketingzwecken nutzen, sondern stellen auch eine weitere Möglichkeit zur Sicherung der Produkte dar. Verpackungen können durch Prägungen oder durch Verwendung bestimmten Materials intelligent gestaltet werden, wodurch Verbrauchern, Händlern und Zollbehörden die Unterscheidung von Original und Fälschung erleichtert wird.

---

[103] Vgl. Fuchs (2006), S. 275.
[104] Vgl. Fuchs (2006), S. 278.
[105] Vgl. Weiser/Olsen (2004), S. 26.
[106] Vgl. Fischer et al. (2002), S. 82.
[107] Vgl. o.V. (2008), S. 6.
[108] Vgl. Kroboth (2006), S. 68.

Technische Sicherungsmethoden wie Hologramme oder RFID-Etiketten werden zumeist auf der Verpackung angebracht und bieten Beweise für Manipulationen oder Eingriffe in das Produkt bzw. den Inhalt. Widerrechtliche Entfernung oder gar ein Austausch des Originals durch eine minderwertige Fälschung kann durch intelligente Verpackung aufgedeckt werden.[109]

Zudem ist es sinnvoll, wenn auf Verpackungen immer wieder kleine Details verändert werden. Somit bleibt das Unternehmen den Nachahmern einen Schritt voraus und erschwert diesen das Herstellen originalgetreuer Produktverpackungen.

Wird die Verpackung nicht im Unternehmen hergestellt, sondern durch Fremdvergabe von einem Zulieferer bezogen, so muss dieser auf vollkommene Sicherheit überprüft werden. Der Zulieferer muss darauf achten, dass keine überschüssigen Verpackungen verloren gehen oder entwendet werden.[110]

4.2.2 Preis

4.2.2.1 Preispolitik

Neben der Produktpolitik bietet auch die Preispolitik eine Reihe von Maßnahmen, die die Ausbreitung von Produktpiraterie vermeiden.

Um zu verhindern, dass Konsumenten, die sich hochpreisige Markenprodukte nicht leisten können, Fälschungen erwerben, bietet es sich an, ein Alternativprodukt zu einem günstigeren Preis, jedoch mit gleicher Qualität, auf den Markt zu bringen.[111] Um das Image des ersten Produktes nicht zu gefährden, muss allerdings besonders darauf geachtet werden, beide Produkte klar voneinander abzutrennen. Nur so kann das günstigere Produkt vom guten Ruf des ersten Produktes profitieren.[112]

Zudem bietet die Preisdifferenzierung eine Möglichkeit, das Premium-Segment sowie das Low-Cost-Segment mit dem gleichen Produkt abzudecken. Der Hersteller unterteilt hierbei den Markt für seine Produkte in verschiedene Segmente und bearbeitet jedes dieser Segmente mit verschiedenen Marken- und Preisstrategien. So bieten beispielsweise Lebensmittelhersteller ihre Produkte mit unterschiedlicher Verpackung sowohl in gewöhnlichen Läden als auch in Discountern an. Diese Strategie der Preis-

[109] Vgl. Harte-Bavendamm (2000), S. 38.
[110] Vgl. Fischer et al. (2002), S. 83.
[111] Vgl. Fischer et al. (2002), S. 88.
[112] Vgl. Welser/González (2007), S. 306.

differenzierung verhindert, dass Produktpiraten in das Low-Cost-Segment eintreten und sich von dort aus auf das Premium-Segment ausbreiten.[113]

Darüber hinaus sind leicht imitierbare Produkte mit hohen Margen für Produktpiraten besonders attraktiv. Daher erweist es sich für den Originalhersteller als vorteilhaft, hohe Margen auf schwer imitierbare Waren umzulegen und damit leicht imitierbare Produkte zu subventionieren.[114]

4.2.2.2 Konditionspolitik

Die Konditionspolitik stellt ein weiteres Instrument zur Bekämpfung von Produktpiraterie dar. Sie umfasst alle Maßnahmen, die neben dem Preis Teil der vereinbarten Leistung sind.[115] Hierzu zählt beispielsweise die Rabattpolitik, deren Ziel unter anderem die Erhöhung der Kundentreue ist.[116] Im Kampf gegen Produktpiraterie können Treuerabatte den Anreiz, auf billigere Kopien zurückzugreifen, verringern. In der Softwareindustrie werden oftmals Upgrade-Versionen zu günstigeren Preisen angeboten, um den Kunden vom Kauf von Raubkopien abzubringen.[117] Ein anderer Weg, Kundenloyalität zu schaffen, ist die Gewährung eines Preisnachlasses auf neue Produkte, sofern ältere Waren gleicher Marke eingetauscht werden.[118]

4.2.2.3 Target-Cost-Management

Wie unter Abschnitt 4.2.1.3 beschrieben, wird beim Target-Cost-Management der Produktpreis im Vorhinein festgelegt. Ziel ist es, einen am Markt realisierbaren Preis zu ermitteln. Ausgerichtet an diesem Preis werden Material und Qualität des Produktes bestimmt. Dies ermöglicht dem Hersteller, seine Ressourcen besser zu verteilen und somit Kosten zu sparen. Der erzielte Kostenvorteil wird im Grunde genommen an den Kunden weitergegeben, da das am Markt angebotene Produkt ein attraktives Preis-/Leistungsverhältnis bietet. Da durch Target-Costing Margen klein gehalten werden,

[113] Vgl. Wildemann (2007), S. 116.
[114] Vgl. Wildemann (2007), S. 115.
[115] Vgl. Koch (1999), S. 293.
[116] Vgl. Meffert (1999), S. 294.
[117] Vgl. Fischer et al. (2002), S. 88.
[118] Vgl. Harte-Bavendamm (2000), S. 47.

verlieren Produkte den Anreiz für Fälscher.[119] Billigere Produkte mit gleicher Marge sind nur durch mindere Qualität realisierbar.

4.2.3 Distribution

4.2.3.1 Management des Vertriebs

Der Distributionspolitik kommt bei der Vermeidung von Produktpiraterie eine besonders große Rolle zu. Während des Vertriebs werden häufig originale Waren durch Fälschungen ausgetauscht. Einzig und allein durch illoyale, betrügerische Vertriebspartner entstehen und wachsen graue Märkte, die die Wettbewerbsfähigkeit des Herstellers erheblich schwächen können. Daher gilt es, die Vertriebskette möglichst sicher zu organisieren und geeignete Maßnahmen zu finden, um den Produktpiraten den illegalen Eintritt in Märkte zu erschweren.

Ein gutes Vertriebsmanagement kann verhindern, dass sich Mitarbeiter von Fälschern bestechen lassen. Besonders in China gehören Geldgeschenke oder andere teure Bestechungsgaben zum Alltag der Piraten. Diese internen Lücken lassen sich durch die Bildung von Vertriebsteams schließen, da sich Mitarbeiter in kleinen Teams gegenseitig kontrollieren und somit jeder Vertriebsmitarbeiter überwacht wird.[120]

Darüber hinaus sollten Vertriebsmitarbeiter nicht immer denselben Kundenkreis bedienen. Durch Rotation zwischen verschiedenen Produktgruppen und Kunden wird der Aufbau persönlicher Beziehungen mit außenstehenden Personen verhindert. Im Rahmen des Key-Account-Managements sollten Verkaufsbezirke, Verkaufsquoten, Routen und die Anzahl der Besuche festgelegt werden.[121] So lassen sich die Wege der Produkte und die Arbeit des Vertriebs besser nachverfolgen.

Besondere Achtsamkeit bei der Auswahl der Vertriebspartner ist eine weitere Maßnahme, die illegale Handlungen erschwert. So kann der Hersteller über ein besonderes Zertifizierungsverfahren prüfen, ob der ausgewählte Händler die erforderlichen Sicherheitsmaßnahmen erfüllt und sie auch im Laufe der Partnerschaft beibehält.[122] Dies geschieht z.B. mittels eines Self-Assessment-Questionnaire[123]. Nach der sorgfäl-

[119] Vgl. Kroboth (2006), S. 66.
[120] Vgl. Fuchs (2006), S. 248.
[121] Vgl. Fuchs (2006), S. 249.
[122] Vgl. Fuchs (2006), S. 251.
[123] Es handelt sich hierbei um einen Fragebogen, der vom Händler jährlich ausgefüllt werden muss. Er gibt dem Originalhersteller Auskunft über die Umsetzung der Sicherheitsmaßnahmen seitens des Händlers.

tigen Auswahl der Partner sollte auch vor allem die Gestaltung der Verträge nicht vernachlässigt werden. Enthalten diese Lücken, so können im Falle einer Auseinandersetzung erhebliche Nachteile für den Hersteller entstehen. Ein Piraterie-Agreement, in dem der Händler sich verpflichtet, das geistige Eigentum des Herstellers zu schützen, sollte Bestandteil eines jeden Vertrags sein.[124] Jedoch sollten Hersteller ihren Händlern auch positiv gegenüber stehen. Genau wie bei Belohnsystemen, die intern beim eigenen Personal angewandt werden[125], können durch bestimmte Anreizsysteme Partner motiviert werden, besonders achtsam bei der Ausschau nach Plagiaten zu sein.

Weitere Maßnahmen, wie Schulungen bzw. die Aufklärung der Vertriebsmitarbeiter und Partner, sind im Kampf gegen Produktpiraterie unverzichtbar.[126] Sie ermöglichen eine einfachere Identifizierung von Fälschungen. Zudem sollten Rechtsfolgen, die durch das bewusste Einschleusen von Pirateriepodukten entstehen, unter allen Beteiligten der Vertriebskette eindeutig kommuniziert werden. Letztendlich kann nur ein professionelles Vertriebsmanagement das Unternehmen vor externen Eingriffen schützen.

4.2.3.2 Selektive Vertriebssysteme

Eine besondere Form der Auswahl der Vertriebspartner sind selektive Vertriebssysteme. Hierbei konzentriert sich der Hersteller nur auf eine geringe Anzahl ausgesuchter Verkaufsstellen.[127] Die ausgewählten Händler verpflichten sich, die Produkte nur innerhalb des Vertriebssystems weiterzugeben. Eine Belieferung unerwünschter Händler wird somit ausgeschlossen. Werden Waren außerhalb dieses Vertriebssystems angeboten, so kann davon ausgegangen werden, dass es sich um Fälschungen handeln muss.[128] Zur Strategie des selektiven Vertriebs gehören beispielsweise exklusive Belieferungen selbständiger Einzelhändler, Vertragshandelssysteme, Franchising sowie eigene Filialen.[129]

Obwohl Händler des selektiven Vertriebs einigen vertragsrechtlichen Bestimmungen unterliegen, ist diese Form der Kooperation für sie sehr vorteilhaft. Sie genießen gewisse Exklusivrechte, wodurch sie eine besondere Stellung im Wettbewerb einneh-

[124] Vgl. Fuchs (2006), S. 251.
[125] Vgl. Fuchs (2006), S. 235.
[126] Vgl. Fischer et al. (2002), S. 85.
[127] ebd.
[128] Vgl. Fuchs (2006), S. 249.
[129] Vgl. Fischer et al. (2002), S. 85.

men.[130] Vor allem bei Herstellern der Luxusartikelbranche ist die Form des selektiven Vertriebs weit verbreitet. Sie verhindert, dass die Produkte in imageschädigenden Läden verkauft werden und bewahrt somit die Exklusivität der Marken.[131]

Auch wenn die Form des selektiven Vertriebs für den Hersteller eine gute Möglichkeit bietet, die Verteilung seiner Produkte genau zu überwachen, darf die Gefahr, in Konflikt mit dem Wettbewerbsrecht zu geraten, nicht außer Acht gelassen werden.[132] Es muss somit vorher geprüft werden, ob dem Unternehmen hierdurch Schwierigkeiten entstehen könnten.

4.2.3.3 Schutz der Vertriebskette durch ECR

Der *Efficient Consumer Response* (ECR) ist ein Ansatz, um Teile der Vertriebskette zu verkürzen und somit eine Optimierung der Wertschöpfungskette zu erreichen. Hersteller und Händler arbeiten eng zusammen, wodurch nicht nur für sie eine *win-to-win*-Situation entsteht (z.B. Einsparpotentiale durch Kostenreduktion), sondern auch die Bedürfnisse der Kunden besser befriedigt werden können. Der Abnehmer soll durch die gesichtete Lieferung originaler Waren vor Fälschungen geschützt werden. Schwachpunkte der Lieferkette, wie beispielsweise stehende Lagerbestände, werden durch ECR beseitigt, sodass folglich auch das Risiko eines Angriffs durch Produktpiraten verringert wird.[133]

4.2.3.4 Distributionslogistik

Ein anderes vorbeugendes Mittel gegen Produktpiraterie betrifft die Distributionslogistik. Häufig werden unwesentliche Unternehmensleistungen an externe Dienstleister ausgegliedert. „So überlassen die meisten Industriefirmen ihre Distribution spezialisierten Dienstleistern, die in der Distributionskette Aufgaben wie Lagerung, Kommissionierung, Verladung, Transport und Umschlag übernehmen.“[134] Folglich ist die Wahl des Logistikdienstleisters von wesentlicher Bedeutung.

Es gilt, über Fehlmengen, Fehllieferungen, Schaden- oder auch Schwundquoten im Vorhinein genau zu verhandeln. Nur so kann sich der Hersteller davor schützen, dass

[130] Vgl. Wildemann (2007), S. 123.
[131] Vgl. Welser/González (2007), S. 316.
[132] Vgl. Wildemann (2007), S. 123.
[133] Vgl. Fuchs (2006), S. 254.
[134] Weiser/Olsen (2004), S. 33.

seine Waren nicht anderweitig illegal verwendet werden oder gar ein Austausch durch billige Kopien vorgenommen wird. Aushilfsfahrer oder Frachtführer, die nur einmalig für den Dienstleister tätig sind, stellen eine erhebliche Bedrohung für den Hersteller dar. Daher sollten sich externe Dienstleister dazu verpflichten, nur eigenes Personal zu verwenden. [135]

Durch Tracking und Tracing können Sendungen verfolgt und der Gang der Ware rekonstruiert werden. Ein elektronisches System gibt Auskunft darüber, auf welcher Stufe des Versands sich ein Artikel befindet (Tracking). Der Begriff Tracing hingegen bezeichnet den Sendungsverlauf der Ware, wodurch verfolgt werden kann, was mit den Waren geschehen ist und wo gegebenenfalls Fälschungen durch Schwachstellen eindringen konnten. Die einzelnen Statusmeldungen werden meist durch Mitarbeiter oder einen Barcode-Scan übermittelt, weshalb Echtzeitdaten hiermit nicht gegeben sind. Eine bessere Methode, die eine zeitgenaue Ermittlung des Standortes garantiert, ist die RFID-Technologie (Vgl. Abschnitt 4.2.1.4).[136]

Um eine lückenlose Verfolgung vom Hersteller bis zum Kunden zu ermöglichen, müssen alle Beteiligten der Vertriebskette in das Tracking- und Tracing-System integriert werden. Dies ist allerdings nur zu erreichen, wenn es sich um ein geschlossenes Vertriebssystem mit ausgewählten Händlern handelt.[137]

Auch die eigene Distributionslogistik bietet Maßnahmen, sich vor Produktpiraten zu schützen. So kann durch das Verpacken der Produkte in endkundengerechte Einheiten (*Unit of Use Packaging*) verhindert werden, dass ein Neu- oder Umpacken beim Zwischenhändler stattfindet. Gerade in der Pharmaindustrie kann dies einen erheblichen Vorteil schaffen, da das Umpacken mit einem großen Aufwand und hohen Kosten verbunden ist. [138]

4.2.4 Kommunikation

4.2.4.1 Kommunikations-Mix

Die Strategie der Kommunikationspolitik umfasst sowohl sämtliche unternehmensinterne Informationen, als auch die nach außen gerichtete Kommunikation, die Markt-

[135] Vgl. Fischer et al. (2002), S. 85.
[136] Vgl. Fuchs (2006), S. 252.
[137] Vgl. Welser/González (2007), S. 342.
[138] Vgl. Fuchs (2006), S. 249.

kommunikation. Vor allem kommunikative Maßnahmen, die auf die Absatzmärkte ausgerichtet sind, sollen die Einstellung und das Kaufverhalten der Zielgruppe direkt bzw. indirekt beeinflussen.[139] Daher bietet eine intelligente Kommunikationspolitik eine Reihe von Maßnahmen, um aktiv gegen Produktpiraterie vorzugehen. Aufgrund der zahlreichen Möglichkeiten kann für die Kommunikationspolitik ein eigener Kommunikations-Mix entworfen werden. So bieten klassische Medien (z.B. Printmedien, Werbeformen im TV-Bereich) neben den neuen Medien (z.B. Kommunikation über das Internet) viele Chancen, mit der Zielgruppe zu kommunizieren[140] und diese über die steigende Bedrohung durch Produktpiraterie zu informieren.

Bei der Auswahl und Gestaltung der Werbemittel muss darauf geachtet werden, um welche Zielgruppe es sich handelt. Käufertypen, die bewusst Produktfälschungen erwerben, müssen anders adressiert werden als Konsumenten, die unbewusst handeln und beim Kauf getäuscht werden.[141]

Um die Nachfrage der bewusst getätigten Käufe zu reduzieren, sollte an die Moral und das Rechtsempfinden der Zielgruppe appelliert werden. Vielen dieser Käufer ist nicht bewusst, dass der Diebstahl von geistigem Eigentum eine echte kriminelle Handlung darstellt und der Erwerb von Pirateriewaren die organisierte Kriminalität unterstützt.[142] Werbebotschaften sollten beispielsweise aufzeigen, wie viel Arbeitsplätze jährliche durch Produktpiraterie verloren gehen oder wie viele Steuereinnahmen ausfallen, die dann anderweitig durch Steuererhöhungen kompensiert werden müssen. Erst wenn Konsumenten erkennen, dass sie mit dem Kauf billiger Kopien nicht nur dem Staat und den Unternehmen schaden, sondern persönlich von den negativen Folgen betroffen sind, werden sie davon ablassen. Hinweise auf Sicherheitsrisiken, wie die Gefährdung der eigenen Gesundheit, sind effektive Maßnahmen, um die Nachfrage nach gefälschten Produkten zu verringern.

Die billige Kopie einer Designersonnenbrille, die im Urlaub auf einem der zahlreichen Fälschermärkten erworben wird, ist i.d.R. von minderer Qualität. Zumeist werden diese Fälschungen aus einfachem Material hergestellt, sodass sie nicht einmal UV-Schutz bieten. Folglich könnte eine Strategie des Originalherstellers sein, auf Plakaten und Werbespots besonders die Sicherheit und Qualität seiner Produkte hervorzuheben.

[139] Vgl. Koch (1999), S. 332.
[140] Vgl. Unger/Fuchs (2005), S. 147.
[141] Vgl. Fischer et al. (2002), S. 87.
[142] Vgl. Welser/González (2007), S. 364.

Beim unbewussten Erwerb von Fälschungen gilt besonders darauf zu achten, den Verbraucher im Rahmen von Informationskampagnen über das Auftreten von Fälschungen aufzuklären. So sollte zum einen der Konsument geschützt werden, zum anderen sollte signalisiert werden, dass das Unternehmen um die Qualität der Produkte, die den Markennamen tragen, bemüht ist.[143] In diesem Zusammenhang ist es wichtig, dass der Konsument weiß, wie er technische Schutzmaßnahmen, die zur Unterscheidung an dem Produkt angebracht werden, erkennen kann. So informiert die Firma Rolex zum Beispiel in Zeitungsannoncen über die Sicherheitskennzeichnung ihrer Produkte. Nachteil hierbei ist, dass durch diese Kampagnen auch Produktpiraten sensibilisiert und aufgeklärt werden.[144] Werden Produkte über ein selektives Vertriebssystem in den Handel gebracht, so muss der Verbraucher darüber informiert werden, dass er originale Waren nur über diesen exklusiven Händlerkreis erwerben kann.[145]

Darüber hinaus sollte in der Kommunikationsbotschaft die bildhafte und emotionale Komponente betont werden.[146] Wirkungsvolle Botschaften müssen das Interesse des Empfängers wecken, was in erster Linie über das visuelle Wahrnehmungssystem geschieht.[147] Wird eine Botschaft nicht wahrgenommen, so bleibt sie erfolglos und ihre Entwicklungs- und Umsetzungskosten wären besser anderweitig eingesetzt worden. In China beispielsweise sollte im Kampf gegen Produktpiraterie nicht auf Massenkommunikation gesetzt werden. Innovative und originelle Ansätze, wie „[…] die theatralische Inszenierung von Unternehmens- und Produktmarken mit faszinierenden Bilderwelten sind in der Volksrepublik oft viel wirksamer."[148] Daneben sind moderne Kommunikationsmaßnahmen wie *direct mailings* oder *podcasts* geeignet, das Interesse des Verbrauchers zu wecken und diesen auf Fälschungen hinzuweisen.

Hersteller können überdies Messen und Ausstellungen nutzen, um weitere Aufklärungsarbeit zu leisten. Ein Beispiel hierfür ist die Ambiente in Frankfurt. Als der Designer Rido Busse 1977 auf der Ambiente eine 100%ige Fälschung seiner Brief-/Diätwaage 8600 entdeckte, beschloss dieser, einen Negativpreis für die dreisteste Fälschung zu verleihen. Somit sollten die Öffentlichkeit und der Gesetzgeber aufmerksam gemacht und über die negativen Auswirkungen von Plagiaten und Fälschungen aufge-

[143] Vgl. Wildemann (2007), S. 121.
[144] Vgl. Fischer et al. (2002), S. 87.
[145] Vgl. Welser/González (2007), S. 363.
[146] Vgl. Fuchs (2006), S. 303.
[147] Vgl. Unger/Fuchs (2005), S. 516.
[148] Fuchs (2006), S. 303.

klärt werden. Seitdem findet die Verleihung des „Plagiarius“ jährlich auf der Ambiente statt. 2007 ging der erste Preis an die Isolierkanne „Sophie“, welche im Original von der alfi GmbH Wertheim stammt. Das Plagiat kam vom Hersteller He Shan Jia Hui Vacuum Flask & Vessel Co., Ltd., Guangzhou, P.R. aus China.[149]

Die Produkte der alfi GmbH waren bislang acht Mal bei der „Plagiarius“-Verleihung vertreten. Das Unternehmen hat dies als Maßnahme zur Bekämpfung von Produktpiraterie in ihre Schutzstrategie integriert: Durch den hohen Aufmerksamkeitswert sollen Endkunden sensibilisiert werden. Außerdem ist hier die Kenntnis der Öffentlichkeit bei der Durchsetzung von Ansprüchen hilfreich.[150]

Zudem unterstützen viele Messen ihre Aussteller im Kampf gegen Produktpiraterie. Die Messe Frankfurt tut dies beispielsweise seit 2006 mit der Aktion „Messe Frankfurt against Copying."[151]

4.2.4.2 Öffentlichkeitsarbeit

Ein weiterer Bereich der Kommunikationspolitik ist die Öffentlichkeitsarbeit. Unternehmen können Tageszeitungen, Rundfunk und Fernsehen nutzen, um direkt mit ihrer Zielgruppe zu kommunizieren. Umso häufiger das Thema Produktpiraterie in den Medien diskutiert wird, desto mehr Aufmerksamkeit schenkt ihm die Gesellschaft. Dies wiederum schreckt mögliche Produktpiraten ab, da sich das Risiko des Entdecktwerdens potenziell erhöht.

Zudem sind Einzelaktionen in den Medien eine wirksame Maßnahme, um die Öffentlichkeit über das Problem der Produktpiraterie aufzuklären. So lassen viele Hersteller beschlagnahmte Fälschungen unter dem Auge der Presse vernichten. Dies beeindruckt den Verbraucher und ist überdies relativ kostengünstig.[152]

Nahezu jedes Unternehmen verfügt heutzutage über einen Internetauftritt.[153] Das Internet bietet viele Möglichkeiten, den Verbraucher über das Unternehmen und dessen Produkte zu informieren. Allerdings bedienen sich auch Produktpiraten des Internets,

[149] Vgl. Plagiarius e.V. (2008).
[150] Vgl. alfi GmbH (2006).
[151] Vgl. Messe Frankfurt GmbH (2008).
[152] Vgl. Fischer et al. (2002), S. 88.
[153] Vgl. Welser/González (2007), S. 364.

um an Produktinformationen zu gelangen. Demzufolge sollten Unternehmen darauf achten, im Internet nicht allzu viele Details über ihre Produkte preiszugeben.[154]

4.2.4.3 Kommunikationspolitik im eigenen Unternehmen

Wichtig ist auch die Kommunikationspolitik im eigenen Unternehmen. Es gehört zu den Aufgaben der internen Kommunikation, Mitarbeitern den richtigen Umgang mit vertraulichem Know-how zu vermitteln. Mitarbeiter mit Zugang zu kritischem Know-how sollten daher einer Verschwiegenheitsverpflichtung unterliegen, sodass sie die ihnen bekannte Information nur mit anderen autorisierten Mitarbeitern teilen.[155]

Außerdem sollte die Identität des Unternehmens (Corporate Identity) nicht nur nach außen die Sicherheitsorientiertheit des Unternehmens repräsentieren. Auch nach innen müssen die Ziele, Werte und Spielregeln kommuniziert werden. Es sollte ein einheitliches Bild bei den Mitarbeitern geschaffen werden, sodass ein Gefühl der Unternehmenszugehörigkeit entsteht und jeder Mitarbeiter diese Identität durch ein verantwortungsvolles Handeln unterstützt.[156] Nur wenn Mitarbeiter bereit sind, das geistige Eigentum des Unternehmens zu schützen, kann der Verlust von wichtigen Informationen und Daten verhindert werden.

4.2.5 Kundenbetreuung/-bindung

4.2.5.1 After-Sales-Management

Die Kundenbetreuung/-bindung wird im modernen Marketing häufig als „5tes P" angesehen. Ziel des gesamten Marketing-Mix ist es, nicht nur neue Kunden zu gewinnen, sondern auch bestehende an das Unternehmen zu binden. Aus diesem Grund verfolgen Unternehmen neben der Verbesserung der Beziehung mit Partnern, die direkten Einfluss auf die Wertschöpfungskette haben, auch eine Intensivierung der Kundenbeziehung.[157] Gerade auf gesättigten Märkten, auf denen sich das Produktangebot der Anbieter immer weniger differenziert[158], gilt es, die Kunden durch Qualität und Service

[154] Vgl. Wildemann (2007), S. 120.
[155] Vgl. Fuchs (2006), S. 231.
[156] ebd.
[157] Vgl. Kotler/Bliemel (2001), S. 81.
[158] Vgl. Koch (1999), S. 248.

an sich zu binden. Dadurch werden Märkte für Piraten schwer zugänglich und unattraktiv, da diese nur über hohe Investitionen bedient werden können.

Zusätzliche Dienstleistungen, die nach dem Kauf des Produktes dem Kunden zur Verfügung stehen, werden unter dem Begriff *After-Sales* zusammengefasst.[159] Der Service umfasst i.d.R. eine produktgebundene Dienstleistung wie beispielsweise einen Ersatzteilservice, einen Austauschmodul-Service oder einen 24-Stunden-Produkt- und Businesssupport. Garantieleistungen, die über die gesetzlichen Gewährleistungsansprüche hinausgehen, zählen zudem zu den verkaufsfördernden Instrumenten, da sie dem Kunden den Eindruck einer hohen Servicebereitschaft und Produktqualität vermitteln.[160]

Die Entwicklung von Zusatzleistungen sollte am Kundennutzen ausgerichtet werden. Ein hoher Kundennutzen verspricht loyale Kunden, die zu Folgekäufen bereit sind. Daher sollte bereits bei der Entwicklung von Produkten an spätere Serviceleistungen gedacht werden.[161] Zudem handelt es sich bei Produkten des After-Sales meist um immaterielle Güter, die schwer zu imitieren sind. So bieten Serviceleistungen die Möglichkeit, sich vom Wettbewerb zu differenzieren und darüber hinaus Markteintrittsbarrieren für Produktpiraten zu schaffen.[162]

4.2.5.2 Customer-Relationship-Management

Das *Customer-Relationship-Management* (CRM) ist eine Form des integrierten Beziehungsmarketings, die sich aus dem CAS (*Computed-Aided-Selling*) weiterentwickelt hat. Neben dem ursprünglichen Ziel des CAS, die Kosten im Vertrieb zu reduzieren, soll im CRM durch eine verstärkte Kundenorientierung die Wettbewerbsfähigkeit des Unternehmens gesteigert werden. Abteilungsübergreifend werden Mitarbeiter des Marketings, des Vertriebs und des Kundendienstes miteinander verbunden.[163] CRM-Systeme sollen die Kommunikation mit dem Kunden erleichtern. Auf Grundlage einer Datenbank und Software werden alle wichtigen Kundendaten festgehalten. Jeder Mitarbeiter, der mit dem Kunden in Kontakt steht, kann das CRM-System nutzen und die Informationen abrufen. Kennt ein Hersteller die Vorzüge seines Kunden, so lässt sich durch das Anbieten kundenindividueller Produkte verhindern, dass der Kunde Konkur-

[159] Vgl. Wildemann (2007), S. 124.
[160] Vgl. Koch (1999), S. 251.
[161] Vgl. Wildemann (2007), S. 124.
[162] Vgl. Wildemann (2007), S. 125.
[163] Vgl. Kotler/Bliemel (2001), S. 143.

renzprodukte in Erwägung zieht. Das Customer-Relationship-Management steigert nachweislich die Kunden- und Lieferantenbeziehung[164] und ist somit ein bedeutender Erfolgsfaktor bei der Bekämpfung von Produktpiraterie.

5 Maßnahmenevaluation

5.1 Wirkungshorizont der Maßnahmen

Um herauszufinden, welche Maßnahmen nachhaltig und welche nur von kurzer Dauer sind, sollten Unternehmen für jede Maßnahme einen Wirkungshorizont bestimmen.

Weniger komplexe Maßnahmen sind meist leichter umzusetzen und ihre Wirkung ist sich schnell sichtbar. Jedoch sind sie für Piraten i.d.R. einfach zu durchschauen, was ihnen eine rasche Anpassung ermöglicht.[165] Daher ist die zeitliche Wirkung nur sehr kurz, sodass sich die Kosten, die bei der Einführung der Maßnahmen entstehen, wahrscheinlich nicht lohnen. Es gilt, die Kosten der Maßnahmen und ihre Nachhaltigkeit bestmöglich abzustimmen. Generell lässt sich feststellen, dass die Entwicklung und Einführung von komplexeren Maßnahmen zwar zeit- und kostenintensiv ist, Produktpiraten diese allerdings später wahrnehmen und weniger schnell reagieren können.

Da Maßnahmen unterschiedlich schnell greifen, bietet es sich an, die unter Gliederungspunkt 4 behandelten Maßnahmen in strategische und operative Maßnahmen aufzugliedern. Strategische Maßnahmen haben eine mittelfristige (1-3 Jahre) bis langfristige (> 3 Jahre) Wirkung. Operative Maßnahmen hingegen greifen bereits im ersten Jahr (< 1 Jahr) der Einführung. Bei der Gestaltung des Maßnahmen-Mix sollten operative sowie strategische Maßnahmen verwendet werden, sodass der gesamte Produktlebenszyklus abgedeckt wird (Vgl. Tabelle 2/Tabelle 3).[166]

[164] Vgl. Winkelmann (2005), S. 203.
[165] Vgl. Fuchs (2006), S. 121.
[166] ebd.

5.2 Operativer Maßnahmenplan

Tabelle 2: Operativer Maßnahmenplan
Quelle: eigene Darstellung.

Operativer Maßnahmenplan	
Kurzfristige Wirkung (<1 Jahr)	
1	Identitätsbestimmung durch technischen Produktschutz – Hologramme, OVD/DOVIDs, Siegel, Folien, DNA-Markierung, digitale Wasserzeichen…
2	Nutzung intelligenter Verpackung zur Vermeidung von Missbrauch
3	Verpackung und Versand der Produkte in endkundengerechten Einheiten
4	Technische Sicherung durch RFID
5	Verschiebung der Margen auf schwer imitierbare Produkte – Preisreduzierung bei Produkten mit hoher Fälschungsgefahr
6	Kundenbindung durch Gewährung von Rabatten, speziell bei neuen Produkten
7	Sicherung der Vertriebsschnittstellen durch Bildung von Vertriebsteams
8	Rotation der Vertriebsmitarbeiter zwischen Produktgruppen und Kunden
9	Vertragliche Abkommen mit Partnern zur Sicherung des geistigen Eigentums
10	Belohnungssysteme für Partner, die den Abfluss von Know-how verhindern oder Spionage aufdecken
11	Aufklärung über Folgen, wenn Partner Rechte verletzen
12	Sicherung des Warenversands durch Tracking und Tracing oder RFID

5.3 Strategischer Maßnahmenplan

Tabelle 3: Strategischer Maßnahmenplan
Quelle: eigene Darstellung.

Strategischer Maßnahmenplan	
Mittelfristige Wirkung (1-3 Jahre)	
13	Entwicklung schutzfähiger Produkte – gleichzeitiger Schutz benachbarter Produktfelder durch strategische Patente
14	Intelligentes Design von Produkten und ergänzenden Produkten
15	Qualitätslevel der Produkte durch FMEA und QFD erhöhen
16	Entwicklung kundenindividueller Produkte durch "add on‘s", Module und Upgrades
17	Verkürzung von Innovationszyklen durch ein effizientes Änderungswesen und Zielkostenmanagement
18	Segmenterweiterung – Einführung von Billigprodukten und deren Positionierung gegen Produktpiraten
19	Preisdifferenzierung, um Premium- und Low-Cost-Segment gleichzeitig abzudecken
20	Target-Cost-Management zur Erzielung eines optimalen Preis-/Leistungsverhältnisses
21	Überprüfung der Vertriebspartner durch Zertifizierungsverfahren
22	Training der Vertriebspartner zur Sensibilisierung
23	Reduzierung der Vertriebspartner durch selektive Vertriebssysteme
24	Verkürzung der Vertriebskette durch ECR
25	Schaltung von Werbekampagnen, um die Nachfrage nach Fälschung zu reduzieren

Strategischer Maßnahmenplan	
Mittelfristige Wirkung (1-3 Jahre)	
26	Informationskampagnen, um über Unterscheidungsmerkmale der Originale aufzuklären
27	Nutzung moderner Medien, um die Aufmerksamkeit der Konsumenten zu erlangen
28	Nutzung von Messen und Ausstellungen, um Aufklärungsarbeit zu leisten
29	Nutzung der Tagespresse zur Erinnerung der Verbraucher an das Thema Produktpiraterie
30	Sicherung des Know-hows durch festgelegte interne Kommunikation – Verschwiegenheitsverpflichtung für Mitarbeiter
31	Nutzung eines professionellen After-Sales-Management zur Erzielung einer besseren Kundenbindung
32	Einführung von CRM – Steigerung der Wettbewerbsfähigkeit durch loyale Kunden
Langfristige Wirkung (> 3 Jahre)	
33	Innovationsführer am Markt werden
34	Klare Kommunikation der Corporate Identity

5.4 Managementmodell zur Maßnahmenplanung entlang des Produktlebenszyklus

Um den Schutz von Produkten sicherzustellen, sollten die Maßnahmen aus dem Marketing-Mix entlang des Produktlebenszyklus angeordnet werden (Vgl. Abbildung 9).

In der Einführungsphase sollten bereits alle Maßnahmen zur Bekämpfung von Produktpiraterie aktiv sein. Zwar werden in dieser Phase selten Fälschungen am Markt erscheinen, jedoch liegt am Ende der Einführungsphase, dort wo die erzielten Erlöse erstmals die Kosten decken, der *Break-Even-Punkt*.[167] Treten an diesem kritischen Punkt bereits die ersten Fälschungen auf, hat dies negative Auswirkungen auf den gesamten Verlauf der Gewinnkurve zur Folge. Hierbei gilt besondere Achtsamkeit, da durch die Verkürzung der Innovationszyklen auch die Gewinnkurven zunehmend verkürzt werden. Lassen sich Gewinne aufgrund von Piraterieprodukten erst später realisieren, werden folglich in diesem Produktlebenszyklus die gesamten Gewinne niedriger ausfallen.

In der Wachstumsphase eines Produktes entsteht der meiste Wettbewerb. Andere Marktteilnehmer wollen in dieser Phase durch *Me-Too*-Produkte Käufer anlocken.[168] Vor allem für Fälscher ist diese Phase besonders interessant, da nach der Einführungsphase das Flop-Risiko gegen Null geht und die Produktakzeptanz stetig zunimmt. Zu-

[167] Vgl. Koch (1999), S. 185.
[168] ebd.

dem werden in dieser Phase die meisten Gewinne erzielt. Aufgrund des hohen Fälschungsrisikos gilt es, in den ersten beiden Phasen besonders viele Barrieren zu schaffen, um somit frühzeitig Märkte für Produktpiraten zu blockieren.

Gelingt es in der Einführungs- und Wachstumsphase, Produktpiraten fernzuhalten, sinkt die Umsatzrentabilität in der Reifephase verhältnismäßig langsamer. Zwar werden in dieser Phase weitere Mitbewerber am Markt auftreten, was das Durchsetzen hoher Preise erschwert, jedoch wird eine Zerstörung der „normalen" Marktgegebenheiten durch eine Überflutung des Marktes mit Pirateriewaren verhindert.

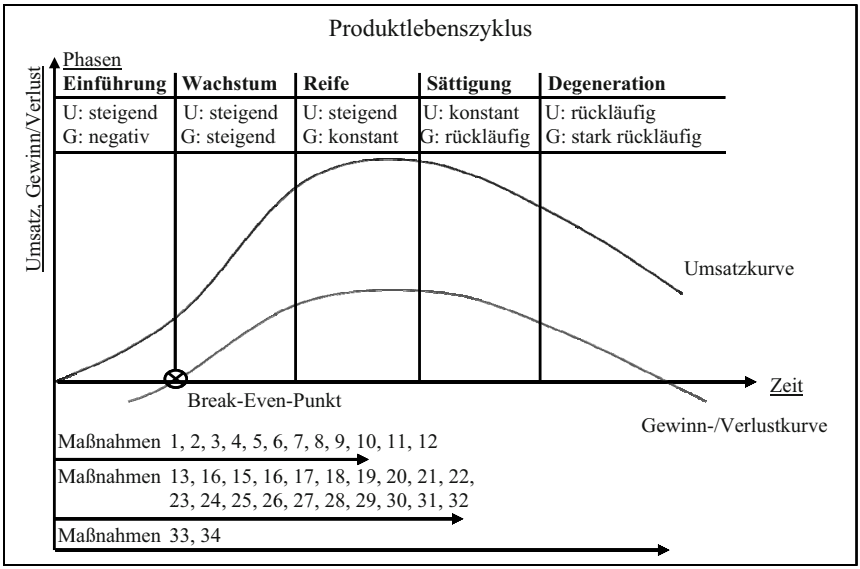


Abbildung 9: Managementmodell zur Maßnahmenplanung entlang des Produktlebenszyklus
Quelle: nach Wöhe (2002), S. 511.

Der Übergang zur Sättigungsphase lässt sich oft schwer bestimmen. Daher sollte auch hier noch ein Großteil der Maßnahmen aktiv sein. Erst gegen Ende dieser Phase und mit Beginn der Degenerationsphase nimmt die Relevanz der Maßnahmen mit einem kurzen und mittelfristigen Wirkungshorizont ab. Sinkende Erlöse charakterisieren diese Phase, sodass der Markt für andere Wettbewerber nicht mehr attraktiv ist. Sind Produktpiraten zu diesem Zeitpunkt nicht auf dem Markt vertreten, werden Fälschungen auch nicht mehr auftreten.

Jedoch sind hier noch Maßnahmen mit langer Wirkungsdauer aktiv. Ist ein Unternehmen beispielsweise Innovationsführer am Markt (Maßnahme 33), beeinflusst dies die Produktlebenszyklen neuer Produkte. Das Unternehmen nutzt die Vorteile der Pionierstrategie (Vgl. Abschnitt 3.2.1) und gibt sogleich ein klares Signal an seine Wettbewerber. Die Zeitabstände zwischen den Einführungsphasen neuer Produkte werden vom Innovationsführer konsistent verkürzt. Folglich schließt diese Maßnahme den Kreis zwischen Produkteinführung und -eliminierung und spielt somit eine entscheidende Rolle im Kampf gegen Produktpiraterie.

6 Marketing als Teil eines unternehmensweiten Schutzkonzeptes

Am 09.02.2008 wurde erneut im Rahmen der Frankfurter Ambiente Messe der „Plagiarius“ verliehen. Auch in diesem Jahr ging der Negativ-Preis an einen chinesischen Hersteller für die Kopie eines Salz- und Pfeffersets von WMF. Dennoch wurde deutlich, dass die dreisten Fälschungen nicht mehr nur aus dem asiatischen Raum stammen. Unter den „Gewinnern“ fanden sich auch deutsche Unternehmen wie z.B. die Aalener Heinrich Winkelmann GmbH, die ein Druckgefäß für eine Heizungsanlage eines Schweizer Herstellers kopierte. Ebenso fiel die Kopie eines Urologie-Resektoskopes auf einen deutschen Nachahmer zurück.[169]

Es ist immer häufiger festzustellen, dass Produktpiraterie nicht mehr ausschließlich ein Problem der Luxusgüterbranche ist. Alle Branchen und Industrien müssen sich darüber bewusst werden, dass auch sie vor Angriffen der Produktpiraten nicht gefeit sind. So hieß es kürzlich in einem Bericht der Frankfurter Allgemeinen Sonntagszeitung, dass Käsepiraten u.a. schuld an der Käsekrise sind. Sie bringen gefälschte Markennamen auf Billigkäse an und erzielen somit ein gutes Geschäft. Allerdings vernichten sie den Geschmack guten Käses. Um dieser Entwicklung entgegenzuwirken, werden Zöllner zu Käseverkostern geschult. Sie sollen echte Käsequalität erkennen und dadurch der Fälschung von Käse vorbeugen.[170] Dieser Fall zeigt, dass sich auch die Lebensmittelbranche vor Produkt- und Markenpiraten schützen muss.

[169] Vgl. o.V. (2008a).
[170] Vgl. Oberhuber (2008), S. 42.

Betrachtet man die schwerwiegenden Auswirkungen der Produktpiraterie auf Staaten, Unternehmen und Konsumenten, so wird schnell deutlich, dass ein alsbaldiges Handeln aller Parteien notwendig ist.

Die Zusammenarbeit mit Verbänden wie beispielsweise dem APM, einem branchenübergreifenden Verband, der seit 1997 im Kampf gegen Produkt- und Markenpiraterie tätig ist,[171] scheint unerlässlich. Unternehmen schließen sich hier zusammen, um gemeinsam Aufklärungsarbeit zu leisten, Erfahrungen und Informationen untereinander auszutauschen und weitere Barrieren für Produktpiraten zu schaffen.

Internationale Organisationen wie die OECD oder das ICC arbeiten hart daran, der Unwissenheit und Überforderung vieler Unternehmen entgegenzuwirken. Durch die Hilfestellung bei Rechtsverfahren sowie die Bereitstellung von Informationen und Hinweisen zur Umsetzung von Maßnahmen soll ein Umdenken der Hersteller, Händler und Konsumenten erzielt werden.

Die unter den Gliederungspunkten 3 und 4 erarbeiteten Strategien und Maßnahmen sollen als konkrete Handlungsansätze im Marketing dienen. Allerdings müssen sie zusätzlich mit anderen unternehmensweiten Konzepten und Methoden verknüpft werden. Um eine angriffssichere Wertschöpfungskette zu schaffen, sollten alle Prozesse und Abläufe eines Unternehmens bestmöglich aufeinander abgestimmt werden: von der Beschaffung und Zulieferung, über die operativen Prozesse im Unternehmen bis hin zu den Vertriebs- und Logistikprozessen. Nur so kann ein umfassender Schutz vor Produktpiraterie erzielt werden.

Jedes Unternehmen muss unter Berücksichtigung der unternehmensspezifischen Situation die bestehenden Gefahren analysieren und ihre Konsequenzen abschätzen. Vor der Einführung der Maßnahmen empfiehlt es sich, eine Kosten-Nutzen-Analyse durchzuführen. Besonders kleine und mittelständische Unternehmen schätzen den Kosten- und Zeitaufwand, der bei der Entwicklung und Einführung von Schutzmaßnahmen entsteht, oftmals höher als den Nutzen. Daher konzentrieren sich diese häufig auf den juristischen Schutz und verzichten auf die Einführung betriebswirtschaftlicher Maßnahmen.

Allerdings ist diese Einschätzung irrtümlich. Besonders strategische Maßnahmen haben eine langfristige Wirkung. Sie zielen darauf ab, Produktpiraterie zu verhindern und nicht erst im Nachhinein zu bekämpfen. Ihre Kosten mögen zwar zu Beginn ver-

[171] Vgl. APM e.V. (2008).

hältnismäßig hoch sein, sie amortisieren sich jedoch im Laufe der Jahre. Unternehmen sollten ihre Maßnahmen regelmäßig prüfen, neu bewerten und gegebenenfalls an veränderte Marktgegebenheiten anpassen.

Letztendlich wird es nicht möglich sein, den Missbrauch geistigen Eigentums völlig auszuschließen. Dennoch kann ein umfassendes Anti-Counterfeiting-System die Bedrohung und Auswirkungen vor Produktpiraterie stark verringern.

Literaturverzeichnis

alfi GmbH (Hrsg. 2006): Historie. Erfahrungsbericht Produkt- und Markenpiraterie. 2006.

APM e.V. (Hrsg., 2008): Aktionskreis Deutsche Wirtschaft gegen Produkt- und Markenpiraterie. URL: http://www2.markenpiraterie-apm.de/index.php?lang=de&rid=2&pid=1 (Stand 2008, Zugriff: 11.02.2008)

Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (Hrsg., 2005): Anmerkungen zur Sicherheitslage der deutschen Wirtschaft 2004/2005. Berlin 2006.

Bialdiga, K. (2008): Unternehmen verzichten auf Patente. In: Financial Times Deutschland, 02.01.2008.

Economist Corporate Network (Hrsg., 2005): China. Intellectual Property Rights, Protecting assets in the information, communications and entertainment market. KPMG Studie 2005.

European Commission (Hrsg., 2006): Summery of Community Customs Activities on counterfeit and piracy. Results at the European Border 2006. URL: http://ec.europa.eu/taxation_customs/resources/documents/customs/customs_controls/counterfeit_piracy/statistics/counterf_comm_2006_en.pdf (Stand: 2006, Zugriff: 07.10.2007)

Fischer, St./Eck, R./Richter, H.-J. (2002): Was sich gegen Produktpiraterie tun lässt. In: Harvard Business Manager (HBM), Ausgabe 1/2002, S. 80-91.

Fuchs, H. J. (2006): Piraten, Fälscher und Kopierer. Strategien und Instrumente zum Schutz gestiegen Eigentums in der Volksrepublik China. 1. Auflage, Gabler Verlag, Wiesbaden 2006.

Fussan, C. (2007/2008): Forschungsprojekt Produktpiraterie an der betriebswirtschaftlichen Fakultät der Georg-Simon-Ohm Hochschule Nürnberg, 2007/2008.

Harte-Bavendamm, H. (2000): Handbuch der Markenpiraterie in Europa. München 2000 (C.H. Beck Verlagsbuchhandlung, Manz'sche Verlags- und Universitätsbuchhandlung, Wien, Verlag Stämpfli AG, Bern).

Homburg, Chr./Daum, D. (1997): Marktorientiertes Kostenmanagement. Kosteneffizienz und Kundennähe verbinden. Frankfurter Allgemeine Zeitung, Verlagsbereich Wirtschaftsbücher, Frankfurt am Main 1997.

Hopkins, D. M./Kontnik, L. T./Turnage, M. T. (2003): Counterfeiting Exposed. Protecting Your Brands and Customers. New Jersey USA, 2003.

ICC-Studie (Hrsg. 2007): The International Anti-Counterfeit Directory. URL: http:// www.icc-ccs.org/pdfs/IACD2007.pdf (Stand: 2007, Zugriff: 18.10.2007)

Interbrand (Hrsg., 2001): Best Global Brands 2001. URL: http://www.ourfishbowl.com/images/surveys/IB_SV_BW_8_6_01.pdf (Stand: 2001, Zugriff: 22.10.2007)

Interbrand (Hrsg., 2007): Best Global Brands 2007. URL: http://www.ourfishbowl.com/images/surveys/Interbrand_BGB_2007.pdf (Stand: 2007, Zugriff: 22.10. 2007)

Johansson, J. K. (2000): Global marketing. Foreign entry, local marketing, and global management. 2nd ed. USA, 2000.

Koch, J. (1999): Marketing, Managementwissen für Studium und Praxis. Einführung in die Marktorientierte Unternehmensführung. Oldenbourg Verlag, 1.Auflage, München 1999.

Kotler, Ph./ Bliemel, F. (2001): Marketing-Management. Analyse, Planung und Verwirklichung. 10. Auflage, Schäffer-Poeschel Verlag, Stuttgart 2001.

Kroboth, D. (2006): Präventionsmaßnahmen gegen Marken- und Produktpiraterie. Strategien für Unternehmen auf europäischer und internationaler Ebene. Shaker Verlag, Aachen 2006.

Kutschker, M./Schmid St. (2005): Internationales Management. 4. Auflage, Oldenbourg Verlag, München 2005.

Lachmann, J./Kühl, Chr./Kühl, M. (2007): Tod aus der Tube. In: Financial Times Deutschland, 11.07.2007.

Ledbury Research (Hrsg., 2007): Counterfeiting Luxury. Exposing the Myths. Davenport Lyons. URL: http://www.a-cg.com/docs/luxDLapr06.pdf (Stand: 2007, Zugriff: 04.09.2007)

Meffert, H. (1998): Marketing. 8. Auflage, Wiesbaden 1998. In: Koch, Jörg (1999): Marketing. Managementwissen für Studium und Praxis. Einführung in die Marktorientierte Unternehmensführung. 1.Auflage, Oldenbourg Verlag, München 1999.

Messe Frankfurt GmbH (Hrsg., 2008): Messe Frankfurt against Copying. URL: http://www.messefrankfurt.com/corporate/de/home_messefrankfurtagainstcopying.htm (Stand: 2008, Zugriff: 14.01.2008)

Oberhuber, N. (2008): Käse in der Krise. In: Frankfurter Allgemeine Sonntagszeitung, 03.02.2008.

OECD-Studie (Hrsg., 2007): The Economic Impact of Counterfeiting and Piracy. URL: http://www.oecd.org/dataoecd/13/12/38707619.pdf (Stand: 2007, Zugriff: 03.09.2007)

o.V. (2006): Die besten Ideen von Michael E. Porter. In: Harvard Business Manager. Harvard Business School Publishing 1979. Ausgabe 1/2006.

o.V. (2007): Allianz gegen Produktpiraterie. In: Fürther Nachrichten, 18.09.2007.

o.V. (2008): Dem Wettlauf mit Fälschern entkommen. In: VisAvis Economy, Beilage der Financial Times Deutschland, Heft 1/2008.

o.V. (2008a): Dreisteste Produkt-Kopierer ausgezeichnet. In: Fürther Nachrichten, 09.02. 2008.

Philips, T. (2005): Knockoffs. The deadly trade in counterfeiting goods. USA, 2005.

Plagiarius e.V. (Hrsg., 2008): Die Plagiarius Story. URL: http://www.plagiarius.com/aktion_plag.html (Stand: 2008, Zugriff: 14.01.2008)

Stockinger, B. (2007): Focus Marketing. Kampf den Piraten. In: Sportswear International, Ausgabe Juli/August 2007, Nr. 214.

The Patent Office (Hrsg., 2007): A Brief Guide to IP and Anti-Counterfeiting. URL: http://www.a-cg.com/docs/counter-book.pdf (Stand: 2007, Zugriff: 18.09.2007)

Unger, F./Fuchs, W. (2005): Management der Marketing-Kommunikation. 3. Auflage, Springer Verlag, Berlin Heidelberg 2005.

Vereinigung zur Bekämpfung von Produktpiraterie e.V. (Hrsg., 2007): Main. URL: http://www.vbp.org/de/main.asp (Stand: 2007, Zugriff: 18.10.2007)

VDMA-Untersuchung (Hrsg., 2007): Produkt- und Markenpiraterie in der Investitionsgüterindustrie. URL: http://www.original-ist-genial.de/fileadmin/icc_dokumente/VDMA_Produktpiraterie_2007_Mitteilung.pdf (Stand: 2007, Zugriff: 19.10. 2007)

Weiser, A./Olsen, G. S. (2004): Management von Markenpiraterie. Idealtypische Ausgestaltung und praktische Umsetzung. Universität Mannheim 2004.

Welser, M. v./González, A. (2007): Marken- und Produktpiraterie. Strategien und Lösungsansätze zu ihrer Bekämpfung. 1. Auflage, WILEY Verlag, Weinheim 2007.

WHO (Hrsg., 2006): Counterfeit Medicines. An update on estimates. URL: http:// www.who.int/medicines/services/counterfeit/impact/TheNewEstimatesCounterfeit.pdf (Stand: 2006, Zugriff: 28.10.2007)

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

Winkelmann, P. (2005): Vertriebskonzeption und Vertriebssteuerung. Die Instrumente des integrierten Kundenmanagements (CRM). 3. Auflage, Verlag Vahlen, München 2005.

Wöhe, G. (2002): Einführung in die Allgemeine Betriebswirtschaftslehre. 21. Auflage, Verlag Vahlen, München 2002.

Marion Fricke

D Schutzmaßnahmen gegen Produktpiraterie im Funktionalbereich Logistik

Inhaltsverzeichnis

1 Piraterie heute 187

2 Gegenstandsbereich und Hemmnisse bei der Bekämpfung von Produktpiraterie 187

2.1 Begriff der Produktpiraterie 187

2.2 Kulturelle Unterschiede als Ursache von Pirateriеverhalten 189

2.3 Hemmnisse bei der Bekämpfung von Produktpiraterie 190

3 Logistik als Angriffspunkt für Produktpiraten 192

3.1 Bedeutung des Funktionalbereichs Logistik 192

3.2 Mögliche Schwachstellen und Problemlösungsansätze in logistischen Prozessen 195

4 Technische Schutzmaßnahmen in der Logistik 198

4.1 Technologien gegen Produkt- und Verpackungsfälschungen 198

4.1.1 Hologramme 199
4.1.2 OVDs 200
4.1.3 Sicherheitstinten 201
4.1.4 Sicherheitsdrucke 202
4.1.5 Sicherheitspapiere 204
4.1.6 Mikroaufdrucke 205
4.1.7 Mikroskopische Kunststoffpartikel 206
4.1.8 Biologische, chemische und magnetische Marker 207
4.1.9 Digitale Wasserzeichen 208
4.1.10 Holographische Projektionen 208

4.2 Technologien gegen das Öffnen der Verpackungen 209

4.2.1 Versiegelungstechniken 209
4.2.2 Folien 210

4.3 Schutz des Vertriebssystems durch Tracking und Tracing 210

4.3.1 Tracing-Nummern 211

4.3.2 Barcodes ... 211
4.3.3 RFID ... 212
4.4 Anwendungsgebiete der Schutzmaßnahmen ... 213

5 Betriebswirtschaftliche Schutzmaßnahmen in der Logistik ... 219
5.1 Personelle Aspekte der Logistik ... 220
5.2 Maßnahmen in der Lagerlogistik ... 223
5.3 Schutz der Transportsysteme ... 226
5.4 Maßnahmen in der Beschaffungslogistik ... 232
5.5 Maßnahmen in der Produktionslogistik ... 236
5.6 Maßnahmen in der Distributionslogistik ... 237
5.7 Maßnahmen im Service und in der Entsorgungslogistik ... 240

6 Managementempfehlungen ... 241

Literaturverzeichnis ... 244

1 Piraterie heute

Piraten, die einst mit Augenklappe und Schwertern auf hoher See das Eigentum anderer stahlen, gibt es auch heute noch. Allerdings ist ihre Ausrüstung nun um einiges moderner und ihre Angriffe genau geplant und vorbereitet. Moderne Piraten bedrohen Unternehmen auf der ganzen Welt: Sie versuchen, an das Know-how der Unternehmen zu gelangen, um Markenprodukte möglichst vor oder kurz nach Markteinführung imitieren zu können. Sie fälschen Originale aus jeder Branche und das überall auf der Welt. Die Produktpiraterie hat mittlerweile ein derartiges Ausmaß erreicht, dass mit ihrer Bekämpfung ein neuer Markt geschaffen wurde: Entwickler von Sicherheitstechnologien, Sicherheitsfirmen, Sicherheitsexperten und Anwälte sind dabei nur einige Dienstleister, die Unternehmen gegen ungewollte Know-how-Abflüsse unterstützen und damit verbundene Gefahren eindämmen.

Thematisch befasst sich der folgende Beitrag mit den gängigsten technischen und betriebswirtschaftlichen Maßnahmen, die Unternehmen zum Schutz vor Produktpiraten ergreifen können. In diesem Zusammenhang wird ein besonderes Augenmerk auf ihre Anwendbarkeit bei der Verwirklichung logistischer Aufgaben gelegt. Speziell technische Schutzmaßnahmen sollen dabei Produkte sowie deren Verpackungen als Originale kenntlich machen, um einen unbemerkten Austausch der Originalware gegen Imitate zu verhindern. Zusätzlich erörtert der Beitrag die präferierten betriebswirtschaftlichen Schutzmaßnahmen der Unternehmen, die entsprechend der logistischen Unternehmensbereiche differenziert wurden.

2 Gegenstandsbereich und Hemmnisse bei der Bekämpfung von Produktpiraterie

2.1 Begriff der Produktpiraterie

Für den Begriff „Produktpiraterie“ existiert keine gesetzliche Definition, sodass die Frage nach einer eindeutigen Erklärung auch in der Literatur sehr kontrovers beantwortet wird. Das *Institut der deutschen Wirtschaft* definiert den Begriff als „das verbotene Nachahmen und Vervielfältigen von Waren, für die rechtmäßige Hersteller Erfindungs-, Design- und Verfahrensrechte besitzen.“[1] Es handelt sich folglich um die be-

[1] Informationsdienst des Instituts der deutschen Wirtschaft Köln (2002).

wusste Verletzung bzw. illegale Verwendung von gewerblichen Schutzrechten sowie die Verletzung der durch das Gesetz gegen den unlauteren Wettbewerb geschützten Rechtspositionen durch Nachahmung oder Fälschung.[2] Eine Imitation ist dann illegal, wenn sie:

- „ein eingetragenes Warenzeichen oder einen Handelsnamen, und/oder
- ein nicht eingetragenes Eigentumsrecht bezüglich der Darbietung und Aufmachung („Trade Dress") oder der Benennung eines Erzeugnisses, und/oder
- ein Patent, Gebrauchsmuster, Geschmacksmuster und/oder
- ein Urheberrecht"[3] verletzt.

Der Tatbestand der kriminellen Schutzrechtsverletzung wird durch Plagiatoren gezielt, massenhaft und mit Gewinnabsicht begangen. Es geht nicht um gelegentlich auftauchende Schutzrechtsverletzungen, wie sie in der Wirtschaft unvermeidlich sind, sondern um zahllose Angriffe, die aus dem In- und Ausland vorgetragen werden.[4] Produktpiraterie umschreibt das Geschäft mit Nachahmerwaren, die mit dem bewussten Ziel hergestellt werden, der Originalware zum Verwechseln ähnlich zu sein. Sie zählt zu den am rasantesten zunehmenden Wirtschaftsverbrechen. Plagiatoren treten längst nicht mehr vereinzelt auf und bauen daheim die Originale nach; sie sind Teil eines organisierten Netzes. Mittlerweile gehört Produktpiraterie zur organisierten Kriminalität – eine Einordnung, die ebenfalls die hohe Profitabilität einer gewerbsmäßigen Verletzung geistigen Eigentums bestätigt.[5]

Marken- und Produktpiraterie wird auf gesetzlicher Seite nicht eindeutig voneinander abgegrenzt. In der Vergangenheit wurde überwiegend von Markenpiraterie gesprochen, da man den Vorgang der rechtswidrigen Übernahme des Markenzeichens als Hauptproblem ansah. Die steigende Zahl der Produktnachahmungen, die nicht mit einer Fälschung des Markenzeichens verbunden sind, machte allerdings eine Ausweitung des Begriffs nötig. Stattdessen wird heute das Problemfeld der Markenpiraterie, wie auch die übrigen Verletzungen gewerblicher Schutz- und Urheberrechte durch Nachahmung, mit dem Oberbegriff Produktpiraterie abgedeckt.[6]

---

2 Vgl. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (2007).
3 Olgalime (2001).
4 Vgl. Beier et al. (1991).
5 Vgl. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2007).
6 Vgl. Lutz/Koppelmann (1997).

2.2 Kulturelle Unterschiede als Ursache von Piraterieverhalten

Obwohl es zahlreiche Bestrebungen des Staates und der Unternehmen zur Verhinderung von Produktpiraterie gibt, kann das Problem nicht vollständig eingedämmt werden. Die Gründe dafür können sehr unterschiedlich sein. Zum einen sind einige Ursachen, die zur Zunahme von Produktpiraterie führen, zwar durch Schutzmaßnahmen zugunsten des Unternehmens beeinflussbar, diese Handlungen können aber mit anderen Unternehmenszielen in Konkurrenz stehen. Die Verminderung des Interesses von Produktpiraten am Unternehmen und die gleichzeitige Erzielung einer möglichst hohen Gewinnspanne sind beispielsweise zwei entgegenwirkende Zielrichtungen.

Tabelle 1: Aufteilung der Fälle nach Herkunftsländern in Prozent der Aufgriffe
Quelle: Bundesministerium der Finanzen (2006), S. 35.

Aufgriffe nach Herkunftsländern (in Prozent)

	2003	2004	2005	2006
China	12,86	23,58	35,80	32,85
Thailand	24,85	23,45	10,20	8,61
Türkei	9,04	10,22	8,73	8,71
USA	3,81	8,44	11,23	12,66
Hongkong	5,87	7,68	11,45	11,12
Tschechien	11,44	3,57	0,97	0,80
Polen	10,03	3,56	0,59	0,56
Indien		1,79		1,36
Malaysia	3,64	1,31		0,58
Japan			0,45	0,76
V.A.E.			1,27	1,63
Vietnam				2,72
Schweiz				1,19
Sonstiges*	18,46	16,40	19,31	16,47

*Afghanistan, Kosovo, Kanada, Südkorea, Brasilien, Singapur, Taiwan, Bulgarien, Russland, Ukraine, Iran, Philippinen, Pakistan, Usbekistan, Kroatien, Argentinien, Spanien, Israel, Australien, Slowakei

Andere Ursachen, die ebenfalls die Durchführung von Produktpiraterie fördern, können wiederum nicht durch unternehmensinterne Sicherungsmaßnahmen beeinflusst werden. Zu ihnen zählen u.a. die Globalisierung und die unterschiedliche kulturelle Auffassung von geistigem Eigentum in einigen Ländern. Dies ist einer der Gründe, warum es zum Beispiel im asiatischen Raum so viele Imitationen gibt. Ihre Kultur befürwortet das Kopieren von Produkten, es wird als wetteiferndes Nachahmen gesehen. Sie richten ihr Augenmerk entsprechend der Kaizen-Philosophie auf die Verbesserung einer Idee oder Innovation und nicht auf die Entwicklung. Zudem fühlen sich viele

Unternehmen in Schwellenländern oder in der Dritten Welt im Recht, unerschwingliche Medikamente oder Technologien nachzuahmen. Auch hier wird geistiges Eigentum als gemeinsamer Besitz betrachtet, wodurch die dort geltenden Gesetze keinen vertretbaren Schutz vor Produktpiraterie bieten.[7] In diesem Zusammenhang zeigt die vorangegangene Tabelle 1 die häufigsten Herkunftsländer von Pirateriewaren in den Jahren von 2003 bis 2006.

Selten ist jedoch eine Ursache allein der Grund für einen Angriff auf das Unternehmen. Vielmehr fördern viele verschiedene Ursachen die Zunahme von Produktpiraterie. Für die richtige Auswahl der Maßnahmen ist daher eine Ursachenanalyse unumgänglich. Die folgende Grafik zeigt dazu einen Überblick der bedeutungsvollsten Ursachen für die Zunahme von Produktpiraterie:

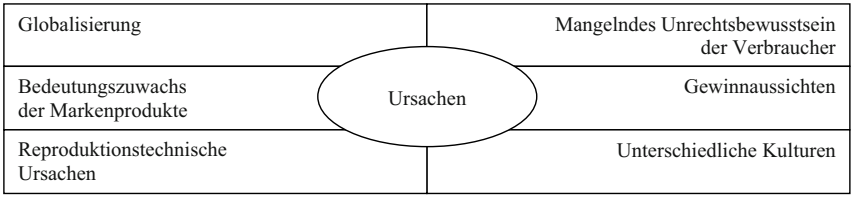


Abbildung 1: Ursachen für die Zunahme von Produktpiraterie
Quelle: eigene Darstellung, in Anlehnung an: Podhorsky (2006).

2.3 Hemmnisse bei der Bekämpfung von Produktpiraterie

Der *Deutsche Industrie- und Handelskammertag* schätzt den finanziellen Schaden, der jährlich für die deutsche Volkswirtschaft durch Produktpiraterie entsteht, auf 30 Mrd. EUR.[8] „Wenn bei hohen Investitionen in Innovation das Risiko besteht, dass wegen Produktpiraterie keine ausreichende Rendite erzielt werden kann, führt das zu weniger Investitionen und damit letztlich zu gebremstem technischen Fortschritt, zu Arbeitsplatzabbau, Wettbewerbsverzerrungen und einer Destabilisierung der Märkte."[9]

Die Unternehmen kennen durchaus die Gefahren, die Produktpiraten für ihre eigene Existenz und den Markt verursachen. Dennoch verschließt sich immer noch ein Großteil der Firmen vor der Realisierung möglicher Schutzmaßnahmen, da sie nicht der Meinung sind, dass auch sie von Produktpiraterie betroffen sein könnten. Vor allem

[7] Vgl. Müller/Kornmeier (2000).
[8] Vgl. Lang/Schäfer (2007).
[9] Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (2007).

kleine und mittelständische Unternehmen glauben, dieses Problem beträfe nur Luxusmarkenhersteller. Doch keine Branche und kein noch so unscheinbares Produkt ist vor Fälschern sicher. Selbst Güter in unteren Preiskategorien, wie Steckdosen, Haushaltsgeräte und Koch-Utensilien, werden vielfach gefälscht.[10] Abbildung 2 verdeutlicht, welche Sortimentsbreite die Plagiatoren mittlerweile erreicht haben.

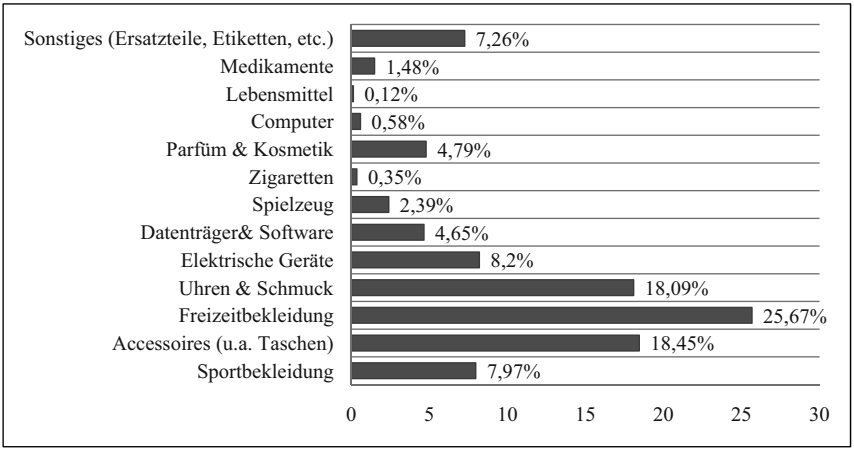


Abbildung 2: Aufteilung der Piratenfälle nach Warenkategorie in Prozent
Quelle: eigene Darstellung, in Anlehnung an: Bundesministerium der Finanzen (2006), S. 35.

Neben Risiken, die das eigene Unternehmen betreffen, wird aber oftmals auch die Gefahr ignoriert, dass Fälschungen auch den Betrieb von Geschäfts- und Handelspartnern beeinträchtigen können. Die meisten Hersteller sind überzeugt, sie würden nur mit vertrauenswürdigen Händlern kooperieren.[11] Doch schwarze Schafe, die hinter dem Rücken ihrer Partner Plagiate veräußern, gibt es allerorts. Unternehmen müssen daher sensibel auf Änderungen im Geschäftsbetrieb reagieren. Weichen Kennzahlen signifikant von den Normalwerten ab, sollte eine genauere Prüfung erfolgen. Indizien für Fälschungen können zum Beispiel ein plötzlicher Rückgang von Marktanteilen, insbesondere im Exportgeschäft, vermehrte Kundenbeschwerden bezüglich der Erzeugnisse und eine erhöhte Aktivität neuer Marktteilnehmer auf Fachmessen sein. Entsprechende Informationen liefern externe Partner des Herstellers wie Branchenverbände, Mitbe-

[10] Vgl. Olgalime (2001).
[11] ebd.

werber und andere Partner in der Handelskette. Vor allem Vertragshändler erkennen oft als Erste Anzeichen von Produktpiraterie in ihrem Gebiet; andere Informationsquellen sind z.B. Rundfunk, Zeitungen, Fachzeitschriften und das Internet.[12]

Aber auch wenn die Notwendigkeit eines expliziten Schutzes gegen die bestehende Bedrohung, die von Plagiatoren ausgeht, von den Unternehmen akzeptiert wird, empfinden viele die Auseinandersetzung mit den angebotenen Schutzmöglichkeiten als zu zeitintensiv. Besonders kleinen und mittelständischen Firmen fällt es schwer, alle rechtlichen Maßnahmen auszuschöpfen, da sie oftmals ein gewisses juristisches Verständnis voraussetzen. Größere Unternehmen beschäftigen dafür zum Teil hauseigene Anwälte. Kleinere Unternehmen haben diese Möglichkeit nicht und scheuen sich aus Kostengründen davor, Anwälte zu beauftragen.

Zudem ist der Einsatz technologischer und betriebswirtschaftlicher Schutzmaßnahmen für viele Unternehmen mit Hindernissen verbunden. Die Einführung von Technologien und neuen Strategien bedeutet immer Kosten und Aufwand. Viele Unternehmen bezweifeln jedoch, dass Sicherheitsrisiken durch entsprechende Sicherheitsmaßnahmen überhaupt beherrschbar sind oder signifikant reduziert werden können. Sie halten den Einsatz kosten- und arbeitsintensiver Sicherheitsmaßnahmen nicht für lohnenswert. Dabei vernachlässigen viele Hersteller, dass diese Investitionen zwar am Anfang hoch erscheinen, aber langfristig Marktanteile sichern. Sie werden als ökonomische Belastungen empfunden und nicht als Existenzsicherung des Unternehmens.[13]

3 Logistik als Angriffspunkt für Produktpiraten

3.1 Bedeutung des Funktionalbereichs Logistik

Bei der Bekämpfung der Produktpiraterie können sich Unternehmen auf die für die jeweiligen Waren angemeldeten Schutzrechte oder auch auf das Gesetz gegen unlauteren Wettbewerb stützen.[14] Im Detail zählen hierzu:

- das Urheberrecht (UrhG, UrWahrnG),
- der gewerbliche Rechtsschutz (u.a. PatG, GebrMG, GeschmMG, MarkenG),

[12] Vgl. Olgalime (2001).
[13] Vgl. Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (2005).
[14] Vgl. Harke (2000)

- das Wettbewerbsrecht (UWG, kartellrechtliche Vorschriften),
- das Steuerrecht (AO), sowie
- das Zollrecht.

Um Produktpiraterie wirkungsvoll abzuwehren, reichen diese rechtlichen Maßnahmen allerdings nicht aus. Analog dazu verfolgen daher viele Hersteller interne Unternehmens- und Vertriebsstrategien. Die Logistik als zentrale Querschnittsfunktion in der Wertschöpfungs- und Vertriebskette spielt in diesem Zusammenhang eine besonders wichtige Rolle[15], da Innovationen alle logistischen Bereiche von der F&E bis zum Verkauf der Waren durchlaufen müssen.

Logistik nach dem heutigen Verständnis beschreibt die integrierte Planung, Gestaltung, Abwicklung und Kontrolle des gesamten Material- und Informationsflusses vom Lieferanten in das eigene Unternehmen, innerhalb dieses Unternehmens, vom Unternehmen zum Kunden und im Sinne der Entsorgung auf dem Versorgungsweg zurück.[16] Sie unterteilt sich dabei in die Beschaffungs-, Produktions-, Distributions- und Entsorgungslogistik (Vgl. Abbildung 3).

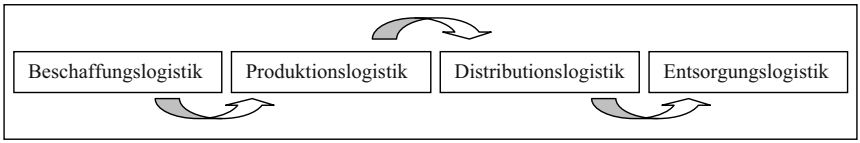


Abbildung 3: Teilgebiete der Logistik
Quelle: eigene Darstellung.

In allen Bereichen können Maßnahmen getroffen werden, um die Aufgaben der Logistik – sprich die Bereitstellung:

- der richtigen *Menge*
- der richtigen *Objekte* (u.a. Güter, Personal, Informationen)
- am richtigen *Ort* im System
- zum richtigen *Zeitpunkt*
- in der richtigen *Qualität*
- zu den richtigen *Kosten*[17] – systematisch zu erfüllen.

[15] Vgl. Günthner/Meißner (2006).
[16] Vgl. Blom/Harlander (2000).
[17] Man spricht in diesem Zusammenhang von den „6 Richtigen“.

Für die Produktion benötigte Betriebsstoffe und Waren werden von beauftragten Lieferanten besorgt. Aus diesem Grund ist es wichtig, dass die Qualitätsansprüche der Lieferanten mit denen des eigenen Unternehmens konform sind. Schwachpunkte in der Logistikkette können von Produktpiraten ausgenutzt werden, sodass bei Defiziten gefälschte Zulieferteile eingeschleust und wichtige Aufgaben der Logistik – wie die Güterbereitstellung in der richtigen Qualität und zur den richtigen Kosten – nicht erreicht werden können. Soll das Endprodukt also die Erwartungen des Kunden erfüllen, dürfen in der gesamten Lieferantenkette keine Schwachstellen auftreten, welche Qualitätseinbußen nach sich ziehen. Der Hersteller muss deshalb ein Auswahlverfahren entwickeln, um seine Lieferanten rational bewerten zu können.[18]

Auch bei langjährigen Kooperationspartnern sollte auf Kontrollen und Stichproben, durch die Beschädigungen und Fälschungen ausfindig gemacht werden können, nicht verzichtet werden. Mitarbeiter, die mit derartigen Untersuchungen beauftragt werden, müssen sich mit dem Unternehmen identifizieren und ein geschultes Auge für Fälschungen haben, sodass sie sensibel auf Abweichungen reagieren können.[19]

Dem gegenüber ist es Aufgabe der Unternehmensführung, das *eigene* Personal durch personalpolitische Maßnahmen zu beobachten, zu begleiten und zu fördern. Während sich Computer durch Zugriffkontrollen und Authentifizierungen vor Unbefugten schützen lassen, handeln Menschen oft irrational und emotional. Sie lassen sich folglich schwerer kontrollieren. Daher besteht immer die Gefahr, dass Geheimnisse durch die eigenen Mitarbeiter nach außen getragen werden. Eine möglichst lange Mitarbeiterbindung sowie gelebte Werthaltungen minimieren dieses Risiko jedoch.[20]

Neben Logistikprozessen, die speziell die Belieferung des eigenen Unternehmens betreffen, müssen desweiteren alle Tätigkeiten, die in Zusammenhang mit der Auslieferung der firmeneigenen Produkte stehen, bei der Erarbeitung eines Logistikkonzepts berücksichtigt werden. Die Auswahl der geeigneten Vertriebskanäle und Händler darf nicht routinemäßig erfolgen, geeignete Transportmethoden müssen geplant und seriöse Händler gefunden werden.[21]

[18] Vgl. Fuchs (2006).
[19] ebd.
[20] Vgl. Fuchs (2006).
[21] ebd.

3.2 Mögliche Schwachstellen und Problemlösungsansätze in logistischen Prozessen

Als Bindeglied zwischen der Beschaffung, Produktion und dem Vertrieb[22] eines Unternehmens weisen logistische Prozesse eine Vielzahl von Schnitt- und Schwachstellen auf, die den Produktpiraten einen gezielten Eingriff in die Unternehmensorganisation erleichtern. Schnittstellen sind dabei Trenn- bzw. Verbindungsstellen von arbeitsteiligen Prozessen sowie Übergabestellen in arbeitsteiligen Systemen. In ihnen kommt der Warenfluss zum Stillstand, wenn zwischen Unternehmen, Unternehmensbereichen und Subsystemen Verantwortlichkeiten zu Ende gehen und neue beginnen.[23] Die Abbildung 4 zeigt dazu eine Logistikkette vom Lieferanten, über den Kunden, bis zur Entsorgung sowie deren Schnitt- bzw. mögliche Schwachstellen.

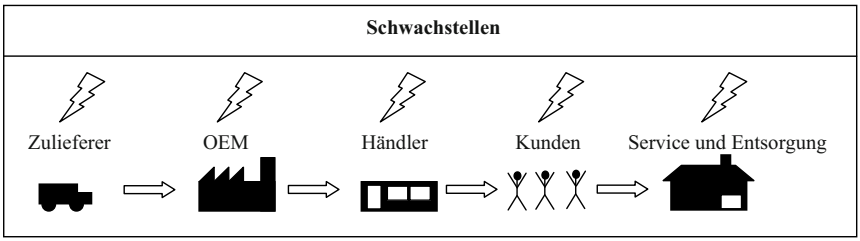


Abbildung 4: Schwachstellen in der Logistikkette
Quelle: eigene Darstellung, in Anlehnung an: Günthner/Meißner (2006).

Will man einen Know-how-Abfluss verhindern, müssen zunächst die Angriffsmöglichkeiten von Produktpiraten analysieren werden: Erste Sicherheitsdefizite können bereits bei der Beschaffung auftreten. Durch den immer stärker werdenden Konkurrenzkampf werden viele Unternehmen gezwungen, einzelne Fertigungsstufen an andere Unternehmen oder Tochtergesellschaften abzugeben, um sich auf diese Weise Wettbewerbsvorteile zu verschaffen. Das Outsourcing bietet den Herstellerunternehmen die Möglichkeit, sich auf ihr Kerngeschäft und auf ihre eigenen Stärken zu konzentrieren. Sie haben durch die Einsparung von Maschinen, Facharbeitern und Produktionshallen eine geringere Kapitalbindung und können bei Zuverlässigkeit der Partnerunternehmen Aufträge zeitnaher realisieren.[24] Diese Vorteile sind jedoch immer auch

[22] Vgl. Thome (2007).
[23] Ein Beispiel hierfür wäre der Eigentümerwechsel von Einzelteilen oder Waren.
[24] Vgl. Gienke/Kämpfer (2005).

mit Nachteilen verbunden, die in den meisten Fällen direkten Einfluss auf die Unternehmenssicherheit haben: Indem das Herstellerunternehmen Verantwortungen abgibt, werden Know-how-Vorsprünge aufgegeben und Partnerunternehmen in Firmengeheimnisse eingeweiht. Bei Auslagerung der Produktion besteht beispielsweise die Gefahr, dass der Wertschöpfungspartner mehr produziert oder Plagiate herstellt und diese über zwielichtige Wege zugunsten des Vertreibers abgesetzt werden.[25] Die Entwicklungs- und Produktionskosten trägt weiterhin der Hersteller.

Um bei Störungen in der Versorgungskette die Produktion nicht zu gefährden, werden zudem Zulieferteile von Partnern häufig zwischengelagert. Lagerhallen bilden ebenfalls ein Sicherheitsrisiko, da sie schwer gegen unbefugtes Eintreten geschützt werden können. Durch den regen Ein- und Ausgangsverkehr kann es besonders in stressigen Situationen vorkommen, dass Fahrer unbemerkt mehr Ware auf ihre LKWs laden als eigentlich vorgesehen, um sich auf diese Weise selbst zu bereichern.[26]

In der Distributionslogistik muss ein Unternehmen außerdem damit rechnen, dass Händler wissentlich oder unwissentlich Produktplagiate an andere Händler oder Kunden verkaufen. Kommt es bei Nutzung der gefälschten Produkte zu Schäden, zieht dies gegebenenfalls Gewährleistungs- und Produkthaftungsansprüche mit sich. Reparaturleistungen an minderwertigen Plagiaten, die gar nicht oder zumindest nicht sofort erkannt werden, verschlingen folglich unnötige Kosten. Zudem besteht auch immer die Gefahr, dass Kundendienste am Originalprodukt Service mit gefälschten Ersatzteilen leisten, da Plagiatoren neben kompletten Produkten oftmals auch Ersatzteile für den Handel fertigen.[27] Die Lieferung und der Einbau gefälschter Ersatzteile beim Kunden bergen somit ebenfalls enorme Gefahren für Kunden und Hersteller.

Nicht zu vernachlässigen sind überdies die Aufwendungen, die bei der Vernichtung und Entsorgung von Nachahmerprodukten entstehen. Den Großteil der Entsorgung für beschlagnahmte Ware übernimmt der Zoll, aber auch den Herstellerunternehmen und Vertriebspartnern werden immer wieder Produkte zugeschickt, die einer Prüfung bedürfen. Da sie ein besonderes Interesse an der Vernichtung der Fälschungen haben, werden von den Herstellern häufig Aufrufe an Verbraucher gestartet, in denen um die Zusendung möglicher Plagiate gebeten wird.[28] Zusätzlich muss in der Entsorgungslo-

[25] Vgl. Fuchs (2006).
[26] ebd.
[27] Vgl. Fuchs (2006).
[28] ebd.

gistik die Vernichtung von Dokumenten, Produktentwürfen und Ausschüssen so gestaltet werden, dass diese nicht in die Hände von Imitatoren fallen können.

Um die beschriebenen Problemfelder der Logistik zu schließen, sind effektive Schutzmaßnahmen notwendig, die fest in die Wertschöpfungskette integriert werden können. Sinnvoll ist dabei der Einsatz präventiver Maßnahmen, die sich möglichst schwer umgehen lassen.[29] Einen uneingeschränkten Schutz gegen Produktpiraterie gibt es jedoch nicht. Zur Eindämmung der Produktpiraterie kann der Originalhersteller juristische, technische und betriebswirtschaftliche Schutzmaßnahmen nutzen. Unternehmen mit zahlreichen Schnittstellen haben es aber selbst bei ausreichender Budgetierung schwer, Produkte und Know-how vor organisierten Angriffen zu schützen.

Juristische Maßnahmen bilden durch Gesetze und Schutzrechtsanmeldungen die Grundlage eines Schutzkonzeptes, jedoch entfalten sie ihre Wirkung meist erst, nachdem der Schaden bereits eingetreten ist. Sie dienen demzufolge der Nachsorge, aber auch der Abschreckung, da eine Verletzung der Gesetze mit Strafen verbunden ist. Für einen nachhaltigen Schütz müssen rechtliche Maßnahmen durch weitere präventive Mittel unterstützt werden.[30]

Technische und betriebswirtschaftliche Maßnahmen dienen dem Präventivschutz, sie sollen eine Nachahmung von vorneherein verhindern. Sicherheitsüberlegungen und Schutzmaßnahmen sollten von diesem Grundsatz der Prävention geprägt sein. Sie sollten möglichst frühzeitig in Entscheidungsprozessen und Verfahren Berücksichtigung finden. Alle Ideen und Produktentwicklungen, auch wenn sie erst in der Zukunft sicherheitsrelevant werden, müssen in die Überlegungen einbezogen werden. Präventive Maßnahmen sind im Bereich der Logistik gut anwendbar. Diese Maßnahmen können von den Unternehmen frei gewählt und gestaltet werden, dabei gibt es keine Vorgaben oder Einschränkungen des Staates. Jedes Unternehmen kann selbst entscheiden, welchen Aufwand es zur Bekämpfung der Produktpiraterie aufbringen will.

[29] Vgl. Günthner/Meißner (2006).
[30] Vgl. Wildemann et al. (2007).

4 Technische Schutzmaßnahmen in der Logistik

Technische Schutzmaßnahmen können nach ihrer Anbringung oder Integration für die Erfüllung von Logistikaufgaben genutzt werden. So ermöglichen sie es beispielsweise Mitarbeitern und Logistikdienstleistern, sich in allen Teilgebieten der Logistik von der Richtigkeit der Ware zu überzeugen. Die charakteristischen Besonderheiten einzelner technischer Schutzmaßnahmen werden dabei in zwei Gruppen gegliedert: in offene und/oder verborgene Merkmale. Offene Merkmale befinden sich auf sichtbaren Technologien, die von allen Nutzern und Verbrauchern überprüft werden können, während so genannte verdeckte Merkmale nur mit speziellen Lesegeräten erkennbar sind.[31] Diese Lesegeräte sind vorrangig für die Hersteller, den Handel und die Behörden, wie beispielsweise den Zoll, bestimmt. Eine gute Technologie sollte folgende Merkmale besitzen:

- Sie sollte exklusiv sein,
- sie muss mit dem Erzeugnis fest verbunden sein,
- sie muss einfach zu kontrollieren und zu erkennen sein,
- sie darf nicht zu kopieren, entfernen oder ändern sein,
- sie muss eine vernünftige Kosten-Nutzen-Relation aufweisen.[32]

Im Folgenden werden die wesentlichsten technischen Möglichkeiten, die zur Bekämpfung von Produktpiraterie dienen, vorgestellt:

4.1 Technologien gegen Produkt- und Verpackungsfälschungen

Um Güter vor Nachahmungen zu schützen, besteht die Möglichkeit, Technologien direkt auf das Produkt oder die Verpackung aufzutragen oder einzumischen. Dabei muss es sich um eine Technologie handeln, die das Produkt bzw. die Verpackung mit Eigenschaften versieht, die schwer zu kopieren sind. Es genügt nicht, einfach das Produkt und die Verpackung nachzuahmen. Imitatoren müssen gezwungen sein, auch die Sicherheitstechnologien zu fälschen, um das Imitat verkaufen zu können. Da dies oftmals mit viel Aufwand verbunden ist, wird der Nachbau des Produkts von Plagiatoren

[31] Vgl. Fuchs (2006).
[32] Vgl. Orgalime (2001).

im besten Fall für unwirtschaftlich gehalten.[33] Ein Beispiel für eine derartige Technologie ist das Hologramm.

4.1.1 Hologramme

Ein Hologramm ist eine Struktur, die aus winzigen Linien besteht, die durch fotographische Projektion produziert werden. Durch Beleuchtung des Hologramms erscheint ein dreidimensionales Bild.[34] Im Unterschied zu 3D-Graphiken, in denen das Bild in eine zweidimensionale Oberfläche projiziert und die Tiefe lediglich illusioniert wird, sind Hologramme tatsächlich dreidimensionale Bilder, die weder spezieller Lesegeräte noch spezieller Blickwinkel bedürfen.[35]

Ein Hologramm entsteht aus der Überlagerung kohärenter Lichtstrahlen, die von einem Laser erzeugt, geteilt und über das Objekt bzw. direkt auf eine Fotoplatte projiziert werden.[36] Hologramme besitzen ein prägnantes Aussehen und sind von Fälschungen einfach zu unterscheiden, da diese meist nicht die Qualität des Originals erreichen. Allerdings ist der direkte Vergleich nur möglich, wenn Original und Fälschung parallel angeboten werden.

Hologramme, die zum Schutz vor Produktpiraterie verwendet werden, sind meist so genannte *Prägehologramme*. Sie besitzen einen komplizierten optischen und technischen Aufbau, sodass die Wiedergabe dieses Musters schwierig ist und sie sich mit keinem bekannten Kopierverfahren vervielfältigen lassen. Um Prägehologramme fertigen zu können, bleibt Fälschern folglich nur die Wiederholung des gesamten Herstellungsprozesses. Hierzu benötigen sie die richtige Ausrüstung und das spezielle Know-how der Techniker.[37] Dies ist jedoch mit hohen Kosten verbunden, sodass sich die Beschaffung der entsprechenden Ausstattung für Produktpiraten nicht lohnt.

Bei der tatsächlichen Herstellung von Hologrammen erreichen spezielle Maschinen eine extreme Zeitersparnis, wobei auch die eingesetzten Materialien relativ günstig sind.[38] Aus diesem Grund ist der Preis eines massenhaft hergestellten Hologramms verhältnismäßig gering. Dennoch sind Hologramme nicht für den Einsatz an preisgünstigen Alltagsgütern geeignet, da selbst für die Herstellung eines Standardholo-

[33] Vgl. Fuchs (2006).
[34] Vgl. Holografia Polska agencja monitorowania produktu (2006).
[35] Vgl. The tech-faq (2007).
[36] Vgl. LINK Interactive Systems KEG (2003).
[37] Vgl. topac MultimediaPrint GmbH (2007).
[38] Vgl. Holografia Polska agencja monitorowania produktu (2006).

gramms Kosten von 8 bis 24 EUR-Cent anfallen und ihr Einsatz wirtschaftlich nicht sinnvoll ist.[39] Trotzdem ist die Verwendung von Hologrammen weit verbreitet, da sie in vielen Variationen und Kombinationen mit anderen Technologien, wie Nummerierungen oder Sicherheitsfolien, genutzt werden können. Aufgrund ihrer übermäßigen Verfügbarkeit bieten Hologramme heutzutage jedoch nur ein eingeschränktes Sicherheitsniveau.

4.1.2 OVDs

Eine weitere Möglichkeit zur eindeutigen Identifikation von Original und Fälschung bilden OVDs. Die Abkürzung OVD steht für optisch variable Grafiksysteme (englisch: Optically Variable Devices[40]) und bezeichnet eine flächenhafte Struktur, die bei Betrachtung aus unterschiedlichen Blickwinkeln unterschiedliche Bildinhalte wiedergibt.

Die einfachsten OVDs sind die diffraktiven Muster. Dabei handelt es sich um Motive aus flächenhaften Beugungsgittern mit einigen 100 bis über 1000 parallelen Linien pro Millimeter, die in unterschiedlichen Farben erscheinen. Der Farbwechsel wird durch Lichteinfall und Betrachtungswinkel erzeugt, weshalb sie auch als Kippfarben bezeichnet werden.[41] Einfache OVDs werden häufig auf Etiketten und Folien erstellt.

Neben den einfachen OVDs gibt es auch so genannte Kinegramme, deren Linien der Beugungsgitter genau definierte Profilformen besitzen. Hier werden durch die Änderung der Betrachtungsrichtung nicht nur Farbänderungen erzeugt, sondern auch sprunghafte Änderungen des Bildinhalts, die so genannten Flippeffekte.

Im Gegensatz zum Hologramm entsteht bei OVDs kein 3D-Effekt. Diffraktive Muster und Kinegramme sind meist silbrig glänzend, besitzen einen zweidimensionalen Bewegungsablauf und vermitteln ein flächenhaftes Bild ohne Tiefenwirkung. Speziell Markenprodukte, die vor Fälschern geschützt werden sollen, tragen solche OVDs.

Ebenso wie bei Hologrammen können auch OVDs nicht mit einfachen Kopiervorgängen nachgeahmt werden, da die winkelabhängigen Beugungseffekte bei einem Kopiervorgang verloren gehen. Die Fälschungssicherheit der OVDs beruht darauf, dass für deren Fertigung ein hohes Spezialwissen der Hersteller und eine umfangreiche Apparateausstattung erforderlich sind.

---

[39] Vgl. Fuchs (2006).
[40] siehe dazu auch Abschnitt *4.2.1.4 Technische Maßnahmen zur Produktkennzeichnung* von Selina Rehn.
[41] Vgl. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin.

4.1.3 Sicherheitstinten

In Sicherheitstinten werden Flüssigkristalle, wasserlösliche Harze und chemische Zusätze verwendet, die das Fließverhalten und andere Eigenschaften der Tinte verbessern bzw. verstärken.[42] Sie werden zur Markierung von Produkten, Verpackungen und Dokumenten eingesetzt und besitzen im Gegensatz zu den handelsüblichen Tinten besondere Eigenschaften, die je nach Art der Sicherheitstinte variieren.

Ein Leistungsparameter ist beispielsweise die Haftfestigkeit auf schwer bedruckbarem Gummi, Kunststofffolien und Kunststoffen wie Nylon, PVC, PE und PP.[43] Um einen erstklassigen Kontrast auf hellen oder dunklen Materialien zu erzielen, gibt es Sicherheitstinte nicht nur in Schwarz, sondern auch in zahlreichen anderen Farben wie Rot oder Weiß. Alle Farben müssen über einen langen Zeitraum farb- und lichtbeständig sein.

Ein weiterer Parameter ist die Haltbarkeit bei starker Wärmeeinwirkung und Einflüssen durch Flüssigkeiten wie Wasser, Alkohol oder Alkalilösungen. Besonders für Rohre und Kabel ist eine gute Wärmebeständigkeit wichtig. Außerdem sollten die meisten Farben Manipulationen mit Flüssigkeiten standhalten. Eine Ausnahme bildet hier die temporäre Codierung von Mehrwegfalschen in der Getränkeindustrie und von Behältern bzw. Reagenzgläsern für den Labor- und medizinischen Bereich. Dort kann der trockene Code durch Wasser- oder Säurekontakt entfernen werden.[44]

Für den Aufdruck auf Lebensmitteln wurden spezielle Lebensmitteltinten entwickelt, die ausschließlich essbare Rohstoffe enthalten. Diese Tinten sind eine sichere Methode zur Markierung essbarer Produkte und Verpackungen, die mit Lebensmitteln in Berührung kommen.[45]

Neben den sichtbaren Tinten existieren aber auch Sicherheitstinten, die bei normalem Licht nahezu unsichtbar sind, jedoch unter UV-Licht fluoreszieren. Sie gibt es in verschiedenen Farben, die gebräuchlichsten sind dabei Blau/Violett und Rot. Speziell für die diskrete Kennzeichnung von Alkohol-, Tabak-, Pharma-, Software- und Musikprodukten wurde diese Tinte entwickelt, sodass sie auf einer Vielzahl von Untergründen wie Papier, Glas oder Metall hält. Zudem haben einige Anbieter UV-Tinten entwi-

[42] Vgl. Fuchs (2006).
[43] Vgl. Linx Printing Technologies Ltd. (2005a).
[44] Vgl. Linx Printing Technologies Ltd. (2005b).
[45] Vgl. Linx Printing Technologies Ltd. (2005c).

ckelt, die nicht toxisch oder schädlich für die Umwelt sind und sich folglich sogar für den Einsatz an Lebensmitteln und Tabakwaren eignen.

4.1.4 Sicherheitsdrucke

Die Herstellung eines Sicherheitsdrucks als eine weitere technische Schutzmaßnahme im Bereich der Logistik stellt hohe Ansprüche an die Hersteller und deren Technik. Nur Spezialisten sind in der Lage, den Sicherheitsdruck mit der gewünschten Qualität und Präzision zu fertigen.[46] Sicherheitsdrucke gibt es in vielen Formen, sie werden mit speziellen Techniken auf Etiketten, Verpackungen und auf die Produkte selbst gedruckt. Je nach Sicherheitsdruck unterscheiden sich das Aussehen und die Eigenschaften der einzelnen Formen:

a) Sicherheitsfäden

Der Sicherheitsfaden wird nicht, wie in der Vergangenheit üblich, auf das Papier gedruckt, er wird in vielen Fällen in das Papier integriert. Der Sicherheitsfaden wird nur sichtbar, wenn er wie beim Wasserzeichen gegen eine Lichtquelle gehalten wird. Er erscheint auf beiden Seiten als dunkler Streifen.[47] Aufgedruckte Streifen sind für den Betrachter leichter sichtbar, aber sie besitzen einen geringeren Sicherheitsstatus. Die eingebetteten und aufgedruckten, größtenteils metallischen Sicherheitsfäden können Farbwechseleffekte und Texte in sehr kleiner Schrift enthalten.

b) Guilloche

Die Guilloche ist ein ornamentales Muster, das aus mehreren ineinander verwickelten und überlappenden Linienzügen besteht. Von weitem erscheint die Guilloche als ein Motiv mit Tiefenwirkung, erzielt durch die mehrfarbigen, verschlungenen Streifen, die bei näherer Betrachtung sichtbar werden. Die einzelnen Linien bilden dabei schnurartige, oft symmetrische, geschlossene Ellipsen oder auch Kreisbahnen.[48]

c) Irisdrucke

Der Irisdruck ist keine eigene Drucktechnologie, er wird vielmehr beim Hoch-, Flach- und Siebdruck angewendet. Dabei werden mehrere lasierende Farben mit ineinander

[46] Vgl. Fotorotar AG (2007),
[47] Vgl. Landeskriminalamt Baden-Württemberg (2006).
[48] Vgl. Südwestrundfunk (2006).

verlaufenden Farbrändern in einem Druckgang gedruckt. Beispielsweise werden die drei Grundfarben in den Farbkasten der Offsetmaschine gegeben: in die linke Hälfte ein zartes Gelb, in der Mitte ein helles Rot und in die rechte Hälfte ein helles Blaugrün. Beim Irisdruckverfahren entsteht dann ein spezieller Effekt. Die seitliche Verreibung der Farben durch leicht hin- und herbewegliche Farbwalzen lässt an den Grenzlinien die Farben übereinander drucken. Es ergibt sich bei der richtigen Farbwahl durch das langsame Vermischen der Grundfarben ein Muster, das alle Farben ineinander verlaufend wiedergibt.[49] Der Irisdruck wird häufig mit dem Guillochendruck kombiniert.

d) Wasserzeichen

Wasserzeichen sind durchscheinende Hintergrundbilder auf Papier, es sind keine Prägungen und keine Drucke. Im Unterschied zu chemischen Wasserzeichen, die mit Hilfe von speziellen Flüssigkeiten in das fertige Papier wie ein Druck eingebracht werden, wird das echte Wasserzeichen mit einem komplexen Verfahren in das Papier integriert.

Die Herstellung eines echten Wasserzeichen-Papiers gestaltet sich als sehr aufwendig. Sie kann nur in einer Papierfabrik auf einer Papiermaschine mit Hilfe eines Egoutteurs – einer Siebwalze, auf der das Wasserzeichen aufgebracht ist – erfolgen. Das Muster der Walze hinterlässt einen Abdruck im Papier.[50] Die Faserschichten sind an einigen Stellen dünner und lassen dort das Licht stärker durch; an anderen Stellen ist der Stoff angereichert, wodurch weniger Licht durchströmen kann. Die unterschiedlichen Lichtdurchlässigkeiten erzeugen das so genannte Wasserzeichen; werden Vertiefungen und Erhöhungen geschickt verknüpft, ist selbst eine Imitation von Halbtönen möglich.

Der Vorteil von echten Wasserzeichen besteht in ihrer langen Haltbarkeit: Während unechte Wasserzeichen nach einiger Zeit verblassen oder gar gänzlich verschwinden, halten echte Wasserzeichen solange wie das Papier selbst.[51]

e) Stanz- oder Prägedrucke

Beim Stanz- oder Prägedruck wird ein Muster oder in vielen Fällen ein Logo auf eine Verpackung, ein Papier oder ein Produkt erzeugt. Es bezeichnet folglich das Umfor-

[49] Vgl. Hubert (1998).
[50] Vgl. Stiassny Papier Grosshandlung GmbH (2007a).
[51] ebd.

men von Werkstoffen ohne wesentliche Veränderung der Dicke und geschieht durch die Stempelwirkung der Presse. Dabei muss keine Farbe eingesetzt werden, das Muster wird durch die Einprägungen sichtbar und lässt sich leicht ertasten.

Des Weiteren können beim Stanzdruck auch ganze Stücke aus dem Material geschnitten werden, wobei sich ein wiederkehrendes Muster erkennen lässt. Diese Art des Stanzdruckes kommt häufig bei Verpackungssiegeln zum Einsatz, die Sicherheitsstanzungen verhindern dabei ein zerstörungsfreies Ablösen des Etiketts und zeigen eine Manipulation sofort an.[52]

f) Intagliodrucke

Ähnlich wie der Stanzdruck ist auch der Intaglio-Druck ertastbar, da seine Motive reliefartig und fühlbar sind. Im Unterschied zum Stanzdruck erhält der Intagliodruck jedoch Linienstrukturen, die entsprechend ihrer variablen Tiefe und Fläche verschiedene Farbintensitäten und Linienstärken erzeugen.[53] Die so entstandenen Muster zeigen ein außergewöhnlich plastisches Porträt und zeichnen sich durch eine sehr feine Linienführung und scharfe Konturen aus.

Eine pastenartige Druckfarbe wird über die Farbauftragswalzen auf den Druckzylinder übertragen. Die überschüssige Farbe wird mittels einer gegenläufigen Papierbahn vom Druckzylinder gewischt. Die in dem Relief verbliebene Farbe wird direkt und mit sehr hohem Druck auf das Papier übertragen.[54]

4.1.5 Sicherheitspapiere

Neben den verschiedenen Möglichkeiten des Sicherheitsdrucks können von Piraterie gefährdete Produkte auch durch so genannte Sicherheitspapiere geschützt werden. Dies entspricht der Philosophie, dass „die Sicherheit eines schutzwürdigen Dokumentes […] seinen Anfang beim Druckträger selbst, dem Papier, [nimmt].“[55]

Mit dem Einzug der digitalen Bildverarbeitung sowie von leistungsfähigen Farbkopierern, Scannern und Druckern ist das Fälschen bedeutsamer Dokumente für alle Personen möglich geworden. Ein Sicherheitspapier unterscheidet sich von handelsüblichen Papieren, da seine bestimmten Eigenschaften die Nachahmung der Dokumente er-

[52] Vgl. Hubert (1998).
[53] Vgl. Saueressig GmbH & Co. KG (2006).
[54] Vgl. Bundesdruckerei GmbH (2007).
[55] Landqart (2004).

schweren. Sie stellen ein Hindernis für illegale Kopiervorgänge dar, indem sie die Authentizität des Dokumentes sichern.[56]

Zertifikate, Aktienurkunden, Formulare, Transportdokumente, Skizzen, Warengutscheine, Schecks, Tickets, Steuermarken und Warenmarken sind Produkte, die täglich verwendet werden, bis heute aber kaum abgesichert sind. Hier können die Unternehmen die Sicherheitspapiere einsetzen: Sie besitzen eine lange Haltbarkeit sowie Festigkeit und sind in der Lage, extreme Beanspruchungen, wie Nässe, Hitze und häufiges Knicken, gut zu überstehen. Sicherheitspapiere erfüllen die unterschiedlichen Ansprüche an die papierphysikalischen Werte und beschränken die Anwendungsmöglichkeiten nicht, d. h. sie bleiben trotzdem bedruckbar und beschreibbar.[57]

Besonderes Sicherheitspapier besitzt zusätzlich Sicherheitsmerkmale, die nur im UV-Licht erscheinen und mit einer für das bloße Auge unsichtbaren Struktur versehen sind. Um die Struktur sehen zu können, sind Prüfgeräte mit Schwarzlicht nötig. Bei derartigem Sicherheitspapier wird zur Verhinderung der Dokumentenfälschung zudem ein zweifacher Schutz eingesetzt: Zum einen leuchtet das Hintergrundmuster blau, zum anderen erscheint eine gelbe Seriennummer. Diese Nummer wird vom Käufer protokolliert und kann im Missbrauchsfall bei polizeilichen Ermittlungen helfen.[58] Solche Sicherheitspapiere lassen sich, wie alle anderen guten Sicherheitstechnologien, nicht mit Kopierern, Scannern oder Farblaserdruckern vervielfältigen.

4.1.6 Mikroaufdrucke

Kommt Sicherheitspapier als technische Schutzmaßnahmen nicht in Frage, können Unternehmen auch auf so genannte Mikroaufdrucke zurückgreifen: Mit Hilfe spezieller Drucktechniken lassen sich dabei extrem winzige Symbole oder Texte in das Produktdesign einarbeiten. Sie erscheinen bei einfacher Betrachtung entweder separat als dünne Linie oder als Teil eines Bildes oder eines Elementes.[59]

Der Mikroaufdruck kann in allen Farben auf das Objekt gedruckt werden. Je nach Größe können die winzigen Symbole mit einer starken Lupe, einem Mikroskop oder speziellen Lesegeräten sichtbar gemacht werden. Ein Kopier- oder Druckvorgang zerstört diesen Effekt, sodass zur Herstellung eines Mikroaufdruckes spezielle Drucker

[56] Vgl. Landqart (2004).
[57] ebd.
[58] Vgl. The WIVA Company-Marmorkönig (2004).
[59] Vgl. STI – Gustav Stabernack GmbH (2007).

benötigt werden. Da ihre Produktion dennoch relativ einfach und kostengünstig ist, sollten Mikroaufdrucke immer mit anderen Technologien kombiniert werden.[60]

4.1.7 Mikroskopische Kunststoffpartikel

Die Firmen *Simons Security Systems GmbH* und *XSYS Print Solutions* bieten eine weitere Sicherheitstechnologie an, die sich MICROTAGGANT nennt. Diese Technologie wurde entwickelt, um Unternehmen mit einzigartigen Farbecodes vor Fälschungen zu schützen.

Neben dem MICROTAGGANT verfügt die *Simons Security Systems GmbH* jedoch über ein weiteres Produkt aus äußerst feinem Pulver: Das SECUTAG besteht aus melamine Alkyd-Polymere als Grundmaterial und hat einen Kern aus mikroskopisch kleinen, thermisch und chemisch äußerst widerstandsfähigen Partikeln.[61] Die Partikel haben eine Größenordnung von 5 bis 45 µm und können mit 4 bis 11 farblich unterschiedlichen Schichten der im Sandwich-Verfahren erzielten Farbcodes realisiert werden. Unternehmen können dabei zwischen verschiedenen Normalfarben, UV-Farben, magnetischen Farben und Infrarotfarben wählen. Durch die Kombination der Farben lassen sich über 4,3 Mio. Basisfarbcodes herstellen.[62]

Mit bloßem Auge sind die Partikel des SECUTAG nicht sichtbar, sie lassen sich nur durch Vergrößerung mit einem Mikroskop oder einem automatischen Lesegerät erkennen. Jeder Farbecode wird wie ein genetischer Fingerabdruck ausschließlich einem Anwender zugestanden. Verschiedene Produkte oder Designs können dadurch dem Originalhersteller zugeordnet werden.

Zur Herstellung von SECUTAG werden spezielle Maschinen benötigt, die für potentielle Fälscher eine kaum zu überwindende Hürde darstellen. Zusätzlich verhindern kontinuierliche Veränderungen im Produktionsablauf eine spätere Analyse des verwendeten Materials.

Fast alle Produkte und Materialien lassen sich mit mikroskopischen Kunststoffpartikeln sichern: Angefangen von Glas, Papier, Metall, über Flüssigkeiten, bis hin zu Pulver. Selbst Pflanzen und Tiere können auf diese Weise gekennzeichnet werden.

[60] Vgl. STI – Gustav Stabernack GmbH (2007).
[61] Vgl. Simons Druck + Vertrieb GmbH (2007).
[62] ebd.

SECUTAG ist zudem extrem hitzebeständig und kann mit organischen Lösungsmitteln und den meisten Chemikalien nicht zerstört werden.[63]

4.1.8 Biologische, chemische und magnetische Marker

Weitere Lösungen zur Sicherung von Produkten sind der Einsatz von DNA und magnetischen Markern sowie die Beimischung von organischen bzw. anorganischen Molekülen in Druckfarben, auf Verpackungen oder dem Produkt selbst:

a) Biologische Marker

Mit Hilfe von DNA-Technologien können individuelle und kundenspezifische Codes erstellt werden, da es eine Vielzahl von Kombinationsmöglichkeiten gibt.

Verwendung finden derartige Codes speziell als Marker für die Kennzeichnung von Industrieprodukten wie Fluiden (z.B. Lacke, Öle, Schmiermittel), papierbasierten Materialien und Dokumenten, Tinte, Pharmazeutika, medizinischen Proben und organischen Materialien. Sie stellen eine unsichtbare Technologie dar und zeigen sich nur mit speziellen Lesegeräten. Da DNA-Codes molekular sind, können in ihnen zusätzliche Produktinformationen gespeichert werden.[64]

Ein solches Produkt-Identifikations-System stellt die Firma *HERMA* her. BIOSafe ist eine optisch nicht wahrnehmbare Markierung, die erst durch eine aufgetragene spezifische Testflüssigkeit auf der Oberfläche des Produkts sichtbar wird. Das Ergebnis kann anschießend wieder verborgen werden, wodurch der Vorgang beliebig oft wiederholbar wird. Die Bio-Marker lassen sich unsichtbar in alle Farben und Lacke einarbeiten und schützen auch Etiketten vor Fälschungen.[65]

b) Chemische Marker

Originalprodukte lassen sich auch durch chemische Markierungsstoffe, die Codes erzeugen, erkennen. Die organischen oder anorganischen Marker werden in den Faserbrei des Papiers sowie in Glas, geschmolzene Metalle, Druckfarben und viele andere Materialien eingearbeitet. Durch ihre stabile Struktur können die Chemikalien anschließend mit einfachen Testverfahren direkt nachweisen. Um die verborgenen Mar-

[63] Vgl. Simons Druck + Vertrieb GmbH (2007).
[64] Vgl. Fuchs (2006).
[65] Vgl. Herma GmbH (2007).

ker erkennen zu können, bedarf es jedoch – wie auch bei der DNA-Technologie – spezieller Lesegeräte.[66]

c) Magnetische Marker

Neben den biologischen und chemischen Markern, gibt es noch die Möglichkeit, durch Beimischung von magnetischen Markern Produkte zu schützen. Diese ordnen sich zufällig in der Druckfarbe an und erstellen auf diese Weise ein individuelles, produktspezifisches und lese- und speicherfähiges Interferenzmuster, das eine hohe Fälschungssicherheit gewährleistet.[67]

4.1.9 Digitale Wasserzeichen

Digitale Wasserzeichen setzen Unternehmen ein, um Verpackungen und Etiketten gegen die Vervielfältigung durch Kopieren und Scannen zu schützen. Sie basieren auf kryptografischen und steganografischen Techniken. Druckdaten werden so verändert, dass sich ein kundenspezifisches Bild ergibt. Äußerlich sind die Veränderungen kaum wahrnehmbar, aber maschinell lesbar. Digitale Wasserzeichen betten Informationen in einen digitalen Inhalt ein. Sie sind direkt mit dem Inhalt verflochten und können nur durch einscannen und mit Hilfe einer speziellen Erkennungssoftware entschlüsselt werden. Vorteile liegen in der Beständigkeit des Zeichens bei Formatkonvertierungen und anderen Operationen.[68]

4.1.10 Holographische Projektionen

Holographische Projektionen werden in Form von selbstklebenden Polymer-Etiketten auf das Produkt aufgetragen. Die Firma Tesa entwickelte dazu ein Etikett, welches verschiedene offene und verdeckte Sicherheitsmerkmale enthält. Informationen werden dort als verschlüsselte holographische Struktur abgelegt und können erst durch spezielle Lesegeräte wieder sichtbar gemacht und entschlüsselt werden.

Das Informationsfeld ist nur wenige Quadratmillimeter groß und die Informationen lassen sich ohne spezielle Lesegeräte nicht erkennen.[69] Jedes einzelne Originalprodukt erhält ein individuelles Etikett, inklusive aller sicherheits- und vertriebsrelevanten In-

[66] Vgl. Fuchs (2006)
[67] Vgl. Welser/González (2007).
[68] Vgl. Fuchs (2006).
[69] Vgl. tesa scribos GmbH (2005).

formationen, wie beispielsweise Logos, Produktinformationen und spezifische Produktnummern.

4.2 Technologien gegen das Öffnen der Verpackungen

Die unter Abschnitt 4.1 vorgestellten Maßnahmen zur Sicherung von Produkten sowie deren Verpackungen vor Fälschern sind ein wichtiger Aspekt des Unternehmensschutzes im Rahmen der Logistik, aber dennoch nicht ausreichend. Durch den zunehmenden Diebstahl von Originalverpackungen gewinnen auch Technologien gegen das Öffnen der Verpackung zum Schutz vor Produktpiraterie immer mehr an Bedeutung.

Eine Verpackung ist dabei eine feste, relativ leicht zu beseitigende, vollständige oder teilweise Umhüllung des Produktes.[70] Zu ihren Funktionen zählen u.a.:

- die Erhöhung des Wiedererkennungswerts durch Design, Logo und Farbe,
- die Erregung der Aufmerksamkeit der Verbraucher durch Marketing- und Werbebotschaften,
- der Erhalt von Informationen über das Produkt,
- das Bündeln von Einzelteilen,
- der Schutz des Produkts während des Transportes, z.B. vor Zerstörung, und
- der Schutz vor äußeren Einflüssen wie Temperaturschwankungen, Schmutz und Nässe.[71]

Fälscher wissen um diese Funktionen, vor allem um die verkaufsfördernden Eigenschaften. Aus diesem Grund werden Fälschungen oft in alten oder gestohlenen Originalverpackungen vertrieben. In der Vergangenheit war eine Originalverpackung auch ein Garant für Originalwaren, heute ist das nicht mehr der Fall. Verpackungen brauchen deshalb Sicherungen, die erkennen lassen, ob sie Ausschuss sind oder bereits genutzt wurden.

4.2.1 Versiegelungstechniken

Versiegelungstechniken sind besondere Aufkleber bzw. Klebestreifen, die an Verpackungen und Transportbehältnissen angebracht werden. Diese Erstöffnungs- und Ma-

[70] Vgl. Specht (1992).
[71] ebd.

nipulationsnachweise schützen Produkte gegen Diebstahl, verhindern den Warenaustausch und sichern Gewährleistungsansprüche.[72]

Sie werden an Stellen platziert, an denen das Siegel bei erstmaliger Öffnung durch Zerreißen irreversibel zerstört wird.[73] Bessere Techniken hinterlassen beim Entfernen zudem Rückstände wie Farbspuren oder ein Gitternetz auf dem Produkt. Gitternetze oder Siegel mit individuellen Rautenmustern zeigen ein Überkleben deutlich an. Starke Permanentkleber sorgen für optimale Haftbarkeit auch auf schwierigen Untergründen.

4.2.2 Folien

Eine weitere Möglichkeit, Verpackungen und Produkte gegen unbemerktes Öffnen zu schützen, ist der Einsatz von Folien. Sie veredeln die Verpackungen und schützen das Produkt, ohne das Produktdesign zu verändern. Ihr Vorteil liegt darin, dass andere Sicherheitstechnologien und Produktinformationen unter der Folie erkennbar bleiben. In den Folien selbst lassen sich zusätzlich bestimmte Sicherheitsmerkmale integrieren; dazu zählen Originalschriftzüge oder Hologramme i. V. m. dem Firmenlogo. Besonders schwer nachzuahmen sind transparente, diffraktive Spezialfolien, da sie ein hohes folientechnisches Know-how erfordern. Durch Fertigungsverfahren wie Demetallisierung, nanometrische Dünnfilme, winzige Schriftzüge und Farbwechseleffekte lassen sich weitere Sicherheitsmerkmale entwerfen.[74]

4.3 Schutz des Vertriebssystems durch Tracking und Tracing

Tracking und Tracing bezeichnet ein elektronisches System zur Sendungsverfolgung, wobei der Begriff *Tracking* die Ermittlung des aktuellen Status beschreibt, während *Tracing* die Rekonstruktion des genauen Sendungsverlaufs ex post mit allen wichtigen Ereignissen definiert.[75]

Solche Systeme ermöglichen eine ständige Übersicht und Kontrolle des Werdegangs eines Produktes; je mehr Informationen darüber gespeichert werden, desto besser kann

[72] Vgl. Gauss (2006).
[73] Vgl. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (2007).
[74] Vgl. Fuchs (2006).
[75] Vgl. Fuchs (2006); Wildemann et al. (2007).

man ihn nachvollziehen. Diese Historie kann anschließend statistisch aufbereitet werden und so die Grundlage für Sicherheits- oder Marketingmaßnahmen bilden.

Basis für die effiziente Verwirklichung der Rückverfolgbarkeit bilden dabei umfassende standardisierte Identifikations- und Kommunikationssysteme. Weit verbreitete dabei sind Tracing-Nummern, Barcodes und RFID-Systeme[76]:

4.3.1 Tracing-Nummern

Individuelle Tracing-Nummern werden auf das Etikett bzw. die Verpackung des Produktes geklebt oder direkt auf das Produkt aufgetragen. Sie gestatten dem Verbraucher, eine Echtheitsverifizierung des gekauften Produkts direkt bei Hersteller durchführen zu lassen.[77] Dazu werden nicht wie bei den anderen Tracking und Tracing-Systemen spezielle Lesegeräte oder Scanner benötigt: Der Code ist eine einfache Zahlenfolge, die über das Internet oder eine angegebene Rufnummer überprüft werden kann. Auch Unternehmen nutzen diese Nummerierungen, um nach der Lagerung oder nach Transporten die Korrektheit der Produkte zu überprüfen.

4.3.2 Barcodes

1D-Barcodes oder Strichcodes bestehen, wie man es aus dem Supermarkt kennt, aus verschiedenen breiten Lücken und Balken (auch Bars genannt), die horizontal nebeneinander angeordnet werden.[78] Enthaltene Daten sind individuelle Produktnummern, Herstellerdaten oder Produktdaten, die mittels Scanner gelesen und verarbeitet werden können. Zu den 1D-Barcodes zählen beispielsweise EAN/UPC-Codes, Code 39, Code 128 oder Postcodes.

Der 2D-Barcode als Weiterentwicklung benötigt dem gegenüber weniger Platz, um Daten unterzubringen.[79] Er wird aus einer Aufstellung von Punkten, Quadraten oder Strichen auf einer zumeist rechtwinkligen Fläche generiert und ist auch unter dem Synonym Matrixcode in der Literatur zu finden.[80] Bei 3D-Barcodes (Prooftag) kommt als dritte Dimension Farbe hinzu.

---

[76] Vgl. GS1 Germany GmbH (2007).
[77] Vgl. Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (2007); Wildemann et al. (2007).
[78] Vgl. Fuchs (2006).
[79] ebd.
[80] Vgl. COSYS Ident GmbH (2007).

In Gegensatz zu den RFID-Technologien können die Barcodes nicht aus weiter Entfernung gelesen, sondern müssen unverdeckt und nah an die Lesegeräte gehalten werden.

4.3.3 RFID

„RFID ist eine Technologie zur berührungslosen automatischen Identifizierung von Objekten über Funkerkennung.“[81] Dabei werden auf programmierbaren Datenträgern, auch Transponder genannt, Informationen gespeichert und diese anschließend über eine Antenne ausgesendet, sobald sich der Transponder im elektronischen Feld einer Schreib-/Lesestation befindet.[82] Daten werden vom Rechner auf den Etikettendrucker übertragen, anschließend auf das Etikett gedruckt und der Transponder gleichzeitig programmiert. Gespeichert wird eine weltweit einzigartige Seriennummer, aber auch Artikelnummern, das Mindesthaltbarkeitsdatum, Liefertermine/-mengen oder Loskennzeichnungen sind möglich. Über die Seriennummern lassen sich zuverlässig, fehlerfrei und schnell Produkte und Transportträger identifizieren.

Die im Transponder gespeicherten Daten können im Gegensatz zu Barcodes verändert, ergänzt oder erweitert werden. Durch den Einsatz der RFID-Technologie lassen sich die Produkte entlang der gesamten Liefer- und Wertschöpfungskette jederzeit identifizieren, auch Transportrouten lassen sich protokollieren und Produkthistorien aufzeichnen.[83]

Für den Lesevorgang muss kein Sichtkontakt zwischen Lesegerät und Datenträger bestehen. Die Technologie ermöglicht die Erfassung vieler Datenträger gleichzeitig (Pulkerfassung) oder einzelner, gesonderter Datenträger. Die Erfassungsgeschwindigkeit von RFID-Systemen ist wesentlich höher als bei Strichcodes. Indem die räumliche Positionierung der Versandeinheit entfällt, werden überflüssige Stillstandzeiten bei Transportbändern oder Ähnlichem vermieden.[84]

Man unterscheidet zwischen Transpondern mit aktivem batteriebetriebenen Sender und passiven Transpondern ohne eigene Signalsendung und ohne Batterie.[85] Die Kosten für einen Transponder sind je nach Einsatzgebiet, Größe und Bauart sehr unter-

[81] Vgl. IHK Köln (2007).
[82] Vgl. Kämpf (2005); Wildemann et al. (2007).
[83] Vgl. Wildemann et al. (2007).
[84] Vgl. Kämpfer (2005).
[85] Vgl. Fuchs (2006).

schiedlich, jedoch zählen sie zu den teureren technischen Schutzmaßnahmen. In der unteren Preislage liegen passive Transponder ab 20 EUR-Cent; durch die zu erwartende Massenproduktion aufgrund der Anwendungssteigerung kann der Preis aber auf 5 EUR-Cent sinken.

4.4 Anwendungsgebiete der Schutzmaßnahmen

In der Beschaffungslogistik werden viele Betriebsstoffe und Fertigerzeugnisse verbraucht; so unterschiedlich wie die benötigten Materialien sind aber auch die einzusetzenden Technologien. Herstellerunternehmen können den Zulieferern den Einsatz von Sicherheitstechnologien nicht vorschreiben. Sie müssen versuchen, einen Partner zu finden, der sich gleichermaßen vor Fälschungen schützt und seine Produkte dennoch zu marktüblichen Preisen anbieten kann.[86]

Rohstoffe werden zwar nur selten manipuliert, für hochwertige oder von Fälschern präferierte Rohstoffe empfiehlt sich aber der Einsatz von mikroskopischen Kunststoffpartikeln sowie biologischen und z.T. chemischen Markern, da sie sowohl bei festen, aber vor allem auch bei flüssigen und pulverförmigen Aggregatszuständen einsetzbar sind. Desweiteren bieten sich zur Rohstoffsicherung Verpackungen und Transportbehältnisse an. Um die transportierten Stoffe zu schützen, werden Versiegelungstechniken für Kartons, Boxen und Folien eingesetzt, da sie Manipulationen während des Transports und der Lagerung aufdecken. Vorteilhaft bei diesen Technologien ist zudem die gleichzeitige Sicherung gegen unabsichtliches Öffnen.[87]

Bei Waren und Montageteilen können dagegen viele Technologien eingesetzt werden; Einschränkungen liegen hier vor allem im Preis und in der vermuteten Vorgehensweise der Fälscher. Technologien im unteren Preissegment sind Hologramme, Sicherheitsdrucke bzw. -tinten, Mikroaufdrucke, OVDs und mikroskopische Kunststoffpartikel. Sie finden ihre Anwendung bei günstigen Produkten. Hochwertige Produkte werden eher durch chemische, biologische und magnetische Marker, holographische Projektionen und RFID gesichert, aber auch die günstigeren Technologien erfreuen sich hier zunehmender Beliebtheit.[88]

[86] Vgl. Fuchs (2006); Wildemann et al. (2007).
[87] Vgl. Fuchs (2006).
[88] Vgl. Wildemann et al. (2007).

In der Produktionslogistik unterscheidet sich der Einsatz der Technologien danach, ob Unternehmen ihre Produkte komplett im eigenen Haus fertigen oder einzelne Schritte nach außen verlagern. Verlassen die Produkte während der Fertigung das Unternehmen nicht, fällt die Sicherung meist spartanisch aus: Erst am Ende des Fertigungsprozesses werden die Produkte für den Vertrieb gerüstet und Sicherheitstechnologien integriert und aufgetragen. Einige Technologien wie mikroskopische Kunststoffpartikel oder Stanzdrucke können aber auch zu einem früheren Zeitpunkt eingearbeitet werden, da sie trotz Weiterverarbeitung erhalten bleiben.[89]

Bei Produkten aus zusammengesetzten Teilen greifen Unternehmen mitunter zur Sicherung einzelner Teile. Dies erfolgt am Ende der jeweiligen Fertigungsstufe. Für größere, nur stückweise verdeckte oder verkleidete Teile im Inneren des Produktes ist es sinnvoll, mit permanenten Sicherheitstinten zu arbeiten, da Technologien, bei denen die Teile einer genaueren Untersuchung bedürfen, erst demontiert werden müssen. Dies ist den Unternehmen meist zu aufwendig. Bei sehr kleinen Teilen ist der Platzbedarf der Tinten oftmals nicht ausreichend, sodass sich dort Mikroaufdrucke als ideal erweisen. Sicherheitstinten sind speziell in der Lebensmittel- und Medikamentenindustrie einsatzfähig: Im Gegensatz zu anderen Technologien gibt es Sicherheitstinten, die gefahrlos verzehrt werden können. Da gerade der Pharmabereich immer stärker von Produktpiraterie betroffen ist, verhindern dort Codes direkt auf den Medikamenten Imitationen und den Austausch der Originaltabletten in den Verpackungen.[90]

Verlagert ein Unternehmen Fertigungsstufen nach außen, wächst die Gefahr, aufgrund der entstehenden Schnittstellen eingeschleuste Fälschungen zu erhalten. Im allen Produktionsstätten müssen daher die Einzelteile gesichert werden. Den größten Nutzen haben dabei Tracking und Tracing-Systeme, weil dort eine Datenspeicherung für die Rückverfolgung möglich ist. Für Einzelteile mit permanenter Kennzeichnung werden Nummerierungen und Barcodes mit Sicherheitstinte oder durch Stanzdruck verwendet, da sie trotz Weiterverarbeitung beständig bleiben. Prozesstolerante Tinten werden aber auch für Verpackungsbeschriftungen eingesetzt. Ein gedruckter Code auf Verpackungen kann den Koch-, Sterilisations- oder Pasteurisierverfahren standhalten.[91]

Für vorübergehende Kennzeichnungen können Codes auf Etiketten aufgetragen werden, die sich anschließend rückstandsfrei entfernen lassen. Etiketten und Tinten sind

[89] Vgl. Fuchs (2006); Wildemann et al. (2007).
[90] Vgl. Fuchs (2006).
[91] Vgl. Linx Printing Technologies Ltd (2005d); Wildemann et al. (2007).

im Gegensatz zu RFID sehr günstig, wobei alle Systeme zur Verifizierung einzeln gelesen und ausgewertet werden müssen. Diese Prüfung ist für Unternehmen jedoch oft zu zeitintensiv. Mit RFID-Technologien lassen sich derartige Kontrollen in viel kürzerer Zeit realisieren. Bei RFID müssen die Produkte zunächst in der Produktion oder zu Beginn des Vertriebes markiert werden, sodass in allen darauffolgenden Logistikstufen eine Registrierung und Verifizierung über IT-Systeme möglich ist.[92] Sie erlauben die Prüfung des Produkts im gesamten Distributionsprozess. Die lückenlose Verfolgung der Bestands- und Bewegungsdaten verhindert das unbemerkte Einschleusen von Plagiaten bis zum Handel.[93] Die RFID-Technologie erspart durch Pulkerfassung viel Zeit beim Lesen der Daten, ist aber teuer. Die Größe der Transponder ist je nach Einsatzgebiet sehr unterschiedlich. Die Transponder für Container sind mitunter um ein vielfaches größer als die Transponder auf einem Autoersatzteil. Gibt es im innerbetrieblichen Produktionsprozess viele Schnittstellen, an denen gelagert sowie be- und entladen wird, sorgen die gleichen Systeme für einen effizienten Einsatz.

In der letzten Stufe der Logistikkette muss das fertige Produkt zu den Händlern und Kunden gelangen. Beauftragte Spediteure und Transportunternehmen sind gezwungen, von der Echtheit der Waren auszugehen, da sie zumeist verpackte Waren bekommen. Bei nationalen und internationalen Transporten ist ein Schutz durch Verpackungen i. V. m. aufgedruckten Sicherheitstechnologien, Folien und Versiegelungstechnologien erdenklich. Transporteure erkennen dadurch, ob während der Pausen oder Ruhezeiten Manipulationen stattgefunden haben. Außerdem sehen die Empfänger auf den ersten Blick, ob die Ware so eingetroffen ist, wie sie losgeschickt wurde.[94]

Der Vertrieb stellt für die Unternehmen das wohl größte Risiko dar. Dies betrifft nicht ausschließlich die Transporte der Fertigprodukte; jede Lieferung – die von Einzelteilen eingerechnet – zieht Plagiatoren an. Aus diesem Grund sollten sowohl die Produkte als auch ihre Verpackungen gesichert werden. Aber auch hier gilt, dass nicht jeder Absatzmittler in der Lage ist, alle verdeckten Markierungen zu überprüfen. Händler können nicht jedes Produkt nach verborgenen Sicherheitsmerkmalen absuchen; außerdem ist es den Anwendern bei der Vielzahl der unterschiedlichen Lesegeräte und Maschinen nicht möglich, sich sämtliche der teuren Geräte zu kaufen.[95]

---

92 Vgl. Günthner/Meißner (2006).
93 ebd.
94 Vgl. Fuchs (2006).
95 ebd.

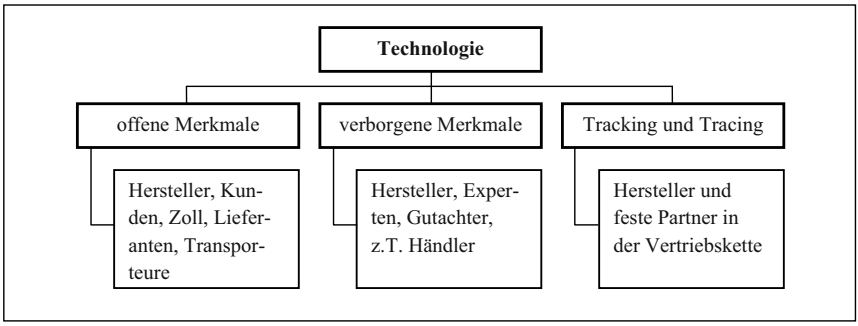


Abbildung 5: Einteilung der Anwender von Sicherheitstechnologien
Quelle: eigene Darstellung.

Originalhersteller betrachten es als wichtige Aufgabe, ihre Lieferanten, Händler und vor allem Kunden vor Fälschungen zu schützen. Dazu entwickeln sie geheime Merkmale, die je nach Inhalt zusätzlich oder ausschließlich an der Verpackung fixiert und beim Eingang oder bei der Verarbeitung der Teile überprüft werden. Holographische Projektionen und digitale Wasserzeichen zählen beispielsweise zu diesen Sicherheitstechnologien. Die so genannten verborgenen Merkmale werden nur von einem engen Kreis von Spezialisten ausgewertet (Vgl. Abbildung 5).

Bei Verdachtsmomenten können Händler, Lieferanten und Kunden die Produkte dem Unternehmen zuschicken und sie auf ihre Echtheit überprüfen lassen. Die Kontrolle ist dadurch zwar deutlich aufwendiger, aber bedeutend treffsicherer. Für Produktpiraten ist die Nachahmung verdeckter Technologien nicht sehr reizvoll; zum Teil wissen sie gar nicht um die Existenz der Technologien, und wenn doch umgehen sie einfach den kleinen Kreis der Kontrolleure und nutzen andere Vertriebswege.[96]

Unternehmen mit erlesenen Produkten und festen Handelspartnern sind in der Lage, ihre Händler mit den nötigen Lesegeräten auszustatten. Im Groß- und Einzelhandel ist dies aus Kostengründen aber nicht durchführbar. Zudem erfordert die Kontrolle einen hohen Zeitbedarf. Geeigneter für Händler sind Hologramme, OVDs, Sicherheitsdrucke und Sicherheitstinten; gleiches gilt auch für die Kunden. Offene Merkmale können schnell erkannt werden, oft ist ein flüchtiger Blick ausreichend. Gleichzeitig können die Merkmale durch viele Personen überprüft werden (Vgl. Abbildung 5). Jedoch müssen Unternehmen hier auf die Datenspeicherung verzichten. Viele sichtbare

[96] Vgl. Fuchs (2006).

Schutzmaßnahmen werden bereits auf die Verpackung aufgetragen, damit sie nicht erst beim Auspacken erscheinen. Aus Unternehmenssicht entsteht ein positiver Nebeneffekt, da Hologramme, OVDs, Sicherheitsaufdrucke und Mikroaufdrucke verkaufsfördernde Instrumente sind. Es ist eine äußerst dekorative Produktaufwertung. Durch den Lichteinfall entsteht zum Beispiel bei Hologrammen eine meist silbrig glänzende, regenbogenfarbende Form, die das Interesse der potentiellen Kunden erregt.[97] OVDs wechseln je nach Betrachtungswinkel Farbe oder Bildinhalte, Interessenten werden dazu verleitet, das Produkt aus dem Regal zu nehmen und die Verpackung genauer zu betrachten. Sicherheitsaufdrucke ziehen ebenso wie Hologramme und OVDs die Aufmerksamkeit des Verbrauchers auf das Produkt; die meisten Sicherheitsaufdrucke sind zusätzlich noch ertastbar, wodurch auch hier das Verlangen der Berührung verstärkt wird.

Jedoch können offensichtliche Merkmale keine Garantie für Originalprodukte sein. Auch Nachahmerprodukte werden vermehrt mit diesen Technologien ausgestattet. Sie sind zum Teil einfach zu beschaffen, da es viele Anbieter gibt. Verbraucher werden mit diesen Marketinginstrumenten derart überflutet, dass es ihnen Schwierigkeiten bereitet, die Besonderheiten der individuellen Designs zu erkennen und einfache Imitate zu verifizieren. Somit spielt die Qualität oder Genauigkeit zur Originaltechnologie eine untergeordnete Rolle, vor allem wenn der direkte Vergleich fehlt oder bei Zeitdruck der Prüfer. Mitunter kann es sogar vorkommen, dass Nachahmer den Originalherstellern einen Schritt voraus sind und auf ihre Produkte Hologramme kleben, während das Original gar nicht mit dieser Technologie ausgestattet ist. Dadurch richtet sich die Aufmerksamkeit der Verbraucher auf das Nachahmerprodukt und billige Imitationen werden für hochwertig gehalten. Fälscher sparen Kosten für F&E und können dadurch mehr für Originalitätsnachweise ausgeben. Wenn Unternehmer das vermeiden wollen, müssen offene Technologien nicht nur eingesetzt werden, sondern Verbraucher auch Informationen darüber erhalten. Ebenso müssen die Zollbehörden von den Schutzmaßnahmen in Kenntnis gesetzt und entsprechend für die Suche nach Plagiaten ausgebildet und unterstützt werden. Für die Zollbehörden ist es besonders schwierig, offene Sicherheitstechnologien auf ihre Korrektheit zu überprüfen, da die große Auswahl bei z.T. geringen Kosten unzählige Nutzer mit sich zieht.[98]

[97] Vgl. Holografia Polska agencja monitorowania produktu (2006).
[98] Vgl. Fuchs (2006).

Tabelle 2: Sicherheitstechnologien im Überblick
Quelle: eigene Darstellung.

Technologie	**offene Sicherheitstechnologie**			**offene bzw. verborgene Sicherheits-technologie**	**verborgene Sicherheits-technologie**	**Tracking und Tracing-Systeme**	
Parameter	*Hologramme*	*OVD*	*Versiegelungen*	*Sicherheitstinte*	*Mikroskopische Kunststoff-partikel*	*RFID*	*Barcode*
Kosten (inklusive Lesegeräte)	gering bis mittel	gering	gering	gering	gering	hoch	einmalig teuer (Lesegeräte und Software), Druck günstig
Lesbarkeit	ohne Hilfsmittel	ohne Hilfsmittel	ohne Hilfsmittel	ohne Hilfsmittel bzw. UV-Licht	mit gutem Mikroskop	mit spezielle Lesegerät und Software	mit Scanner oder Kamera und Software
Datenspeicherung	nein	nein	nein	nein	nein	ja	ja
Manipulations- und Fälschungs-sicherheit	niedrig bis mittel	mittel	niedrig	niedrig bis mittel	hoch	leicht manipulierbar, fälschungssicher	niedrig

Unternehmen können des Weiteren Sicherheitspapiere zur Zertifizierung der Produkte nutzen. Beim Verkauf der Produkte liegt das Echtheitszertifikat anbei, Händler können bei Erhalt der Waren diese Bescheinigung überprüfen. Fehlt sie komplett oder fehlen die Sicherheitsmerkmale, kann der Absatzmittler von einer eingeschleusten Lieferung ausgehen. Auch Kunden bekommen beim Kauf das Zertifikat ausgehändigt, der Wartungs- und Reparaturdienst kann dadurch vor Beginn der Arbeit die Echtheit überprüfen. Bei diesen Zertifikaten bieten sich unsichtbare Merkmale wie UV-Papiere oder fluoreszierende Muster an. Garantiekarten und Bedienungsanleitungen können durch Sicherheitspapier ebenfalls gegen Fälschung geschützt werden; hier empfiehlt sich der Einsatz von sichtbaren Merkmalen als Kopierschutz. Denn Garantiekarten und Bedienungsanleitungen werden von Nachahmern gern gefälscht, um zögerliche Verbraucher von der Echtheit der Ware zu überzeugen. Hologramme, Kippfarben und Sicherheitsdrucke können von Kunden schnell identifiziert werden. Produkte, die für den Verkauf bestimmt sind, sollten also mit einer Kombination verschiedener Technologien präpariert werden. Jede der Technologien hat Vor- und Nachteile, deshalb kann eine einzelne Technologie nie die Sicherheit bieten wie eine Kombination mehrerer. Der Einsatz offener und verdeckter Technologien sowie Tracking und Tracing-Systeme deckt viele Schwachstellen ab und kombiniert die Vorteile.[99] Oft verwendete Technologien sind in Tabelle 2 dargestellt.

Unternehmen sollten den Stand ihrer Sicherheitstechnologien immer im Auge behalten. Anbieter versuchen stetig, sie weiter- oder neue zu entwickeln, um den Fälschern eine Nachahmung erheblich zu erschweren.

5 Betriebswirtschaftliche Schutzmaßnahmen in der Logistik

Betriebswirtschaftliche Schutzmaßnahmen gehören ebenso wie die technologischen Schutzmaßnahmen zu den präventiven Schutzmechanismen, erfordern aber einen hohen Planungsaufwand.

Viele der betriebswirtschaftlichen Schutzmaßnahmen lassen sich nicht kurzfristig verwirklichen, sie bedürfen einer vorherigen Auseinandersetzung mit der Materie, damit das Management die richtigen Entscheidungen treffen kann. Risiko- bzw. Gefährdungsanalysen dienen der Gesamteinschätzung des Unternehmens und sollten vor al-

[99] Vgl. Wildemann et al. (2007).

len Sicherheitsentscheidungen durchgeführt werden. Dabei wird zunächst der Ist-Zustand hinsichtlich der von außen wirkenden Gefahren auf das Unternehmen und die internen Bedrohungen untersucht. Das Ziel der Analyse ist es, das Zusammenspiel aller Gefahrenquellen und -potentiale möglichst bereits im Ansatz zu erkennen. Die Erkenntnisse bilden die Grundlage für die durchzuführenden Maßnahmen.

Anschließend werden die Maßnahmen in die Unternehmensprozesse integriert. Eine Einführung und Integration der betriebswirtschaftlichen Schutzmaßnahmen verursacht deutlich höhere Kosten als die Sicherheitstechnologien. Doch jedes Unternehmen, welches sich vor Produktpiraten effizient schützen möchte, sollte ein angemessenes Budget für diese Präventionen zur Verfügung stellen.[100]

5.1 Personelle Aspekte der Logistik

Eine an die Logistik angepasste Personalpolitik[101] ist Vorrausetzung für die Erfüllung aller Logistikaufgabe und damit wichtig für den Schutz der Produkte.[102]

Eine personalpolitische Maßnahme ist die Einstellung besonders qualifizierter Mitarbeiter, die in logistischen Gebieten tätig sind. Logistische Aufgaben müssen in allen Unternehmensabteilungen erfüllt werden.

Eine sorgfältige Personalauswahl kann bereits im Ansatz Informationsverluste vermindern. Zur sorgfältigen Auswahl gehören die Sichtung und Überprüfung der Bewerbungsunterlagen auf Echtheit und Lückenlosigkeit sowie der persönliche Eindruck während des Vorstellungsgespräches. Eingestellte Mitarbeiter müssen während des gesamten Beschäftigungszyklus betreut und begutachtet werden, da ihre Loyalität von existenzieller Bedeutung ist.[103]

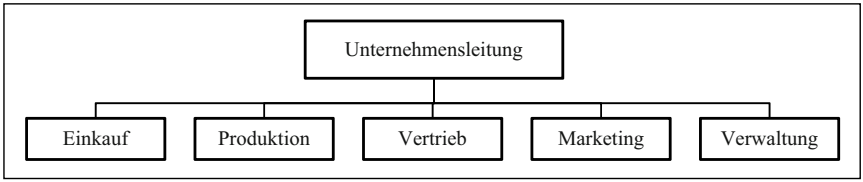


Abbildung 6: Organigramm eines Unternehmens
Quelle: eigene Darstellung.

[100] Vgl. Fuchs (2006).
[101] siehe dazu auch Abschnitt *5.3 Personelle Schutzmaßnahmen* von Gundula Warnecke.
[102] Vgl. Schulte (1995).
[103] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004).

Um gewährleisten zu können, dass an jeder Stelle Mitarbeiter mit den nötigen Kompetenzen vorhanden sind, muss eine genaue Hierarchie festgelegt werden. Klare Verantwortungsbereiche erschweren das Einschleusen von Fälschungen, da nicht jeder Mitarbeiter überall Zugang erhält. Auch die Korruptionsgefahr ist geringer, wenn jeder Angestellte einen Vorgesetzten hat, der ihn kontrolliert. Mitarbeiter gehen nicht so schnell „in den Massen verloren", wenn jeder Vorgesetzte eine überschaubare Mitarbeiteranzahl betreut. Die Arbeiter wissen auf diese Weise auch genau, an wen sie sich im Verdachtsfall wenden müssen.[104]

Teilweise wird ein Sicherheitsverantwortlicher im Gesamtunternehmen eingesetzt oder Personen benannt, die in den einzelnen Teilprozessen für die Produktpiraterie verantwortlich sind. Diese Personen sollten in der Firmenhierarchie möglichst weit oben stehen. Nur durch die Gewährung von Einblicken in alle sicherheitsrelevanten Abteilungen und Prozesse kann der Mitarbeiter seine Aufgabe effizient erfüllen. Besonders bedeutsam erscheint hierbei eine enge Zusammenarbeit mit den Bereichen Forschung und Entwicklung, Vertrieb, IT sowie mit der Personalabteilung.[105]

Unternehmensgrundsätze, die aus der Unternehmensphilosophie und unternehmenspolitischen Aspekten abgeleitet werden, schaffen die Rahmenbedingungen für die Planung und erleichtern eine Führung durch Ziele. Zu den Unternehmensgrundsätzen gehört auch, dass Informationen nicht nach außen gegeben werden. Die Grundsätze sollten niedergeschrieben und von allen Personen eingehalten werden. Speziell für die Arbeitnehmer kann eine Arbeitsordnung verfasst werden. Aus dem Gesetz, der Arbeitsordnung und dem Arbeitsvertrag ergeben sich Rechte und Pflichten für beide Vertragsparteien. Arbeitsentgelt, Arbeitszeit, Beendigung des Arbeitsverhältnisses, Unfall- und Schadenvergütung, Informationspflicht bis hin zu eventuell auftretenden Schäden, sonstigen Störungen und der Verschwiegenheitspflicht der Arbeitnehmer sind dort fixiert. Um die Regeln rechtsgültig zu machen, werden zusätzlich in den Arbeitsverträgen – insbesondere mit Know-how-Trägern – Geheimhaltungsklauseln vereinbart. Dabei muss der Schutzgegenstand und die Geltungsdauer des Schutzes so genau wie möglich definiert werden.[106]

Die Mitarbeiter müssen von Anfang an in Sicherheitsüberlegungen eingebunden werden. Ein anspruchsvolles Unternehmen, welches stets bemüht ist, Produktpiraten fern-

[104] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004).
[105] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004); Fuchs (2006).
[106] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004).

zuhalten oder zu entlarven, muss seinen Mitarbeitern die Gelegenheit geben und sie dazu motivieren, regelmäßig an Schulungen teilnehmen. Diese Maßnahmen zeigen Mitarbeitern, wie sie Fälschungen erkennen können und wie sie im Falle eines Verdachts handeln sollten.[107] Erfahrungen, die die Mitarbeiter dabei sammeln, können fortlaufend in die Entscheidungsprozesse eingebracht werden. Die gewonnenen Erkenntnisse über Produkte und ihre Merkmale werden betriebsintern dokumentiert und helfen den Vertriebsmitarbeitern bei der Identifizierung der Originale. Damit verbunden schaffen die Unternehmen Anreize, die Mitarbeiter bei der Aufdeckung von Fälschungen bekommen können, und erläutern gleichzeitig straf- und personalrechtliche Konsequenzen im Falle krimineller Handlungen.

Innovative Unternehmen mit qualifizierten Mitarbeitern sind für Imitatoren beliebte Spionageobjekte. Vertriebsmitarbeiter verfügen i. d. R. nicht über das gleiche Know-how wie die Entwickler oder Produzenten, aber dennoch gehen Entwicklungen und neue Produkte nicht unversehens an ihnen vorbei. Aus diesem Grund sollte das Unternehmen immer versuchen, seine Mitarbeiter möglichst lange an sich zu binden. Die Fluktuation der Mitarbeiter muss eingedämmt werden, denn mit jedem Mitarbeiter verlässt ein Stück Wissen das Unternehmen. Vor allem entlassene Mitarbeiter sind häufig enttäuscht und unzufrieden: Wechseln sie zur Konkurrenz, ist das ein hohes Sicherheitsrisiko. Aber auch Mitarbeiter, die aus freien Stücken das Unternehmen verlassen, stellen ein Risiko dar, da sie eventuell geheime Informationen weitergeben, um ihre Karriere schnell voranzutreiben.[108]

Das Wach- und Nachtpersonal wird zur Überwachung der Grundstücke und Gebäude, inklusive der Lager, eingesetzt. Gerade in den Nachtstunden sind Unternehmen nur mit einem Mindestpersonal besetzt, das zur Produktion gebraucht wird. Für Piraten verringert sich dadurch das Risiko, entlarvt zu werden. Sie versuchen im Schutz der Dunkelheit an vertrauliches Wissen über Neuentwicklungen zu gelangen. Das Wachpersonal ist für ein Unternehmen jedoch sehr teuer und muss zudem auf seine Effizienz geprüft werden. Viele Unternehmen beauftragen Sicherheitsfirmen für diese Aufgabe; dabei können sie entscheiden, ob das Personal ständig im Unternehmen ist oder in regelmäßigen Abständen einen Rundgang macht. Sowohl eigenes als auch fremdes Sicherheitspersonal wird meistens mit Pförtneraufgaben beauftragt.[109] Ihr Lohn ist

[107] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004).
[108] ebd.
[109] ebd.

trotzdem verhältnismäßig sehr gering, sodass sie anfällig für Bestechungsgelder sind. Sie sollten daher sorgfältig ausgesucht werden.

Aber auch bei Beauftragung betriebsfremder Arbeiter muss auf eine vertrauensvolle Sicherheitsfirma geachtet werden. Parameter für die Wahl der richtigen Firma sind:

- das Unternehmensimage,
- die Durchführung einer Betriebsbesichtigung durch die Sicherheitsfirma vor Vertragsabschluss,
- die erfolgreiche Absolvierung der Sachkundeprüfung durch alle Mitarbeiter,
- das Auftreten der Mitarbeiter (inklusive Dienstbekleidung),
- das polizeiliche Führungszeugnis der Mitarbeiter,
- die Ausstattung der Mitarbeiter mit Dienstausweisen, Funkgeräten, Waffen, Hunden und ähnlichem, sowie
- die Vertragsmodalitäten.

5.2 Maßnahmen in der Lagerlogistik

Jedes Unternehmen, welches sich vor Produktpiraten schützen möchte, sollte außerdem bestimmte bauliche Maßnahmen ergreifen. Beispiele hierfür sind Mauern, Zäune oder Stacheldraht als Gebietsabgrenzungen sowie Lagerhallen, in denen die Fenster mit Panzerglas und Schlössern sowie die Türen mit Beschlägen, Riegeln, Überfallen und Schließzylindern gesichert sind. Lager dienen den Unternehmen als Puffer, um trotz eines Informationsdefizits bezüglich:

- der exakten Bedarfsmengen künftiger Perioden,
- der Liefermengen,
- der Bedarfszeitpunkte, sowie
- der Lieferzeitpunkte oder ähnliches keinen Produktionsstillstand zu verursachen.[110]

Aber eine Lagerung verursacht Schwund wie durch Diebstahl. Um ihn erkennen zu können, müssen die Bestände des Lagers und des Ersatzteilbereichs regelmäßig über-

[110] Vgl. Ehrmann (1999).

prüft werden.[111] Kann nicht auf die Lagerung verzichtet werden, müssen die Lager und Transportbehältnisse geschützt werden. Zum Einsatz kommen dort Alarmanlagen, Kameras und/oder Wachpersonal.

Auch Materialentnahmen für die Produktion sollten nicht jedem Mitarbeiter gestattet werden, besser ist der Einsatz weniger Entnahmebefugter. Das erleichtert der Unternehmensführung das Nachvollziehen der Materialgänge. Bei Make-or-Buy-Überlegungen steht das Unternehmen vor der Entscheidung, ob es bestimmte Leistungen selbst erbringen oder Dritte damit beauftragen soll. Im Rahmen der Logistik betrifft dies überwiegend Entscheidungen bezüglich einer Eigen-/Fremdlagung sowie eines Eigen-/Fremdtransports. Trifft das Unternehmen die Entscheidung zur Fremdlagerung, spart es hohe Investitionskosten; gleichzeitig entsteht aber eine Abhängigkeit gegenüber Dritten. Sie müssen sich darauf verlassen können, dass die Logistikdienstleister ihre Hallen ebenso schützen, wie das Unternehmen selbst es tun würde.[112]

Verbunden mit einer externen Lagerhaltung ist auch die Gefahr des Know-how-Abflusses: Der Originalhersteller kennt die Arbeiter nicht und auch die Arbeiter haben keine Bindung zum Ursprungsunternehmen. Sie sind anfälliger für Korruptionen und werden bei Bestechungen schneller vertrauliche Informationen oder Teile weitergeben. Die Zusammenarbeit mit externen Dienstleister sollte geprüft werden, um gemeinsam gegen Produktpiraten vorgehen zu können. Um die Anreize für Piraten abzuschwächen, sollten nur Rohstoffe und Module fremdgelagert werden.

Weit verbreitet sind auch Sicherheitssysteme zum Schutz der Lagerhallen; sie verhindern, dass sich Betriebsfremde im Lager bewegen. Dazu zählen beispielsweise Alarmanlagen: Wird ein Fenster eingeschlagen, eine Tür aufgebrochen oder ein Signal übertreten, melden viele Anlagen Alarm über einen lauten Ton. Er soll den Täter verunsichern, zur Hektik treiben und ihm somit den Raub erschweren. Der Ton erregt Aufmerksamkeit auf das Objekt und eventuell den Täter.

Außerdem gibt es noch Zutrittskontrollsysteme, die nur autorisierten Personen den Zutritt erlauben. Die Erkennung der Authentizität einer Person erfolgt mittels Code, Magnetkarte oder durch biometrische Identifikation. Der Vorteil der Zugriffscodes liegt darin, dass nicht jedem Mitarbeiter eine Magnetkarte ausgehändigt werden muss; je nach Mitarbeiterstamm lassen sich dadurch viele Kosten sparen. Codes können al-

[111] Vgl. Fuchs (2006).
[112] ebd.

lerdings durch Beobachtung bei der Eingabe leicht ausspioniert werden. Hat ein Unbefugter den Code erst einmal in Erfahrung gebracht, kann er sich leicht Zutritt verschaffen. Soll nur einer bestimmten Anzahl an Mitarbeitern Zutritt gewährt werden, sind auch Magnetkarten gut einsetzbar. Magnetkarten bevollmächtigen nur den Eigentümer zum Zutritt.

Am fälschungssichersten sind biometrische Systeme wie die Fingerprint-, Gesichtsfeld- und Iriserkennung. Sie stellen die Identität einer bestimmten Person aufgrund menschlicher Merkmale fest, die dauerhaft und untrennbar an eine Person gebunden sind.[113] Dadurch können sie nicht verloren gehen. Diese Systeme sind aber im Gegensatz zu den anderen Sicherheitssystemen sehr teuer und jeder neue Mitarbeiter, dem Zugang gewährt werden muss, erfordert weitere Installationskosten. Aus diesem Grund sind biometrische Systeme vor allem bei Lagerhallen mit hochsensiblen und teuren Gütern beliebt.

Eine weitere präferierte Sicherungsmethode in der Lagerlogistik sind Videoüberwachungssysteme. Kameras werden dabei zur Überwachung des Eingangsbereiches oder flächendeckend eingesetzt. Sie zeichnen Bilder auf, um eine spätere Identifizierung der im Lager befindlichen Personen zu ermöglichen. Kameras werden aber auch zur Echtzeitüberwachung genutzt. So können Pförtner oder Sicherheitsdienstleister vom Monitor aus Unregelmäßigkeiten erkennen.[114]

Bei allen Sicherheitssystemen sollte das Unternehmen unbedingt Firmen mit der Installation beauftragen. Sie verfügen über das fachliche Know-how und können die Systeme genau auf die Kundenbedürfnisse zuschneiden. Außerdem sollte mit ihnen ein Wartungsvertrag zur regelmäßigen Überprüfung der Systeme auf ihre Funktionstüchtigkeit und zur Neueinstellung der Geräte abgeschlossen werden.

Zudem gibt es noch die Alternative, durch die Lagertypen seine Güter zu schützen. Zu den sichersten Arten zählen das Verschieberegallager, das Sicherheitslager und das Hochregallager: Das Verschieberegallager besteht aus einzelnen Fachbodenregalen, die auf Fahrgestellen montiert sind. Zur Sicherung werden die Regale ineinander geschoben und verschlossen; dadurch wird Fremden der Zugriff verwehrt. Allerdings lohnt sich dieses System nur bei Gütern, die nicht täglich gebraucht werden. Einschränkungen bestehen je nach Bauart in der Tragfähigkeit der Regale und des Bodens

[113] Vgl. Fuchs (2006).
[114] Vgl. Sicherheitsforum Baden-Württemberg (2005).

sowie im Platzbedarf der Güter.[115] Das Sicherheitsregal besteht aus einzelnen Schließfächern, die sich separat abschließen lassen. Genutzt wird dieses Regal speziell für besonders wertvolle und sensible Teile von kleiner bis mittlerer Größe. Genau wie beim Verschieberegallager ist auch hier die Entnahme aufwendig.[116]

Eine weitere Lagerart ist das Hochregallager. Dieses kann eine Höhe von bis zu 50 Metern erreichen, wobei sich zwischen den Regalreihen ein Durchgang befindet, in dem sich schienengebundene Regalbediengeräte bewegen.[117] Sie werden manuell oder automatisch gesteuert und befördern die Güter von der Warenausgangszone zum Lagerplatz oder vom Lagerplatz zur Warenausgangszone. Bei einem Lager mit Automatikbetrieb ist der Lagerbereich mittels Zaun und/oder Lichtschranke für den Zutritt durch Personen abgesichert. Hochregallager sind für die Lagerung größerer Mengen und Güter geeignet. Für die sichere Lagerung von Dokumenten, Konstruktionsplänen, Prototypen usw. werden auch Tresore genutzt.

5.3 Schutz der Transportsysteme

Eine weitere betriebswirtschaftliche Schutzmaßnahme betrifft die Entscheidung des Unternehmens darüber, wie es seine Materialien zur Fertigungsstätte und seine Produkte zum Händler und Kunden befördert:

a) Post- und Kleingutverkehr

Unternehmen nutzen den Post- und Kleingutverkehr, wenn sie kleinere Mengen befördern wollen. Einige Unternehmen haben eigene Kuriere, die die Ware auf direktem Weg vom Unternehmen zum Kunden bringen. Diese Methode ist jedoch sehr zeit- und kostenintensiv. Alternativ können die Hersteller auch Spezialisten, wie Paket-, Kurier- und Expressdienste, beauftragen. Die Ware wird hierbei beim Hersteller abgeholt, in Paket- oder Briefzentren sortiert und dann zum Kunden gebracht. Die Dienste beschränken sich meist auf die Lieferung innerhalb des Landes. Greifen Hersteller auf den Paketversand zurück, sollten sie das Unternehmen auf ihre Zuverlässigkeit über-

[115] Vgl. Ehrmann (1999).
[116] ebd.
[117] Vgl. Lebinger (2007).

prüfen. Neben dem Luftverkehr ist der Postverkehr mit 43% am risikoreichsten, aber aufgrund der kleinen Mengen ist der Wert der sichergestellten Waren sehr gering.[118]

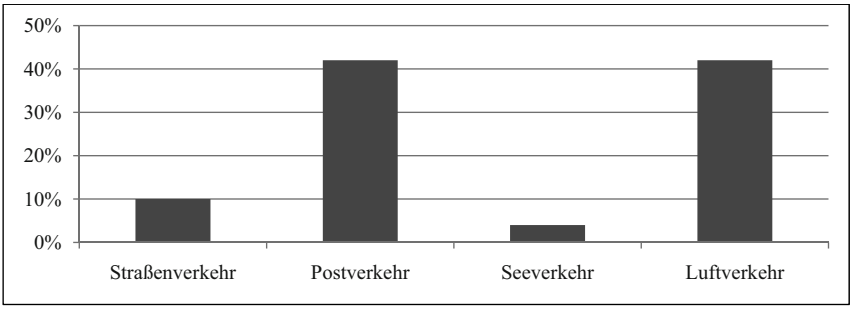


Abbildung 7: Anzahl der Übergriffe nach Verkehrsart in Prozent (Stand 2006)
Quelle: eigene Darstellung, in Anlehnung an: Bundesministerium der Finanzen (2006), S. 34.

Bei den meisten Paket-, Kurier- und Expressdiensten können die Waren gegen Diebstahl und Zerstörung versichert werden. Gibt es diese Möglichkeit nicht, sollte ein anderer Anbieter gesucht werden. Auch der gesamte Abwicklungsprozess gibt Anhaltspunkte über die Professionalität der Dienstleister. Folgende Fragen sollte jeder Hersteller beantworten können, um das passende Unternehmen zu finden:

- Wird die Übergabe unterschriftlich bestätigt?
- Welchen Eindruck hinterlassen die Fahrer?
- Sind die Lieferfahrzeuge in einem ordnungsgemäßen Zustand, besitzen sie sogar zusätzliche Sicherungen?
- Mit welcher Sorgfalt wird die Ware verladen?

b) Luftverkehr

Der Luftverkehr wird sowohl für den Rohstofftransport zur Produktionsstätte als auch für den Warentransport zum Handel und zum Kunden genutzt. Der Luftverkehr ist eine sehr teure Beförderungsmethode, daher wird er meist nur bei hochwertigen Waren- und Rohstofflieferungen eingesetzt. Auch bei sehr weiten Distanzen oder schnell ver-

[118] Vgl. Bundesministerium der Finanzen (2006).

derblichen Gütern kommen Frachtflugzeuge zum Einsatz, da sie im Gegensatz zum Seeverkehr beachtlich schneller sind.[119]

Nachteilig für Hersteller, die per Luftpost befördern, sind die Flughafenbindung und die damit verbundene Schnittstellenabhängigkeit. Die Lieferung muss mehrmalig vom Flugpersonal und Zoll kontrolliert werden. Die Gefahr des Einschleusens von Fälschungen ist bei Unachtsamkeit des Personals sehr hoch, auch die Flughafenlager sind ein Sicherheitsrisiko. Generell werden Unbefugte vom Flughafengelände ausgeschlossen, jedoch sind Kontrollen aufgrund der Gebietsgröße sehr schwierig. Zur Verhinderung von Manipulationen werden die Waren meist in verschlossenen oder verplombten Containern gelagert, bei Zollkontrollen werden die Container gegebenenfalls geöffnet und neu verplombt.[120]

Beim Luftverkehr gibt es viele Missbrauchsfälle, darunter fallen auch im Urlaub erworbene Imitate und gefälschte Zigaretten privater Haushalte. Aus diesem Grund ist der prozentuale Warenwert der Aufgriffe mit 16% deutlich hinter dem des Seeverkehrs (74%).[121] Hersteller können die Frachtkontrollen nicht verhindern; die Beamten müssen sich davon überzeugen, dass sich keine illegalen oder gefährlichen Güter in den Containern oder Verpackungen befinden. Bei Rohstoffen kann nur die Wareneingangskontrolle bei der ausländischen Produktionsstätte Manipulationen aufdecken. Jedoch sind Eingriffe bei Rohstoffen eher selten. Problematischer sind Produkt- und Teilelieferungen, auf die sich das Hauptaugenmerk der Plagiatoren richtet.

Neben den Sicherheitstechnologien gibt es noch eine weitere Möglichkeit, wie sich das Unternehmen schützen kann. Dabei werden die verschiedenen Produktkomponenten in ein unauflösbares Modul integriert. Das Ergebnis ist eine Black Box, ein Funktionssystem mit unbekannter innerer Struktur.[122] Das besondere an der Black-Box-Bauweise ist, dass das Produkt nicht zerlegt werden kann, ohne das Modul dabei zu zerstören. Technisch sensible Produktkomponenten können auch in Kunstharz gegossen werden, um Reverse Engineering zu vermeiden.[123] Erlangen Fälscher in den Besitz eines Produktes, versuchen sie durch das Reverse Engineering, das Produkt zu analysieren, um einen Konstruktionsplan zu erstellen.

[119] Vgl. Ehrmann (1999).
[120] ebd.
[121] Vgl. Bundesministerium der Finanzen (2006).
[122] Vgl. Ehrmann (1999).
[123] Vgl. Fuchs (2006).

Unternehmen sollten die Zahl der Absatzmittler im Ausland überschaubar halten: Wenn sie wenige Händler mit dem Verkauf beauftragen, besteht ein engerer und regelmäßigerer Kontakt.[124] Nicht selten stattet das Herstellerunternehmen ausländischen Verkäufern einen Besuch ab, um sich vor Ort über das Unternehmen zu informieren.

c) Straßenverkehr

Am häufigsten werden Waren über den Straßenverkehr vertrieben, über 50% aller Güterlieferungen erfolgen durch LKWs und Transporter. Große Unternehmen besitzen häufig eigene Fahrer und LKWs, sie können durch eine Reihe von Maßnahmen ihre Waren schützen. Viele Fahrzeuge verfügen über moderne Navigationssysteme, wodurch die Routenführungen überprüft werden können. Die Fahrzeugortung erfolgt per GPS-Satellit und wird auf einer digitalen Straßenkarte im Internet dargestellt.[125] Neben der aktuellen Fahrzeugposition wird auch die Fahrtroute als Spur in einer Straßenkarte angezeigt.

Durch den Einsatz des Navigationssystems lassen sich:

- Fahrtstrecken und Fahrtziele,
- Fahrtzeiten und Leerlaufzeiten,
- Stand-, Pausenzeiten, Fahrunterbrechungen und Aufenthaltszeiten,
- Datum, Uhrzeit, Kilometerstand, Geschwindigkeit und Wegstrecke, sowie
- Betriebszeiten wie Motor, Zündung, Drehzahl speichern und auswerten.[126]

Weicht ein Fahrer von der vorgegebenen Route ab, um beispielsweise ein illegales Lager anzufahren und Originalteile gegen Plagiate auszutauschen, kann das sofort nachgewiesen werden.

Die Gründung von Vertriebsteams kann ebenso hilfreich sein. Das Team besteht aus Mitgliedern verschiedener Bereiche: Sie übernehmen Auftragsabwicklung, Verpackung, Warenausgang, Ladungssicherung und den Transport. Die wechselnden Zuständigkeiten verhindern die Planung krimineller Aktivitäten. Außerdem können die Mitglieder sich gegenseitig kontrollieren.[127]

[124] Vgl. Sepp (2007).
[125] Vgl. BaumaschinenOrtung (2007b).
[126] Vgl. BaumaschinenOrtung (2007a).
[127] Vgl. Fuchs (2006).

Bei sehr teuren Frachtgütern werden in seltenen Fällen auch zwei Arbeiter gleichzeitig eingesetzt, wobei einer den Vertrieb übernimmt und der andere die Abwicklung kontrolliert. Bei weniger exklusiven Gütern ist das aufgrund der hohen Personalkosten wirtschaftlich nicht sinnvoll. Deutlich günstiger ist der Einsatz des Rotationsprinzips. Dort wechseln die Mitarbeiter zwischen verschiedenen Produktgruppen oder Kunden. Unternehmen wollen auf diese Weise erreichen, dass keine persönlichen Beziehungen entstehen, in denen es zu Absprachen kommen kann. Grundsätzlich sollte der Vertriebsleiter den Mitarbeitern nicht grenzenlos vertrauen, aber sie auch nicht ständig überwachen. Es sollten temporäre Stichprobenüberprüfungen durchgeführt werden, denn oft sind Originale und Plagiate in ein und derselben Lieferung vermischt. Dafür ist der Aufbau eines transparenten und kontrollierbaren Vertriebssystems nötig, in dem Verkaufsquoten, Routen und Besuchshäufigkeiten festgelegt sind.[128]

Werden Transportunternehmen mit der Lieferung beauftragt, sollten die Speditionsverträge immer so gestaltet werden, dass ergänzende Punkte für Logistikdienstleister enthalten sind. Ein Vertragspunkt, um die Produktpiraterie zu minimieren, sollte festlegen, dass der Spediteur keine Aushilfsfahrer und keine fremden Frachtarbeiter beschäftigen darf. Es werden feste Routen geplant und die Fahrer verpflichtet, die festgelegten Routen genau einzuhalten.[129] Es dürfen keine Bedarfstouren abgewickelt werden. Außerdem legt der Hersteller fest, dass Stichproben durch ihn jederzeit möglich sind. Der Vertrag überträgt das Risiko auf das Transportunternehmen: Wenn also während der Lieferung ein Austausch der Originalware erfolgt, wird der Transporteur zur Verantwortung gezogen und muss eventuell die Versicherung einschalten.

d) Seeverkehr

Der Seeverkehr ist eine Vertriebsmethode, die aufgrund der Wasser- und Hafenbindung viele Schnittstellen haben kann, an denen die Güter umgepackt werden müssen. Dennoch werden sehr wenige Fälschungen sichergestellt, da es trotz alledem ein sehr zuverlässiges Verkehrsmittel ist. Es gibt sehr wenige Plagiatsfälle beim Seeverkehr, doch dadurch, dass die Schiffe teure Waren und Waren in sehr großen Mengen transportieren, ist dort der Warenwert der Angriffe unter allen Verkehrsmethoden am

[128] Vgl. Fuchs (2006).
[129] ebd.

höchsten.[130] Der Seeverkehr wird für Lieferungen über weite Entfernungen genutzt, die keinen Termindruck haben, da Schiffe eher langsam sind.

Gefahrenquellen sind beim Seeverkehr eher das Be- und Entladen; Reedereien mit vertrauenswürdigem Personal sorgen für eine einwandfreie Abwicklung. Sie sind nicht so weit verbreitet wie Speditionsunternehmen, deshalb ist die Auswahl weniger aufwendig, aber dennoch nicht einfacher. Da auf Schiffen viel Platz ist, können Unternehmen Vertriebskooperationen eingehen und auf die Reeder Einfluss hinsichtlich der Pirateriebekämpfung nehmen und sie zu einer erhöhten Achtsamkeit aufrufen. Eine Vertriebskooperation birgt jedoch hohe Gefahren, da hier im Gegensatz zu den Einkaufskooperationen bereits fertige Produkte transportiert werden. Das Unternehmen sollte sich Partner suchen, die nicht aus der gleichen Branche stammen. Auf See, wo keine Fremden das Schiff betreten können, und beim Umladen, sofern keine weitere Kontrolle erfolgen muss, kann das Unternehmen durch Verplombung der Container Manipulationen verhindern.[131] Ergänzend kann das Unternehmen, wie beim Luftverkehr auch, die Black-Box-Bauweise nutzen.

e) Schienenverkehr

Der Schienenverkehr macht im Gegensatz zu den anderen Methoden nur einen geringen Anteil aus und ist eher rückläufig. Demzufolge ist auch die Zahl der Übergriffe gering.[132] Der Schienenverkehr wird fast ausschließlich für große Gütermengen und sperrige Produkte genutzt. Auch bei dieser Methode wird die Containerverplombung und Black-Box-Bauweise angewendet. Es ist die einzige Vertriebsmethode, wo eine Lieferantenauswahl überflüssig ist, da der Schienengütertransport primär von der Deutschen Bundesbahn betrieben wird.

Beim Luft-, Schienen- und Seeverkehr muss der Transport immer mit anderen Methoden, vor allem LKW-Verkehr, kombiniert werden. Dadurch sollten immer Maßnahmen ergriffen werden, die sowohl beim Luft-, Schienen- und Seeverkehr, als auch beim Straßenverkehr anwendbar sind. Die Kombination kann sogar soweit gehen, dass der LKW mit Fahrer beim See-, Luft- und Schienenverkehr gleich mitfährt. Dieser

[130] Vgl. Bundesministerium der Finanzen (2006).
[131] Vgl. Fuchs (2006).
[132] Vgl. Bundesministerium der Finanzen (2006).

Huckepackverkehr[133] ist meist zu kostenintensiv, hat aber dennoch den Vorteil, dass die Ware zusätzlich durch den verschlossenen Transporter und Fahrer gesichert ist.

5.4 Maßnahmen in der Beschaffungslogistik

Eine große Herausforderung für Unternehmen ist die zuverlässige und qualitätsgerechte Lieferung eingekaufter Rohstoffe, Einzelteile und Waren. Eine sorgfältige Auswahl der Lieferanten ist dabei wichtig. Bei der Bewertung der Lieferanten müssen sowohl die Hard Facts, wie die Preise, Mitarbeiterzahlen, Produktqualität und Fehlerraten, als auch die Soft Facts Beachtung finden.

Die Soft Facts lassen sich deutlich schwieriger bewerten, da sie an subjektiven Kriterien ausgemacht werden. Einige dieser Kriterien sind das F&E-Know-how, die Bereitschaft zur gemeinsamen Planung und Problemlösung, Vertrauen und Offenheit, die Informations- und Kommunikationsfähigkeit, das Ansprechverhalten, die Verhandlungsmacht, der Wettbewerbskontakt sowie die Einstellung zur Produktpiraterie.[134] Dies ist wichtig, um eine illegale Mehrproduktion zu vermeiden und die Lieferantenkette gegen Produktfälscher abzusichern. Speziell der Einkauf in anderen Ländern ist schwierig, da der Beschaffungsmarkt in den meisten Schwellen- und Entwicklungsländern sehr intransparent ist. Dementsprechend sind auch die Informationen nur schwer zu erhalten bzw. ihre Korrektheit unsicher.[135] Eine genaue Analyse des Beschaffungsmarktes ist daher unumgänglich und Lieferanten müssen auf Fälschungsaktivitäten und -potenziale hin überprüft werden. Neben den Preis- und Produktinformationen bekommen die Hersteller Daten über den Aufbau sowie die Bewegungen der Märkte. Die Herkunftsländer der Pirateriewaren können sehr mannigfaltig sein. In Tabelle 3 wird dazu die Herkunft der Pirateriewaren nach Ländern unterteilt.

Bei der Beschaffungsplanung sollte ein Unternehmen Länder mit hoher Pirateriewahrscheinlichkeit meiden oder seine Aktivitäten zur Informationserhaltung verstärken und Kontrollen durchführen.[136] Dabei prüft das Herstellerunternehmen beispielsweise, ob die Lieferantenware Schutzrechte verletzt, vor allem bei Ähnlichkeiten mit bekannten Markenprodukten. Im Rahmen einer Angebotsprüfung (Due Diligence) werden alle wesentlichen Informationen durch Gespräche mit den Lieferanten, Unternehmensbe-

[133] Vgl. Thome (2007).
[134] Vgl. Fuchs (2006).
[135] ebd.
[136] ebd.

Tabelle 3: Aufteilung der Fälle nach Warenkategorie und Herkunftsländern in Prozent der Stückzahl der Waren
Quelle: Bundesministerium der Finanzen (2006), S. 36.

Warenkategorie	Rang 1	Rang 2	Rang 3	Rang 4	Rang 5	Rang 6	Rang 7	Rang 8	Rang 9	
Sportbekleidung	97,48% China	1,72% Vietnam								0,82% sonstige
Accessoires	82,01% China	6,19% Südkorea	5,90% Türkei	3,07% Hongkong						2,84% sonstige
Freizeitbekleidung	66,75% China	14,21% Türkei	6,49% Vietnam	2,33% Indien	1,38% Südkorea	0,89% Hongkong	0,57% USA			7,38% sonstige
Uhren & Schmuck	75,08% China	5,61% Hongkong	1,83% Thailand	1,75% USA	1,04% V.A.E.	0,95% Polen	0,87% Syrien	0,59% Bolivien		12,28% sonstige
Sonstiges	51,84% China	21,22% Türkei	5,41% Vietnam	3,73% Hongkong	3,28% Südafrika	2,93% Mexiko	1,41% USA	1,30% Brasilien	0,92% Thailand	8,52% sonstige
Elektr. Geräte	54,52% China	16,71% GB	15,40% Hongkong	4,49% V.A.E.	1,58% Südkorea	1, 30% USA	1,03% Taiwan	0,96% Philippinen	0,84% Ukraine	3,17% sonstige
Datenträg., Software	90,18% China	4,58% Singapur	2,54% Japan	0,71% Hongkong	0,55% USA					1,44% sonstige
Spielzeug	81,49% China	11, 49% Hongkong	4,55% Paraguay	0,78% V.A.E.	0,88% Brasilien					1,01% sonstige
Zigaretten	99,09% China									0,10% sonstige
Parfüm & Kosmetik	35,46% China	21,86% Hongkong	21,46% Türkei	11,33% Belarus	7,07% USA	0,94% Vietnam				1,88% sonstige
Computer	58,21% China	23,72% Hongkong	9,25% USA	2,82% Malaysia	2,13% V.A.E.	1,97% Tschechien	0,85% Türkei	0,85% Südkorea		0,20% sonstige
Lebensmittel	97,12% Unbekannt	1,55% Thailand	0,86% Schweiz							0,47% sonstige
Medikamente	54,74% Philippinen	22,57% China	6,05% Norwegen	5,48 Indien	5,01% USA	2,36% Argentinien	0,58% Dom. Rep.			3,21% sonstige

sichtigungen und die Sichtung der Unternehmensunterlagen gesammelt. Hierzu gehört die Prüfung auf Richtigkeit der Dokumente, Qualitätsbescheinigungen sowie der Inhaltsangaben durch die ausstellenden Institutionen (wie SGS, TÜV, LGA, etc.) und durch unabhängige Prüfinstitute.[137]

Neben den betriebswirtschaftlichen sind juristische, steuerliche oder auch kulturelle Faktoren zu beachten. Unternehmen sollten des Weiteren die Zulieferer von Verpackungsmaterialen überprüfen, da viele Fälschungen in Originalverpackungen verkauft werden.

Generell sind Lieferanten empfehlenswert, die ein Sicherheitsniveau haben, welches dem des eigenen Unternehmens entspricht. Lieferanten, die ihren guten Ruf sowie Kunden und Investitionen zu verlieren haben, sind für eine vertrauenswürdige Zusammenarbeit bestens geeignet. Es empfiehlt sich dabei, den ausländischen Geschäftspartner u.a. durch die deutschen Auslandshandelskammern oder Wirtschaftsauskunfteien prüfen zu lassen.[138] Bei allen Zulieferern sollte das Unternehmen stets bemüht sein, Teilaufträge an unterschiedliche Zulieferer, die keinen Kontakt miteinander haben, zu vergeben. Durch diese Maßnahme erhalten sie keine Komplettlösung, mit der sich illegale Produktionen abwehren lassen. In diesem Zusammenhang dürfen Unternehmen nur Know-how vergeben, das Zulieferer zur Fertigung der Module benötigen, das heißt, sie geben so viele Informationen wie nötig und so wenig wie möglich weiter.[139] Die Endmontage, Funktionstests und Qualitätskontrollen sollten im eigenen Unternehmen bzw. im Mutterkonzern durchgeführt werden.

Durch eine professionelle Vertragsgestaltung können Fälschungsrisiken eingedämmt werden. Die Verträge bedürfen einer eindeutigen Formulierung. Der Hersteller kann beispielsweise seine Lieferanten dazu verpflichten, ein Qualitätsmanagementsystem nach DIN EN ISO 9001:2000 einzuführen, „das auch Fälschungen in Materialien, Teilen, Produktionsmitteln, Dienstleistungen, Software oder sonstigen Vorlieferungen von Unterlieferanten einbezieht."[140] Das kann so weit gehen, dass Lieferanten einen Nachweis erbringen müssen, der die Echtheit aller ihm gelieferten Produkte und Leistungen bestätigt und für Schäden aufkommt, die im Zusammenhang mit den gefälschten Zulieferteilen stehen. Des Weiteren sollte die Sicherstellung einer lückenlosen Rückver-

[137] Vgl. Sepp (2007).
[138] ebd.
[139] Vgl. Bundesverband der Deutschen Industrie e. V. (2007).
[140] Fuchs (2006).

folgung der Produkte ein Bestandteil der vertraglichen Vereinbarungen sein.[141] Weitere Gestaltungsmodalitäten zwischen Hersteller und Lieferanten können die Informationspflicht bei Zuliefererwechsel des Lieferanten und ein Verbot des Verkaufes von Produkten und Teilen an andere Hersteller sein.[142] Vertraulichkeitsvereinbarungen sollten zudem neben Vertragsstrafen bei Verstoß eine Beweislastumkehr zugunsten des eigenen Unternehmens enthalten.[143] Jede Lieferung erfordert eine strikte Wareneingangskontrolle, bei der die Zahl bzw. Qualität der beschafften Teile kontinuierlich mit denen der gefertigten Produkte verglichen werden muss.[144] Die Wareneingangskontrolle fällt je nach Rohstoff- und Teilelieferung sehr unterschiedlich aus. Rohstoffe werden stichprobenartig kontrolliert. Sie sind in den seltensten Fällen durch Sicherheitstechnologien geschützt, aus diesem Grund werden hier:

- die Mengenangaben,
- die Einhaltung der Qualitätsstandards, und
- die richtige Zusammensetzung untersucht.[145]

Mengenangaben können durch einfaches Zählen, Wiegen, Messen sowie Schätzen überprüft werden. Zur Kontrolle der Qualität und der Zusammensetzung ist allerdings ein Labor notwendig. Jede Warenlieferung muss mit größter Sorgfalt bearbeitet werden. Unternehmen sollten verhindern, dass Warenlieferungen außerhalb der Annahmezeit erfolgen, da die Ware dann unbeobachtet auf der Rampe bleibt. Generell dürfen Waren nicht auf der Rampe abgestellt, sondern immer gleich eingelagert oder verbraucht werden.[146] Auch die Einlagerung beschädigter Ware oder Einzelteile darf nicht vernachlässigt werden, sie sind genauso beliebt bei Fälschern.

Obwohl Rohstoffe weniger beliebte Spionagegüter sind, steigt die Zahl der kennzeichnenden Stoffe, die den Originalrohstoffen und -chemikalien beigemischt werden. Bei exklusiven, teuren und sicherheitsrelevanten Gütern sind Stichproben nicht ausreichend. Das Unternehmen sollte mehr Zeit und Personalkosten in Kauf nehmen und wenn möglich jedes Produkt überprüfen. Die standardisierten Kontrollen sind mit Hilfe von Checklisten durchzuführen, um Abweichungen erkennen zu können. Wichtig

[141] Vgl. Fuchs (2006).
[142] ebd.
[143] Vgl. Bundesverband der Deutschen Industrie e. V. (2007).
[144] Vgl. Fuchs (2006); Sepp (2007).
[145] Vgl. Fuchs (2006); Ehrmann (1999).
[146] ebd.

bei allen Wareneingangskontrollen ist vertrauenswürdiges Personal,[147] denn ohne dies sind die besten Technologien, Prüfgeräte und Checklisten hinfällig.

Innerhalb der Beschaffungslogistik existiert für KMUs meist keine andere Möglichkeit, als eine Kooperation mit anderen Unternehmen einzugehen. Nur über diesen Weg sind kleine und mittelständische Betriebe in der Lage, ähnliche Angebotsvolumina wie Großunternehmen bei den Lieferanten zu erreichen und damit auch die Kosten zu verringern. Nur wenn ihre Verkaufspreise sich denen der großen Unternehmen annähern, sind sie konkurrenzfähig. Dank Kooperationen mit Unternehmen kann der Hersteller weitere Vorteile beim Einkauf erringen. Kooperationspartner, die gleiche Rohstoffe oder Einzelteile benötigen, verlangen eine äußerst tiefgehende Analyse. Durch Einkaufkooperationen lässt sich das Wissen aller Beteiligten bündeln.[148] Die Nutzung von Marktkenntnissen der Partner erleichtern die Erschließung neuer Vertriebs- und Beschaffungswege, wodurch sich langfristig die Kosten und damit auch die Preise reduzieren lassen. Außerdem besitzen sie eine größere Einkaufsmacht, mit der sie Einfluss auf den Lieferanten in Richtung Pirateriebekämpfung ausüben können.

5.5 Maßnahmen in der Produktionslogistik

In der Produktionslogistik wird das Flussprinzip angewendet, das heißt, der Material-, Informations- und Wertfluss soll möglichst ohne Stillzeiten ablaufen. Just-in-Time, eine weitestgehende lagerlose Fertigung, sorgt für eine produktionssynchrone Materialbeschaffung, sodass eine fortdauernde Verschwendung und Verzögerung in den jeweiligen Produktionsstufen minimiert werden können.[149] Durch diese JIT-Konzepte können Schnittstellen in der Lagerhaltung reduziert und zu Fließstellen umgewandelt werden. Solche Konzepte erfordern aber eine exakte Planung, da Fehler zum Produktionsstillstand führen.

Durch das JIT-Verfahren sinkt das Spionagerisiko im Lager entscheidend. Die schnelle Materiallieferung direkt zum Einsatzort sorgt für eine Verkürzung der Produktionszeiten. Je schneller fertige Produkte auf den Markt kommen, umso weniger Zeit haben Plagiatoren zur Nachahmung. Sie müssen innerhalb kürzester Zeit Wissen erspähen und Imitate produzieren. Ist das Originalprodukt bis zum Markteintritt des Plagiates

[147] Vgl. Fuchs (2006).
[148] ebd.
[149] Vgl. Ehrmann (1999).

bereits fest auf dem Markt etabliert, haben Billigimitate schlechte Absatzchancen.[150] Außerdem kann der Kundenbedarf bis zur Einführung der Fälschungen bereits gesättigt sein. Viele Unternehmen nehmen an ihren Produkten immer wieder kleine optische oder technische Änderungen vor, damit Imitatoren bei Markteinführung bereits ein veraltetes Produkt anbieten und mit ihrer Produktion nicht hinterherkommen.[151]

5.6 Maßnahmen in der Distributionslogistik

Der Vertrieb erfordert erhöhte Aufmerksamkeit. Genau wie jede Warenlieferung eine Wareneingangskontrolle mit sich zieht, sollte bei jedem Warenversand eine Warenausgangskontrolle durchgeführt werden. Dort wird kontrolliert, ob der Bestell- bzw. Lieferschein und die verpackte Ware übereinstimmen. Außerdem erfolgt eine Überprüfung der Warenqualität; hierunter zählt die Echtheitskontrolle der Ware. Die Waren lassen sich – egal ob Groß- oder Kleinkunde – endkundengerecht zusammenstellen. Ein fälschungskritisches Neu- und Umverpacken entfällt dadurch.[152]

Um das Vertriebsnetz zu sichern, gibt es die Möglichkeit des selektiven Vertriebs. Dazu wird in das Vertriebsnetz nur eine kleine Anzahl von Händler integriert, sodass auch Weiterverkaufsmöglichkeiten stark begrenzt sind.[153] Der Originalhersteller sucht sich zuverlässige Handelsunternehmen, wodurch nicht selten langfristige Kooperationen entstehen. Das Unternehmen wählt Händler, die bestimmte Anforderungen hinsichtlich der Verkaufsmethode, Verkaufsfläche, Sortimentsstruktur und der Reputation erfüllen. Die Hersteller-Händler-Beziehung wird oftmals durch einen Vertragsabschluss gefestigt. Händlerverträge enthalten bestenfalls eine Vereinbarung zum Schutz des geistigen Eigentums.[154] Dabei regelt der Vertrag, dass der Händler keine Produkte der Konkurrenz oder gar gefälschte Produkte vertreiben darf. Der Händler hat sich nach besten Kräften von der Echtheit der gehandelten Ware zu überzeugen. Die Vereinbarung kann genau festlegen, wie der Händler seine Versorgungskette zu sichern und zu kontrollieren hat und welche technischen Schutzmaßnahmen er zur Verifizierung überprüfen muss. Der Absatzmittler bekommt Informationen, wie genau er seine Verkäufe zu dokumentieren und welche Nachweise er über die Vertriebswege vorzulegen hat. Jeden Hinweis auf Plagiate muss der Händler sofort an den Hersteller wei-

[150] Vgl. Fuchs (2006).
[151] ebd.
[152] Vgl. Sepp (2007).
[153] Vgl. SCADPlus (2007).
[154] Vgl. Sepp (2007).

terleiten. Ein Vertragsbruch führt zur sofortigen Auflösung der Kooperation. Außerdem zieht er eine empfindliche Vertragsstrafe mit sich und führt gegebenenfalls zu Schadenersatzleistungen. Außerdem verpflichtet sich der Händler, die Produkte nur an die Endkunden zu verkaufen. Dadurch verhindert der Hersteller, dass seine Produkte an unseriöse Zwischenhändler außerhalb seines Vertriebssystems geraten und diese dann Original und Fälschung nebeneinander anbieten.

Für den Hersteller bedeutet dies eine erhebliche Erleichterung bei der Kontrolle des Vertriebsnetzes. Er kennt seine Vertriebspartner, demzufolge können unseriöse Händler, die ohne Zustimmung seine Produkte verkaufen, sofort identifiziert werden. Genau wie der Hersteller argwöhnt auch der Käufer, dass Produkte, die außerhalb dieses selektiven Vertriebssystems angeboten werden, Fälschungen sein müssen.[155]

Das Franchising ist eine Form des selektiven Vertriebs. Es ist ein Vertriebssystem, bei dem ein Lizenzgeber (i. d. R. der Hersteller) einem rechtlich selbständigen Lizenznehmer (i. d. R. der Händler) gegen Entgelt das Recht überlässt, Waren und Dienstleistungen des Lizenzgebers in seinem Geschäft anzubieten. Der Hersteller kann somit Einfluss auf die Absatzpolitik des Händlers nehmen, ohne Kapital investieren zu müssen. Der Händler wird beim Aufbau und bei der Führung des Betriebes unterstützt. Der Lizenzgeber gewährt ihm Gebietsschutz, das heißt das exklusive Verkaufsrecht für ein bestimmtes Gebiet, in dem kein anderer Franchisenehmer des Herstellers verkaufen darf. Im Gegenzug verpflichtet sich der Händler, keine Konkurrenzprodukte zu vertreiben und die Herstellerprodukte auch nur in seinem Gebiet abzusetzen. Alle Aufgaben und Pflichten der beiden Vertragsparteien werden in einem Franchisevertrag festgeschrieben.[156]

Eine sehr sichere Vertriebsform ist der Direktvertrieb. Hier werden keine Absatzmittler im Vertriebsnetz zwischengeschaltet. Der Versand erfolgt ohne Umweg direkt zum Kunden. Dadurch lassen sich viele Gefahrenquellen ausschalten. Der Hersteller kann den gesamten Vertriebsprozess kontrollieren, von der Produktion bis zum Endkunden. Die Form des Direktvertriebes wird als Business-to-Consumer (B-to-C) bezeichnet; als größtes und bekanntestes Direktvertriebsunternehmen der Welt gilt Dell Inc. Nach 23 Jahren des Direktvertriebs begann das Unternehmen 2007, einige Produkte auch über Händler zu verkaufen; in Deutschland ist der indirekte Vertrieb für Februar 2008 geplant, doch der Großteil der Unternehmenshardware wird weiterhin über den Direkt-

[155] Vgl. Fuchs (2006).
[156] Vgl. Fischer et al. (2002).

vertrieb abgesetzt.[157] Der Kontakt zwischen Hersteller und Kunde kommt meist über das Internet, Post oder Telefon zustande. Der Hersteller verpackt die georderte Ware endkundengerecht in Pakete, sodass niemand mehr Kontakt zu den Produkten hat. Den Versand übernimmt dann das OEM oder ein beauftragtes Transportunternehmen.[158]

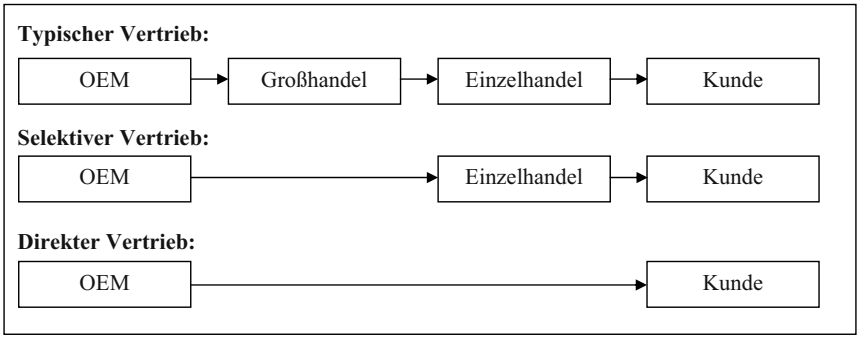


Abbildung 8: Vertriebsformen
Quelle: eigene Darstellung, in Anlehnung an: Kotler/Bliemel (2001).

Das Factory-Outlet-Center (FOC) oder auch Fabrikverkaufszentrum ist eine andere, in Deutschland allerdings sehr seltene Vertriebsform. Beim Fabrikverkaufszentrum bieten mehrere Herstellerunternehmen ihre Produkte in einer gemeinsamen Verkaufsstätte an; bei einem reinen Fabrikverkauf indessen bietet nur ein Hersteller seine Produkte an.[159] Beide Formen werden zentral geplant, verwirklicht und überwacht. Die Originalhersteller bieten die Waren zu günstigeren Preisen an. Die Kunden müssen keinen Händleraufschlag zahlen; dadurch sind sie bei ihnen sehr beliebt. Die Kunden können von der Echtheit der Ware ausgehen, da sie sie direkt vom Hersteller beziehen. Aus diesem Grund ergeben sich auch Vorteile für den Originalhersteller. Im Umkreis dieser Verkaufsorte haben dubiose Händler, die billige Imitate anbieten, weniger Chancen diese zu veräußern. Allerdings nimmt diese Vertriebsform viel Platz in Anspruch. Sie erreicht eine Größe von mehreren tausend Quadratmetern. Des Weiteren verdrängen Fabrikverkaufszentren andere Unternehmen in der Region, was zu einer Verschlechterung des Wettbewerbs führt.[160] Aber gerade in ausländischen Märkten ist es eine her-

[157] Vgl. Leierseder (2007).
[158] Vgl. Wildemann et al. (2007).
[159] Vgl. Kotler/Bliemel (2001).
[160] ebd.

vorragende Alternative zum Schutz vor Fälschern. Diese Märkte sind für deutsche Unternehmen schwierig zu kontrollieren, ein Fabrikverkauf oder Fabrikverkaufszentrum erübrigt die Kontrolle der dortigen Händler. Vor allem in ausländischen Metropolen mit einer hohen Bevölkerungsdichte wie Hongkong ist diese Vertriebsform sehr beliebt.

Beim Exklusivvertrag oder Alleinvertrieb beliefert der Hersteller in einer bestimmten Region ausschließlich einen Vertragshändler. Gleichzeitig beschränkt die Vereinbarung den Vertriebshändler, die Produkte in anderen Gebieten zu verkaufen, in denen ein Alleinvertriebsrecht besteht.[161] Dadurch kann der Hersteller das Netz der Absatzmittler nach bestimmten qualitativen oder quantitativen Kriterien selbst gestalten. Bei Alleinvertriebsvereinbarungen wird die Kundengruppe auf einen bestimmten Umfang begrenzt, sodass der Vertriebshändler nur einem zuvor festgelegten Kundenkreis die Produkte anbieten kann.[162] Dies wird meist bei sehr teuren Produkten angewendet, sie sollen nur einem bestimmten Kundenkreis vorbehalten sein. Neben dem Vermögen spielen dort beispielsweise Macht und Einfluss eine Rolle. Der Hersteller kann zum einen Fälle von Nachahmung besser erkennen, zum anderen sorgt er für die Erhaltung der Exklusivität der Marke.

Ist die Erfüllung eines sicheren Transports und Vertriebes im Ausland besonders schwierig, sollte das Unternehmen ein Markteintritt in diesem Gebiet noch einmal abwägen. Bei jeder Vertriebsform hat das Unternehmen die Möglichkeit, Mitarbeiter und Partner in der Distributionskette als Informationsquelle zu nutzen.[163] Besonders Absatzmittler im Ausland kennen sich im dortigen Markt besser aus.

5.7 Maßnahmen im Service und in der Entsorgungslogistik

Mit der Übergabe der Ware an den Kunden ist die Aufgabe des Unternehmens noch nicht abgeschlossen. Eine gute Kundenbetreuung nach dem Kauf trägt zur Bindung und Zufriedenheit der Nachfrager bei. Durch umfassende Serviceleistungen kann das Unternehmen den Käufermarkt beobachten. Ist das Servicepersonal ausreichend auf das Erkennen von Fälschungen spezialisiert, ist es in der Lage, über Verkäufer, Vertriebsweg oder Absatzgebiet Auskunft zu geben.[164]

[161] Vgl. SCADPlus (2007).
[162] ebd.
[163] Vgl. Sepp (2007).
[164] Vgl. Wildemann et al. (2007).

Bei Wartung und Reparatur hat das Personal Kontakt zu vielen der verkauften Produkte und Händler bzw. Endkunden. Entdeckt er bei der Erledigung seiner Aufgaben gefälschte Teile, kann er die Information sofort an den Hersteller weiterleiten und versuchen, durch den Kunden den Vertreiber der Piraterieware herauszubekommen.[165] Kann der Kundendienst jedoch nicht zwischen Original und Fälschung unterscheiden, erfüllt er womöglich Garantieleistungen an Fälschungen, die dem Unternehmen in Rechnung gestellt werden. Das kann für das Unternehmen teurer werden als regelmäßige Schulungen des Servicepersonals.

Außerdem sollte das Unternehmen mit Händlern und Kunden kommunizieren. Sie sollten beispielsweise auf ihrer Internetseite Informationen veröffentlichen, wie Kunden Fälschungen erkennen können und welche technischen Schutzmaßnahmen sie nutzen. Über Kontaktdaten, u.a. durch eine Telefonhotline, können Kunden oder Händler Verdachtsfälle melden und eventuelle Fälschungen zur Kontrolle einschicken.

Während der Entwicklung, Produktion und Lieferung fällt zudem immer wieder Abfall oder Ausschuss an. Produktpiraten durchsuchen den Müll nach Vorlagen, die sie verwenden können. Ideenskizzen, Vertragsentwürfe und andere für Fälscher relevante Dokumente müssen vor der Entsorgung durch einen Aktenvernichter unkenntlich gemacht werden. Bruchstücke, Fehlerteile und Materialreste sind vom Unternehmen kontrolliert zu entsorgen und gegebenenfalls klein zu häckseln; gleiches gilt für Produktentwürfe. Bei Fälschern sehr beliebt sind Verpackungen, Garantiekarten oder Bedienungsanleitungen, die unbedacht entsorgt werden. Durch Originalkartons und -dokumente werden Kunden in die Irre geführt, sie werden unachtsam und nehmen die Produkte nicht genauer in Augenschein.[166]

6 Managementempfehlungen

Die Bekämpfung der Produktpiraterie gewinnt sowohl beim Staat als auch bei den Unternehmen immer stärker an Bedeutung. Die Unternehmen sorgen für eine ausreichende Budgetbereitstellung; mit diesen finanziellen Mitteln planen sie effektive Maßnahmen, um das Problem einzudämmen. Dabei wirken einzelne Methoden meist nur par-

[165] Vgl. Fischer et al. (2002).
[166] Vgl. Fuchs (2006).

tiell. Um eine flächendeckende Problemlösung zu erzielen, sind komplexe und bereichsübergreifende Maßnahmen empfehlenswert.

Betriebswirtschaftliche Maßnahmen haben den Vorteil, dass sie vom Inneren des Unternehmens heraus wirken. Plagiatoren haben dadurch Schwierigkeiten, das Vorgehen der Unternehmen nachzuvollziehen. Die Prozesse des Unternehmens bleiben undurchsichtig. Je mehr Energie die Plagiatoren aufwenden müssen, um Produkt-Know-how und Wissen über das Unternehmen zu erlangen, desto unattraktiver ist es.

Die Logistik ist eine große Schwachstelle des Unternehmens hinsichtlich der Know-how-Sicherheit. Hier gibt es die meisten Schnittstellen. Jede Schnittstelle ist ein Sicherheitsrisiko, da an diesen Stellen der Informationenfluss gestört sein kann. Plagiatoren können sich dort besonders gut einschleusen, um Know-how zu bekommen oder ihre Produkte mit der Originalware zu vermischen. Bei den betriebswirtschaftlichen Maßnahmen kann das Unternehmen durch Auswahl und Einsatz weniger Mittel kein befriedigendes Ergebnis erzielen. Beispielsweise macht eine sorgfältige Lieferantenauswahl keinen Sinn, wenn eine schlecht kontrollierte Lagerlogistik Unbefugten den Eintritt ermöglicht. Alle Logistikbereiche benötigen einzelne Maßnahmen, die aber miteinander verflochten sind.

Unternehmen mit einem engen finanziellen Rahmen sollten ihr Hauptaugenmerk auf den sicheren Vertrieb legen. Kontrollierbare Vertriebsformen sollen das Einschleusen von Fälschungen verhindern. In der Produktion wird das Know-how der Unternehmen umgesetzt, im Vertrieb wird dann das fertige Produkt auf den Markt platziert. Eine kurze Time-to-Market verhindert eine schnelle Nachahmung. Während des Vertriebes können die Produkte zusätzlich durch technische Schutzmaßnahmen gesichert werden. Unternehmen, die ihre Produkte wirkungsvoll schützen wollen, nutzen meist mehrere Sicherheitstechnologien. Da das aber für die Unternehmen höhere Kosten verursacht, versuchen die Hersteller der Sicherheitstechnologien, Kombinationsmöglichkeiten verschiedener Technologien zu entwickeln. Um die verschiedenen Eigenschaften der einzelnen Technologien zu bündeln und synchron die Kosten zu reduzieren, werden beispielsweise Barcodeetiketten oder -drucke durch Zugabe mikroskopischer Kunststoffpartikel zu Sicherheitsetiketten bzw. Drucken mit einem hohen Sicherheitsniveau. Einfache Barcodeetiketten oder Tinten sind andernfalls sehr fälschungsanfällig und im Gegensatz zu den Farbecodes nicht individuell für das Unternehmen. Jeder mit einer Gewerbeanmeldung und zum Teil auch Privatkunden können sie bekommen. Vorteil

der Kombination ist die Möglichkeit der Datenspeicherung. Die mikroskopischen Kunststoffpartikel sind im Bereich der verdeckten Produktkennzeichnung die effektivste Lösung, da hier die Kosten im Gegensatz zu vielen anderen Technologien minimal sind. Simultan zählen sie zu den fälschungssichersten Schutztechnologien. Zusätzlich werden sie vor Gericht bei Haftungsansprüchen zugelassen, was für Unternehmen eine klare Kosten- und Aufwandsreduzierung in der Beweissammlung zur Folge hat.

Hologramme mit Nummerierungen versprechen ebenso eine Datenspeicherung während des Vertriebes bei gleichzeitiger Verifikationsmöglichkeit durch den Endkunden. Sie erreichen aber nicht das Kosten-Nutzen-Verhältnis der oben genannten Kombinationen, da gute, schwer imitierbare Hologramme deutlich teurer sind. Weiterentwicklungen in der RFID können in Zukunft die Datenspeicherung revolutionieren. Momentan besitzen die Transpondertechnologien noch viele Schwachstellen. Sie sind sehr anfällig bei Kontakt mit magnetischen Gegenständen. RFID-Chips können leicht zerstört, entfernt oder manipuliert werden. Entwickler arbeiten an einer stetigen Verbesserung der Technologie. Transponder im Mikrobereich würden beispielsweise eine einfache Entfernung verhindern. Gegen das unberechtigte Lesen von Daten werden Verschlüsslungen eingesetzt. Diese sind aber sehr teuer und wenig standardisiert. Können dort die Kosten deutlich reduziert werden, sind sie im logistischen Bereich die beste Lösung zur Sicherung der Produkte.

Die Kombination sorgfältig aufeinander abgestimmter technischer und betriebswirtschaftlicher Maßnahmen führt zur bestmöglichen Lösung und garantiert eine umfassende Schutzwirkung. Verzichtet das Unternehmen auf diese Kombination und ergreift nur einseitig Maßnahmen, führt das zwangsläufig zu Sicherheitslücken.

Literaturverzeichnis

Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (Hrsg., 2005): Anmerkungen zur Sicherheitslage der deutschen Wirtschaft 2004/2005. Berlin 2006.

Auswertiges Amt (2007): Schengener Übereinkommen. URL: http://www.auswaertigesamt.de/diplo/de/WillkommeninD/EinreiseUndAufenthalt/Schengen.html (Stand: 2007; Zugriff: 15.12.2007).

BaumaschinenOrtung (2007a): GPS Telekomatik Ortung. Fahrtenbuchung. URL: http://www.baumaschinenortung.de/fahrtenbuchg.html (Stand: 2007; Zugriff: 2.01.2008).

BaumaschinenOrtung (2007b): GPS Telekomatik Ortung. Fahrzeugortung. URL: http://www.baumaschinenortung.de/fahrzeugortung.html (Stand: 2007; Zugriff: 2.01.2008).

Beier, J./Bossert, P.C./Brouer, D. et al. (Hrsg., 1991): Produktpiraterie. Verlag TÜV Rheinland, Köln 1991.

Blom, F./Harlander, N. A. (2000): Logistik-Management. Der Aufbau ganzheitlicher Logistikketten in der Theorie und Praxis. 1. Auflage, Expertverlag, Renningen-Malsheim 2000.

Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (Hrsg., 2007): Verbraucherleitfaden. Schutz vor Produkt- und Markenpiraterie. Dortmund 2007.

Bundesdruckerei GmbH (2007): Wertdruck. URL: http://www.bundesdruckerei.de/de/wertdruck/2_4/2_4_3/index.html (Stand: 2007; Zugriff: 12.12.2007).

Bundesministerium der Finanzen (Hrsg., 2006): Gewerblicher Rechtsschutz. Jahresbericht 2006. Berlin 2006.

Bundesverband der Deutschen Industrie e.V. (Hrsg., 2007): Produkt- und Markenpiraterie verhindern. Präventionsstrategien der deutschen Wirtschaft. BDI-Drucksache Nr. 393, Berlin 2007.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Hrsg., 2007): Thesenpapier zur Produktpiraterie. Berlin 2007.

COSYS Ident GmbH (2007): COSYS forciert Softwarelösungen für mobile Datenerfassung. URL: www.cosys.de (Stand: 2007; Zugriff: 13.11.2007).

Dietl, H./Franck, E./Royer, S. (2006): Strategische Wettbewerbsvorteile und Wertschöpfungsorganisation. Konzeptionelle Überlegungen und Gestaltungsempfehlungen zur zwei- und mehrseitige Dienstleistungsmärkte. Universität Zürich, Working Paper No. 63, Zürich 2006.

Deutsche Welle (2007): Counterfeiting Thrives in Expanded EU. URL: http://www.dw-world.de/dw/article/0,2144,1564168,00.html (Stand: 2007; Zugriff: 23.11.2007).

Ehrmann, H. (1999): Logistik. 2. Auflage, Friedrich Kiehl Verlag, 1999.

Fischer, St./Eck, R./Richter, H.-J. (2002): Was sich gegen Produktpiraterie tun lässt. In: Harvard Business Manager (HBM), Ausgabe 1/2002, S. 80-91.

Foerderland (2006): Produkt- und Markenpiraterie. URL: http://www.foerderland.de/1534.0.html (Stand: 2006; Zugriff: 30.10.2007).

Fotorotar AG (2007): Sicherheitsdruck. URL: http://www.fotorotar.ch/produkte/sicherheitsdruck.cfm (Stand: 2007; Zugriff: 6.12.2007).

Friedel, G. (2006): Alles nur gefälscht. In: IHK-Magazin Düsseldorf, Ausgabe 11/2006.

Fuchs, H. J. (2006): Piraten, Fälscher und Kopierer. Strategien und Instrumente zum Schutz gestiegen Eigentums in der Volksrepublik China. 1. Auflage, Gabler Verlag, Wiesbaden 2006.

Gauss (2006): Software Patent. Methods and security label for applying confidential data on a carrier. URL: http://gauss.ffii.org/PatentView/EP1302921. (Stand: 2006, Zugriff: 18.11.2007)

Gienke, H./Kämpfer, R. (2005): Chancen und Risiken von Outsourcing. URL: http://www.ebz-beratungszentrum.de/logistikseiten/stratio/outsourcing.html (Stand: 2005; Zugriff: 16.01.2008)

GS1 Germany GmbH (2007): Tracking & Tracing. URL: http://www.gs1-germany.de/internet/content/projekte/tracing__tracing/index_ger.html (Stand: 2007; Zugriff: 12.12.2007).

Günthner, W.A./Meißner, S. (2006): Logistischer Schutz vor Produktpiraterie. In: Logistics Journal, Ausgabe 11/2006, S. 1-4.

Harke, D. (2000): Ideen schützen lassen? Patente, Marken, Design, Copyright, Werbung. 1. Auflage, Deutscher Taschenbuch Verlag DTV, München 2000.

Herma GmbH (2007): Industrielösungen. URL: http://www.herma.de/cgi-bin/index.cgi?sid=24003414938&action=sparte_e::loesungen_branchen_details&LOESUNGID=13&BEREICHID=4 (Stand: 2007; Zugriff: 18.12.2007).

Holografia Polska agencja monitorowania produktu (2006): Hologramme. URL: www.holografia.pl (Stand: 2006; Zugriff: 21.11.2007).

Hubert, B. (1998): Die Herstellung. Ein Handbuch für die Gestaltung, Technik und Kalkulation von Buch, Zeitschrift und Zeitung. 4., überarbeitete und erweiterte Auflage, K. G. Saur Verlag, München 1998.

Huxold, S. (1990): Marketingforschung und strategische Planung von Produktinnovationen. Ein Früherkennungsansatz. Erich Schmidt Verlag, Berlin 1990.

IHK Köln (2007): IHK-Informationen: RFID-Technologie im Handel. URL: http://www.ihk-koeln.de/Navigation/InnovationUndUmwelt/RFID/index.jsp (Stand: 2007; Zugriff: 12.12.2007).

Informationsdienst des Instituts der deutschen Wirtschaft Köln (2002): Produktpiraterie. Viel heiße Ware. URL: http://www.iwkoeln.de/default.aspx?p=pub&i=963&pn=2&n=n963&m=pub&f=4&a=16351 (Stand: 2002; Zugriff: 29.10.2007).

Kämpf, R. (2005): RFID- Systeme in der logistischen Kette. URL: http://www.ebz-beratungszentrum.de/logistikseiten/artikel/rfid.html (Stand: 2005; Zugriff: 16.01.2008).

Kotler, Ph./Bliemel, F. (2001): Marketing-Management. Analyse, Planung und Verwirklichung. 10. Auflage, Schäffer-Poeschel Verlag, Stuttgart 2001.

Kotzbauer, N. (1992): Erfolgsfaktoren neuer Produkte. Der Einfluss der Innovationshöhe auf den Erfolg technischer Produkte. Peter Lang Europäische Hochschulschriften, Frankfurt am Main 1992.

Landesamt für Verfassungsschutz Baden-Württemberg (Hrsg., 2004): Know-how-Schutz. Handlungsempfehlungen für die gewerbliche Wirtschaft. E. Kurz & Co., Stuttgart 2004.

Landeskriminalamt Baden-Württemberg (2006): Flyer-Sicherheitsmerkmale. URL: http://www.polizei-bw.de/lka/download/falsch_50.pdf (Stand: 2006; Zugriff: 13.12.2007).

Landqart (2004): Sicherheitspapiere. URL: http://www.landqart.com/index.php?id=8&L=0 (Stand: 2004; Zugriff: 12.12.2007).

Lang, K.-H./Schäfer, A. (2007): Produktpiraterie und ihre Bekämpfung durch Innovative Technologien. In: WISO direkt, Dezember 2007.

Lebinger, T. (2007): Volumen und Mehr. Hochregallager. Technische Universität Wien, 2007.

Leierseder, W. (2007): Dell geht indirekt – in Deutschland ab Februar 2008. URL: http://www.channelpartner.de/unternehmenundmaerkte/251832/index2.html (Stand: 2007; Zugriff: 14.12.2007).

LINK Interactive Systems KEG (2003): Wie ein Hologramm entsteht. URL: http://www.is.co.at/hologramme_technik.html (Stand: 2003; Zugriff: 21.11.2007).

Linx Printing Technologies Ltd (2005a): Tinten mit erhöhter Haftfestigkeit. URL: http://www.linxglobal.com/default.asp?p=40&pc=9&pr=29&pt=0 (Stand: 2005; Zugriff: 12.12.2007).

Linx Printing Technologies Ltd (2005b): Lösliche Codiertinten. URL: http://www.linxglobal.com/default.asp?p=40&pc=10&pr=35&pt=0 (Stand: 2005; Zugriff: 12.12.2007).

Linx Printing Technologies Ltd (2005c): Lebensmitteltinten. URL: http://www.linxglobal.com/default.asp?p=40&pc=10&pr=15&pt=0 (Stand: 2005; Zugriff: 12.12.2007).

Linx Printing Technologies Ltd (2005d): Prozesstolerante Tinten. URL: http://www.linxglobal.com/default.asp?p=40&pc=10&pr=36&pt=0 (Stand: 2005; Zugriff: 12.12.2007)

Lutz, A./Koppelmann, U. (1997): Plagiate im Produktdesign. Fördergesellschaft Produkt-Marketing, Köln 1997.

Müller, S./Kornmeier, M. (2000): Marken- und Produktpiraterie. Arbeitspapier der Wirtschaftswissenschaftlichen Fakultät, TU Dresden, Dresdner Beiträge zur Betriebswirtschaftslehre Nr. 37/00, Dresden 2000.

Olgalime (Hrsg., 2001): Wirksame Bekämpfung von Marken- und Produktpiraterie. Ein praktischer Leitfaden für die europäische Investitionsgüter-Industrie. Olgalime-Verbund, Brüssel 2001.

Pfohl, H.-Chr. (2004): Erfolgsfaktor Kooperation in der Logistik. Outsourcing - Beziehungsmanagement – Finanzielle Perfomance. Erich Schmidt Verlag, Berlin 2004.

Podhorsky, P. (2006): Marken- und Produktpiraterie in China. Problem, Kosten und Folgen für ausländische Unternehmen. Fachhochschule für Ökonomie und Management (FOM) Deutschland. 2006.

Saueressig GmbH & Co. KG (2006): Technologie & Verfahrung. URL: http://www.saueressig.de/ (Stand: 2006; Zugriff: 12.12.2007).

SCADPlus (2007): Leitlinien für vertikale Beschränkungen. URL: http://www.euramis.net/scadplus/leg/de/lvb/l26061.htm (Stand: 2007; Zugriff: 7.01.2008).

Schulte, C. (1995): Logistik. Wege zur Optimierung des Materials- und Informationsflusses. 2., überarbeitete und erweiterte Auflage, Verlag Vahlen, München 1995.

Schwenn, K. (2006): Wettbewerb. Die Fußball-WM ist Großkampfzeit gegen Produktpiraten. In: FAZ, Nr. 132/2006, S. 15.

Sepp, V. (2007): Keine Chance den Produktpiraten. URL: http://www.ihk-muenchen.de/.../international/Anhaenge/MBpr_ ventivma_nahme_gegen_produktpiraterie.pdf (Stand: 2007; Zugriff: 16.11.2007).

Sicherheitsforum Baden-Württemberg (Hrsg., 2005): Mit Sicherheit erfolgreich. Erfolgsfaktor Know-how-Schutz. Information und Prävention. Wilhelm Stober GmbH, Eggenstein 2005.

Simons Druck + Vertrieb GmbH (2007): SECUTAG. Nottuln, S. 1-5.

Sonn, H. (2006): Markenrecht und Produktpiraterie im Binnenmarkt. Vortragsreihe beim Symposium „Original und Fälschung“, Wien 2006.

Specht, G. (1992): Distributionsmanagement. 2., überarbeitete und erweiterte Auflage, Kohlhammer Verlag, Stuttgart 1992.

STI – Gustav Stabernack GmbH (2007): Sicherheitsmerkmale auf einen Blick. URL: http://www.sti-group.com/web/content/de_1/news/neue_technologien/Brand_Protection_ Engel_Teufel_2.html (Stand: 2007; Zugriff: 21.11.2007).

Stiassny Papier Grosshandlung GmbH (2007a): Wasserzeichenpapier. URL: http://www.wasserzeichenpapier. at/index.htm (Stand: 2007; Zugriff: 13.12.2007).

Stiassny Papier Grosshandlung GmbH (2007b): Wasserzeichenpapier. Herstellung. URL: http://www.wasserzeichenpapier.at/Herstellung.html (Stand: 2007; Zugriff: 13.12.2007).

Strompen, N. (2007): Innovationsnachrichten. In: IHK Koblenz Newsletter, Ausgabe 7/2007, S. 5.

Südwestrundfunk (2006): Echt Antik. URL: http://www.swr.de/echtantik/2006/10/01/index.html (Stand: 2006; Zugriff: 05.12.2007).

tesa scribos GmbH (2005): Sicherheitstechnologien. URL: http://www.tesa-scribos.de/sicherheitstechnologien/tesa-holospot.htm (Stand: 2005; Zugriff: 19.12.2007).

The tech-faq (2007): Was sind Hologramme?. URL: http://www.tech-faq.com/lang/de/holograms.shtml (Stand: 2007; Zugriff: 21.11.2007).

The WIVA Company-Marmorkönig (2004): Sicherheitspapier. URL: http://www.sicherheitspapier.de/ (Stand: 2004; Zugriff: 13.12.2007).

Thome, R. (2007): Logistische Aufgaben und Prozesse. Grundlagen logistischer Aufgaben. Julius-Maximilians-Universität Würzburg, Betriebswirtschaftliches Institut, Würzburg 2007.

topac MultimediaPrint GmbH (2007): Hologramme als Sicherheits- und Echtheitsnachweis. URL: http://www.topac-holographie.de/3126.0.html (Stand: 2007; Zugriff: 9.12.2007).

Vereinigung zur Bekämpfung von Produktpiraterie e.V. (2006): Vereint in den Kampf gegen Produktpiraterie. URL: http://www.vbp.org/de/main.asp (Stand: 2006; Zugriff: 29.10.2007).

Welser, M. v./González, A. (2007): Marken- und Produktpiraterie. Strategien und Lösungsansätze zu ihrer Bekämpfung. 1. Auflage, WILEY Verlag, Weinheim 2007.

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

Gundula Warnecke

E Quellen illegalen Know-how-Abflusses aus Industrieunternehmen und Strategien gegen Industriespionage

Inhaltsverzeichnis

1 Industriespionage als Reaktion auf den verschärften Wettbewerb ... 255

2 Grundlagen der Industriespionage ... 256

2.1 Begriffserläuterung Industriespionage ... 256

2.2 Abgrenzung zur Wirtschaftsspionage und Competitive Intelligence ... 257

2.3 Gefährdete Unternehmen und Wirtschaftsbranchen ... 258

2.4 Methoden der illegalen Informationsbeschaffung ... 259

2.4.1 Personelle Methoden ... 259

2.4.2 Technische Methoden ... 261

2.5 Methode der offenen Informationsbeschaffung (OSINT) ... 262

2.6 Quantitative und qualitative Bewertung des Schadens ... 263

3 Information und Wissen als Wettbewerbsfaktor und Spionagegut ... 264

3.1 Bedeutung von Information und Wissen für Unternehmen ... 264

3.2 Abgrenzung der Begrifflichkeiten ... 265

3.3 Wissenssystematisierung im Unternehmen ... 267

3.3.1 Implizites und explizites Wissen ... 267

3.3.2 Individuelles und kollektives Wissen ... 268

3.4 Wissensträger im Unternehmen ... 269

4 Quellen illegalen Know-how-Abflusses entlang der Wertkette ... 271

4.1 Das Konzept der Wertkette nach Michael E. Porter ... 271

4.1.1 Idealtypischer Aufbau der Wertkette ... 271

4.1.2 Verknüpfungen innerhalb der Wertkette ... 274

4.1.3 Verknüpfungen mit anderen Wertketten ... 275

4.2 Umgang mit sensiblen Informationen in Industriebetrieben ... 277

4.2.1 Risiken eines illegalen Know-how-Abflusses gemäß der Wertaktivitäten ... 277
4.2.1.1 Risikofelder entsprechend der primären Wertaktivitäten ... 277
4.2.1.2 Risikofelder entsprechend der unterstützenden Wertaktivitäten ... 284
4.2.2 Gefahren durch Vernetzungen und Verknüpfungen ... 290
4.2.2.1 Informationsabflüsse durch Verknüpfungen innerhalb der Wertkette ... 290
4.2.2.2 Informationsabflüsse durch Verknüpfungen mit anderen Wertketten ... 291

5 Strategien zur Vorbeugung und Abwehr von Industriespionage ... 294
5.1 Grundsätze der innerbetrieblichen Spionageabwehr ... 294
5.2 Entwicklung eines integrierten Informationsschutzkonzeptes ... 295
5.3 Personelle Schutzmaßnahmen ... 296
5.3.1 Personalauswahl und -freisetzung ... 296
5.3.2 Personalführung ... 297
5.3.3 Sensibilisierung der Mitarbeiter ... 298
5.3.4 Beschäftigung von Fremdpersonal ... 300
5.4 Organisatorische Schutzmaßnahmen ... 302
5.4.1 Festlegung von Sicherheitsstandards ... 302
5.4.2 Benennung eines Sicherheitsverantwortlichen ... 303
5.4.3 Zuweisung von Zugangs- und Zutrittsrechten ... 304
5.4.4 Durchführung von Kontrollen ... 305
5.5 Technische Schutzmaßnahmen ... 307
5.5.1 Bautechnische Absicherung ... 307
5.5.2 Sicherung der Informations- und Kommunikationstechnik ... 309
5.6 Rechtliche Schutzmaßnahmen ... 311
5.6.1 Geheimhaltungs- und Wettbewerbsvereinbarungen ... 311
5.6.2 Patent- und Lizenzvergaben ... 313
5.7 Schutzmaßnahmen bei der Zusammenarbeit mit Fremdfirmen ... 316

6 Managementempfehlungen zur Spionageabwehr ... 318

7 Gefahren der Industriespionage weiterhin unterschätzt 320

Literaturverzeichnis 322

Anhang: Übersicht Managementempfehlungen 327

1 Industriespionage als Reaktion auf den verschärften Wettbewerb

Die zunehmende Globalisierung der Märkte und die damit einhergehende Verschärfung des Wettbewerbsdrucks machen auch vor Deutschland nicht halt. Im Ringen um Marktanteile sehen sich deutsche Unternehmen, deren Erfolg vorwiegend auf den innovativen Fähigkeiten ihrer Mitarbeiter beruht, zunehmend mit den Mitteln der Industriespionage konfrontiert. So wuchs die Zahl der registrierten Spionagefälle im Jahr 2005 von 2.366 auf 2.990 im Folgejahr, was einem Anstieg von 24,6% entspricht.[1] Dabei ist Spionage nicht mehr länger das alleinige Beschäftigungsfeld von Nachrichtendiensten. Auch immer mehr Unternehmen auf nationaler und internationaler Ebene nehmen davon Gebrauch, um Forschungs- und Entwicklungskosten zu sparen, und verzerren dadurch den Wettbewerb.[2] Die Geschwindigkeit, in der die Generierung neuer Innovationen realisiert wird, erschwert zusätzlich den Erhalt von Wissensvorsprüngen und Wettbewerbsvorteilen.

Die wachsende Bedrohung der deutschen Wirtschaft durch Industriespionage verdeutlicht, wie essentiell eine effiziente Absicherung des unternehmerischen Know-hows zum Schutz der deutschen Pionierstellung in vielen Bereichen der Wirtschaft ist. Der vorliegende Betrag verfolgt aus diesem Grunde zwei Hauptanliegen:

Zunächst sollen durch die Erörterung der charakteristischen Eigenschaften von innovativem Wissen sowie dessen Existenz im betrieblichen Alltag denkbare Quellen eines illegalen Know-how-Abflusses aus Industriebetrieben aufgezeigt werden. Erst die Analyse der Spionageziele, der räumlichen Entstehung und Verarbeitung von Know-how sowie der methodischen Vorgehensweise spionierender Unternehmen gestattet es, ein effizientes Informationsschutzkonzept aus den zahlreichen präventiven Schutzmaßnahmen zu entwickeln.

Anschließend erfolgt eine differenzierte Betrachtung von möglichen Strategien zur Spionageabwehr, die maßvoll und den tatsächlichen Bedrohungen angepasst sind und in konkrete Managementempfehlungen für den Umgang mit Spionagerisiken im Unternehmen münden.

---

[1] Vgl. Corporate Trust (2007), S. 5.

[2] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 14. In diesem Zusammenhang wird zwar von Volkswirtschaften gesprochen, diese Aussage lässt sich aber auch auf einzelne Unternehmen übertragen.

2 Grundlagen der Industriespionage

2.1 Begriffserläuterung Industriespionage

Das Bundesamt für Verfassungsschutz definiert Industriespionage als „Ausforschung, die ein (konkurrierendes) Unternehmen gegen ein anderes betreibt.“[3] In den meisten Fällen handelt es sich dabei um die illegale Beschaffung von betriebsinternen Informationen, wenngleich sich eine klare Abgrenzung zum Konzept der *Competitive Intelligence* als schwierig erweist (Vgl. Abschnitt 2.2).

Die Spionageaktivität der konkurrierenden Unternehmen beschränkt sich dabei nicht allein auf Konkurrenten im engeren Sinne, sondern bezieht sich auf das gesamte Wettbewerbsumfeld, zu dem auch Lieferanten, Abnehmer und Hersteller von Ersatzprodukten zählen.[4] Gerade kleine und mittelständische Unternehmen betreiben oft nur sehr wenig Aufwand, um betriebsinterne Informationen zu schützen, sodass besonders sie von Spionageangriffen betroffen sind.[5]

Ziel einer solchen Spionage ist es, unbemerkt an Informationen zu gelangen, die die Wirtschaftskraft des eigenen Unternehmens verbessern und vor unerwarteten Entwicklungen schützen.[6] Neben Kenntnisse über neue Produkttechnologien können auch Informationen über innovative Produktionsabläufe von Interesse sein. Das methodische Vorgehen ähnelt dabei sehr den Arbeitsweisen der Wirtschaftsspionage, wodurch sich gerade in der Anfangsphase eines Verdachts eine exakte Zuordnung kaum vornehmen lässt (Vgl. Abschnitt 2.2).[7]

Die Bekämpfung von Industriespionage gehört nicht zum Aufgabenbereich der Verfassungsbehörden, obwohl die von der Spionageabwehr empfohlenen Präventivmaßnahmen auch Schutz vor Angriffen konkurrierender Unternehmen bieten.[8] Das Bundesamt für Verfassungsschutz empfiehlt dennoch, bei Verdacht auf Spionage die Behörden zu informieren oder zumindest externe Spezialisten zu Rate zu ziehen, da es in den meisten Unternehmen kaum ausreichend qualifizierte Experten im Bereich der Spionageabwehr gibt.

---

3 Bundesamt für Verfassungsschutz (2006b), S. 2.
4 Vgl. Lux/Peske (2002a), S. 30.
5 Vgl. Corporate Trust (2007), S. 14.
6 Die Erklärung bezieht sich zwar auf Wirtschaftsspionage, lässt sich aber auf Industriespionage ableiten. Vgl. Bundesamt für Verfassungsschutz (2006b), S. 2.
7 Vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 9.
8 ebd.

2.2 Abgrenzung zur Wirtschaftsspionage und Competitive Intelligence

Wirtschaftsspionage ist im Vergleich zur Industriespionage die „staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben."[9] Der Hauptunterschied liegt demzufolge beim Initiator der Spionageaktivität: Während Industriespionage überwiegend von privatwirtschaftlichen Akteuren betrieben wird, fungiert bei der Wirtschaftsspionage der Staat als Auftraggeber.[10]

Die Durchführung der illegalen Informationsbeschaffung erfolgt dabei über Nachrichtendienste, die mit Hilfe geheimdienstlicher Mittel unbemerkt an Informationen über das zu beobachtende Objekt gelangen.[11] Eine einheitliche Zielsetzung gibt es nicht, vielmehr orientieren sich ihre Aufklärungsziele am technologischen Stand und den spezifischen Bedürfnissen der handelnden Staaten.[12] Im Wesentlichen sollen nationale Geheimdienste strategische Überraschungen, die nicht nur wirtschaftlicher, sondern auch militärischer oder politischer Natur sein können, vermeiden und Spionageaktivitäten fremder Nationen abwehren.[13] Besonders seit dem 11. September 2001 treten daher zunehmend militärische Ziele und der Schutz vor dem internationalen Terrorismus in ihr Wirkungsfeld.

Anders als bei der Wirtschaftsspionage ergibt sich die Unterscheidung zwischen Industriespionage und Competitive Intelligence nicht aus dem Spionageinitiator, sondern aus der Legalität der eingesetzten Mittel[14]: Durch die legale Sammlung und Auswertung öffentlich zugänglicher Informationen über konkurrierende Unternehmen und das Wettbewerbsumfeld ist es den Unternehmen möglich, Veränderungen des Marktumfeldes frühzeitig wahrzunehmen, die Aktivitäten von Wettbewerbern zeitnah zu verfolgen, von den Fehlern und Erfolgen der Konkurrenz zu lernen und die eigenen strategischen Ziele, Produkte und Prozesse weiterzuentwickeln.[15] Die Erlangung eines Wissensvorsprungs ist folglich nicht zwangsläufig mit der illegalen Beschaffung von Informationen verbunden. Die richtige Wahl der Informationsmethode und eine ge-

[9] Bundesamt für Verfassungsschutz (2006b), S. 2.
[10] Entsprechend dem Verfassungsschutzbericht gelten die Russische Föderation und die Volksrepublik China als Hauptauftraggeber der Spionageaktivität in Deutschland. Spätestens seit Bekanntwerden der Existenz des Spionagesystems ECHELON rücken aber auch immer mehr westliche Nationen in das Blickfeld des Verfassungsschutzes. Vgl. Bundesministerium des Inneren (2007), S. 254; Harbich (2006), S. 20.
[11] Vgl. Meissinger (2005), S. 7.
[12] Vgl. Bundesamt für Verfassungsschutz (2006b), S. 6.
[13] Vgl. Harbich (2006), S. 4; Ein Beispiel hierfür wäre die Ölkrise von 1973.
[14] Begründer der Competitive Intelligence ist Michael E. Porter. Vgl. Lux/Peske (2002b), S. 16.
[15] Vgl. Brellochs (2000), S. 39.

naue, zielgerichtete Analyse der gewonnenen Erkenntnisse gestatten es Unternehmen, sich auch auf legalem Wege Wettbewerbsvorteile zu verschaffen. Die zunehmende Internationalisierung vieler deutscher Unternehmen führt jedoch zu einer Gradwanderung zwischen Legalität und Illegalität, die nicht zuletzt aus den unterschiedlichen Gesetzgebungen resultiert.

2.3 Gefährdete Unternehmen und Wirtschaftsbranchen

Die Bundesrepublik Deutschland ist als Heimatland vieler technologisch hoch entwickelter Unternehmen und Betriebe ein besonders attraktives Ziel für Spionage. Das Interesse richtet sich dabei hauptsächlich auf so genannte Global Players, Branchenführer und innovative Unternehmen mit herausragendem Know-how.[16] Die Größe des Unternehmens, auf das das Interesse fällt, spielt in diesem Zusammenhang häufig keine Rolle. Es zeigt sich sogar, dass besonders kleine und mittelständische Unternehmen gefährdet sind:[17] Trotz vieler innovativer Ideen und meist führenden Positionen auf dem Weltmarkt mangelt es hier an Sicherheitsvorkehrungen, sodass Spione ein leichtes Spiel haben.[18] Zudem werden immer öfter kleine, „unbedeutende" Zulieferbetriebe zum Zielobjekt der Spionage, da auch sie Informationen über Abläufe, Zustände und Organisationen der eigentlichen Opfer liefern können.[19]

Vor allem forschungsintensive Unternehmen in der Technologiebranche – wie Automobil-, Luftfahrzeug-, Schiffs- und Maschinenbaufirmen – sind stark von unbeabsichtigten Informationsabflüssen betroffen.[20] Aber auch Unternehmen im Bereich der Eisen- und Stahlindustrie sowie der Metall- und Grundstoffverarbeitung bilden laut einer deutschlandweiten Studie der Unternehmensberatung Corporate Trust lohnenswerte Ziele. Eine Übersicht der Untersuchungsergebnisse zeigt Abbildung 1.

Bei Betrachtung der Ergebnisse fällt auf, dass Unternehmen der Chemie- und Pharmaindustrie sowie Banken, Finanzdienstleister und Versicherungen entgegen der Vermutungen nicht in der Studie zu finden sind. Dies ist vermutlich auf die hohe Sensibilität der Branchen zurückzuführen. Aus Furcht vor eventuellen Reputationsverlusten als Resultat des unrechtmäßigen Datentransfers werden Angaben zu Spionagevorfällen in

[16] Vgl. Hummelt (1997), S. 37.
[17] Mit 38,5% bzw. 57,6% sind kleine und mittelständische Unternehmen am häufigsten von Industriespionage betroffen, gefolgt von großen Konzernen mit nur 3,9%. Vgl. Corporate Trust (2007), S. 14.
[18] Vgl. Corporate Trust (2007), S. 14.
[19] Vgl. Hummelt (1997), S. 37.
[20] Vgl. Corporate Trust (2007), S. 15.

diesen Branchen vermieden, sodass es zu einer Verfälschung der Studienergebnisse kommt.[21] Untersuchungen zu Industriespionage sind daher grundsätzlich mit Vorsicht zu genießen.

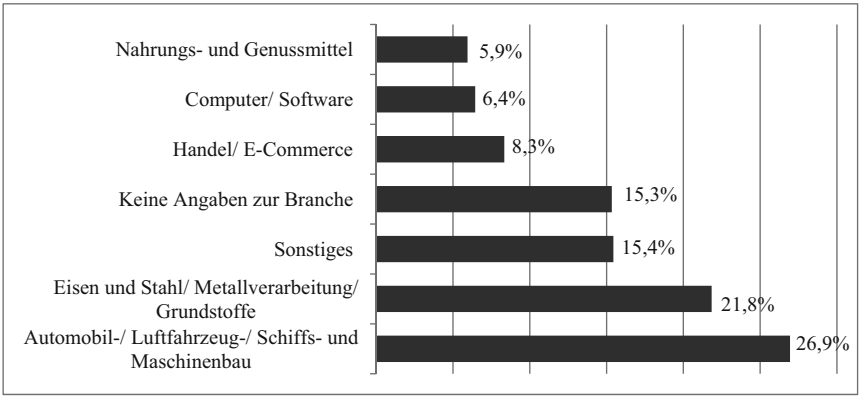


Abbildung 1: Gefährdete Wirtschaftsbranchen
Quelle: eigene Darstellung, in Anlehnung an: Corporate Trust (2007), S. 15.

2.4 Methoden der illegalen Informationsbeschaffung

2.4.1 Personelle Methoden

Die Methoden der illegalen Informationsbeschaffung lassen sich entsprechend der Art des Wissenstransfers in personengebundene und technikgebundene Methoden unterteilen. Wird Wissen mit Hilfe menschlicher Akteure transferiert, spricht man von Human Source Intelligence (HUMINT).[22]

Die Wege der Informationsbeschaffung sind dabei vielfältig. Bereits durch eine einfache Gesprächsabschöpfung ist es möglich, unbedachten Mitarbeitern auf Messen oder sonstigen öffentlichen Veranstaltungen betriebsinterne Informationen zu entlocken, die in den Händen der Konkurrenz großen Schaden anrichten können.[23] Dabei wird die Gutgläubigkeit des Gesprächspartners ebenso wie die Bestrebung vieler Wissenschaft-

[21] Vgl. Corporate Trust (2007), S. 15.
[22] Die Bezeichnungen Human Source Intelligence sowie Technical Intelligence sind hauptsächlich in Zusammenhang mit Wirtschaftsspionage gebräuchlich; durch die inhaltliche Übereinstimmung mit den Methoden der Industriespionage werden die Begrifflichkeiten hier simultan verwendet. Vgl. Meissinger (2005), S. 67ff.
[23] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 30.

ler und Experten, ihr Wissen mit anderen zu teilen, zum Vorteil des spionierenden Unternehmens ausgenutzt.[24]

Eine weit gefährlichere Form der HUMINT beschreibt jedoch die soziale Manipulation (Social Engineering): Unter Vorspiegelung falscher Tatsachen wird hier das persönliche Umfeld der Betroffenen ausspioniert, um im späteren Verlauf der Bekanntschaft in den Besitz geheimer Informationen zu gelangen, die zum Teil zur Durchführung weiterer Spionageaktivitäten genutzt werden. So ist das eigentliche Ziel, das beim Aufbau privater Beziehungen verfolgt wird, die Erlangung von Zugriffsdaten wie Passwörter oder Identifikationen, mit denen dem spionierenden Unternehmen Einblicke in interne Strukturen gewährt werden.[25]

Sowohl bei der Gesprächsabschöpfung als auch bei der sozialen Manipulation ist der bespitzelten Person nicht bewusst, dass sie gerade für die Zwecke anderer Unternehmen missbraucht wird.[26] Aber nicht nur die Gutgläubigkeit oder Geschwätzigkeit mancher Mitarbeiter gefährden das Know-how des Unternehmens, sondern auch die Illoyalität einiger Kollegen, die wissentlich Vertraulichkeitsvereinbarungen durchbrechen.

Die Motive für einen Verrat in den eigenen Reihen sind vielfältig und können finanzieller Natur sein, aber auch im Zusammenhang mit Erpressung oder mit purem Berufsfrust stehen.[27] Eine generelle Eingrenzung der gefährdeten Personen lässt sich nicht vornehmen, da nicht nur Mitarbeiter in höheren Positionen über Zugriff auf Know-how verfügen, sondern es beispielsweise auch für Praktikanten oder Reinigungspersonal oftmals ein Leichtes ist, Papiere zu kopieren und an die Konkurrenz zu leiten.[28] Die eigenen Mitarbeiter bilden generell den größten Unsicherheitsfaktor für Unternehmen und Betriebe, was nicht zuletzt darauf zurückzuführen ist, dass sie zentralen Zugriff auf große Mengen von Informationen haben.[29]

Spione können aber nicht nur unternehmenseigene Mitarbeiter sein, sondern auch Verbündete der Konkurrenz, die in das Unternehmen eingeschleust wurden.[30] Der Ein-

[24] Vgl. Ministerium des Innern und für Sport Rheinland-Pfalz (1997), S. 12.
[25] Bei der Durchführung präventiver Schulungsmaßnahmen sollte jedoch darauf geachtet werden, dass es zu keiner „Angstmacherei“ kommt. Vgl. securitymanager.de (2006), S. 58.
[26] Vgl. Landesamt für Verfassungsschutz Baden-Würtemberg und Bayern (2006), S. 30; Bundesamt für Verfassungsschutz (2006a), S. 17.
[27] Vgl. Bundesamt für Verfassungsschutz (2006a), S. 2.
[28] Vgl. Kaufmann (2007), S. 4.
[29] Vgl. Kaufmann (2007), S. 1; Corporate Trust (2007), S. 8.
[30] Vgl. Harbich (2006), S. 12.

satz eines externen Spions erfordert jedoch einen immensen Zeitaufwand und wird daher in Zusammenhang mit der meist kurzweiligen Industriespionage nicht sehr häufig gesehen.[31] Die größte Schwierigkeit bildet hierbei der Zugriff auf sensibles Material. Als Außenstehender ist der Spion gezwungen, sich zunächst eine entsprechende Position im Unternehmen zu erarbeiten, bevor er das Konkurrenzunternehmen mit interessantem Material beliefern kann.[32]

2.4.2 Technische Methoden

Die Gewinnung von Informationen durch technische Hilfsmittel wird dem gegenüber als Technical Intelligence (TECHINT) bezeichnet.[33] Zu dieser Methode der illegalen Informationsbeschaffung zählt unter anderem das klassische Hacking von Informations- und Telekommunikationssystemen, das Belauschen von vertraulichen Besprechungen und das Abhören von Telefonaten.[34]

Die zunehmende Vernetzung sowohl großer als auch kleiner und mittelständischer Firmen unterstützt das Aufkommen technischer Spionageangriffe.[35] So zeigte die Studie der Corporate Trust, dass bereits 14,9% der befragten Unternehmen einen Schaden durch Hackerangriffe auf das eigene EDV-System erlitten haben.[36] Eine Ursache für diese Verletzlichkeit ist besonders in den rasanten Entwicklungs- und Innovationzyklen zu finden, die es speziell kleinen und mittelständischen Unternehmen schwer machen, im Bereich der technischen Sicherheit immer auf dem neuesten Stand zu bleiben.

Technische Neuerungen können aber nicht nur als Mittel zum Zweck dienen, vielmehr sind sie auch immer häufiger das eigentliche Ziel von Spionageaktivitäten.[37] Die illegale Übermittlung von Wissen erfolgt in diesen Fällen nicht auf elektronischem Wege, sondern durch den bloßen Diebstahl ganzer Hardware wie Notebooks, Handys, Datenträger und sonstige Speichermedien.[38] Der Schaden, der aus der Entwendung dieser zumeist mobilen Endgeräte entsteht, ist kaum vergleichbar mit den finanziellen Ver-

[31] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 9.
[32] Vgl. Harbich (2006), S. 12.
[33] Vgl. Meissinger (2005), S. 67ff.
[34] Vgl. Corporate Trust (2007), S. 19; Mangstl (2005a), S. 64.
[35] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 31ff.
[36] Vgl. Corporate Trust (2007), S. 18.
[37] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 31.
[38] Vgl. securitymanager.de (2006), S. 58; Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 28f.

lusten, die aus dem Abgang der auf ihnen gespeicherten Informationen resultieren.[39] Speziell in Zusammenhang mit der Entwendung technischer Datenträger wie Laptops ist das spionierende Unternehmen auf die Unterstützung durch menschliche Informationsquellen angewiesen. Ebenso wie bei der Weitergabe nicht-technischer Datenträger wie Geschäftsunterlagen zeigt sich auch hier, dass der Erfolg eines technischen Spionageangriffs von menschlicher Beihilfe abhängt und die eigenen Mitarbeiter als größte Schwachstelle im Unternehmen zu bezeichnen sind.

2.5 Methode der offenen Informationsbeschaffung (OSINT)

Die Ausnutzung konspirativer Methoden der Informationsbeschaffung ist jedoch nicht die einzige Möglichkeit, um unbemerkt an Informationen über Konkurrenzunternehmen zu gelangen und somit die eigene Wirtschaftsstärke zu sichern. Auch eine gründliche Auswertung von Daten, die über frei verfügbare Quellen gewonnen werden, gestattet es Unternehmen, sich ein Gesamtbild über das Wettbewerbsumfeld zu machen und somit Wissensvorteile zu generieren. So nutzen viele Unternehmen die Kundenorientierung anderer Firmen, um Rückschlüsse auf deren aktuelles Know-how und zukünftige Projekte zu ziehen.[40]

Die Möglichkeiten der legalen Informationsbeschaffung sind vielfältig. Neben Veröffentlichungen in Fachzeitschriften, Dissertationen und Produktbeschreibungen kann auch der Besuch von öffentlichen Veranstaltungen wie Messen, Kongressen und Symposien einen Überblick über die derzeitige Marktsituation geben.[41] Als wichtigste Informationsquelle der so genannten Open Source Intelligence (OSINT) gilt aber das World Wide Web.

Durch den immer stärker werdenden Konkurrenzkampf zwischen den Unternehmen ist eine angemessene Firmenpräsentation im Internet unabdingbar, um potentielle Kunden auf das eigene Unternehmen und dessen Produkte sowie Dienstleistungen aufmerksam zu machen. Die Online-Präsenz der Firmen gibt aber auch konkurrierenden Unternehmen die Möglichkeit sich zu informieren.[42] So können im Internet veröffentlichte Jobangebote Auskunft über die zukünftigen Aktivitäten der Mitbewerber geben. Zudem

[39] Einer Studie der FBI/CSI zufolge betrugen der Gesamtschaden, der bei den befragten Unternehmen durch diese Form des Know-how-Abflusses zu verzeichnen war, 2005 allein 4.107.300 USD. Vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 43f.

[40] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 29f.

[41] ebd.

[42] Vgl. Harbich (2006), S. 7.

können mit Hilfe von Nachrichtendiensten unter Verwendung der richtigen Schlagwörter binnen Sekunden die wichtigsten Zeitungsmeldungen des Tages in allen unternehmensrelevanten Bereichen gefunden werden.[43]

Der größte Vorteil beim Sammeln frei zugänglicher Informationen liegt in der Legalität der Informationsbeschaffung: Die gewonnenen Erkenntnisse können bei Bedarf an die Öffentlichkeit getragen werden, da der Besuch von offiziellen Events und die Aneignung frei zugänglichen Wissens im weitesten Sinne keine Form der Industriespionage ist.[44] Sie sind vielmehr eine Methode der Competitive Intelligence. Indem das Konzept der Open Source Intelligence mit anderen Formen der Informationsgewinnung – wie der unbemerkten Abschöpfung von Fachgesprächen auf Messen – kombiniert wird, kann diese Möglichkeit der legalen Informationsbeschaffung aber auch als Vorstufe für illegale Aufklärungsaktivitäten dienen.[45]

2.6 Quantitative und qualitative Bewertung des Schadens

Der finanzielle Schaden, der deutschen Unternehmen jährlich durch den unrechtmäßigen Abgang von Know-how entsteht, ist groß. Nach Einschätzung der Corporate Trust beläuft sich die Schadenssumme auf rund 2,8 Mrd. EUR im Jahr.[46] Zu diesem Ergebnis kam die Unternehmensberatung durch ihre 2007 durchgeführte Studie über Industriespionage in der deutschen Wirtschaft. Unter Berücksichtigung des prozentualen Anteils der von Spionage betroffenen Unternehmen und deren Angaben zum finanziellen Umfang des Schadensfalls ergab sich bei Hochrechnung des Ergebnisses auf Gesamtdeutschland ein Schadensbetrag von 2,8 Mrd. EUR. Die tatsächlich durch Industriespionage entstehenden Verluste sind jedoch vermutlich viel höher.

Die größten Probleme, die bei der Quantifizierung des Schadens auftreten, sind zum einen die schwierige Abgrenzung der Begrifflichkeiten.[47] Oft kann nicht genau geklärt werden, ob es sich um Industrie- oder Wirtschaftsspionage handelt, zumal eine Ermittlung des Täterkreises besonders bei Ausspähungen durch technische Hilfsmittel schwer möglich ist. Zusätzlich führt auch die mangelnde Meldebereitschaft betroffener

[43] Vgl. Brellochs (2000), S. 45.
[44] Vgl. Harbich (2006), S. 8.
[45] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 28.
[46] Die Angaben beziehen sich ausschließlich auf Industriespionage. Berücksichtigt wurden nur Unternehmen mit jährlich mindestens 10 Mio. EUR Umsatz bzw. 10 Mitarbeitern. Vgl. Corporate Trust (2007), S. 17.
[47] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 9; Lux/Peske (2002a), S. 102.

Unternehmen zu einer ungenauen Schätzung des Gesamtschadens. Die Gefahr von möglichen Imageverlusten wird als zu groß ermessen, sodass in vielen Fällen weder Polizei noch der Verfassungsschutz informiert wird.[48] Erschwerend kommt hinzu, dass ein großer Teil der illegalen Know-how-Übertragungen überhaupt nicht bemerkt wird.[49]

Der Schaden, der den Unternehmen durch Industriespionage entsteht, lässt sich jedoch nicht allein auf finanzielle Aspekte reduzieren, sondern ist oft auch mit Reputationsverlusten bei den Kunden verbunden. Indem die Abnehmer durch qualitativ minderwertige Kopien das Vertrauen in das Produkt verlieren, gerät der wirtschaftliche Erfolg des Unternehmens in Gefahr. Die daraus resultierende unsichere Arbeitsplatzsituation führt zusätzlich zu Mitarbeiterabwanderungen.[50] Ohne Nachfrage und einen entsprechend qualifizierten Mitarbeiterstamm wird der wirtschaftliche Druck auf das Unternehmen verstärkt. Zusätzlich wird transferiertes Wissen mit der Konkurrenz geteilt und somit Wettbewerbsvorteile eingebüßt. Die daraus resultierenden Nachahmerprodukte und Plagiate steigern außerdem den Wettbewerbsdruck.

3 Information und Wissen als Wettbewerbsfaktor und Spionagegut

3.1 Bedeutung von Information und Wissen für Unternehmen

Die Betrachtung von Wissen und Information als strategischen Wettbewerbsfaktor gewinnt im Zuge der zunehmenden Globalisierung immer mehr an Bedeutung. Staaten wie Deutschland können als Produktionsstandort immer weniger mit so genannten Billiglohnländern mithalten und sind somit auf die innovativen Fähigkeiten ihrer Einwohner angewiesen, um ihre Wirtschaftsstärke zu festigen.[51] Durch die Ungleichverteilung von Information und Wissen zwischen Ländern und Unternehmen ergeben sich Wissensvorsprünge, mit deren Hilfe Wettbewerbsvorteile verwirklicht und gesichert werden können.[52]

[48] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 18; Corporate Trust (2007), S. 22.
[49] Vgl. Corporate Trust (2007), S. 5 und S. 29.
[50] Vgl. Corporate Trust (2007), S. 22.
[51] Vgl. Pawlowsky (1998), S. 10; Bundesverband der Deutschen Industrie e.V. (2006), S. 3.
[52] Vgl. North (2005), S. 59; Rehäuser/Krcmar (1996), S. 14; Marwehe/Weißbach (2000), S. 14.

Eine wesentliche Voraussetzung, die erst die wirtschaftliche Nutzung von Wissenspotenzialen ermöglicht, besteht demzufolge „im Erkennen von wirtschaftlich relevanten Informations- bzw. Wissensunterschieden."[53] Dies geschieht durch die Analyse der unternehmenseigenen Kernkompetenzen. Denn erst eine kritische Beurteilung der individuellen Kompetenzen gibt Auskunft über die Leistungsfähigkeit des Unternehmens und darüber, wo wettbewerbsrelevantes bzw. schützenswertes Know-how liegt.[54]

Anders als von vielen Geschäftsführern angenommen, sind die wichtigsten Geschäftsprozesse eines Unternehmens nicht immer gleichzusetzen mit Prozessen, in denen Kernkompetenz-Know-how zum Einsatz kommt. Allein die Umsetzung von Fähigkeiten, die auch die Konkurrenz hat, ist keine Kernkompetenz. Es gilt vielmehr zu analysieren, was genau das Unternehmen besser kann als alle relevanten Wettbewerber am Markt. Aus der entsprechenden Geschäftsaktivität muss ein für den Kunden wahrnehmbarer Vorteil entstehen, der diesem auch wichtig ist. Zudem sollten Konkurrenzunternehmen sich das Know-how nicht leicht aneignen können, sodass die Nachhaltigkeit des Wettbewerbsvorteils zumindest für einen angemessenen Zeitraum besteht.[55]

Besonders das letzte Kriterium zeigt, dass sich Unternehmen ihrer Stärken und Kompetenzen sehr gut bewusst sein müssen, um diese in entsprechendem Umfang schützen zu können. Da die Realisierung von Wissenspotentialen und Wettbewerbsvorteilen nur unter hohem Einsatz meist knapper finanzieller Mittel erfolgen kann[56], ist das Risiko eines ungewollten Informationsabflusses hoch. Gefahren gehen dabei sowohl von nationalen als auch internationalen Konkurrenten aus, die durch die illegale Wissensbeschaffung Kosten sparen und folglich den Wettbewerb verzerren.[57]

3.2 Abgrenzung der Begrifflichkeiten

Zum effektiven Schutz wettbewerbsrelevanter Wissensbestände ist neben der Ermittlung der Kernkompetenzen auch eine eindeutige Abgrenzung und Identifikation von Information und Wissen sowie die Strukturierung verschiedener Wissensformen zwingend notwendig. Nur so können Schutzmaßnahmen getroffen werden, die individuell an die Besonderheiten der Wissensbestände angepasst sind.

---

[53] Picot (1990), S. 6.
[54] Vgl. Best/Weth (2007), S. 49.
[55] Vgl. Best/Weth (2007), S. 51; Kotler/Bliemel (2001), S. 102.
[56] Vgl. Ernst (2002), S. 293.
[57] Vgl. Corporate Trust (2007), S. 3; Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 14.

Aus betriebswirtschaftlicher Sicht beschreiben Informationen Daten, die in den Kontext eines Problemzusammenhangs gestellt wurden und interpretierbar sind.[58] Daten über Photosynthese bilden für ein Maschinenbauunternehmen beispielsweise keine Information, da diese nicht in Zusammenhang mit der Problemstellung stehen und dementsprechend für das Unternehmen irrelevant sind.[59] Daraus folgt, dass Daten erst durch einen entsprechenden Kontext zu Informationen werden.[60]

Wissen beschreibt dem gegenüber einen Prozess, der aus den persönlichen Überzeugungen eines Menschen resultiert. Es entsteht durch die zweckdienliche Verknüpfung, Verarbeitung und Verankerung von Daten und Informationen im Gehirn.[61] Informationen sind somit eine unerlässliche Voraussetzung zur Generierung von Wissen. Sie werden mit Vorwissen verknüpft und zu Wissen transformiert.[62] Aber erst durch die Notwendigkeit der verarbeiteten Informationen für den Produktionsprozess bzw. die Ergänzung oder Ersetzung bereits vorhandenen Wissens entsteht Wissen im betriebswirtschaftlichen Sinne.[63]

Im Gegensatz zu Daten und Informationen ist Wissen immer personengebunden. Indem es in den Köpfen von Individuen konstruiert wird, repräsentierte es deren subjektiven Erwartungen über Ursache-Wirkungs-Zusammenhänge.[64] Entsprechend dieser Auslegung liegt die Vermutung nahe, dass Wissen selbst nicht speicherbar ist. Denn durch seine Gebundenheit an Einzelpersonen ist eine Übertragung auf Speichermedien wie Computer oder Karteikarten kaum möglich. Stattdessen handelt es sich bei dem auf Datenträgern vermeidlich befindlichen Wissen eigentlich um reine Information.[65] Doch durch die meist hohe Qualität der gespeicherten Informationsbestände kommen diese dem Wissensbegriff recht nah. Die Abgrenzung von Information und Wissen ist dennoch für die Optimierung der Informations- und Wissenssicherheit im Unternehmen unerheblich. Erst durch die Systematisierung des Wissensbegriffes in implizites und explizites Wissen kann eine logische Trennung verschiedener Begrifflichkeiten erfolgen, die tatsächlich dem Schutz von Information und Wissen dient.

[58] Vgl. Rehäuser/Krcmar (1996), S. 5.
[59] Vgl. Marwehe/Weißbach (2000), S. 1.
[60] Vgl. Probst et al. (1999), S. 34; Rehäuser/Krcmar (1996), S. 5.
[61] Vgl. North (2005), S. 40f.
[62] Vgl. Osterloh/Frost (2006), S. 203.
[63] Vgl. Marwehe/Weißbach (2000), S. 2.
[64] Vgl. Probst et al. (1999) S. 44.
[65] Vgl. Fick et al. (2002), S. 12.

3.3 Wissenssystematisierung im Unternehmen

3.3.1 Implizites und explizites Wissen

Die Unterscheidung in explizites und implizites Wissen ist die am häufigsten verwendete Form der Wissenssystematisierung.[66] Explizites Wissen beschreibt dabei bewusst greifbares Wissen, das ohne Probleme sprachlich artikuliert oder schriftlich reproduziert werden kann.[67] Im betrieblichen Alltag wird es durch Datenbanken, Handbücher, Arbeitsanweisungen, technische Zeichnungen oder E-Mails übertragen und vermittelt.[68] Der Fortschritt im Bereich der Informations- und Kommunikationstechnologie begünstigt zusätzlich seine schnelle Verarbeitung und Transferierung.[69]

Explizites Wissen macht jedoch nur einen kleinen Teil des Wissensbestandes in einem Unternehmen aus. Eine viel größere Bedeutung kommt dem impliziten Wissen zugute.[70] Bei implizitem Wissen handelt es sich um unbewusste, personengebundene Kenntnisse, die in ihrer ursprünglichen Form nicht speicherbar sind, da sie im hohen Maße von den subjektiven Erfahrungen, Überzeugungen und vom Vorwissen der jeweiligen Person abhängig sind.[71] Eine authentische Übermittlung von impliziten Wissensbeständen kann aufgrund dessen nur durch einen persönlichen Austausch erfolgen.[72]

Implizites Wissen ermöglicht es, Probleme zu erkennen, diesen nachzugehen und im Verlauf der Problemlösung Zusammenhänge zu erfassen, die bis dato noch nicht wahrgenommen wurden.[73] Es ist somit Voraussetzung für die Generierung von neuem Wissen und Innovationen. Neben intellektuellen Fertigkeiten zählt auch die Beherrschung einer körperlichen Routine wie die komplexe Feinmotorik eines Computertechnikers zu den impliziten Kenntnissen.[74]

Entsprechend der vorangestellten Erläuterungen von impliziten und expliziten Wissen können Tendenzen, die die Methoden der illegalen Informationsbeschaffung betreffen, abgeleitet werden. Da implizites Wissen nur in den „Köpfen" der Mitarbeiter vorhan-

---

[66] Die Differenzierung von Wissen in explizit und implizit wurde maßgeblich Michael Polanyi geprägt. Vgl. North (2005), S. 43; Frost (2005), S. 156.
[67] Vgl. North (2005), S. 43; Best/Weth (2007), S. 204.
[68] Vgl. Frey/Osterloh (2002), S. 60.
[69] Vgl. Picot et al. (2003), S. 73.
[70] Vgl. Frey/Osterloh (2002), S. 36f.
[71] Vgl. Best/Weth (2007), S. 205; Frey/Osterloh (2002), S. 37.
[72] Vgl. Picot et al. (2003), S. 73; Best/Weth (2007), S. 204.
[73] Vgl. Frost (2005), S. 158.
[74] Vgl. Frey/Osterloh (2002), S. 61.

den ist, ist die Arbeit mit menschlichen Kontaktpersonen im Kontext der Industriespionage unumgänglich. Denn erst durch den persönlichen Austausch ist es möglich, sensible Informationen authentisch darzustellen und implizites Wissen zu vermitteln.[75] Daher ist das ausspähende Unternehmen auf die Kooperationsbereitschaft interner Mitarbeiter oder den langwierigen Einsatz betriebsfremder Spione angewiesen. Technische Mittel ermöglichen nur den Zugriff auf explizites, formal verfasstes Wissen, das in geschriebener Form vorhanden oder zumindest verbal erklärbar ist. Tabelle 1 bildet die gewonnenen Erkenntnisse zu den wesentlichen Merkmalen von impliziten und expliziten Wissen ab.

Tabelle 1: Gegenüberstellung explizites und implizites Wissen
Quelle: eigene Darstellung.

Wissensform / Merkmal	explizites Wissen	implizites Wissen
Bewusstsein	bewusst	unbewusst
Übertragung und Speicherung	frei artikulierbar und reproduzierbar, Speicherung durch verschiedene Medien möglich	personengebunden Speicherung
Wissensgehalt	weitestgehend objektiv	weitestgehend subjektiv
Gefahren durch Spionagemethoden	sowohl personen- als auch technikgebundene Spionagemethoden	überwiegend personengebundene Spionagemethoden

3.3.2 Individuelles und kollektives Wissen

Je nach Zugänglichkeit und Anzahl der Wissensträger ist auch eine Differenzierung des Wissensbegriffs in individuelles und kollektives Wissen möglich.[76]

Individuelles Wissen bezeichnet dabei Fähigkeiten und Kenntnisse, die auf den Erfahrungen eines einzelnen Menschen basieren und dementsprechend an eine Einzelperson gebunden sind. Neben impliziten Fertigkeiten zählt beispielsweise auch technisches Fachwissen, das im Rahmen der Geschäftstätigkeit nur einzelnen Mitarbeitern zur Verfügung steht, zum individuellen Wissensbestand eines Menschen.[77]

Durch seinen teilweise expliziten Charakter ist eine Übertragung individuellen Wissens auf andere Organisationsmitglieder prinzipiell möglich. Der Transfer persönlicher Kenntnisse auf eine größere Anzahl Menschen bildet damit die Grundlage für die Ent-

[75] Vgl. Best/Weth (2007), S. 204.
[76] Vgl. North (2005), S. 43.
[77] Vgl. Prange (2002), S. 27.

stehung kollektiven Wissens, das erst durch die effiziente Kombination ehemals individueller Wissensstände generiert wird und dabei mehr als die Summe der Fähigkeiten und Kenntnisse seiner Wissensträger umfasst.[78] Erst die kollektive Nutzung von Wissenspotenzialen ermöglicht es, neue Problemlösungstechniken abzuleiten und somit Wettbewerbsvorteilen zu entwickeln.[79] Daher sind Unternehmen auf einen kontinuierlichen Wissensaustausch angewiesen, um vorhandene Wissensbestände zu nutzen und neues Wissen zu generieren. Speziell die Verarbeitung, Speicherung und Verbreitung von individuell- und kollektiv-explizitem Wissen erfolgt meist über betriebliche Informations- und Telekommunikationssysteme, sodass hier eine besonders große Gefahr von Hacking-Angriffen besteht, die den Tatbestand der Spionage erfüllen. Zum besseren Verständnis bezüglich der Unterscheidung von individuellem und kollektivem Wissen sowie deren Verbindung mit implizitem und explizitem Wissen zeigt Tabelle 2 Beispiele für die Verknüpfungen der betrachteten Wissensformen.

Tabelle 2: Beispiele für die Verknüpfung der betrachteten Wissensformen
Quelle: eigene Darstellung, in Anlehnung an: Klabunde (2003), S. 90.

	individuell	**kollektiv**
implizit	persönliche Erfahrungen, Werte oder Normen, eigene Meinung	Leitlinien oder Verhaltensweisen, die von allen Organisationsmitgliedern geteilt werden, aber nicht dokumentiert sind
explizit	persönliche Aufzeichnungen, passwortgeschützte Dokumente auf dem PC, spezifisches Fachwissen	Standardverfahren oder Stellenbeschreibungen; Fachwissen Einzelner, das nur in Kombination zur Produkterstellung führt

3.4 Wissensträger im Unternehmen

Wie bereits die vorangegangenen Abschnitte deutlich machten, ist neben einer qualitativen Differenzierung des Wissensbegriffs auch eine Aufspaltung von Wissen anhand von Wissensträgern möglich. Der Begriff Wissensträger beschreibt dabei „Objekte, Personen oder Systeme, die in der Lage sind, Wissen zu speichern und zu repräsentieren.“[80] Sie sind immer physischer Natur und können in natürliche und unnatürliche Trägermedien untergliedert werden.

[78] Vgl. Breunung (2007), S. 27; Werner (2004), S. 23.
[79] Vgl. Bodrow/Bergmann (2003), S. 39.
[80] Rehäuser/Krcmar (1996), S. 16.

Zu den natürlichen Wissensträgern im Unternehmen gehören neben einzelnen Individuen auch Gruppen von Organisationsmitgliedern sowie deren Gesamtheit. Sie bilden die Hauptwissensträger im Unternehmen und sind als einziges Trägermedium fähig, Informationen zu transformieren und Wissen aktiv weiterzuentwickeln.[81] Zudem ist die Speicherung und Entwicklung von impliziten Wissenspotenzialen ebenso wie die Nutzung kollektiven Wissens an die Existenz von natürlichen Wissensträgern gebunden.

Tabelle 3: Verbindung der Wissenssystematisierung mit den maßgeblich zuzuordnenden Spionagemaßnahmen
Quelle: eigene Darstellung.

Wissensform	Wissensträger	Spionagemaßnahmen	
individuell-implizit	natürliche	personell:	Anwerben von Mitarbeitern, *soziale Manipulation*
individuell-explizit	natürliche	personell:	Anwerben von Mitarbeitern, Gesprächsabschöpfung, soziale Manipulation
	unnatürliche	personell:	Einsatz von Spionen, Anwerben von Mitarbeitern
		technisch:	Einsatz technischer Hilfsmittel (z.B. Haking), Entwendung unnatürlicher Wissensspeicher
kollektiv-implizit	natürliche	personell:	Einsatz von Spionen, Anwerben von Mitarbeitern
kollektiv-explizit	natürliche	personell:	Einsatz von Spionen, Anwerben von Mitarbeitern, Gesprächsabschöpfung, soziale Manipulation
		technisch:	Einsatz technischer Hilfsmittel (z.B. Lauschangriffe…)
	unnatürliche	personell:	Einsatz von Spionen, Anwerben v. Mitarbeitern
		technisch:	Einsatz technischer Hilfsmittel (z.B. Haking), Entwendung unnatürlicher Wissensspeicher

Unnatürliche Wissensträger können dem gegenüber nur explizites Wissen speichern und sind aufgrund ihrer fehlenden Eigenständigkeit nicht maßgeblich am Transformierungsprozess beteiligt. Sie dienen vielmehr als bloße (Zwischen-)Speicher.[82] Entsprechend der Annahme, dass qualitativ hochwertige Informationen im weitesten Sinne als Wissen anzusehen sind, zählen beispielsweise schriftliche Aufzeichnungen, Dokumente und elektronische Medien sowie Daten-, Methoden- und Modellbanken zu den unnatürlichen Wissensspeichern.

[81] Vgl. Rehäuser/Krcmar (1996), S. 18.
[82] Vgl. Werner (2004), S. 17.

Unter Berücksichtigung der bereits unter den vorangegangenen Abschnitten gewonnenen Erkenntnisse zeigt Tabelle 3 eine Gegenüberstellung der betrachteten Wissensformen, der ihnen entsprechenden Wissensträger sowie der ihnen maßgeblich zuzuordnenden Spionagemaßnahmen. Es wird deutlich, dass lediglich natürliche Wissensträger als Speicher jeder Wissensform geeignet sind. Während individuell-implizites Wissen jedoch von einzelnen Organisationsmitgliedern getragen wird, handelt es sich bei den Trägern von kollektiv-implizitem Wissen um Gruppen innerhalb der Organisation bzw. um das Unternehmen insgesamt. Außerdem verdeutlicht die Gegenüberstellung der Erkenntnisse, dass die Verwendung spezifischer Spionagemaßnahmen nicht nur von der Form des gefährdeten Wissens abhängt, sondern auch von den Wissensträgern, auf denen es gespeichert ist.

4 Quellen illegalen Know-how-Abflusses entlang der Wertkette

4.1 Das Konzept der Wertkette nach Michael E. Porter

4.1.1 Idealtypischer Aufbau der Wertkette

Nachdem in den Kapiteln 2 und 3 die wichtigsten Methoden der illegalen Informationsbeschaffung sowie ihre Anwendung mit Bezugnahme auf die Wissenssystematisierung erläutert wurden, stellt sich nun die Frage, inwieweit Wissen und damit möglicherweise Wettbewerbsvorteile im Unternehmen existieren und wo diese zu finden sind. Eine Möglichkeit der Analyse bietet dabei das Konzept der Wertkette nach Michael E. Porter.[83]

Porter definiert darin das Unternehmen als eine Ansammlung physisch und technologisch unterscheidbarer Geschäftstätigkeiten, die dazu dienen, ein Produkt oder eine Dienstleistung zu entwerfen, herzustellen, zu vertreiben, auszuliefern und zu unterstützen.[84] Zur Veranschaulichung der betrieblichen Zusammenhänge entwickelte er das Abbild einer idealtypischen Unternehmenswertkette, in der allgemein zwischen primären und unterstützenden Wertaktivitäten unterschieden wird. Diese verkörpern die

[83] Michael E. Porter (*1947) ist einer der führenden Ökonomen auf dem Gebiet der Wettbewerbsanalyse und der Nutzung von Wettbewerbsvorteilen. Er verwendet den Begriff „Wertkette“, wobei Wert den Gesamtwert des hergestellten Produkts oder der Dienstleistung beschreibt, während die Wertschöpfung den durch die Bearbeitung in einem Unternehmen zusätzlich geschafften Wert definiert. Zurzeit unterrichtet er an der Harvard Business School. Vgl. Harvard Business School (2007); Porter (1999).

[84] Vgl. Porter (1999), S. 67.

Bausteine, durch die ein Unternehmen ein für den Kunden wertvolles Produkt erzeugt.[85]

Zu den primären Wertaktivitäten zählen Eingangslogistik, Fertigung (Operationen), Ausgangslogistik, Marketing/Vertrieb und Kundendienst. Die eigentliche Erstellung des Produkts sowie dessen Verkauf, die Übermittlung an den Abnehmer und die Kundenbetreuung sind somit Teil des primären Aufgabenkomplexes. Die strategische Bedeutung, die diesen Wertaktivitäten zuteil wird, hängt von der jeweiligen Branche sowie dem Erzeugnis und der Segmentierung des Unternehmens ab. Produzenten von hochwertigen Hightech-Anlagen werden verstärkt auf den Kundendienst achten, während bei Handelsunternehmen der Wareneingang und -ausgang im Vordergrund steht. Unabhängig von der Gewichtung existieren jedoch alle Kategorien der primären Wertaktivitäten bis zu einem gewissen Grad in jedem Unternehmen.[86]

Die unterstützenden Wertaktivitäten dienen zur Aufrechterhaltung der primären Tätigkeiten, indem sie für eine kontinuierliche Verfügbarkeit von Inputs, Technologie, menschlichen Ressourcen und verschiedenen anderen Funktionen sorgen. Sie sind in jedem Geschäftsfeld vorhanden und stehen nicht in unmittelbarem Zusammenhang mit der Leistungserstellung. Neben der Beschaffung, Technologieentwicklung und Personalwirtschaft gehört auch die Unternehmensinfrastruktur zu den sekundären Geschäftsfunktionen. Erstere tragen dabei zum reibungslosen Ablauf einzelner primärer Tätigkeiten bei, während die Unternehmensinfrastruktur die Wertkette in ihrer Gesamtheit unterstützt.[87]

Die Untergliederung des Wertschöpfungsprozesses in primäre und unterstützende Wertaktivitäten sowie in die in Abbildung 2 dargestellten Grundtypen von Tätigkeiten ist jedoch nicht endgültig. Das konkrete Aussehen der Wertkette wird zusätzlich von der Branchenstruktur, der Unternehmensstrategie sowie der Unternehmensgeschichte bestimmt. Eine allgemeingültige Wertkette gibt es folglich nicht.[88] Vielmehr lassen sich die beschriebenen Wertaktivitäten in eine Reihe weiterer Funktionen unterteilen.[89]

[85] Vgl. Porter (1999), S. 65 und S. 68.
[86] Vgl. Porter (1999), S. 71.
[87] Vgl. Porter (1999), S. 69.
[88] Vgl. Porter (1999), S. 65. Das von Porter entwickelte Modell einer Wertkette zeigt vielmehr den idealtypischen Aufbau einer Wertkette (Vgl. Abschnitt 4.1.2).
[89] Vgl. Porter (1999), S. 70f.

Unternehmen der gleichen Branche können dabei zwar ähnliche Wertketten haben, aber erst Unterschiede zwischen ihnen führen zu Wettbewerbsvorteilen.[90]

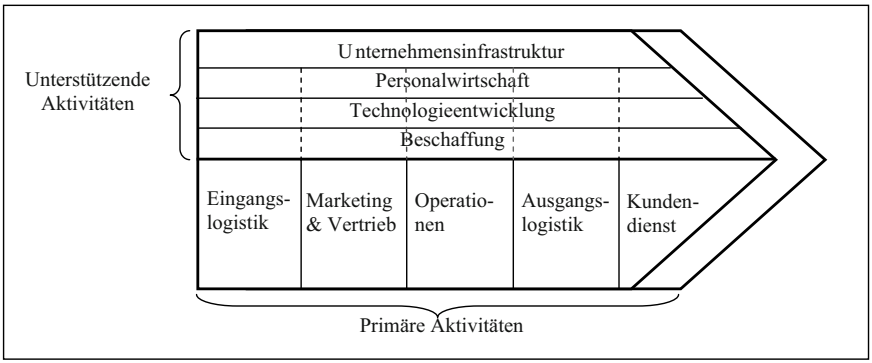


Abbildung 2: Idealtypischer Aufbau der Wertkette nach Porter
Quelle: Porter (1999), S. 66.

Porters Konzept ist ein analytisches Instrument zur Bestimmung dieser Wettbewerbsvorteile und kein Organisationskonzept.[91] Durch die Analyse der Wertaktivitäten zeigt sich, in welchen Bereichen des Unternehmens welche Arten von Informationen liegen und wo diese entstehen. Tatsächlich wird in jeder Wertaktivität Wissen in irgendeiner Form eingesetzt und generiert, um Funktionen zu erfüllen. Dabei kann es sich beispielsweise um Kundendaten im Auftragseingang handeln oder um Leistungsparameter bei Prüfverfahren. Es gilt, den Wert der Informationen für den Unternehmenserfolg zu ermitteln, sodass sie angemessen vor Industriespionage geschützt werden können. Aus welcher Aktivität Wettbewerbsvorteile entstehen, wird vom Unternehmen sowie der Branche, in der das Unternehmen aktiv ist, bestimmt. Vorteile werden nicht aus den Tätigkeiten des Unternehmens selbst generiert, sondern bilden sich aus den überlegenen Fähigkeiten und Wissensvorsprüngen, die ein Unternehmen im Rahmen seiner Wertaktivitäten besitzt.[92]

[90] Eine Differenzierungsbasis können die Segmentierung, der Integrationsgrad, das geografische Umfeld sowie das Branchenfeld bilden. Vgl. Porter (1999), S. 65 und 86f.
[91] Vgl. Porter (1999), S. 63 und S. 93f.
[92] Vgl. Hutzschenreuter (2007), S. 375f.

4.1.2 Verknüpfungen innerhalb der Wertkette

Bei den Wertaktivitäten eines Unternehmens handelt es sich jedoch nicht um eine Ansammlung voneinander unabhängiger Tätigkeiten. Sie sind durch Material- und Informationsflüsse miteinander verbunden und stehen in Wechselwirkung zueinander, was zur Bildung horizontaler Synergien führen kann.[93] Durch die detaillierte Analyse der Unternehmensaktivitäten und ihren Verknüpfungen wird sichtbar, in welchen Teilen des Unternehmens Wissen entsteht, in welchem Rahmen es weiterverarbeitet wird und inwieweit zwischen den Aktivitäten Informationsflüsse existieren.

Die offensichtlichste Verbindung von Wertaktivitäten besteht zwischen primären und unterstützenden Geschäftstätigkeiten.[94] So hat beispielsweise die Personalwirtschaft einen maßgeblichen Einfluss auf die Fertigung und Auftragsabwicklung, indem sie für eine angemessene Verfügbarkeit und Qualifizierung von Mitarbeitern sorgt. Es existieren aber auch Verknüpfungen zwischen den primären und unterstützenden Wertaktivitäten selbst.[95] Wird bereits bei der Herstellung eines Erzeugnisses verstärkt auf die Qualität der Zwischenprodukte geachtet, können Kosten im Kundendienst eingespart werden, da weniger Nacharbeiten erforderlich sind. Durch die Koordination und Optimierung von Tätigkeiten über die Bereichsgrenzen hinaus können demzufolge Wissensvorsprünge und Wettbewerbsvorteile entstehen, die zum Erfolg der Unternehmung beitragen und die langfristige Existenz des Unternehmens sichern.

Die Nutzung solcher Verknüpfungen setzt allerdings entsprechende Informationen und Informationsflüsse voraus.[96] Da eine papierbasierende Informationsübermittlung schnell ihre Grenzen erreicht, sind besonders Unternehmen, die über keinen zentralen Standort verfügen und Informationsströme über größere Distanzen realisieren müssen, auf neue Informationstechnologien angewiesen. Aber auch kleinere Unternehmen nutzen zur Verarbeitung und Verbreitung von Informationen immer häufiger technische Anwendungen wie das Intranet. Daraus ergeben sich nicht nur neue Möglichkeiten, sondern auch Gefahren, die zu einem illegalen Informationsabfluss führen können.

---

[93] Vgl. Porter (1999), S. 80 und S. 409f.; Osterloh (2006), S. 222.
[94] Vgl. Porter (1999), S. 81.
[95] ebd.
[96] Vgl. Porter (1999), S. 82.

4.1.3 Verknüpfungen mit anderen Wertketten

Gemäß Porters Theorie existieren Verknüpfungen aber nicht nur innerhalb einer Wertkette, sondern bestehen auch zu den Wertaktivitäten anderer Unternehmen. Grundlage dieser Annahme bildet die These, dass die Wertkette eines jeden Unternehmens in einem breiten Strom von vor- und nachgelagerten Tätigkeiten integriert ist, der als Wertsystem bezeichnet wird.[97] Bereits durch die Verwendung des Begriffs *Wertkette* wird diese unternehmensübergreifende Sichtweise deutlich, da sich der Wert eines Produkts oder einer Dienstleistung nicht ausschließlich auf die wertschöpfenden Aktivitäten eines Unternehmens reduzieren lässt.[98]

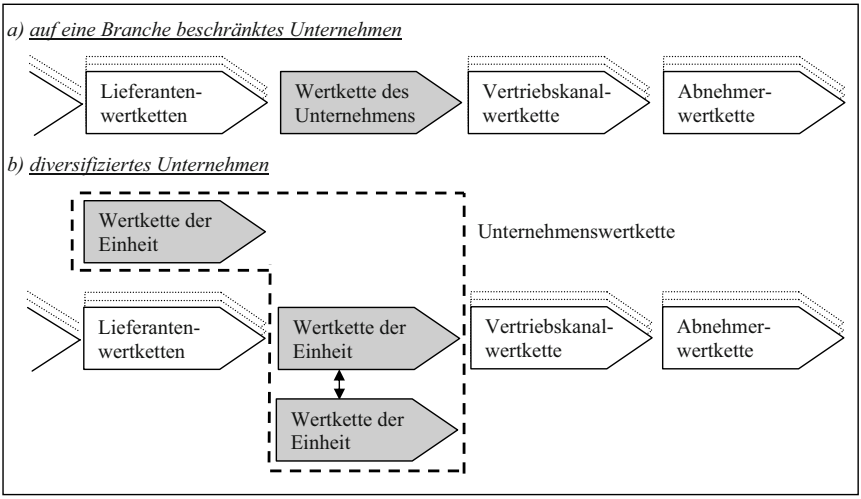


Abbildung 3: Das Wertsystem nach Porter
Quelle: Porter (1999), S. 64.

Zu den vorgelagerten Tätigkeiten zählen beispielsweise die Wertaktivitäten der Lieferanten, mit deren Hilfe die durch das Unternehmen gekauften Inputs geschaffen und geliefert werden.[99] Die Wertketten der Vertriebskanäle und Abnehmer sind demzufolge nachgelagerte Aktivitätskomplexe. Abbildung 3 veranschaulicht diese Systematik, indem sie im oberen Bereich das Wertsystem eines Unternehmens aufzeigt, dessen Tätigkeitsfeld sich auf eine Branche beschränkt. Der untere Teil beschreibt ein diversi-

[97] Vgl. Porter (1999), S. 63.
[98] Vgl. Porter (1999), S. 68.
[99] Vgl. Porter (1999), S. 63.

fiziertes Unternehmen, dessen Wertkette branchenübergreifend in drei Teilketten gliedert ist.

Bereits einfache Wechselwirkungen innerhalb der Wertaktivitäten zweier Ketten führen zu Verknüpfungen zwischen den Unternehmen.[100] Beziehungspunkte dieser Art existieren beispielsweise zwischen den Bereichen Beschaffung und Eingangslogistik eines Unternehmens und dem Auftragssystem eines anderen. Abbildung 4 zeigt in diesem Zusammenhang typische Verknüpfungen, die aus den Beziehungen von Unternehmen und ihrer Lieferanten hervorgehen können. Die optimale Abstimmung dieser Verbindungen ermöglicht den Ausbau zusätzlicher Wettbewerbsvorteile, setzt aber auch eine kontinuierliche Kommunikation und weitreichende Informationsflüsse voraus.[101]

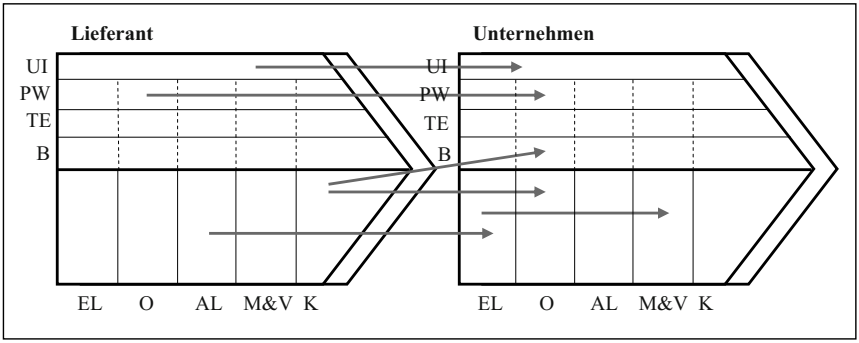


Abbildung 4: Charakteristische Verknüpfungen zwischen den Wertketten eines Unternehmens und seiner Lieferanten
Quelle: eigene Darstellung, in Anlehnung an: Porter (1999), S. 185.

Verknüpfungen können aber auch aus der Arbeitsteilung zwischen einem Unternehmen und seinen Lieferanten, Vertriebskanälen und Abnehmern entstehen.[102] Der Einkauf von unterstützenden Aktivitäten wie Lohn- und Gehaltsabrechnung dient dabei ebenso zur Generierung von Wettbewerbsvorteilen wie der Zukauf von Vorprodukten oder die Übernahme von Marketingfunktionen durch die Vertriebskanäle. So gibt es eine Vielzahl von Verknüpfungsmöglichkeiten, die zu einer Verringerung der eigenen Leistungstiefe führen und eine Konzentration auf die Kernkompetenzen des Unter-

[100] Vgl. Porter (1999), S. 83.
[101] Vgl. Porter (1999), S. 83 und S. 85.
[102] Vgl. Porter (1999), S. 66f. und S. 89.

nehmens ermöglichen. Die zielgerichtete Nutzung solcher Beziehungen kann jedoch nur erfolgen, wenn das Unternehmen sich über seine Kernkompetenzen und die mit ihnen einhergehenden Wissensvorsprünge im Klaren ist, sodass die Gefahr eines Kompetenzverlustes vermieden werden kann.[103] Denn besonders das Outsourcing von vermeintlich unbedeutenden Unternehmensbereichen kann nicht nur zu ungewollten Informationsabflüssen, sondern zum vollständigen Verlust von notwendigem Know-how führen.

Durch die Bildung von Koalitionen werden ebenfalls Verknüpfungen zwischen Unternehmen generiert. Dabei handelt es sich um „langfristige Vereinbarungen zwischen den Unternehmen, die über normale Geschäfte hinausgehen, aber noch keine ausgesprochenen Unternehmenszusammenschlüsse sind."[104] Während die bereits beschriebenen Beziehungen zwischen Kunden und Lieferanten sowie Outsourcing-Partnern als vertikale Kooperationen bezeichnet werden, handelt es sich bei Joint Ventures, virtuellen Unternehmen und strategischen Allianzen um horizontale Kooperationen.[105] Je nach Koalitionsvereinbarung werden einzelne Wertaktivitäten von einer unabhängigen Firma übernommen oder gemeinsam mit ihr abgewickelt.[106] Dies ermöglicht ebenfalls die Generierung von Wettbewerbsvorteilen, ist aber ähnlich wie das Outsourcing mit der Weitergabe sensibler Informationen verbunden und kann daher zu spionagewirtschaftlichen Aktivitäten führen.

4.2 Umgang mit sensiblen Informationen in Industriebetrieben

4.2.1 Risiken eines illegalen Know-how-Abflusses gemäß der Wertaktivitäten

4.2.1.1 Risikofelder entsprechend der primären Wertaktivitäten

Um besondere Risikofelder eines illegalen Know-how-Abflusses entlang der Wertschöpfungskette aufdecken zu können, soll nun systematisch analysiert werden, in welchem Umfang die verschiedenen Wissensformen aus Abschnitt 3.3 in den einzelnen Wertaktivitäten eines Unternehmens vorhanden sind. Ziel ist es, Tendenzen für den Einsatz von gesetzwidrigen Informationsbeschaffungsmethoden zu erkennen, so-

[103] Vgl. Osterloh (2006), S. 225.
[104] Porter (1999), S. 91.
[105] Vgl. Arndt (2006), S. 177.
[106] Vgl. Porter (1999), S. 91.

dass daraus im späteren Verlauf Handlungsempfehlungen für das Management abgeleitet werden können.

a) Eingangslogistik

Die Eingangslogistik definiert die erste primäre Wertaktivität im Wertschöpfungsprozess eines Unternehmens und umfasst alle Tätigkeiten, die im Zusammenhang mit dem Empfang, der Lagerung und der Verteilung von Betriebsmitteln für die Leistungserstellung stehen.[107] Sie ist somit für den Materialfluss innerhalb des Betriebes sowie für die Eingangsprüfung, Lagerhaltung und Bestandskontrolle verantwortlich.

Besonders Wissen, das im Rahmen neuer Transport-, Lager- und Konservierungstechnologien entwickelt wurde, bildet ein interessantes Spionagegut. Durch die Optimierung der Eingangslogistik ist es möglich, interne Lieferprozesse zu verbessern und Wettbewerbsvorteile zu generieren, die auch für andere Unternehmen von Bedeutung sind. Aus diesem Grund sollten innovative Logistiksysteme zum Erhalt der eigenen Wettbewerbsfähigkeit geschützt werden muss.

Neben herausragendem Know-how im Bereich des Lagermanagements können aber auch Zu- und Abgangsstatistiken in das Interessenfeld von spionierenden Unternehmen rücken. Diese geben Aufschluss über die Fertigung sowie einzelne Produktmerkmale. Anhand von Lieferscheinen kann beispielsweise analysiert werden, welche Inputs zur Verwirklichung innovativer Erzeugnisse benötigt werden. Desweiteren können Prüfprotokolle Informationen über die Qualität der gelieferten Ware geben, sodass daraus Rückschlüsse über das Niveau der Lieferunternehmen gewonnen werden können.

Zur Ausübung eingangslogistischer Tätigkeiten wird folglich überwiegend kollektiv-explizites Wissen benötigt, das etwa auf Lieferscheinen und Prüfprotokollen fixiert und durch Eingangsbuchungen und Lagerpläne im Informationssystem gespeichert wird.[108] Darüber hinaus sind kognitiv-implizite Fähigkeiten zur Koordination der Lagerhaltung und Materialtransporte erforderlich.

Da hauptsächlich Liefer- und Lieferantendaten sowie Informationen zur Optimierung von Lagerhaltungs- und Materialtransportsystemen im Fokus spionierender Unternehmen stehen, können illegale Informationsabflüsse sowohl durch personelle, als

[107] Vgl. Porter (1999), S. 70.
[108] „Kollektiv“ ist dabei auf den Bereich bezogen und nicht auf das gesamte Unternehmen.

auch technische Spionagemethoden verursacht werden. Beispiele hierfür wären das Eindringen in IT-Systeme oder der Diebstahl von Daten durch Externe, die sich z.T. unter Vorspiegelung falscher Tatsachen (Social Engineering) Zutritt zum Firmengelände verschaffen.

b) Operationen

Die operativen Tätigkeiten eines Industriebetriebes sind gleichzusetzen mit den Funktionen der Fertigung und beschreiben alle Aktivitäten, die sich mit der Be- und Verarbeitung der Inputs zu Output befassen.[109] Besonders Unternehmen, deren Kernkompetenzen aus den innovativen Fähigkeiten der Forschungs- und Entwicklungsabteilungen gewonnen werden, sind in diesem Bereich stark von Industriespionage betroffen, da hier die neuen Produktideen verarbeitet werden.[110] Ebenso können aber auch Informationen über ein neuartiges oder kostengünstiges Herstellungsverfahren von Interesse sein.

In jedem Fall ist implizites und explizites Wissen gleichermaßen für den Leistungserstellungsprozess notwendig, weil erst die Verknüpfung von formal fixierbarem Know-how und den individuell-impliziten Fähigkeiten der Mitarbeiter eine Produktrealisierung möglich macht. Implizites Wissen bezieht sich dabei nicht nur auf die körperlichen Fertigkeiten einer Person, zu denen physische Kraft oder eine Begabung im Bereich der Feinmotorik zählen, sondern meint auch die Fähigkeit, die eigenen Erfahrungen mit neuem Wissen zu verbinden, um Probleme zu beseitigen, die sich aus neuen Produkten und Produktionstechnologien ergeben.

Die Gleichverteilung von implizitem und explizitem Wissen hat zur Folge, dass auch technische und personelle Spionagemaßnahmen im gleichen Umfang zum Einsatz kommen. Speziell durch den Diebstahl von Konstruktionsunterlagen und Produkten sowie durch die Illoyalität von Mitarbeitern können Informationen über das Erzeugnis abgezogen werden. Aber auch Firmenbesichtigungen werden unter Verwendung von technischen Hilfsmitteln genutzt, um beispielsweise Produktionssoftware zu stehlen oder Einblicke in Fertigungsstraßen zu erhalten.

[109] Vgl. Porter (1999), S. 70.
[110] Vgl. Corporate Trust (2007), S. 21.

c) Ausgangslogistik

Die Ausgangslogistik ist das Gegenstück der Eingangslogistik und folgt der Produktion. Sie beinhaltet alle Tätigkeiten, die im Zusammenhang mit der Sammlung, Lagerung und anschließenden Verteilung der hergestellten Ware an den Abnehmer stehen.[111] Informationen, die hierfür genutzt werden, beinhalten beispielsweise Angaben zu den Verbrauchs- und Bestandsdaten der Abnehmer. Auf ihrer Grundlage werden vom Vertrieb Statistiken erarbeitet, die Aufschluss über die Produkte und Neuentwicklungen der weiterverarbeitenden Kunden geben. Im Falle eines illegalen Informationsabflusses führt dies zwar nicht zu Schäden im eigenen Unternehmen, verursacht aber bei Bekanntwerden Reputations- und Vertrauensverluste.

Neben Kundenstammdaten können auch Auskünfte über innovative Ausgangslogistiksysteme in das Interessenfeld spionierender Firmen treten. Besonders bei Unternehmen, deren Kernkompetenzen weniger in der Produktion und mehr in der weltweiten und zeitnahen Belieferung verstreuter Abnehmer liegen, ist die Gefahr einer Ausspähung groß.

Aus diesem Grund ist die Verteilung der Wissensbestände nur in Abhängigkeit von dem jeweiligen Unternehmen zu sehen. In kleinen Zulieferbetrieben reicht zur Koordination einfacher Logistikprozesse die Existenz von kollektiv-explizitem Wissen aus, um einzelne Großkunden optimal beliefern zu können. Wissensträger sind hierbei u.a. Lieferverträge, Lieferpläne, computergestützte Informationssysteme sowie schriftlich fixierte Handlungsanweisungen. Unternehmen, die im Rahmen der Globalisierung aber weltweite Kundenbeziehungen pflegen, sind auch auf die kognitiv-impliziten Fähigkeiten ihrer Logistikmitarbeiter angewiesen.

Ausgeklügelte Logistiksysteme können somit nicht durch den Diebstahl physischer Datenträger in ihrer Gesamtheit verstanden werden. Erst der Einsatz eingeschleuster Spione oder illoyaler Mitarbeiter sowie das Hacking von ganzen IT-Systemen ermöglichen die Erfassung globaler Zusammenhänge. Sind jedoch Kundendaten das eigentliche Spionageziel, genügt die Entwendung von Informationen durch das Kopieren von Lieferverträgen oder Lieferpapieren, um im Zielobjekt Schäden in Millionenhöhe anzurichten.

[111] Vgl. Porter (1999), S. 71.

d) Marketing und Vertrieb

Die Bereiche Marketing und Vertrieb beschäftigen sich mit allen Prozessen, die den Verkauf eines Produktes fördern. Neben der klassischen Werbung, Verkaufsförderung und Angebotspromotion umfassen sie auch den Verkaufsaußendienst sowie die Wahl und Pflege der Vertriebswege.[112]

Entgegen den Vermutungen zeigte die Studie der Corporate Trust, dass der Vertrieb eines Unternehmens am Stärksten von illegalen Informationsabflüssen betroffen ist und nicht, wie angenommen, die Forschungs- und Entwicklungsabteilungen.[113] Es gilt als selbstverständlich, neue Produktideen und Design-Studien vor fremden Zugriffen zu schützen. Dabei wird häufig übersehen, dass auch Informationen über Kunden- und Vertreternetzwerke sowie Produktangebote und die Strukturierung von Distributionskanälen besonders für Konkurrenten im näheren Umfeld von Interesse sind.[114]

Neben explizitem Hintergrundwissen über Kunden- und Marktanforderungen sind speziell implizite Fähigkeiten bei der Entwicklung neuer Marketing- und Vertriebskonzepte erforderlich. Durch die Externalisierung impliziten Wissens und dessen Kombination mit expliziten Erkenntnissen aus Marktanalysen können Konzepte und gemeinsame Zielvorstellungen bezüglich der Kundenansprache erarbeitet werden.[115] Auch im direkten Vertrieb sind neben Fachwissen über spezifische Produkteigenschaften individuell-implizite Fähigkeiten wie Freundlichkeit, höfliche Umgangsformen und Überzeugungskraft im Rahmen der Kundenorientierung und Kundenbindung von Nutzen.

Durch die große Bedeutung der impliziten Wissensbestände ist die Gefahr der Abwerbung von fähigen Mitarbeitern hoch. Umsatzstatistiken können ausgekundschaftet werden und Auskunft über den wirtschaftlichen Erfolg einzelner Organisationsmitglieder geben. Externalisiertes Wissen, das mit Hilfe von Projektdatenbanken, Notizen oder Skizzen dokumentiert wird, ist ebenfalls vor Diebstählen nicht gefeit, sodass die Einmaligkeit von Marketingkonzepten gefährdet ist. Aber auch die Marketingmaßnahmen selbst können durch einen zu freizügigen Umgang mit Informationen zur Open Source Intelligence führen.

[112] Vgl. Porter (1999), S. 71.
[113] Vgl. Corporate Trust (2007), S. 21.
[114] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 27.
[115] Externalisierung beschreibt die Übertragung von impliziten Wissen zu expliziten. Vgl. Osterloh/Frost (2006), S. 206.

e) Kundendienst

Als letzte primäre Wertaktivität ist der Kundendienst mindestens gleichermaßen von Industriespionage betroffen wie der Vertrieb. Er beinhaltet alle Maßnahmen, die mit der Förderungen und Werthaltung eines Produktes nach dessen Verkauf in Verbindung stehen. Dazu zählen Wartungsarbeiten, Reparaturdienste, Ersatzteillieferungen und Produktanpassungen sowie Dienstleistungen, die die Ausbildung der Abnehmer im Umgang mit dem Produkt sowie dessen Nutzung zum Gegenstand haben.[116] Der Kundendienst ist folglich als Teil des Marketings zu sehen, weil er durch zusätzliche Serviceangebote die Kundenbindung fördert.[117]

Speziell Produkte und Dienstleistungen, welche die materiell angebotenen Erzeugnisse ergänzen oder unterstützen, stellen einen Wettbewerbsvorteil dar, den es zu schützen gilt. Interessenfelder für spionierende Unternehmen können demnach das vorhandene Angebot an Zusatzleistungen sowie Informationen über Produkte und Ersatzteile sein. Diese werden zwar in der Konstruktionsabteilung generiert, aber von der Fertigung und Kundenbetreuung realisiert.

Generell setzt ein wettbewerbsfähiger Kundendienst gleichermaßen explizites und implizites Wissen voraus, da erst die Kombination von detailliertem Fachwissen mit den individuell-kognitiven Fähigkeiten der Mitarbeiter zu Problemlösungen führen. Durch das Erkennen von Ursache-Wirkungs-Zusammenhängen können Fehlerquellen aufgedeckt werden, die ohne entsprechendes Know-how verborgen blieben. Zusätzlich haben kollektiv-implizite Werte wie Pünktlichkeit und Zuverlässigkeit großen Einfluss auf das Unternehmensimage und die Kundenzufriedenheit, sodass auch sie als wettbewerbsrelevanter Bestandteil des Kundendiensts gelten.

Die individuellen Abnehmerbedürfnisse sowie die fallspezifischen Lösungsansätze haben zur Folge, dass im Service überwiegend Menschen als Träger von schutzbedürftigem Wissen fungieren. Nur sie können situationsabhängig handeln und auf spezifische Problemfelder eingehen. Dies führt dazu, dass meist personelle Spionagemaßnahmen wie die einfache Gesprächsabschöpfung oder die soziale Manipulation zur illegalen Informationsbeschaffung genutzt werden. Bereits die gründliche Einweisung in die Besonderheiten des Produkts, die im Rahmen von Kundendienstleistungen verwirklicht wird, kann Informationen freigeben. Es sind Fälle bekannt, in denen Firmen

[116] Vgl. Porter (1999), S. 71.
[117] Vgl. Kotler et al. (2003), S. 654.

ihre Mitarbeiter dazu veranlassten, Konkurrenzprodukte zu erwerben, um im Rahmen des Kundendienstes detaillierte Informationen über das Produkt, Dienstleistungsangebote sowie Serviceprozesse zu erhalten.[118] Aber auch Handbücher und Gebrauchsanweisungen, die ebenfalls zur Werterhaltung des Produktes beitragen, sind Wissensträger und können als Informationsquelle dienen. Dabei handelt es sich jedoch um keine illegale Spionageaktivität.

Die Erkenntnisse aus der Risikoanalyse im Bereich der primären Wertaktivitäten werden in Tabelle 4 noch einmal zusammengefasst. Dazu werden neben den maßgeblichen Wissensformen Beispiele für Wissen und Wissensträger genannt sowie daraus resultierende Spionagemethoden.

Tabelle 4: Wissen in den primären Wertaktivitäten
Quelle: eigene Darstellung.

>> Eingangslogistik:

Wissensform	*Wissen/Wissensträger*	*Spionagemethode*
überwiegend kollektiv-explizit	Logistiksysteme, Lieferscheine, Prüfprotokolle, Lagerpläne, Mitarbeiter…	Diebstahl von Speichermedien (in Verbindung mit Social Engineering), Hacking, eigene Mitarbeiter
z.T. implizit (kognitiv)	Mitarbeiter (Koordination von Lager/ Transport)	An- bzw. Abwerben interner Mitarbeiter (Illoyalität, eher selten)

>> Operationen:

Wissensform	*Wissen/Wissensträger*	*Spionagemethode*
kollektiv-explizit	Herstellungsverfahren, Produkte (Stücklisten, Ablaufpläne, Software, Mitarbeiter)	Einsatz von Spionen, Anwerben interner Mitarbeiter, Diebstahl, Social Engineering, Einsatz technischer Hilfsmittel
individuell-implizit	Mitarbeiter (kognitiv und physisch)	Anwerben interner Mitarbeiter (Erpressung, Bestechung…)

>> Ausgangslogistik:

Wissensform	*Wissen/Wissensträger*	*Spionagemethode*
überwiegend explizit	Verträge, Lieferpläne, Lieferpapiere, IT, Mitarbeiter, Handlungsanweisungen…	Anwerben von Mitarbeitern, Einsatz von Spionen, Diebstahl von Speichermedien, Hacking
individuell-implizit	Mitarbeiter (koordinierende Fähigkeiten)	An- bzw. Abwerben interner Mitarbeiter

>> Marketing & Vertrieb:

Wissensform	*Wissen/Wissensträger*	*Spionagemethode*
überwiegend implizit	Mitarbeiter, Projektgruppen (Nutzung kognitiver Fähigkeiten für Konzepte)	Anwerben interner Mitarbeiter, soziale Manipulation (Gesprächsabschöpfung)

[118] Vgl. Kaufmann (2007), S. 5.

>> Marketing & Vertrieb:

Wissensform	*Wissen/Wissensträger*	*Spionagemethode*
z.T. explizit	Vertreternetzpläne, Markt- und Kundenanalysen, externalisiertes Know-how (Skizzen, IT…)	Diebstahl von Speichermedien, Gesprächsabschöpfung, Hacking, Anwerben interner Mitarbeiter, Einsatz von Spionen

>> Kundendienst:

Wissensform	*Wissen/Wissensträger*	*Spionagemethode*
explizit	Kundendienstler (Wissen über Produkte und Anwendung, Zusatzangebote)	Gesprächsabschöpfung, soziale Manipulation, Anwerben interner Mitarbeiter, (Open Ressource Intelligence)
implizit	Mitarbeiter (kognitiv), Unternehmenskultur	Anwerben interner Mitarbeiter, Einsatz von Spionen

4.2.1.2 Risikofelder entsprechend der unterstützenden Wertaktivitäten

Die unterstützenden Wertaktivitäten sind nicht unmittelbar am Leistungserstellungsprozess beteiligt und geben daher nur indirekt Auskunft über Informationen, die das Produkt selbst betreffen. Wie bereits Abschnitt 3.1 – „Bedeutung von Information und Wissen für Unternehmen“ – verdeutlichte, können aber auch sie Kernkompetenz-Know-how enthalten und somit Wettbewerbsvorteile generieren. Es stellt sich nun die Frage, inwieweit wettbewerbsrelevantes Wissen auch in den unterstützenden Wertaktivitäten vorhanden ist und welche Gefahren sich daraus ergeben.

a) Personalwirtschaft

Die Personalwirtschaft umfasst alle Tätigkeiten und Prozesse, die sich mit der Rekrutierung, Einstellung, Entwicklung und Entschädigung von Mitarbeitern befassen.[119] Anders als allgemein angenommen wird, beschränken sich diese Aktivitäten nicht nur auf das Handlungsfeld einer Organisationseinheit, sondern sind im ganzen Unternehmen verteilt. Aus diesem Grund ist die Definition eines eindeutigen Risikobereiches nicht möglich.

Speziell Informationen auf dem Gebiet der Personalentwicklung und Personalbeschaffung sind für spionierende Unternehmen von Interesse. Diese können indirekt Aufschluss über die zukünftigen Vorhaben der Konkurrenz geben und somit vor wirtschaftlichen Überraschungen schützen.

[119] Vgl. Porter (1999), S. 74.

Entsprechend der Annahme, dass besonders die eigenen Mitarbeiter Ursache von illegalen Informationsabflüssen sind, fungieren Angriffe auf das Personalwesen jedoch oft nur als Ausgangspunkt für weitere Spionageaktivitäten.[120] Mit Hilfe von Mitarbeiterdaten können Zuständigkeiten analysiert und eine geeignete Ansprache bestimmt werden. Arbeits- und Führungskräfte, die das Bekanntwerden persönlicher Schwierigkeiten lieber vermeiden möchten, lassen sich leicht erpressen und können so für die Zwecke des Konkurrenzunternehmens genutzt werden. Zudem können auch finanzielle Anreize Mitarbeiter dazu verleiten, betriebsinterne Informationen weiterzugeben. Das Personalwesen ist somit nicht nur Ziel der Spionage, sondern kann auch ein Mittel von illegalen Informationsbeschaffungsmaßnahmen sein.

Im Allgemeinen arbeitet die Personalwirtschaft überwiegend mit expliziten Wissensbeständen. Im Rahmen der Personaleinstellung und -freisetzung ist beispielsweise die Existenz von rechtlichem Know-how unabdingbar, während bei der Rekrutierung von qualifizierten Mitarbeitern fundierte Kenntnisse bezüglich der Methoden der Personalbeschaffung ausschlaggebend sind. Implizite Fähigkeiten werden insbesondere bei Einstellungsgesprächen oder bei der Durchführung von Eignungstest benötigt, da anhand kollektiver Normen und Vorstellungen geprüft wird, ob der entsprechende Kandidat in das Team passt oder sozial ungeeignet ist.

Spionagemöglichkeiten, die sich aus der Reproduzierbarkeit der personalwirtschaftlichen Wissensbestände ergeben, sind beispielsweise das Hacking von IT-Systemen sowie der physische Diebstahl von Informationen. Auf diese Weise können Mitarbeiterdaten, die weiterführende Spionageaktivitäten erlauben oder zumindest unterstützen, in den Besitz von Konkurrenzunternehmen gelangen. Ebenso können mittels sozialer Manipulation telefonisch Auskünfte über einzelne Mitarbeiter eingeholt werden oder durch so genannte Head-Hunter-Anrufe Informationen abfließen. Letztere haben dabei das Ziel, Personal mit besonderem Know-how abzuwerben und werden daher von den meisten Unternehmen grundsätzlich abgewiesen.[121]

b) Technologieentwicklung

Die Technologieentwicklung befasst sich demgegenüber mit Aktivitäten, die zur Generierung neuer Produkt- und Verfahrensideen sowie zur Bildung von innovativem Know-how führen. Sie lässt sich somit keinesfalls auf den Begriff der F&E reduzieren,

[120] Vgl. Corporate Trust (2007), S. 21; Bundesamt für Verfassungsschutz (2006a), S. 13ff.
[121] Vgl. Corporate Trust (2007), S. 21.

da diese Sichtweise alle Neuerungen, die nicht in direktem Zusammenhang mit der Produktion und dem Produkt selbst stehen, ausschließen würde.[122] Technologien können sich neben dem operativen Teil eines Unternehmens auch auf andere Bereiche der Wertkette beziehen. Beispiele hierfür wären Lager- und Konservierungstechniken in der Logistik, Medientechnologien im Marketing oder IT-Systeme, die unternehmensübergreifend zum Einsatz kommen.[123]

Da Neuentwicklungen prinzipiell Grundvoraussetzung für die Generierung von Wettbewerbsvorteilen sind, ist jede Art von Information, die die Forschungsergebnisse der Konkurrenz betrifft, für spionierende Unternehmen interessant. Besondere Risikofelder können folglich nicht definiert werden. Vielmehr sind die individuell-impliziten Fähigkeiten der Wissenschaftler und Konstrukteure ausschlaggebend und somit das wichtigste Gut für die Realisierung von Technologieentwicklungen. Vorhandene implizite Wissensbestände werden miteinander verknüpft und führen zur Bildung neuen Know-hows. Die Externalisierung und Fixierung von innovativem Wissen in computergestützten Modellen, auf Skizzen oder in Notizen hat jedoch zur Folge, dass technische Angriffe möglich sind. Die meisten Unternehmen legen jedoch großen Wert auf die Sicherheit ihrer Forschungsabteilung, sodass fremde Zugriffe weitestgehend ausgeschlossen werden können und eher die eigenen Mitarbeiter Ursache von irregulären Informationsabflüssen sind. Diese werden teils wissentlich als Spione eingesetzt, in anderen Fällen ist ihnen aber nicht bewusst, dass sie als Informationsquelle missbraucht werden. Ein Beispiel hierfür wären Gesprächsabschöpfungen auf öffentlichen Veranstaltungen wie Messen. Wissenschaftler neigen dazu, ihr Wissen mit anderen teilen zu wollen, was von konkurrierenden Unternehmen ausgenutzt wird.

Neuentwicklungen, die sich aus der praktischen Umsetzung von Arbeitsprozessen ergeben, werden weniger geschützt. Ursachen hierfür liegen hauptsächlich im fehlenden Erkennen von schützenswertem Know-how. Unternehmen nehmen nicht wahr, dass beispielsweise ein neu gestaltetes Lagersystem, durch das Zeitersparnisse geschaffen und Tätigkeiten in der Beschaffung vereinfacht werden, auch das Interesse anderer Unternehmen weckt. Aus diesem Grund sind besonders solche Technologien von vielen Arten der Industriespionage bedroht. Neben den bereits oben beschriebenen Möglichkeiten können neu gewonnene Erkenntnisse auch durch Social Engineering, Hacking, eingeschleuste Spione oder den Diebstahl von Datenträgern abgezogen werden.

[122] Vgl. Porter (1999), S. 73.
[123] Vgl. Porter (1999), S. 226.

c) Beschaffung

Die Beschaffung beschreibt alle Funktionen, die im Zusammenhang mit dem Einkauf der in der Wertkette eines Unternehmens verwendeten Inputs stehen. Ihre Tätigkeit bezieht sich somit nicht ausschließlich auf die Realisierung der Produktion, sondern umfasst viele Wertaktivitäten.[124] Neben dem Zukauf von Roh-, Hilfs- und Gebrauchsstoffen ist auch der Erwerb von Verbrauchswaren, Anlagegütern sowie unterstützenden Dienstleistungen Teil der Beschaffungsfunktion.

Besonders Informationen über Lieferanten sowie die in den Verträgen ausgehandelten Konditionen können für konkurrierende Unternehmen wichtig sein. Ein wesentliches Kriterium bei der Suche nach geeigneten Lieferanten ist nämlich die Qualität der angebotenen Inputs, da diese einen maßgeblichen Einfluss auf die Produktrealisierung sowie das Endprodukt haben. Allgemeine Informationen über bessere Beschaffungsmöglichkeiten senken die Herstellkosten[125] und fördern Wettbewerbsvorteile. Auskünfte über einzelne Lieferunternehmen und deren vertragliche Vereinbarungen mit Konkurrenzfirmen gestatten es, ein Gegenangebot mit besseren Konditionen abzugeben bzw. Vertragsverhandlungen zugunsten des eigenen Unternehmens zu beeinflussen.[126] Unterlagen, die Aufschluss über die qualitative Wertigkeit der angebotenen Inputs geben können, sind Lieferantenstatistiken, Lieferantenbewertungen sowie die Reklamationsquote der Firmen.

Mit Hilfe der Beschaffung können aber auch Informationen abgeleitet werden, die das Konkurrenzunternehmen selbst betreffen. Bestellungen, Auftragserteilungen sowie Auftragsbestätigungen geben Auskunft über neue Erzeugnisse und Unternehmensplanungen. So deutet beispielsweise der Zukauf neuer Maschinen auf den Ausbau der Produktion hin. Die illegale Beschaffung von Informationen kann somit Schutz vor operativen Risiken bieten.

Generell wird ein Großteil der überwiegend expliziten Informationen, die im Rahmen der Beschaffung entstehen und verwertet werden, auf unnatürlichen Wissensträgern gespeichert, sodass die Gefahr eines technischen Angriffs hoch ist. IT-Systeme können gehackt oder Unterlagen gestohlen werden. Aber auch die Geschwätzigkeit von manchen Mitarbeitern wird ausgenutzt, um im Verlauf von scheinbar belanglosen Gesprä-

[124] Vgl. Porter (1999), S. 72.
[125] ebd.
[126] Indem Informationen über die Vertragsbedingungen mit anderen Kunden bekannt werden, können Unternehmen Konditionen bestimmen, die dem Lieferanten angemessen sind. Die Aufhebung des Principal-Agent-Problems erleichtert die Vertragsgestaltung zugunsten der Kunden.

chen Informationen über Produktionserweiterungen oder Erzeugnismerkmale zu erhalten.

d) Unternehmensinfrastruktur

Die Unternehmensinfrastruktur unterscheidet sich von den anderen unterstützenden Wertaktivitäten speziell dadurch, dass sie nicht auf einzelne Tätigkeiten, sondern auf die ganze Wertschöpfungskette Einfluss nimmt. Zu ihren Aufgabenfeldern zählen u.a. die gesamte Geschäftsführung, Planung, Finanzierung, Rechnungslegung, rechtliche Aspekte der Unternehmenstätigkeit, der Kontakt zu Behörden und staatlichen Stellen sowie Qualitätskontrollen.[127]

Durch die Komplexität der Funktionen ist das Auftreten von schutzbedürftigem Wissen entlang der Infrastruktur weit gefächert. Mögliche Interessenbereiche können demzufolge marktbezogene Angaben, Gewinn- und Umsatzentwicklungen, die Finanz- und Vermögenslage, unternehmensweite Projekte, Verkaufszahlen, Qualitätsziele und sonstige interne Daten wie die Organisationsstruktur und -kultur sein. Derartige Informationen geben Aufschluss über die Wettbewerbsstärke eines Unternehmens und ermöglichen die Analyse des Gefahrenpotenzials für die eigene Firmenexistenz.

Das für die Umsetzung der Infrastruktur benötigte Know-how ist gleichmäßig auf implizite und explizite Wissensbestände verteilt. Formal reproduzierbare Fähigkeiten umspannen Finanzierungstechniken, Controlling- und Kalkulationskonzepte, Managementansätze, Rechtsgrundlagen und Kommunikationstechniken. Zusätzlich bildet kollektiv-implizites Wissen wie etwa Normen und Einstellungen einen wesentlichen Bestandteil der Geschäftsführung und trägt zur Unternehmenskultur bei. Individuell-implizites Know-how zeigt sich im Führungsverhalten und in der Führungsstärke der Geschäftsleitung und der leitenden Angestellten sowie im Zusammenhang mit koordinierenden Fertigkeiten bei der Planung und Umsetzung von Geschäftstätigkeiten.

Aufgrund der Vielfältigkeit der spionagegefährdeten Informationen sowie deren Verteilung eignen sich das Anwerben von internen Mitarbeitern mit höheren Positionen sowie das Hacking von IT-Systemen am Besten für die illegale Beschaffung von Daten. Auf diese Weise erhält das spionierende Unternehmen einen weit größeren Zugriff auf relevante Informationen, wie dies mit Hilfe von eingeschleusten Spionen der Fall wäre. Weitere Möglichkeiten eines rechtswidrigen Know-how-Abflusses können der

[127] Vgl. Porter (1999), S. 74.

Diebstahl von physischen Datenträgern wie Notebooks oder das Abziehen von Informationen durch technische Hilfsmittel sein. Dabei kann es sich zum Beispiel um das Belauschen von Konferenzen oder Qualitätsgesprächen via Abhörgeräte handeln oder um die Übertragung von computergestützten Informationen auf USB-Sticks.

Tabelle 5 fasst noch einmal die wesentlichsten Erkenntnisse des vorangegangenen Abschnittes systematisch zusammen, sodass auf die gewonnenen Einsichten in Kapitel 6 zurückgegriffen werden kann. Ziel soll es dort sein, Managementempfehlungen für die Verwirklichung eines integrierten Informationsschutzkonzeptes abzuleiten, die sich nach den individuellen Bedürfnissen der einzelnen Wertaktivitäten richten.

Tabelle 5: Wissen in den unterstützenden Wertaktivitäten
Quelle: eigene Darstellung.

>> Personalwirtschaft:

Wissensform	*Wissen/Wissensträger*	*Spionagemethode*
überwiegend explizit	Mitarbeiterdaten, Infos zur Personalentwicklung und Personalbeschaffung	Diebstahl von Speichermedien, Hacking, Social Engineering; (Personalwirtschaft als Mittel und Ziel)
z.T. implizit	Mitarbeiter (Grundsätze, Förderung des Betriebsklimas)	Gesprächsabschöpfung (z.B. über Unternehmenskultur)

>> Technologieentwicklung:

Wissensform	*Wissen/Wissensträger*	*Spionagemethode*
explizit	externalisiertes Wissen (IT-Modelle, Notizen, Skizzen…)	Anwerben interner Mitarbeiter, Social Engineering, Gesprächsabschöpfungen; Hacking, Diebstahl, Einsatz technischer Hilfsmittel
individuell-implizit	Kreativität und Kombinationsfähigkeit von Wissenschaftlern und Entwicklern	An- bzw. Abwerben interner Mitarbeiter

>> Beschaffung:

Wissensform	*Wissen/Wissensträger*	*Spionagemethode*
überwiegend explizit	Lieferantendaten (Lieferverträge, Lieferantenbeurteilungen, Statistiken, Reklamationsquote), Produktionsinfos (Aufträge, Bestellungen)	Diebstahl von Speichermedien, Hacking, Anwerben von Mitarbeitern, Gesprächsabschöpfung (Einsatz von Spione)
bedingt implizit	Mitarbeiter (Pflege von Lieferantenbeziehungen)	Anwerben interner Mitarbeiter

>> Unternehmensinfrastruktur:

Wissensform	*Wissen/Wissensträger*	*Spionagemethode*
implizit	Unternehmenskultur, Führungsstil/-verhalten	Gesprächsabschöpfung, Anwerben von Mitarbeitern
explizit	Umsatzentwicklung, Projekte, Finanz- und Vermögenslage, Qualitätsziele	Anwerben von Mitarbeitern, Hacking, Diebstahl von Speichermedien, Einsatz technischer Mittel

4.2.2 Gefahren durch Vernetzungen und Verknüpfungen

4.2.2.1 Informationsabflüsse durch Verknüpfungen innerhalb der Wertkette

Wie bereits Kapitel 4.1.2 sowie die Darstellung der einzelnen Wertaktivitäten und Wissensbestände in den vorangegangenen Abschnitten deutlich machten, sind alle Unternehmensbereiche miteinander verknüpft. Durch Verbindungen innerhalb der Wertschöpfungskette können Wettbewerbsvorteile generiert werden. Jedoch setzt dies in der Regel einen kontinuierlichen Informationsfluss voraus, mit dessen Hilfe erst Optimierungs- und Koordinierungsprozesse stattfinden können.[128]

Ein Großteil der Informationsweitergabe erfolgt durch mündliche Übertragung. So tauschen Mitarbeiter in persönlichen Gesprächen Daten und Informationen aus, während Führungskräfte in Konferenzen die Realisierung von Aufträgen koordinieren. Die verbale Übertragung von Know-how erreicht aber ebenso wie die papierbasierte Informationsweitergabe schnell ihre Grenzen, sodass viele Unternehmen auf technische Unterstützung angewiesen sind, um Wissen auch in kürzester Zeit über größere Distanzen transportieren zu können.

Neben klassischen Hilfsmitteln wie Telefon, E-Mail, Fax oder Instant Messaging gewinnen immer mehr ausgeklügelte Informations- und Kommunikationssysteme wie beispielsweise SAP R/3 an Bedeutung. Bei ihnen handelt es sich „um soziotechnische Systeme, die menschliche und maschinelle Komponenten umfassen und zum Ziel der optimalen Bereitstellung von Information und Kommunikation nach wirtschaftlichen Kriterien eingesetzt werden."[129] Informationssysteme bestehen aus funktionsbezogene Teilsystemen, die zur Erfassung, Speicherung und Verarbeitung von Daten in den einzelnen Unternehmensbereichen genutzt werden. Die Aufgabe der Kommunikation liegt folglich in der Verbreitung, Übertragung und dem Austausch dieser Daten.[130] Der Vorteil von solchen Systemen beruht darin, dass Informationen und Wissen schnell und kostengünstig über große geografische Distanzen weitergegeben werden können. Zudem ermöglichen sie die Speicherung eines großen Informationsbestandes sowie ein simultanes Arbeiten.

Da die Wissensbestände zur Zeit der Übertragung größtenteils an unnatürliche Wissensträger gebunden sind und in digitalisierter Form vorliegen, ist ihr Charakter vor-

[128] Vgl. Porter (1999), S. 82.
[129] WKWI (1994), S. 80, zitiert durch Krcmar (2005), S. 25.
[130] Vgl. Krcmar (2005), S. 25.

rangig kollektiv-expliziter Natur. Durch die Vielfältigkeit der legalen Weitergabemethoden lässt sich daran jedoch keine eindeutige Präferenz bei der Spionagestrategie ableiten. Liegt der Fokus der Spionageaktivität allerdings auf der Ausspähung von Informations- und Kommunikationssystemen, so ist überwiegend das Hacking der Technik für einen irregulären Informationsabfluss verantwortlich. Die Überwindung der Passwortschranke kann dabei aus der Unachtsamkeit der Mitarbeiter resultieren. Oft werden Standardpasswörter nicht geändert, sodass auch Ungeübte schnell Zugriff zu den gewünschten Informationen erhalten.[131] Im Rahmen des Social Engineering sind außerdem Fälle bekannt, in denen sich Unternehmensfremde als IT-Experten ausgeben und nach den Zugriffsdaten fragen, um ein vermeintliches Problem schnellstmöglich zu beheben. Die mutwillige Weitergabe von derartigen Informationen durch eigene Mitarbeiter ist im Vergleich dazu seltener zu finden, da die Entdeckungsgefahr als zu hoch eingeschätzt wird.

Bei einer papierbasierten Übertragung von Informationen zeichnet sich ein anderes Bild ab. Die mannigfaltigen Vervielfältigungsmöglichkeiten von Unterlagen begünstigen den Informationsabfluss durch interne Mitarbeiter. Ein eindeutiger Nachweis des Täters ist oft nicht möglich. Gleiches ergibt sich bei der verbalen Weitergabe von Know-how. Eine Abschöpfung kann hierbei durch interne Informationsquellen erfolgen, aber auch mit Hilfe technischer Hilfsmittel wie Abhörgeräte und Videokameras.

4.2.2.2 Informationsabflüsse durch Verknüpfungen mit anderen Wertketten

Informationsströme, die intern zur Realisierung der Geschäftstätigkeit fließen, sind im Vergleich zu externen Verknüpfungen weit weniger risikobelastet. Kapitel 4.1.3 zeigte bereits, wie vielfältig die Verbindungen zwischen einem Unternehmen und seiner Umwelt sein können. Neben Kunden, Lieferanten und Vertriebskanälen sind auch Koalitionspartner, Finanzgeber, Anteilseigner, Kammern, Verbände und Gewerkschaften[132] Teil des Wertsystems, da ihre Forderungen ebenfalls die Wertkette des Unternehmens beeinflussen. Das folgende Kapitel konzentriert sich jedoch ausschließlich auf Informationsflüsse und damit einhergehende Risiken, die aus dem Outsourcing und der Bildung von Koalitionen resultieren.

[131] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (2006), S. 40.
[132] Vgl. Prange (2002), S. 80.

Eine Begründung für diese Vorgehensweise ergibt sich aus dem Umstand, dass viele Informationen, die an die Öffentlichkeit und Kunden getragen werden, über frei verfügbare Quellen zugänglich sind, sodass deren Sammlung und Auswertung weniger zur Industriespionage, als viel mehr zur Competitive Intelligence zählen. Diese Sichtweise setzt jedoch voraus, dass es sich bei den Abnehmern um Endkunden handelt und nicht um Unternehmen, die auf die Vorprodukte eines vorgelagerten Outsourcing-Partners angewiesen sind.

Sowohl bei vor- als auch bei nachgelagerten Firmen besteht nämlich immer die Gefahr, dass das im Rahmen einer Geschäftstätigkeit legal übertragene Know-how durch eine vertikale Diversifikation verloren geht. Das ursprüngliche Ziel, durch den Zukauf von Vorprodukten und die Abgabe von untergeordneten Aktivitäten die eigene Leistungstiefe zu reduzieren und sich somit auf die Kernkompetenzen zu konzentrieren[133], wird durchkreuzt. Ein Beispiel hierfür wäre die Produktionsauslagerung auf Fremdfirmen bei gleichzeitiger Konzentration auf Forschung, Marketing und Vertrieb. Dazu werden zunächst explizite Wissensbestände, die überwiegend das Produkt selbst betreffen, an den Vertragspartner transferiert. Dieser gewinnt im Laufe der Geschäftsbeziehung an impliziten Fähigkeiten, während sie im forschenden Unternehmen verloren gehen. Entschließt sich der Produzent nun vorwärts oder rückwärts zu integrieren, kann er damit das ursprüngliche Unternehmen vom Markt verdrängen. Ob die Eingliederung von vor- bzw. nachgelagerten Wertaktivitäten aber zwangsläufig mit einem illegalen Know-how-Abfluss in Verbindung gebracht werden muss, ist fraglich. Dennoch verfügen Outsourcing-Unternehmen über eine große Menge betriebsinterner Informationen, die im Rahmen der späteren Geschäftstätigkeit unrechtmäßig weiter genutzt werden könnten.

Neben primären Wertaktivitäten können auch unterstützende Dienstleistungen wie die Gebäudereinigung oder die Lohn- und Gehaltsabrechnung ausgegliedert werden.[134] Besonders bei sehr komplexen und individuellen Serviceleistungen, die einen enormen Informationstransfer benötigen, ist die Gefahr groß, dass Zulieferunternehmen[135] das Interesse von Konkurrenten wecken. So kann es beispielsweise sein, dass Vertragspartner ausgespäht werden, um auf diese Art Informationen über das eigentliche Zielobjekt zu erhalten. Ebenso kritisch ist die Tatsache zu betrachten, dass Zulieferfirmen

[133] Vgl. Arndt (2006), S. 145ff.
[134] Vgl. Arndt (2006), S. 147.
[135] Zulieferunternehmen beschreiben in diesem Zusammenhang alle Firmen, die das Unternehmen mit Produkten und Dienstleistungen beliefern, die der Realisierung der Unternehmenstätigkeit dienen.

oftmals auch für die Konkurrenz arbeiten, sodass hier die Gefahr eines unbeabsichtigten Informationsverlustes durchaus gegeben ist.[136]

Outsourcing-Partner sind allerdings nicht nur als Opfer illegaler Spionageaktivitäten zu betrachten, sondern können auch aktiv zum Know-how-Abfluss beitragen. Speziell Servicekräfte, die längerfristig im Unternehmen eingesetzt werden und Zugriff auf interne Daten haben, können durch finanzielle Anreize dazu verleitet werden, freiwillig Informationen an konkurrierende Unternehmen weiterzugeben. Grundsätzlich können intern eingesetzte Outsourcing-Dienstleister je nach Tätigkeitsbereich und Zugriffsmöglichkeiten Informationen auf ähnliche Weise übertragen wie betriebseigenes Personal. Zudem sind Unternehmensfunktionen, die von Fremdfirmen auswärtig realisiert werden, von den gleichen Gefahren bedroht, die auch bei einer internen Umsetzung auftreten würden.

Durch die räumliche und rechtliche Trennung der Partnerunternehmen ergeben sich jedoch zusätzliche Sicherheitslücken, die zu einem illegalen Abfluss von Know-how führen können. Einerseits kann die tatsächliche Leistungserstellung sowie die Verwirklichung entsprechender Sicherheitsvorkehrungen weniger kontrolliert werden, als dies im eigenen Unternehmen der Fall wäre. Andererseits fördert der Einsatz von unternehmensübergreifenden Informations- und Kommunikationstechniken zur einfacheren Übermittlung von Daten die technischen Methoden der illegalen Informationsbeschaffung.

Die kritische Auseinandersetzung mit Outsourcing-Partnern deckt zwar Risiken auf, die durch Verknüpfungen zwischen zwei Unternehmen auf verschiedenen Wertschöpfungsstufen verursacht werden, vernachlässigt dabei aber Gefahren, die sich aus der gemeinsamen Durchführung von Wertaktivitäten durch zwei Konkurrenten ergeben.[137] Ziel solcher horizontalen Koalitionen ist es unter anderem, in geografische Bereiche vorzudringen,[138] die aus finanziellen Gründen allein nicht zu bedienen sind (Vertriebskoalitionen). Die Weitergabe von Informationen an die Konkurrenz kann aber dazu führen, dass nach Beendigung des Geschäftsverhältnisses der ehemalige Koalitionspartner das gemeinsame Wissen dazu nutzt, um die Märkte des früheren Verbündeten zu erschließen und ihn somit aus dem Wettbewerb zu verdrängen. Aber auch hier ist ein eindeutiger Zusammenhang zur Industriespionage oft schwer nachzuweisen. Den-

[136] Vgl. Thommen (2004), S. 266.
[137] Vgl. Arndt (2006), S. 177f.
[138] Vgl. Porter (1999), S. 91.

noch handelt es sich ebenfalls um die unrechtmäßige Nutzung von Know-how und sollte daher nicht unerwähnt bleiben.

5 Strategien zur Vorbeugung und Abwehr von Industriespionage

5.1 Grundsätze der innerbetrieblichen Spionageabwehr

Die vorangegangene Analyse der Wertaktivitäten und deren vielfältigen Verflechtungen zeigte, wie wichtig und existenziell Informationen und Wissen für den Leistungserstellungsprozess und den wirtschaftlichen Erfolg eines Unternehmens sind. Aus diesem Grund ist der präventive Schutz von vorhandenen Wissensbeständen unentbehrlich. Die Bedeutung der Unternehmenssicherheit muss in die Unternehmensphilosophie und -strategie integriert werden, sodass Maßnahmen nicht erst nach Eintritt eines Spionagefalls getroffen werden.[139] Ziel sollte es sein, Schäden in jeder Hinsicht zu vermeiden, da bereits einmalige Vorfälle das Ende für eine Unternehmung bedeuten können.[140]

Generell sind Vorkehrungen präventiver Natur effizienter als Abwehrmaßnahmen, die erst nach Bekanntwerden eines illegalen Informationsabflusses ergriffen werden.[141]

Durch die Vielfältigkeit der internen und externen Kommunikationsverbindungen ist die Umsetzung eines vollkommenen Informationsschutzes im Unternehmen jedoch kaum realisierbar. Firmen sind daher gezwungen, ihre Vorkehrungen auf den Kernbestand von zukunftssicherndem Know-how zu beschränken.[142] Denn nicht alles Wissen, das in den einzelnen Wertaktivitäten generiert und verarbeitet wird, ist gleichermaßen schützenswert. Welche der unter Abschnitt 4.2 beschriebenen Wissensbestände tatsächlich zu Wettbewerbsvorteilen führen, hängt vom jeweiligen Unternehmen und dessen Kernkompetenzen ab. Maßnahmen, die zum Schutz der Informationen dienen, sollten sich auf Bereiche konzentrieren, die Kernkompetenz-Know-how generieren und verarbeiten. Dazu ist die Realisierung eines integrierten Informationsschutzkonzeptes notwendig.

---

[139] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2008a), S. 15.
[140] Vgl. Corporate Trust (2007), S. 17. Dies ist beispielsweise bei Start-Up-Unternehmen der Fall, deren Wirtschaftskraft zunächst auf einem innovativen Produkt liegt.
[141] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2008a), S. 1; Corporate Trust (2007), S. 7.
[142] ebd.

5.2 Entwicklung eines integrierten Informationsschutzkonzeptes

Grundstein für die Entwicklung eines integrierten Informationsschutzkonzeptes bildet eine Risiko- und Schwachstellenanalyse.[143] Mit ihrer Hilfe wird zunächst eine Gesamteinschätzung über konkrete Gefahrenpotenziale im Unternehmen erteilt. Dabei werden alle Risiken, die sich aus den Wertaktivitäten sowie den internen und externen Verknüpfungen ergeben, analysiert und entsprechend ihrer Eintrittswahrscheinlichkeit und Schadenshäufigkeit klassifiziert.[144] Ein besonderes Augenmerk gilt in diesem Zusammenhang den Menschen, da nur sie in der Lage sind, bereits vorhandene Schutzmaßnahmen bewusst oder auch unbewusst zu durchbrechen.[145] Auf Basis der Risiko- und Schwachstellenanalyse werden darauf folgend etwaige Schäden, die durch den Verlust von Informationen auftreten können, bewertet. Kriterien sind u.a. die Bedeutung der betroffenen Wissensbestände für das Unternehmen, der Aufwand für ihre Rekonstruktion sowie der strategische Schaden, der durch eine unrechtmäßige Verwendung entsteht.[146]

Ziel der Analyse ist es, das Zusammenwirken verschiedener Risikofaktoren direkt zu erfassen und unter dem Grundsatz der Verhältnismäßigkeit unternehmensbezogene Präventivmaßnahmen zu entwickeln, die den Bedürfnissen der einzelnen Unternehmenseinheiten gerecht werden und das Unternehmen weitestgehend vor Schäden schützen.[147] Die immer detaillierteren Methoden der illegalen Informationsbeschaffung machen dabei eine ganzheitliche Denkweise notwendig, die alle Bereiche des Unternehmens umfasst. Erst durch die sorgfältige Kombination von aufeinander abgestimmten personellen, organisatorischen, technischen sowie rechtlichen Maßnahmen entsteht ein integriertes Informationsschutzkonzept.[148] Bei diesem handelt es sich um mehr als eine Ansammlung von Schutzvorkehrungen. Es gewährleistet, dass alle Aspekte der Informationsgefährdung mit den entsprechenden Informationsformen, Schutzmaßnahmen sowie Arbeitsbereichen berücksichtigt werden.[149]

---

[143] Vgl. Sicherheitsforum Baden-Württemberg (2005), S. 46; securitymanger.de (2006), S. 7.
[144] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 11; Landesamt für Verfassungsschutz Baden-Württemberg (2008a), S. 2.
[145] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 6; Schärges (2008), S. 16.
[146] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2008a), S. 2.
[147] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 4.
[148] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 11; Sicherheitsforum Baden-Württemberg (2005), S. 46.
[149] Vgl. Corporate Trust (2007), S. 49; Sack (2008), S. 20; securitymanager.de (2006), S. 4.

5.3 Personelle Schutzmaßnahmen

5.3.1 Personalauswahl und -freisetzung

Die eigenen Mitarbeiter bilden die größte Gefahr für den Informationsbestand eines Unternehmens, da sie zum Teil über einen nahezu uneingeschränkten Zugriff auf sicherheitsrelevante Firmeninterna verfügen und „hinter" getroffenen Sicherheitsmaßnahmen wie Firewalls sitzen.[150] Darüber hinaus können menschliche Schwächen zu kriminellen Verhalten verleiten und private Schwächen wie Geldschulden oder Suchtprobleme Ansätze für eine Erpressung bieten. Aus diesem Grunde müssen die personellen Maßnahmen zum Schutz sensiblen Know-hows mit der Personalauswahl beginnen und dürfen erst mit der Personalfreisetzung enden.[151]

Bereits eine eingehende Prüfung der Bewerbungsunterlagen sowie der lückenlosen Nachweis aller bisherigen Ausbildungs- und Beschäftigungszeiten im Rahmen des Personalauswahlverfahrens kann das Risiko eines durch Mitarbeiter verursachten Informationsverlustes reduzieren.[152] Zudem sollten auch andere Informationsmöglichkeiten wie frühere Arbeitgeber oder sonstige Referenzen in den Auswahlprozess einbezogen werden, um Sicherheitsrisiken aufzudecken. Derartige Security-Checks sind besonders bei der Besetzung höherer Positionen im Unternehmen nötig, da diese oftmals mit besonders empfindlichem Know-how in Berührung kommen und dem Unternehmen einen entsprechenden Schaden zufügen können.[153]

Bei der Gestaltung des Arbeitsvertrages müssen außerdem datenschutzrechtliche Verpflichtungen sowie Vereinbarungen, die der Geheimhaltungspflicht und einem nachvertraglichen Wettbewerbsverbot dienen, berücksichtigt werden (Vgl. Abschnitt 5.6.1).[154] Es ist empfehlenswert, Stellen in sicherheitsrelevanten Bereichen vorrangig mit innerbetrieblichem Personal zu besetzen, wobei das Vertrauen in den Mitarbeiter nicht ausschließlich an der Dauer seiner Betriebszugehörigkeit festgemacht werden darf.[155]

Personelle Sicherheitsmaßnahmen müssen stets den gesamten Beschäftigungszyklus eines Mitarbeiters umfassen, sodass zu jeder Zeit der Betriebszugehörigkeit eine

[150] Vgl. Sack (2008), S. 19; Corporate Trust (2007), S. 25.
[151] Vgl. Ministerium des Innern und für Sport Rheinland-Pfalz (2008), S. 16.
[152] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004a), S. 6f.
[153] Vgl. Sicherheitsforum Baden-Württemberg (2005), S. 44.
[154] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2008b), S. 2; Landesamt für Verfassungsschutz Baden-Württemberg (2004a), S. 6.
[155] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2008b), S. 2.

sicherheitsmäßige Sensibilisierung realisiert wird (Vgl. Abschnitt 5.3.3).[156] Im Falle einer nicht einvernehmlichen Personalfreisetzung sollte der entsprechende Mitarbeiter mit sofortiger Wirkung von allen sicherheitsempfindlichen Aufgaben entbunden und die Zugänge zu sicherheitsrelevanten Bereichen eingeschränkt werden, um eine illegale Informationsweitergabe aufgrund von Berufsfrust zu vermeiden. Zudem muss auch bei der regulären Beendung des Arbeitsverhältnisses darauf geachtet werden, dass alle betrieblichen Unterlagen und Gegenstände inklusive einer entsprechenden Erklärung zurückgegeben werden. Vollmachten und Berechtigungen müssen gelöscht und Sicherheitsverantwortliche bzw. bei Bedarf auch Geschäftspartner über das Ausscheiden informiert werden. Im Einzelfall sollte außerdem auf Auffälligkeiten, die nach Beendung des Arbeitsverhältnisses auftreten, achtgegeben werden.[157] Zu ihnen kann beispielsweise ein verändertes Kundenverhalten zählen.

Grundsätzlich dienen Sicherheitsvorkehrungen, die im Rahmen der Personalauswahl und -einstellung getroffen werden, der Vermeidung von illegalem Know-how-Abfluss mit Hilfe personeller Methoden der Informationsbeschaffung. Durch die gründliche Überprüfung jeglicher Angaben, die durch einen Bewerber im Auswahlverfahren gemacht werden, können Angriffe durch eingeschleuste Spione oder charakterschwache Menschen weitestgehend vermieden werden. Desweiteren kann die Gefahr eines Verrats von Firmeninterna durch einen ehemaligen Mitarbeiters reduziert werden, indem oben beschriebene Sicherheitsmaßnahmen bei der Personalfreisetzung eingehalten werden.

5.3.2 Personalführung

Um die Loyalität der eigenen Mitarbeiter zu fördern, ist es als Management wichtig, selbst mit gutem Beispiel voranzugehen. Denn nur wer selbst den auferlegten Maßnahmen gerecht wird und den Schutz vor Industriespionage nicht an nachgeordnete Stellen delegiert, kann von seinen Mitarbeitern die gebotene Unterstützung bei der Realisierung eines integrierten Informationsschutzkonzeptes erwarten.[158]

Indem Mitarbeiter mithilfe eines betrieblichen Vorschlagswesens an der Erarbeitung von sicherheitsrelevanten Vorschriften beteiligt werden, wird nicht nur ihre Kreativität

[156] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2008b), S. 2.
[157] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004a), S. 7.
[158] Vgl. Corporate Trust (2007), S. 51; Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 8.

in Sicherheitsfragen ausgenutzt.[159] Vielmehr führt die Einbindung der Mitarbeiter in innerbetriebliche Angelegenheit zu einer Erhöhung der Motivation und Identifikation mit dem Unternehmen.[160] Generell sollten die Risikofelder des Sicherheitsschutzes sowie ihre Lösungsmöglichkeiten in der Unternehmenskultur verankert sein. Diese beruht zwar auf den grundsätzlichen Wertvorstellungen der Mitarbeiter, kann aber durch das gezielte Eingreifen des Managements verändert werden.[161] Neben internen PR-Maßnahmen trägt auch eine leistungsgerechte Bezahlung bei sicherheitsbewussten Verhalten zu einem veränderten Sicherheitsbewusstsein bei.[162]

Mitarbeiter müssen erkennen, dass die getroffenen Regeln innerhalb des Unternehmens ernst genommen werden und dass sie mit der unbefugten Weitergaben von Know-how nicht nur das Unternehmen schädigen, sondern auch ihren eigenen Arbeitsplatz gefährden.[163] In diesem Zusammenhang ist daher eine zielgerichtete Führung und Sensibilisierung des Personals durch das zweckdienliche Eingreifen in die Unternehmenskultur effizienter als die bloße Weisung zur Informationssicherheit.[164]

Maßnahmen des Informationsschutzes, die im Rahmen der Personalführung umgesetzt werden, haben die Aufgabe, präventiv auf die eigenen Mitarbeiter einzuwirken. Die aktive Beteiligung von Mitarbeitern bei der Entwicklung von sicherheitsrelevanten Vorschriften soll die Motivation und Loyalität fördern und somit das Abwerben von frustrierten Mitarbeitern durch Konkurrenzunternehmen erschweren (personelle Methoden). Zudem stellt die Integration von Sicherheitsaspekten in die Unternehmenskultur einen ersten Schritt in Richtung Sensibilisierung von Mitarbeitern dar. Diese werden durch das bewusste Erleben einer Sicherheitskultur nicht nur vor personellen Methoden wie Gesprächsabschöpfung und Social Engineering gewarnt, sondern auch auf technische Methoden der illegalen Informationsbeschaffung vorbereitet.

5.3.3 Sensibilisierung der Mitarbeiter

Die Förderung des Sicherheitsbewusstseins der Mitarbeiter ist eine der wichtigsten Aufgaben bei der Umsetzung eines integrierten Informationsschutzkonzeptes[165], denn

[159] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004a), S. 8.
[160] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2008b), S. 2.
[161] Vgl. securitymanager.de (2006), S. 20.
[162] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004a), S. 8; securitymanager.de (2006), S. 20.
[163] Vgl. Corporate Trust (2007), S. 51.
[164] Vgl. securitymanager.de (2006), S. 6.
[165] Vgl. Sack (2008), S. 19; Landesamt für Verfassungsschutz Baden-Württemberg (2004a), S.7.

die Fixierung von entsprechenden Schutzmaßnahmen allein sorgt noch nicht für Sicherheit. Wird Mitarbeitern das Gefühl vermittelt, sie seien nicht Teil des Prozesses und ihre einzige Aufgabe bestände darin, sich an die für sie unverständlichen Richtlinien zu halten, hat dies häufig eine mangelhafte Einhaltung der festgelegten Sicherheitsmaßnahmen zur Folge.[166] Der Zwang oder das bloße Vertrauen, dass die erarbeiteten Vorkehrungen von den Organisationsmitgliedern befolgt werden, führt dementsprechend nicht zum Ziel der Informationssicherheit.

Für die erfolgreiche Umsetzung eines Sicherheitskonzeptes ist es wichtig, dass die Mitarbeiter die Richtlinien nicht nur kennen, sondern auch von der Richtigkeit und Wichtigkeit der festgelegten Maßnahmen überzeugt sind.[167] Der dauerhafte Aufbau eines entsprechenden Sicherheitsbewusstseins erfolgt mit Hilfe von so genannten Sensibilisierungsprogrammen. Diese umfassen alle Maßnahmen, die dazu dienen, den Beschäftigten eines Unternehmens ein gewisses Verständnis für die Risiken und Gefahren sowie für die an sie gestellten Erwartungen zu vermitteln, und dabei gleichzeitig ihr Interesse wecken. Das Anliegen einer Sensibilisierung ist dementsprechend weniger das Befolgen der Sicherheitsmaßnahmen, als vielmehr die persönliche Auseinandersetzung mit der Thematik und somit die Förderung eines einsichtsvollen Verhaltens.[168] Mitarbeiter müssen lernen, problembewusst zu denken und sicherheitsgefährdende Situationen zu erkennen, da sie nur so zu präventivem Handeln fähig sind.[169]

Die Sensibilisierung der Mitarbeiter ist dabei keine einmalige Sache, sondern ein fortlaufender Prozess, an dessen Anfang eine Grundsensibilisierung steht. Die darin verinnerlichten Werte und Sicherheitsnormen werden mit Hilfe ergänzender Maßnahmen gefestigt, sodass ein stabiles Niveau erhalten bleibt. Darauf aufbauenden schließt sich bei Mitarbeitern in besonders sicherheitsrelevanten Bereichen eine zielgruppenorientierte Sensibilisierung an.[170]

Das grundsätzliche Ziel einer Mitarbeitersensibilisierung ist es, die Beschäftigten mit den Gefahren der Spionage vertraut zu machen und sie über die Wichtigkeit der ge-

[166] Vgl. Ministerium für Innovation, Wissenschaft, Forschung und Technologie des Landes Nordrhein-Westfalen (2006), S. 2.
[167] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 12; Ministerium für Innovation, Wissenschaft, Forschung und Technologie des Landes Nordrhein-Westfalen (2006), S. 4.
[168] Vgl. Ministerium für Innovation, Wissenschaft, Forschung und Technologie des Landes Nordrhein-Westfalen (2006), S. 3.
[169] Vgl. Ministerium des Innern und für Sport Rheinland-Pfalz (2008), S. 16f.; Landesamt für Verfassungsschutz Baden-Württemberg (2008a), S. 2.
[170] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 12.

troffenen Schutzmaßnahmen zu informieren. Mitarbeiter sollen in der Lage sein, Sicherheitsvorkommnisse selbst zu erkennen und sicherheitsbewusst zu handeln. Dabei ist es unwesentlich, ob die Methoden des illegalen Know-how-Abflusses personeller oder technischer Natur sind. Denn durch die Schulung eines entsprechenden Sicherheitsbewusstseins werden die Beschäftigten nicht nur befähigt, Anzeichen für eine Gesprächsabschöpfung oder für ein sicherheitsgefährdendes Verhalten zu erkennen. Ihnen ist es auch möglich, bereits durch kleine Ungereimtheiten Attacken auf firmeninterne IT-Systeme zu erfassen, die eine Firewall oder ein Virenscanner nicht wahrnehmen würde.[171]

5.3.4 Beschäftigung von Fremdpersonal

Die beschriebenen personellen Sicherheitsmaßnahmen lassen sich jedoch nicht allein auf firmeneigenes Personal reduzieren. Durch die zunehmende Auslagerung von Arbeitsabläufen, die im Rahmen der Kostenoptimierung erfolgt, müssen auch immer mehr fremde Personen in die Überlegungen des Sicherheitskonzeptes einbezogen werden. Denn auch externe Mitarbeiter, die nur zeitweise für ein Unternehmen tätig sind und über Zugangsrechte verfügen, können Zugriff auf vertrauliche Informationen und Unterlagen erhalten.[172]

Generell gelten für Leiharbeiter, die für einen befristeten Zeitraum beschäftigt werden, die gleichen Bedingungen wie für firmeneigenes Personal. Sie müssen sich ebenfalls an die unternehmensintern getroffenen Sicherheitsbestimmungen halten und in Sensibilisierungsmaßnahmen einbezogen werden. Zudem ist eine sorgfältige Auswahl der gewerblichen Anbieter von Zeitarbeit unerlässlich, sodass Risiken, die eingeschleuste Spione verursachen, minimiert werden können.[173] Darüber hinaus sollte das Leasing-Personal auch schriftlich zur Einhaltung der geltenden Sicherheitsvorschriften verpflichtet werden.

Die Vorkehrungen, die bei der Beendigung des Auftragsverhältnisses zu treffen sind, entsprechen den Maßnahmen der Personalfreisetzung (Vgl. Abschnitt 5.3.1). Betriebsmittel und Unterlagen sollten zurückgegeben, Zugangsberechtigungen entzogen

[171] Vgl. securitymanager.de (2006), S. 4.
[172] Zu externen Mitarbeitern können außerdem Praktikanten/Studenten gezählt werden. Da diese aber den gleichen Bestimmungen und Risiken wie die eigenen Mitarbeiter unterliegen, werden diese hier nicht näher betrachtet. Vgl. Bundesamt für Sicherheit in der Informationstechnik (2008); Landesamt für Verfassungsschutz Baden-Württemberg (2008b), S. 3.
[173] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2008b), S. 3.

und Sicherheitsverantwortliche sowie Geschäftspartner informiert werden. Auf diese Weise wird sichergestellt, dass im Nachhinein keine Informationen weitergegeben werden können. Zusätzlich sollte deutlich gemacht werden, dass die Geheimhaltungspflicht auch nach Beendigung der Tätigkeit bestehen bleibt.[174]

Für Unternehmen im Service-Bereich sowie deren Mitarbeiter gelten die gleichen Regeln wie für Leasing-Unternehmen.[175] Ist ihr Einsatz jedoch nur von kurzer Dauer oder sogar einmalig, können Service-Dienstleister auch wie Besucher behandelt werden. Das bedeutet beispielsweise, dass ihnen ein Aufenthalt in sicherheitsrelevanten Bereichen nur unter Aufsicht gewährt wird.[176]

Vorkehrungen, die für den Einsatz von Fremdpersonal getroffen werden, dienen folglich dem Schutz vor Informationsverlusten, die durch personelle und technische Methoden der Industriespionage verursacht werden. Die sorgfältige Auswahl der Leasinggeber sowie die ständige Aufsicht von kurzzeitig eingesetztem Service-Personal senken das Risiko von eingeschleusten Spionen. Die Integration von längerfristig eingesetzten Fremdarbeitern in die Sicherheitskultur eines Unternehmens wirkt zudem vorbeugend gegen alle Methoden der Ausforschung.

Tabelle 6: Personelle Schutzmaßnahmen
Quelle: eigene Darstellung.

	Schutzmaßnahmen	**Spionagemethode**
Personalauswahl und -einstellung	▪ Überprüfung von bisherigen Ausbildungs- und Beschäftigungszeiten ▪ datenschutzrechtliche Verpflichtungen im Arbeitsvertrag ▪ Geheimhaltungspflicht, Wettbewerbsverbot ▪ Maßnahmen bei Personalfreisetzung (Rückgabe von Unterlagen, Information…)	▪ Angriffe durch eingeschleuste Spione ▪ unbefugte Weitergabe von Daten durch eigene Mitarbeiter (bewusst), u.a. Datenweitergabe aus Berufsfrust
Personalführung	▪ Management als Vorbild ▪ Belohnung von sicherheitsbewusstem Verhalten und Bestrafung von sicherheitsgefährdendem Verhalten ▪ Beteiligung der Mitarbeiter an Erarbeitung von Schutzvorschriften	▪ Datenverluste durch personelle und technische Spionagemethoden ▪ Datenweitergabe aus Illoyalität/ Berufsfrust

[174] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2008).
[175] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2008b), S. 3.
[176] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2008).

	Schutzmaßnahmen	Spionagemethode
Sensibilisierung der Mitarbeiter	▪ Förderung eines Sicherheitsbewusstsein ▪ Sensibilisierung gegenüber technischen und personelle Methoden der Spionage	▪ Datenverluste durch personelle und technische Spionagemethoden jeder Art
Beschäftigung von Fremdpersonal	▪ sorgfältige Auswahl von Leiharbeitsfirmen ▪ Aufsicht von kurzzeitig eingesetztem Personal ▪ Integration externer Mitarbeiter in Maßnahmen des Sicherheitskonzepts	▪ Angriffe durch eingeschleuste Spione ▪ Datenverluste durch personelle und technische Spionagemethoden

Tabelle 6 fasst abschließend noch einmal alle Erkenntnisse aus Abschnitt 5.3 zusammen, um eine Übersicht über die erörterten Schutzmaßnahmen sowie den ihnen zuzuordnenden Spionagemethoden zu erhalten.

5.4 Organisatorische Schutzmaßnahmen

5.4.1 Festlegung von Sicherheitsstandards

Die organisatorischen Sicherheitsvorkehrungen bilden das zweite tragende Element eines integrierten Informationsschutzkonzeptes und sind unzertrennlich mit den personellen Schutzmaßnahmen verbunden.[177] Erst die Entwicklung von schriftlich fixierten Sicherheitsbestimmungen und Richtlinien ermöglicht einen effizienten Umgang mit schutzbedürftigem Know-how. Das Regelwerk sollte dabei den tatsächlichen Erfordernissen der betrieblichen Praxis entsprechen[178] und die allgemeinen Sicherheitsgrundsätze der Unternehmensphilosophie konkretisieren, sodass sie der Belegschaft bereichsspezifisch und zielgruppenorientiert vermittelt werden können.

Sicherheitsaspekte, die bei der Festlegung der Standards berücksichtigt werden müssen, sind u.a. die Informationsverarbeitung, der Objekt- und Werkschutz, der Besucherverkehr, die Zusammenarbeit mit Fremdfirmen sowie Fremdpersonal, der Umgang mit den Medien, der Schutz der Informations- und Kommunikationstechnik sowie das Verhalten in Krisen- und Schadensfällen.[179] Ein Vergleich mit den bereits beschriebenen Maßnahmen aus dem Personalbereich macht deutlich, dass es Überschneidungen

[177] Vgl. Ministerium des Innern und für Sport Rheinland-Pfalz (2008), S. 17.
[178] Vgl. Corporate Trust (2007), S. 50; Landesamt für Verfassungsschutz Baden-Württemberg (2008a), S. 2.
[179] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004a), S. 10.

gibt, die für integrierte Informationsschutzkonzepte kennzeichnend sind und eine konkrete Abgrenzung zwischen personellen und organisatorischen Schutzmaßnahmen erschweren.

Ein wichtiges Kriterium, das bei der Entwicklung der Sicherheitsbestimmungen und Handlungsanweisungen berücksichtigt werden muss, bezieht sich auf den Geltungsbereich. Die festgesetzten Regeln müssen gleichermaßen von jedem Mitglied der Organisation eingehalten werden. Es dürfen keine hierarchischen Unterschiede geben, die eine Abwälzung der Verantwortung „nach unten" erlauben. Alle Bereiche, einschließlich Geschäftsleitung und Management, sind in derselben Weise zur Einhaltung aller Vorschriften verpflichtet.

Ziel von formal fixierten Sicherheitsstandards ist es, das Unternehmen durch Aufklärung und Information vor unrechtmäßigen Know-how-Abflüssen jeglicher Art zu schützen. Entsprechend der vielfältigen Regelungen beugt beispielsweise eine Clean-Desk-Politik einem physischen Datendiebstahl durch eingeschleuste Spione vor, sodass Ansätze für personelle und technische Spionageaktivitäten durch das unbedachte Verhalten von Mitarbeitern nahezu ausgeschlossen werden können. Aber auch klare Sicherheitsbestimmungen bezüglich der Nutzung, Vervielfältigung und Vernichtung von Informationsbeständen wirken präventiv gegen alle Arten der Informationsbeschaffung im Sicherheitskonzept.

5.4.2 Benennung eines Sicherheitsverantwortlichen

Für die Schaffung eines akzeptablen Sicherheitsniveaus ist neben der Festlegung von verbindlichen Schutzbestimmungen auch die Benennung eines fachlich kompetenten Sicherheitsbeauftragten erforderlich.[180] Dieser ist als zentraler Ansprechpartner unternehmensweit tätig und hat die Aufgabe, die Funktionen des betrieblichen Sicherheitswesens aufrecht zu erhalten und die Einzelelemente des Sicherheitskonzepts zu koordinieren.[181] Dazu zählen beispielsweise die Vorbereitung und Umsetzung risikopolitischer Entscheidungen, die Beratung betrieblicher Entscheidungsträger in Sicherheitsangelegenheiten, die Durchführung der Risiko- und Schwachstellenanalyse sowie die Steuerung des Informationsflusses unter sicherheitsrelevanten Gesichtspunkten.[182]

[180] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 13.
[181] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2008a), S. 2.
[182] Vgl. Finster (2005), S. 21; Landesamt für Verfassungsschutz Baden-Württemberg (2004a), S. 9.

Um die optimale Umsetzung eines nachhaltigen Sicherheitskonzepts gewährleisten zu können, ist er dabei auf die Unterstützung der Geschäftsführung und das Wissen von Fachleuten aus Bereichen wie Datenverarbeitung, Datensicherung und Datentechnik angewiesen.[183] In Abhängigkeit von der Größe und Struktur eines Unternehmens sowie dem Grad der Anfälligkeit der Geschäftsprozesse und Produkte für kriminelle Handlungen ist zudem in Erwägung zu ziehen, ob ein oder mehrerer Mitarbeiter eventuell hauptamtlich mit allen sicherheitsrelevanten Vorgängen betraut werden sollten oder sogar eine entsprechende Unternehmenseinheit einzurichten ist. In jedem Falle sollten Sicherheitsverantwortliche möglichst hoch in der Entscheidungshierarchie integriert sein.[184]

Durch die unternehmensübergreifende Tätigkeit von Sicherheitsverantwortlichen und ihre Einbindung in alle sicherheitsrelevanten Sachverhalte des Unternehmens ist eine Reduzierung ihres Wirkungsfeldes auf die Vorbeugung von Wissensverlusten durch technische *oder* personelle Methoden nicht möglich. Mit der Planung von Sensibilisierungsprogrammen und ihrer Beteiligung am Personalauswahlverfahren werden Risiken minimiert, die durch eigene bzw. fremde Mitarbeiter entstehen. Ebenso können die Gefahren, die auf die Informations- und Kommunikationssysteme des Unternehmens zurückzuführen sind, durch entsprechende Vorgaben und Maßnahmen verringert werden. In beiden Fällen handelt es sich um Tätigkeiten, die im Verantwortungsbereich von Sicherheitsverantwortlichen liegen.

5.4.3 Zuweisung von Zugangs- und Zutrittsrechten

Eine weitere organisatorische Sicherheitsmaßnahme befasst sich mit der Festlegung von Zugangs- und Zutrittsrechten zum Schutz von gefährdeten Daten, Objekten und Räumen.[185] Die Schutzwürdigkeit eines Raumes wird dabei vom Sicherheitsbedarf der Informationen und Informationstechnik bestimmt, die sich in ihm befinden. Gebäudebereiche, die in diesem Zusammenhang ein besonderes Sicherheitsrisiko bergen, sind beispielsweise Archive, Serverräume, Büros und Maschinensäle.[186] Aus Sicherheitsgründen sollte gewährleistet werden, dass nur diejenigen Zutritt zu diesen Bereichen

[183] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2008a), S. 3.
[184] Vgl. Baeck (2006), S. 20.
[185] Vgl. Ministerium des Innern und für Sport Rheinland-Pfalz (2008), S. 17.
[186] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2008b).

erhalten, die diesen zur Wahrnehmung ihrer Aufgaben auch benötigen.[187] Eine Überwachung dieser Zutrittsregeln kann mit Hilfe von Personen wie Pförtnern oder durch technische Einrichtungen erfolgen, wobei letztere von einer einfachen Schlüsselvergabe bis hin zu aufwendigen Identifikationssystemen reichen.[188]

Über Zugangsrechte wird geregelt, in welcher Art und in welchem Umfang ein Mitarbeiter über Wissensbestände verfügen kann. Das Ausmaß der Bevollmächtigungen wird dabei von den Funktionen definiert, die die jeweiligen Personen im Unternehmen wahrnehmen. Entsprechend des Need-to-know-Prinzips sollte darauf geachtet werden, dass keine unnötigen Zugangsrechte vergeben werden. Durch die Begrenzung der Befugnisse soll eine unerlaubte Übertragung von Know-how zu Spionagezwecken vermieden werden. Die Realisierung von Zugangsbeschränkungen erfolgt bei der Datenverarbeitung beispielsweise mit Hilfe einer Nutzererkennung und eines Passwortes.[189] Dabei empfiehlt es sich, bei einer längerdauernden Abwesenheit einer berechtigten Person aus Sicherheitsgründen die Zugangsberechtigung zu sperren, um eine missbräuchliche Verwendung zu verhindern.

Ziel dieser Schutzmaßnahmen ist es, eine unberechtigte Kenntnisnahme und Verarbeitung von Informationen zu erschweren. Indem einzelnen Mitarbeitern und Fremden der Zutritt zu bestimmten Bereichen des Unternehmens verweigert wird, kann die Gefahr eines illegalen Informationsabflusses durch eingeschleuste Spione oder bereichsfremde Mitarbeiter vermindert werden (personelle Spionagemethoden). Zudem wirken Zutrittsbeschränkungen präventiv gegen die Platzierung technischer Hilfsmittel wie etwa Kameras oder Wanzen sowie gegen den Diebstahl physischer Datenträger. Ähnliche Resultate werden auch durch die Festlegung von Zugangsrechten erzielt. Dabei soll speziell das Abziehen von explizitem Know-how im Bereich der Datenverarbeitung sowie die Entwendung und Weitergabe von Wissen durch interne Mitarbeiter verhindert werden.

5.4.4 Durchführung von Kontrollen

Mit Hilfe regelmäßiger Kontrollen wird geprüft, inwieweit festgesetzte Sicherheitsvorkehrungen tatsächlich eingehalten werden bzw. eine Anpassung der Maßnahmen

[187] Vgl. Sack (2008), S. 20.
[188] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2008b).
[189] Vgl. Sicherheitsforum Baden-Württemberg (2005), S. 45.

durch betriebliche Entwicklungen erforderlich ist.[190] Werden Mängel in den konzeptionellen Überlegungen festgestellt, müssen diese unverzüglich beseitigt werden. Sicherheitsverstöße, die auf menschliches Fehlverhalten oder auf Nichtbeachtung der Sicherheitsvorgaben zurückzuführen sind, sollten durch Sanktionen geahndet und besonders sicherheitsbewusstes Benehmen durch Anerkennung belohnt werden. Anderenfalls hat das Fehlen von Konsequenzen zur Folge, dass das entwickelte Schutzkonzept völlig wirkungslos bleibt.[191] Reaktionen auf Sicherheitsverstöße können beispielsweise ein Personalgespräch, Nachschulungen oder arbeitsrechtliche Folgen sein.[192]

Ziel routinemäßiger Kontrollen ist es, Fehler im Sicherheitssystem sowie Missstände, die bei der Umsetzung der Vorgaben auftreten, frühzeitig aufzudecken und somit die Sicherheit des Unternehmens zu gewährleisten. Durch die Prüfung der Einzelmaßnahmen ist es möglich, indirekt auf die Wirksamkeit von personellen, technischen und organisatorischen Schutzvorkehrungen Einfluss zu nehmen. Daraus folgt, dass Kontrollen allein noch keinen Schutz bieten, sie aber unerlässlich für die Effizienz anderer Sicherheitsmaßnahmen sind.

Tabelle 7: Organisatorische Schutzmaßnahmen
Quelle: eigene Darstellung.

	Schutzmaßnahmen	**Spionagemethode**
Festlegung von Sicherheitsstandards	Festlegung von Regeln bzgl.: ▪ Informationsverarbeitung ▪ Objekt-/Werk-/Geheimschutz ▪ Besucherverkehr ▪ Zusammenarbeit mit Fremdfirmen ▪ Umgang mit den Medien ▪ Schutz der Informations- und Kommunikationstechnologie und Technik	▪ illegale Informationsabgänge durch technische und personelle Spionagemethoden
Benennung eines Sicherheitsverantwortlichen	▪ übergreifende Tätigkeit zum ganzheitlichen Schutz des Unternehmens ▪ Einbindung in alle Aspekte der Unternehmenssicherheit	▪ Abflüsse durch technische und personelle Methoden der Industriespionage

[190] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 13.
[191] Vgl. Corporate Trust (2007), S. 51.
[192] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004a), S. 11.

	Schutzmaßnahmen	Spionagemethode
Zuweisung von Zutritts- und Zugangsrechten	▪ Vergabe von Zutrittsrechten für schutzbedürftige Räume ▪ Vergabe von Zugangsrechten für Wissensbestände	▪ Know-how-Abflüsse durch unbefugte Mitarbeiter und Firmenfremde ▪ Angriffe mit technischen Hilfsmitteln ▪ Informationsweitergabe durch Unbefugte
Durchführung von Kontrollen	▪ Kontrollen zur Effizienzmessung der festgesetzten Maßnahmen ▪ Kontrollen zur Beurteilung der Umsetzung von Schutzmaßnahmen	▪ illegale Informationsabgänge durch technische und personelle Spionagemethoden

Tabelle 7 fasst die Ergebnisse des vorangegangen Kapitels noch einmal in einer Übersicht zusammen. Anhand der Gegenüberstellung wird deutlich, dass organisatorische Schutzmaßnahmen zum großen Teil dem Schutz vor allen Spionagemethoden dienen.

5.5 Technische Schutzmaßnahmen

5.5.1 Bautechnische Absicherung

Anders als die erörterten personellen und organisatorischen Schutzmaßnahmen vermuten lassen, dürfen Sicherheitsaspekte nicht erst mit Beginn der Geschäftstätigkeit in das Interessenfeld der Unternehmen rücken. Bereits in der Planungsphase von Bauvorhaben ist es erforderlich, sicherheitsrelevante Gesichtspunkte in die Überlegungen einzubeziehen, um eine nachträgliche und kostenintensive technische Aufrüstung zu vermeiden.[193]

Eine wesentliche Gefahrenquelle für die Sicherheit des Unternehmens resultiert aus der Einfachheit, mit der Betriebsfremde teilweise unerkannt und ohne große Hindernisse in schutzwürdige Bereiche des Unternehmens eindringen können. Fehlende Kontrollen machen die Vergabe von Zutrittsrechten wirkungslos (Vgl. Abschnitt 5.4.3). Daher muss die bauliche, mechanische und elektronische Absicherung des gesamten Unternehmenskomplexes sowie einzelner Gebäude, Gebäudeteile, Räume und Objekte bereits vor Baubeginn geregelt werden.[194] Die festgesetzten Schutzmaßnahmen sollten

[193] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 13.
[194] ebd.

sich dabei an der Risiko- und Schwachstellenanalyse orientieren, sodass es zu keiner Überdimensionierung kommt.[195]

Zur optimalen Geländesicherung sind Umzäunungen sowie Zutrittskontrollanlagen für Mitarbeiter, Besucher und Lieferanten notwendig. Diese stellen sicher, dass keine Unbefugten unbemerkt Zutritt zum Firmengelände erhalten. Desweiteren sollten Meldeanlagen installiert werden, um in Gefahrenfällen schnellstmöglich Hilfe durch die Polizei oder externe Sicherheitsfachleute zu erhalten.[196]

Die Innenraumüberwachung erfolgt u.a. durch Kontrollgänge von Wachpersonal, das auch außerhalb der betrieblichen Arbeitszeit auf Anzeichen von kriminellen Aktivitäten achtet. Zusätzlich sind Kamera- und Videoüberwachungssysteme, Überfall- und Einbruchsmeldeanlagen sowie Türsicherungsvorrichtungen für besonders empfindliche Bereiche einzurichten.[197] Um Informationsabflüsse durch Lauschangriffe abwehren zu können, sollten außerdem gefährdete Büro- und Besprechungsräume über einen entsprechenden Abhörschutz verfügen.

Der Schutz von Einzelobjekten wie etwa geschäftlichen Unterlagen, Prototypen oder sonstigen Sachbeständen wird durch Inventarnachweise und Inventarkontrollen gewährleistet. Durch die Verwahrung von besonders schutzbedürftigen Datenträgern und Einzelobjekten in Aktensicherheitsräumen, Stahlschränken, Datensicherungsschränken oder hinter sonstigen Schließanlagen können Gefahren für die illegale Entwendung eines Risikogutes minimiert werden.

Sowohl bei der Geländesicherung als auch bei der Innenraumüberwachung und beim Schutz von gefährdeten Einzelobjekten muss darauf geachtet werden, dass ein hoher Qualitäts- und Produktstandard sichergestellt ist. Der Einsatz minderwertiger Produkte führt andernfalls zu einer Scheinsicherheit, die dem tatsächlichen Sicherheitsniveau nicht entspricht.[198]

Allgemein soll mit Hilfe eines effizienten bautechnischen Sicherheitssystems das Unternehmen vor den kriminellen Energien Betriebsfremder geschützt werden. Dazu zählt, dass ein unrechtmäßiger Informationsabfluss durch den Diebstahl von Datenträgern sowie durch die Manipulation und Platzierung von technischen Geräten und Hilfsmitteln verhindert wird. Bautechnische Maßnahmen dienen folglich zur Abwehr

[195] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004a), S. 11.
[196] ebd.
[197] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004a), S. 11f.
[198] ebd.

von externen Spionen und sind nur bedingt zum Schutz vor den gesetzwidrigen Handlungen der eigenen Mitarbeiter geeignet.

5.5.2 Sicherung der Informations- und Kommunikationstechnik

Die bautechnische Absicherung des Betriebsgeländes als einzige technische Schutzmaßnahme reicht durch die zunehmende Abhängigkeit der Unternehmen von modernen Informations- und Kommunikationsanlagen allerdings schon länger nicht mehr aus. Je komplexer die IT-Anwendungen werden, desto schwieriger wird es, den neu gewonnenen Komfort mit einer angemessenen Sicherheit zu verbinden. Dies ist jedoch erforderlich, um die Vertraulichkeit, Verfügbarkeit und Integrität der Daten und Informationen zu erhalten.[199]

Zwei wesentliche Bestandteile der IT-Sicherung wurden bereits mit der Benennung eines Sicherheitsverantwortlichen und der Vergabe von Zugangsberechtigungen besprochen. Durch die umfangreichen Anforderungen, die der Schutz der Informations- und Kommunikationssysteme mit sich bringt, ist es jedoch empfehlenswert, neben einem allgemeinen Sicherheitsbeauftragten auch eine kompetente Fachkraft im Bereich der IT-Sicherheit zu beschäftigen. Diese sollte nicht Teil der IT-Abteilung sein, sodass sich die Einheit nicht selbst kontrolliert.[200]

Die Vergabe von Zugriffsrechten gehört ebenso wie die Benennung eines IT-Sicherheitsbeauftragten eigentlich zu den organisatorischen Schutzmaßnahmen. Die technische Umsetzung derartiger Beschränkungen erfolgt aber durch die Fixierung so genannter Benutzerrollen und -profile. Diese orientieren sich an den Tätigkeiten der Mitarbeiter und beschränken die Datenzugriffsmöglichkeiten auf das erforderliche Mindestmaß. Da es sich bei der IT-Sicherheit um einen fortlaufenden Prozess handelt, sollten die Profile und Rechte der User in regelmäßigen Abständen geprüft werden, sodass die Zugriffsberechtigungen der einzelnen Personen auch ihren Aufgabenbereichen entsprechen.[201]

Die Kontrolle solcher Beschränkungen erfolgt über Passwörter und Benutzer-Accounts. Um eine missbräuchliche Nutzung zu vermeiden, müssen die Standardeinstellungen des Herstellers deaktiviert und in regelmäßigen Abständen unter Berück-

[199] Man spricht von den Grundwerten der IT-Sicherheit. Vgl. Bundesamt für Sicherheit in der Informationstechnik (2007), S. 18.
[200] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 16.
[201] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2007), S. 21f.

sichtigung entsprechender Richtlinien neue Passwörter vergeben werden. Generell sollten Computer, Notebooks und auch sonst alle technischen Geräte durch starke Kennwörter geschützt sein, sodass der Zugriff auf interne Daten durch Unbefugte erschwert wird. Besonders bei mobilen Speichermedien wie Laptops können Risiken geschmälert werden, wenn diese über ein Passwort verfügen und die auf ihnen gespeicherten Informationen unter Umständen komplett verschlüsselt sind. Auf diese Weise kann trotz Diebstahl der Hardware ein Informationsverlust weitestgehend vermieden werden.[202]

Neben der Deaktivierung voreingestellter Identifikationen und Passwörter sollten zusätzlich alle Softwarebestandteile entfernt werden, die vom Hersteller eingerichtet wurden und für den betrieblichen Gebrauch nicht zwingend erforderlich sind. Ziel dieser Maßnahme ist es, einen Einbruch in den Server zu verhindern, der nur durch die Existenz dieser Anwendungen möglich ist. An Stelle der unnötigen Programme sollten Firewalls installiert werden, die das eigene Netz vor Fremdzugriffen schützen. Derartige Vorkehrungen sind nicht nur bei Computern mit Internetzugang angebracht, sondern können auch besonders gefährdete Risikobereiche wie die Personalabteilung von anderen innerbetrieblichen Netzwerken isolieren.[203] Voraussetzung für die Gewährung einer längerfristigen IT-Sicherheit ist aber in jedem Falle ein regelmäßiges Update der auf dem Computer oder Server befindlichen Schutzprogramme.

Ergänzt werden diese technischen Sicherheitsbestimmungen durch organisatorische und personelle Schutzmaßnahmen wie die Sensibilisierung von Mitarbeitern und die Festlegung von IT-Sicherheitsstandards, die beispielsweise den Umgang mit defekten oder ausgesonderten Festplatten regeln. Diese sollen aber ebenso wenig zum Gegenstand dieses Kapitels gemacht werden wie Maßnahmen, die das Unternehmen vor dem vollständigen Verlust oder der Zerstörung von Informationen durch Virenangriffe oder fehlenden Sicherheitskopien bewahren. Sie sind zwar auch Teil der IT-Sicherheit, haben aber weniger mit der gezielten Ausspähung von Unternehmen durch die Konkurrenz zu tun.

Aufgabe der beschriebenen technischen Schutzmaßnahmen ist es, explizites Wissen, das in digitalisierter Form abgelegt und zur Weiterverarbeitung freigegeben wurde, vor Innen- und Außentätern zu sichern, die keine Zugriffsberechtigung haben. Firewalls und personelle Identifikationssysteme dienen folglich überwiegend zur Abwehr von

[202] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2007), S. 34.
[203] Vgl. Bundesamt für Sicherheit in der Informationstechnik (2007), S. 25.

Spionen, Hackern und illoyalen Mitarbeitern. Ihr Wirkungsfeld ist jedoch besonders bei letzterem Personenkreis begrenzt. Zudem bieten sie keinen Schutz vor unbewussten, personellen Spionagemethoden wie der Gesprächsabschöpfungen und dem Social Engineering.

Tabelle 8 zeigt noch einmal die wichtigsten Erkenntnisse des vorangegangenen Abschnitts in der Übersicht.

Tabelle 8: Technische Schutzmaßnahmen
Quelle: eigene Darstellung.

	Schutzmaßnahmen	**Spionagemethode**
Bautechnische Absicherung	▪ Umzäunungen des Betriebsgeländes ▪ Installation von Zutrittskontrollanlagen ▪ Installation von Meldeanlagen (Bsp. Alarmanlagen) ▪ Beschäftigung von Wachpersonal ▪ Installation von Kamera- und Videoüberwachungsanlagen ▪ angemessene Türsicherungsvorrichtungen ▪ Inventarkontrollen ▪ Verwahrung von Datenträgern in Sicherheitsschränken und Räumen	▪ Know-how-Abfluss durch Betriebsfremde (Spione) ▪ Informationsabflusses durch den Diebstahl von Datenträgern ▪ Informationsabflüsse durch den Einsatz technischer Hilfsmittel (Bsp. Platzierung von Wanzen) ↘ Gesprächsabschöpfung ▪ Know-how-Abfluss durch illoyale Mitarbeiter (Schutz nur bedingt möglich)
Sicherung der IKT	▪ Festlegung und Überprüfung von Benutzerrollen und Profilen ▪ Vergabe von Nutzer-Accounts ▪ Passwortpflicht, regelmäßiger Wechsel der Passwörter ▪ Verschlüsselung von gefährdetem Wissen ▪ Deinstallation von unnötiger Standardsoftware ▪ Installation und regelmäßige Updates von Schutzprogrammen	▪ Abgänge durch Hacking/Angriffe aus fremden Netzwerken ▪ Abflüsse durch Spione und eigene Mitarbeiter (bedingt möglich) ▪ Informationsabflüsse durch den Diebstahl (mobiler) Hardware

5.6 Rechtliche Schutzmaßnahmen

5.6.1 Geheimhaltungs- und Wettbewerbsvereinbarungen

Rechtliche Schutzmaßnahmen beschreiben den letzten wesentlichen Bestandteil eines integrierten Informationsschutzkonzeptes. Da ihre Schutzwirkung jedoch nicht unmittelbar zu erkennen ist, werden Vorkehrungen wie Wettbewerbsverbote, Geheimhaltungsvereinbarungen sowie Patentanmeldungen und Lizenzvergaben häufig unter-

schätzt.[204] Dennoch tragen gesetzliche und vertragliche Regelungen sowie die aus ihnen resultierenden rechtlichen Ansprüche zum Schutz von betrieblichem Know-how bei.

So existiert beispielsweise nach §60 HGB ein gesetzliches Wettbewerbsverbot, das es einem Arbeitnehmer nicht gestattet, während der Dauer des Arbeitsverhältnisses in Konkurrenz zu seinem Arbeitgeber zu treten.[205] Die sich aus der generell geltenden Treuepflicht des Arbeitnehmers ergebende Verschwiegenheitspflicht verbietet es zudem, Betriebs- und Geschäftsgeheimnisse des Arbeitgebers sowie vertrauliche Informationen, die ihm im Rahmen der Unternehmenstätigkeit offenbart werden[206], an Dritte weiterzugeben. Gemeinsam gewähren diese Maßnahmen bis zur rechtskräftigen Beendigung des Arbeitsverhältnisses einen ausreichenden (rechtlichen) Schutz vor Spionagerisiken, die von den eigenen Mitarbeitern ausgehen.[207]

Durchbrochen kann die Verschwiegenheitspflicht nur werden, wenn dies zur Arbeitserfüllung notwendig ist, der Arbeitgeber einer Offenbarung zugestimmt hat oder andernfalls strafrechtliche Konsequenzen zu befürchten sind. Trifft dies nicht zu und wurden dennoch Informationen und Know-how weitergegeben, sollte das Arbeitsverhältnis nach §626 BGB außerordentlich gekündigt und ein Anspruch auf Schadensersatz geltend gemacht werden.[208] Rechtliche Maßnahmen zum Schutz von Wissen machen nämlich nur Sinn, wenn auf eine Pflichtverletzung auch entsprechende Sanktionen und rechtliche Konsequenzen folgen, sodass der Standpunkt des Unternehmens klar vertreten wird.

Da das gesetzliche Wettbewerbsverbot mit der Beendigung des Arbeitsverhältnisses erlischt, sollten zusätzlich Vereinbarungen getroffen werden, die den Umgang mit Betriebsinformationen nach Vertragsende regeln. Grundlage solcher nachvertraglichen Wettbewerbsverbote bilden die §§74ff. HGB. Mit ihrer Hilfe kann ein Arbeitnehmer vertraglich dazu verpflichtet werden, unternehmerisches Know-how auch über die Dauer des Arbeitsverhältnisses hinaus nicht zu verwerten. Dabei ist es irrelevant, ob es sich bei dem Wissen um Betriebsgeheimnisse handelt oder nicht. Wichtig ist nur, dass derartige Vereinbarungen schriftlich fixiert werden und höchstens über einen Zeitraum

[204] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 14.
[205] In der Rechtsgrundlage wird zwar ausschließlich von Handelsgehilfen gesprochen, sie findet aber analog für alle Arbeitnehmer Anwendung. Vgl. §60 Abs. 1 HGB.
[206] Dabei ist es irrelevant, ob der Arbeitnehmer zufällig in den Besitz dieser Informationen kommt oder sie ihm bewusst anvertraut wurden.
[207] Handelt es sich um externe Mitarbeiter, müssen zusätzliche Vereinbarungen getroffen werden.
[208] Vgl. §626 Abs. 1 BGB; §61 Abs. 1 HGB.

von 2 Jahren nach Ende des Arbeitsverhältnisses gültig sind.[209] Außerdem muss ein berechtigtes Interesse für den Schutz der Informationen bestehen und die Handlungseinschränkung des Arbeitnehmers mit einer angemessenen monatlichen Zahlung entschädigt werden.[210]

Ziel des gesetzlichen Wettbewerbsverbots sowie dessen vertragliche Weiterführung ist es, das Unternehmen vor illegalen Know-how-Abflüssen auf Basis rechtlicher Mittel zu schützen. Speziell fahrlässige oder vorsätzliche Verstöße, die von naiven oder illoyalen Mitarbeitern sowie eingeschleusten Spionen begangen werden, kommen durch derartige Regelungen zur Ahndung. Weniger geeignet sind diese rechtlichen Maßnahmen zum Schutz vor den technischen Methoden des Know-how-Abflusses.

5.6.2 Patent- und Lizenzvergaben

Vertraulichkeits- und Geheimhaltungsvereinbarungen müssen aber nicht nur zwischen Arbeitgebern und Arbeitnehmern bestehen, sondern können auch zwischen Kunden und Lieferanten sowie als Teil einer horizontalen Kooperation geschlossen werden. Zudem können vertrauliche Informationen, die ein Fremdunternehmen im Zuge von Lizenzverhandlungen über Patente erhält, mit Hilfe von Geheimhaltungserklärungen vor einer unrechtmäßigen Nutzung geschützt werden.

Patente dienen der rechtlichen Absicherung von explizitem Know-how. Da sie jedoch nur für Entwicklungen erteilt werden, die „neu sind, auf einer erfinderischen Tätigkeit beruhen und gewerblich anwendbar sind“[211], ist ein universeller Rechtsschutz für alle sensiblen Daten nicht möglich. Das Patentrecht gilt nur für technische Erfindungen[212], die der Öffentlichkeit vor der Patentanmeldung noch nicht zugänglich waren, die sich für einen Fachmann nicht ohne Weiteres aus dem aktuellen Stand der Technik ergeben würden und die auf einem gewerblichen Gebiet nutzbar sind.[213] Außerdem ist die klare Darstellung der Erfindungen eine Grundvoraussetzung für die Patentierbarkeit. Es muss möglich sein, die Erfindungen in der Patentanmeldung zu erläutern.[214] Daher

[209] Vgl. §74 Abs. 1 HGB; §74a Abs. 1 Satz 3 HGB.
[210] Vgl. §74a Abs. 1 Satz 1 HGB; §74 Abs. 2 HGB. Der Umfang der Entschädigung sollte mindestens der Hälfte der zuletzt bezogenen Leistungen entsprechen.
[211] §1 Abs. 1 PatG.
[212] Vgl. Ernst (2002), S. 297.
[213] Vgl. §3 PatG; §4 PatG; §5 PatG. Wird die Geheimhaltungsvereinbarung, die beispielsweise im Rahmen einer Kooperation getroffen wird, verletzt, gilt die Erfindung dennoch als neu.
[214] Vgl. §14 PatG.

können lediglich explizite bzw. explizierbare Wissensbestände, die die beschriebenen Kriterien erfüllen, patentiert und geschützt werden.

Grundsätzlich handelt es sich bei Patenten um Schutzrechte, die es ihren Inhabern erlauben, anderen die gewerbliche Nutzung dieser Erfindungen zu untersagen.[215] Wird im Zuge von illegalen Spionageaktivitäten dennoch das bestehende Recht durchbrochen, hat das geschädigte Unternehmen gemäß §139 Abs. 2 PatG einen Anspruch auf Schadensersatz.[216] Die vorsätzliche Patentverletzung ist zudem eine Straftat und kann strafrechtlich verfolgt werden.[217]

Patentinhaber können ihre Nutzungsrechte aber auch mit Hilfe von Lizenzverträgen auf andere übertragen.[218] Diese schriftlichen Vereinbarungen geben Unternehmen die Möglichkeit, fremde Schutzrechte für festgelegte Marktsegmente und -regionen gegen ein angemessenes Entgelt zu verwenden. Widerrechtliche Handlungen wie etwa eine Weiternutzung des Know-hows nach Vertragsende werden mit Vertragsstrafen geahndet, sodass auch hier der Schutz der Wissensbestände gesichert ist.

Ziel von Patenten und Lizenzen ist es, die Entwicklungen von innovativen Unternehmen vor Nachahmungen zu schützen und damit einhergehende Wettbewerbsvorteile zu erhalten. Speziell bei langwierigen und kostenintensiven Entwicklungsprozessen besteht die Gefahr, dass bereits kurz nach Markteintritt Produktinformationen abgeschöpft werden, die eine einfache Replikation der Erzeugnisse ermöglichen.[219] Es geht folglich weniger darum, das Unternehmen vorsorglich bzw. aktiv vor illegalen Know-how-Abflüssen zu sichern, als viel mehr darum, ihm ein rechtliches Mittel zu geben, das nach Eintritt eines illegalen Informationsabgangs den Schaden begrenzt.

Die Schutzwirkung von Patenten ist speziell bei Produktinnovationen mit einem langen Lebenszyklus höher als dies bei Geheimhaltungsvereinbarungen der Fall wäre. Nicht zuletzt durch die immer komplexeren Vernetzungen zwischen den Unternehmen gelangt technisches Wissen schnell in den Informationsbereich von Wettbewerbern, sodass das Patentrecht zumindest dessen Nutzung verhindert.[220] Aber auch der Patentschutz hat aufgrund der unterschiedlichen Gesetzesgrundlagen in den verschiedenen

[215] Dieses Recht wird als Ausschließlichkeitsrecht bezeichnet. Vgl. §9 PatG; Osterrieth (2007), S. 2.
[216] Vgl. §139 Abs. 2 PatG.
[217] Vgl. §142 Abs. 1 PatG.
[218] Vgl. §15 Abs. 2 PatG; §23 PatG.
[219] siehe dazu auch die Nachhaltigkeit von Wettbewerbsvorteilen aus Abschnitt 3.1.
[220] Vgl. Ernst (2002), S. 300f.

Ländern und der zunehmenden Globalisierung seine Grenzen.[221] Zudem besteht immer die Gefahr, dass spionierende Wettbewerber erst durch die Anmeldung von Patenten auf die innovativen Wissensbestände aufmerksam werden.[222]

Tabelle 9: Rechtliche Schutzmaßnahmen
Quelle: eigene Darstellung.

	Schutzmaßnahmen	**Spionagemethode**
Geheimhaltungs- und Wettbewerbsvereinbarungen	<u>Gesetzliche Maßnahmen:</u> ▪ gesetzliches Wettbewerbsverbot gemäß §60 HGB ▪ gesetzliche Treuepflicht des Arbeitnehmers ↘ defensiver Schutz durch Recht auf Kündigung (§626 BGB) und Schadensersatzanspruch (§61 Abs. 1 HGB) <u>Vertragliche Maßnahmen:</u> ▪ Wettbewerbsverbot für eigene Mitarbeiter gemäß §§74ff. HGB nach Ende des Arbeitsvertrages ▪ Geheimhaltungsvereinbarungen für fremde Mitarbeiter während und nach Beendigung des Arbeitsvertrages ▪ Geheimhaltungsvereinbarungen für bestehende und zukünftige Kooperationspartner (bei Verhandlung) ↘ defensiver Schutz vor Informationsabflüssen	▪ grundsätzlich personelle Methoden der Industriespionage ▪ Informationsabfluss durch illoyale Mitarbeiter und eingeschleuste Spione ▪ Informationsabfluss durch fahrlässig handelnde Mitarbeiter (z.B. Gesprächsabschöpfung) ▪ Informationsverluste unter Einbezug von kooperierenden Fremdfirmen ↘ Know-how-Abfluss durch Fahrlässigkeit der Lieferanten ↘ Nutzung der Lieferanten als Spione[223]
Patent- und Lizenzvergaben	▪ defensiver Schutz von bereits abgeflossenem Know-how durch: ↘ §139 Abs. 2 PatG (Schadensersatzanspruch) ↘ §142 Abs. 1 PatG (strafrechtliche Verfolgung) ▪ Lizenz: vertraglicher Schutz vor widerrechtlicher Nutzung von legal übertragenem Know-how	▪ jegliche Art von Spionagemethode, die einen Abfluss von explizitem und innovativem Wissen zur Folge hat ↘ technisch und personell

[221] So hat China beispielsweise eine ganz andere Auffassung von geistigem Eigentum als Deutschland oder andere europäische Länder. Eine Absicherung solcher Defizite kann nur durch internationale Vereinbarungen wie etwa dem TRIPS-Abkommen erfolgen.

[222] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 14.

[223] Vertikale und horizontale Kooperationspartner müssen aber nicht nur als Mittel der Industriespionage dienen. Es kann sich bei ihnen auch um das eigentlich spionierende Unternehmen handeln.

Tabelle 9 zeigt die vorgestellten rechtlichen Maßnahmen noch einmal in der Übersicht. Es ist festzuhalten, dass dabei kein Anspruch auf Vollständigkeit besteht. Neben gesetzlichen und vertraglichen Wettbewerbsverboten, Geheimhaltungsklauseln, Patentvergaben und Lizenzvereinbarungen existieren noch weit mehr rechtliche Schutzmaßnahmen, zu denen unter anderem auch das Marken- und Urheberrecht zählen.

5.7 Schutzmaßnahmen bei der Zusammenarbeit mit Fremdfirmen

Wie bereits an einigen Stellen der vorliegenden Untersuchung deutlich wurde, bildet die Einbindung von Fremdfirmen in das eigene Sicherheitskonzept eine wesentliche Voraussetzung für den Erfolg von Geschäftsbeziehungen und die Vermeidung von illegalen Know-how-Abflüssen. Im Rahmen der personellen, organisatorischen, technischen und rechtlichen Schutzmaßnahmen wurden Möglichkeiten aufgezeigt, die die Gefahren eines ungewollten Informationsverlustes durch horizontale und vertikale Verknüpfungen mindern.

Grundsätzlich sollte die Auswahl der Geschäftspartner unter Berücksichtigung sicherheitsspezifischer Kriterien erfolgen. Da wirtschaftliche Beziehungen einen kontinuierlichen Informationsaustausch erfordern, ist zudem ein gemeinschaftliches Sicherheitsverständnis angebracht. Aufschluss über derartige Analogien geben vorhandene Schutzmaßnahmen sowie Erfahrungen mit sensiblem Know-how. Außerdem sollte geprüft werden, inwieweit Geschäftsverbindungen zu Staaten bestehen, die ein besonderes Sicherheitsrisiko bergen.[224]

Eine sorgfältige Auswahl der Kooperationspartner stellt jedoch nicht die einzige Schutzmaßnahme im Umgang mit Fremdfirmen dar. Verbindliche Abkommen, zu denen auch Geheimhaltungserklärungen und Lizenzverträge zählen, ermöglichen die legale Nutzung von betriebsfremdem Know-how und schützen gleichzeitig innovative Unternehmen vor spionagebedingten Schäden (Vgl. Abschnitt 5.6). Die vertragsgerechte Umsetzung der Vertraulichkeitsvereinbarungen wird durch entsprechende Sicherheitsstandards gewährleistet. Speziell bei den personellen und technischen Schutzmaßnahmen muss darauf geachtet werden, dass diese konform zum eigenen Sicherheitskonzept realisiert werden.

Die erläuterten Anforderungen an das Sicherheitsniveau der Fremdfirmen werden zusätzlich durch Vorkehrungen im eigenen Unternehmen ergänzt. Derartige Maßnahmen

[224] Vgl. Landesamt für Verfassungsschutz Baden-Württemberg (2004b), S. 17.

beziehen sich vorwiegend auf die interne Beschäftigung von unternehmensfremdem Personal. Die Geschäftsabwicklung sollte nur mit ausgewählten Arbeitskräften erfolgen. Diese müssen aktiv in das Sicherheitskonzept des Unternehmens eingebunden und zur Teilnahme an Sensibilisierungsmaßnahmen verpflichtet werden. Da auch externe Mitarbeiter häufig Zugang zu sensiblem Know-how erhalten, ist es zudem ratsam, schutzbedürftige Wissensbestände durch Geheimhaltungsvereinbarungen vor einer widerrechtlichen Verwendung abzusichern. Gleiches gilt auch bei kurzfristig eingesetzten Arbeitskräften, die beispielsweise für Reparaturdienste tätig sind. Selbst wenn diese nur unter Aufsicht Zutritt zu gefährdeten Unternehmensbereichen erhalten, kann niemals ausgeschlossen werden, dass sie nicht mit sensiblem Know-how in Berührung kommen.[225]

Tabelle 10 zeigt eine Gegenüberstellung der wesentlichsten Schutzmaßnahmen, die in Zusammenhang mit Fremdfirmen getroffen werden sollten. Dabei werden auch Vorkehrungen berücksichtigt, die bereits in früheren Kapiteln behandelt wurden.

Tabelle 10: Schutzmaßnahmen bei Zusammenarbeit mit Fremdfirmen
Quelle: eigene Darstellung.

	Schutzmaßnahmen	**Spionagemethode**
Grundsätzliche Schutzmaßnahmen	▪ sorgfältige Auswahl der Kooperationspartner ▪ vertragliche Absicherung	▪ Informationsabfluss durch eingeschleuste Spione ▪ Social Engineering
Personelle Schutzmaßnahmen	▪ Geheimhaltungspflicht, Wettbewerbsverbote ▪ Sensibilisierung, Integration ins Schutzkonzept	▪ bewusste Weitergabe von Informationen durch Mitarbeiter ▪ technische und personelle Spionagemethoden
Organisatorische Schutzmaßnahmen	▪ Vergabe von Zugangs- und Zutrittsrechten ▪ Aufsicht von kurzzeitig eingesetztem Personal ▪ Durchführung von Kontrollen	▪ Datenverlust durch unbefugte Mitarbeiter und Fremdfirmen ▪ Angriffe durch technische Mittel ▪ technische und personelle Spionagemethoden
Technische Schutzmaßnahmen	▪ innerbetriebliche Sicherung der Informations- und Kommunikationstechnik ▪ Verpflichtung der Fremdfirma zum IKT-Schutz	▪ Datenverlust durch unzureichend gesicherte Unternehmen (technische Methoden der Spionage)
Rechtliche Schutzmaßnahmen	▪ Patentanmeldung und Lizenzvergaben ▪ Geheimhaltungsklauseln, (vertragliche) Wettbewerbsverbote	▪ Informationsverlust durch unrechtmäßige Weiternutzung und Weitergabe sensibler Daten an Dritte (Vgl. Social Engineering)

[225] Eine ungewollte Preisgabe von schutzbedürftigen Informationen kann auch nicht durch Zugangs- und Zutrittsbeschränkungen mit absoluter Sicherheit ausgeschlossen werden, Vgl. dazu auch Abschnitt 5.4.3.

6 Managementempfehlungen zur Spionageabwehr

Zu Beginn der Untersuchung wurden zunächst die wichtigsten Methoden der illegalen Informationsbeschaffung erläutert und anhand der Wissenssystematisierung besondere Risikobereiche im Unternehmen identifiziert.[226] Anschließend erfolgte eine gründliche Analyse der möglichen Strategien zur Vorbeugung und Abwehr von Industriespionage, in deren Verlauf bereits Hinweise zur Schutzwirkung und Anwendung der einzelnen Maßnahmen gegeben wurden.

Es stellt sich nun die Frage, inwieweit aus den gewonnenen Erkenntnissen Managementempfehlungen für den Einsatz spezifischer Sicherheitsvorkehrungen in den einzelnen Wertaktivitäten abgeleitet werden können. Dazu wurde im Anhang dieses Beitrages eine detaillierte Übersicht erstellt, die den jeweiligen Tätigkeitsbereichen nochmals die sich in ihnen befindlichen Wissensformen zuordnet und die daraus resultierenden Spionagegefahren aufzeigt. Auf Basis der in Kapitel 5 beschriebenen Zusammenhänge zwischen den einzelnen Bestandteilen eines integrierten Informationsschutzkonzeptes sowie deren Schutzwirkung auf die typischen Methoden der Industriespionage wurden zudem Sicherheitsmaßnahmen bestimmt, die sich nach den individuellen Bedürfnissen der Wertaktivitäten richten.

Da Mitarbeiter überall im Unternehmen tätig sind und folglich Zugriff auf großen Mengen von Know-how besitzen, ist eine sorgfältige Auswahl des Personals sowie die kontinuierliche Förderung eines grundlegenden Sicherheitsbewusstseins eine Basisvoraussetzung für die Schaffung eines angemessenen Informationsschutzes in allen Unternehmensbereichen. Darüber hinaus fördert auch die Benennung eines Sicherheitsverantwortlichen sowie die regelmäßige Durchführung von Kontrollen das Sicherheitsniveau des gesamten Unternehmens, sodass deren Anwendung nicht auf einzelne Tätigkeitsfelder reduziert werden kann.

Grundlegende Unterschiede zwischen den Wertaktivitäten, die sich anhand der charakteristischen Besonderheiten der Funktionsbereiche ergeben, können in Bezug auf die inhaltliche Ausgestaltung der Sensibilisierungsmaßnahmen diagnostiziert werden. So müssen Mitarbeiter von Unternehmensbereichen, deren Funktionen einen engen Kontakt mit Kunden, Lieferanten und sonstigen externen Kooperationspartnern erfordern, für Anzeichen einer sozialen Manipulation und Gesprächsabschöpfung empfindlich gemacht werden. Die Sensibilisierung der Belegschaft bildet grundsätzlich den einzi-

[226] siehe dazu Abschnitte 2.4, 3.3 sowie 4.2.

gen wirksamen Schutz gegen derartige personelle Spionagemethoden, sodass besonders Arbeitskräfte in der Ein- und Ausgangslogistik, im Vertrieb und im Kundendienst sowie in der Beschaffung auf personengestützte Angriffe vorbereitet werden müssen.

Während sich Sensibilisierungsprogramme in diesen Bereichen auf die Spionagetätigkeit von Außenstehenden konzentrieren, liegt der Fokus bei Wertaktivitäten, in denen das Unternehmen auf die impliziten Wissensbestände der Beschäftigten angewiesen ist, auf Informationsverluste, die auf das bewusste Zutun der eigenen Mitarbeiter zurückzuführen sind. Zu ihnen zählen die Technologieentwicklung, die Fertigung, der Vertrieb, der Kundendienst, das Marketing sowie Tätigkeiten innerhalb der Unternehmensinfrastruktur. Neben der Veröffentlichung von Sicherheitsrichtlinien und der Unterzeichnung von nachvertraglichen Wettbewerbsverboten sollten auch Maßnahmen in Zusammenhang mit der Personalführung ergriffen werden, um fähige Mitarbeiter nicht aufgrund von Motivationsproblemen und Berufsfrust an die Konkurrenz zu verlieren. Da kognitive Fähigkeiten nicht in Geheimhaltungsverträgen fixiert werden können, sind zudem Hinweise zur Treuepflicht sowie Förderungsprogramme zum Erhalt der Betriebszugehörigkeit sinnvoll.

Unternehmensbereiche, die über besonders sensibles explizites Know-how verfügen und stark von illegalen Datenabflüssen betroffen sind, müssen zudem durch bautechnische Schutzmaßnahmen abgesichert werden. Speziell Organisationseinheiten, die in Zusammenhang mit der Technologieentwicklung, der Personalwirtschaft und der Produktion stehen, sind durch Kontrollanlagen und Zutrittsbeschränkungen zu schützen. Desweiteren sollten unnatürliche Wissensträger wie schriftliche Unterlagen und technische Speichermedien in gesicherten Räumen und Schränken verwahrt werden. Ähnliche Maßnahmen sind auch für Bereiche wie die Eingangslogistik angebracht, durch deren Verbindung nach Außen ein unbefugter Zugriff auf unternehmensinternes Know-how durch Fremde erleichtert wird.

Grundsätzlich wird an der Übersicht im Anhang aber deutlich, dass jede Form der Spionageprävention bis zu einem gewissen Grad in allen Wertschöpfungsaktivitäten zu finden ist. In welchem Rahmen diese jedoch realisiert werden, hängt von den charakteristischen Merkmalen der Tätigkeit sowie der Wissensverteilung ab. Lediglich die IT-Sicherung betrifft aufgrund der starken Verknüpfungen innerhalb der Wertkette und des Wertsystems alle Unternehmensbereiche in gleichem Maße. Die Funktionen der Logistik, der Beschaffung und des Kundendienstes haben eine hohe Frequenz an

legalen Informationsübertragungen zu Kunden und Lieferanten, sodass durch den Einsatz externer Netze auch Gefahren für den Unternehmensserver und damit alle angeschlossenen Unternehmensbereiche bestehen.

Zusätzlich ist festzuhalten, dass unternehmensweit ein großes Spektrum an Informationen in expliziter Form vorliegt, welches auf unnatürliche Wissensträger gespeichert wird. Viele Datenbestände, die an computergestützte Speichermedien gebunden sind, können zudem auf andere Speicherformate exportiert werden, sodass die Vergabe von Zugangsrechten und eine kontinuierliche Aktualisierung der IT-Sicherheitsprogramme oft nicht ausreicht. Es zeigt sich, dass in allen Bereichen personelle, organisatorische, technische und rechtliche Schutzmaßnahmen ergriffen werden müssen, um eine entsprechende Sicherheit für sich und seine Kooperationspartner garantieren zu können. Managementempfehlungen zur Spionageabwehr können wie oben beschrieben nur in Einzelfällen gegeben werden, da aufgrund der starken Verknüpfungen zwischen den Bereichen tatsächlich nur durch die Realisierung eines *integrierten* Informationsschutzkonzepts der Informationsbestand des Unternehmens vor illegalen Abflüssen geschützt werden kann.

7 Gefahren der Industriespionage weiterhin unterschätzt

Als Ergebnis der vorliegenden Gesamtanalyse, die sich mit den Quellen von illegalen Know-how-Abflüssen in Industriebetrieben und Strategien gegen Industriespionage beschäftigte, kann festgehalten werden, dass die Risiken eines irregulären Informationsverlustes entsprechend der Wertaktivitäten variieren. Durch die Ungleichverteilung der Wissensbestände ergeben sich Differenzen in der Anwendung der verschiedenen Spionagemaßnahmen, sodass der Einsatz der Abwehrmechanismen zumindest in mancher Hinsicht von den charakteristischen Besonderheiten der jeweiligen Wertaktivität bestimmt wird.

Durch den stärker werdenden Wettbewerbsdruck wird die Gefahr eines illegalen Know-how-Abflusses auch in Zukunft für Unternehmen weiter zunehmen. Vergleichbare Entwicklungen, die bereits in den letzten Jahren zu verzeichnen waren, bestätigen diese Befürchtung (Vgl. Abschnitt 1.1).[227] Doch trotz des hohen Stellenwertes, den

[227] Vgl. Corporate Trust (2007), S. 5.

Wissen bei der Umsetzung von Geschäftsprozessen einnimmt, unterschätzen viele Unternehmen immer noch die Gefahr, die von Industriespionage ausgeht. So glauben zwar 81% der im Rahmen der Corporate-Trust-Studie befragten Firmen, dass die Risiken durch Industriespionage weltweit steigen werden, nur 33,7% sehen aber ihr eigenes Unternehmen zukünftig stärker bedroht.[228] Diese fatale Selbsteinschätzung lässt vermuten, dass auch in Zukunft viel zu wenige Maßnahmen zur Vorbeugung irregulärer Informationsabflüsse ergriffen werden und die Schäden, die durch mangelnde Prävention entstehen, weiter steigen.

[228] Vgl. Corporate Trust (2007), S. 39.

Literaturverzeichnis

Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (Hrsg., 2006): Herausforderungen Annehmen – Sicherheit schaffen. Leitsätze zu Zielen, Positionen und Aufgaben der ASW. Berlin 2006.

Arndt, H. (2006): Supply Chain Management. Optimierung logischer Prozesse. 3. aktualisierte und überarbeitete Auflage, Gabler Verlag, Wiesbaden 2006.

Baeck, C. (2006): Gibt's nicht, geht nicht. Zur Stellung des Sicherheitsverantwortlichen. In: WIK Zeitschrift für die Sicherheit der Wirtschaft, 3/2006.

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

Bodrow, W./Bergmann, Ph. (2003): Wissensbewertung im Unternehmen. Bilanzierung von intellektuellem Kapital. Erich Schmidt Verlag, Berlin 2003.

Brellochs, A. R. (2000): Competitive Intelligence und Knowledge Management. Information über Markt und Wettbewerber als externe Wissensquelle in einem Wirtschaftsforschungsunternehmen. Universität Konstanz, Diplomarbeit. Konstanz 2000.

Breunung, R. (2007): Wissenstransfer unternehmenskulturgetriebener Akteure: Eine kommunikationstheoretische Fundierung. GRIN Verlag, München-Ravensburg 2007.

Bundesamt für Sicherheit in der Informationstechnik (Hrsg., 2007): Leitfaden der IT-Sicherheit. IT-Grundschutz kompakt.

Bundesamt für Sicherheit in der Informationstechnik (Hrsg., 2008a): IT-Grundschutz-Kataloge. M 2.226 Regelungen für den Einsatz von Fremdpersonal. URL: http://www.bsi.de/gshb/deutsch/m/m02226.htm (Stand: 2008, Zugriff: 7.10.2008)

Bundesamt für Sicherheit in der Informationstechnik (Hrsg., 2008b): IT-Grundschutz-Kataloge. M 2.6 Vergabe von Zutrittsberechtigungen. URL: http://www.bsi.de/gshb/deutsch/m/m02006.htm (Stand: 2008, Zugriff: 7.10.2008)

Bundesamt für Verfassungsschutz (Hrsg., 2006a): Ihre Verantwortung – Unsere Sicherheit. Über den Umgang mit vertraulichen Informationen. Druckhaus Locher GmbH, Köln 2006.

Bundesamt für Verfassungsschutz (Hrsg., 2006b): Wirtschaftsspionage. Information und Prävention. Vereinte Verlagsanstalten, Düsseldorf 2006.

Bundesministerium des Inneren (Hrsg., 2007): Verfassungsschutzbericht 2007. Vorabfassung. Berlin 2007.

Bundesverband der Deutschen Industrie e.V. (Hrsg., 2006): Bedeutung der Sicherheit in der Industrie für Deutschland. Positionspapier D0099. Berlin 2006.

Bürgerliches Gesetzbuch (2006), 47., überarbeitete Auflage, Stand: 1.11.2005, DTV Beck-Texte, München 2006.

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

Crane, A. (2003): In the company of spies: The ethics of industrial espionage. Nottingham Universtity. Research Paper Series No. 15-2003.

Dinter, M. (2006): Technologietransfer nach China – Chancen, Risiken, Maßnahmen. Schriftreihe des Institute for International Business & Law. Braunschweig 2006.

Dold, E./Gentsch, P. (Hrgs., 2000): Innovationsmanagement. Handbuch für mittelständische Unternehmen. Luchterhand Verlag, Neuwied-Kriftel 2000.

Ernst, H. (2002): Strategisches Intellectual Property-Management. In: Hommel, Ulrich/Knecht, Th. C. (Hrsg., 2002): Wertorientiertes Start-Up-Management. Grundlagen – Konzepte – Strategien. Verlag Vahlen, München 2002.

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

Finster, E. (2005): Mehr Sicherheitsverantwortliche erforderlich. Querschnittsfunktion auch für den Mittelstand. In: WIK Zeitschrift für die Sicherheit der Wirtschaft, 3/2005.

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

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

Handelsgesetzbuch (2005), 43., überarbeitete Auflage, Stand: 1.09.2005, DVT Beck-Texte, München 2005.

Harbich, P. (2006): Die wachsende Bedeutung privater Akteure im Bereich der Intelligence. Private Akteure als Quellen, Abnehmer, Konkurrenten und Kooperationspartner staatlicher Nachrichtendienste. Universität zu Köln. AIPA 3/2006.

Harvard Business School (Hrsg., 2007): Michael E. Porter. Biography. URL: http://drfd.hbs.edu/fit/public/ facultyInfo.do?facInfo=bio&facEmId=mporter&loc=extn (Stand: 2007, Zugriff: 31.10.2008)

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

Hutzschenreuter, Th. (2007): Allgemeine Betriebswirtschaftslehre. Grundlagen mit zahlreichen Praxisbeispielen. 2., aktualisierte und erweiterte Auflage, Gabler Verlag, Wiesbaden 2007.

Kaufmann, M. (2007): Spionage. Die größte Gefahr geht vom Personal aus. In: manager-magazin.de, November 2007. URL: www.manager-magazin.de/unternehmen/artikel/0,2828, 518676,00.html (Stand: 22.11.2007, Zugriff: 18.07.2008)

Klabunde, St. (2003): Wissensmanagement in der integrierten Produkt- und Prozessgestaltung. Best-Practice-Modelle zum Management von Meta-Wissen. 1. Auflage, Deutscher Universitätsverlag, Wiesbaden 2003.

Kotler, Ph./Armstrong, G./Saunders, J./Wong, V. (2003): Grundlagen des Marketing. 3., überarbeitete Auflage, Pearson Studium, München 2003.

Kotler, Ph./Bliemel, F. (2001): Marketing-Management. 10. Auflage, Schäffer-Poeschel Verlag, Stuttgart 2001.

Krcmar, H. (2005): Informationsmanagement. 4., überarbeitete und erweiterte Auflage, Springer Verlag, Berlin-Heidelberg-New York 2002.

Landesamt für Verfassungsschutz Baden-Württemberg (Hrsg., 2004a): Handlungskonzept für Ihren Know-how-Schutz. E. Kurz & Co., Stuttgart 2004.

Landesamt für Verfassungsschutz Baden-Württemberg (Hrsg., 2004b): Know-how-Schutz. Handlungsempfehlungen für die gewerbliche Wirtschaft. E. Kurz & Co., Stuttgart 2004.

Landesamt für Verfassungsschutz Baden-Württemberg (Hrsg., 2008a): Prävention. Schutzkonzept gegen Informationsverluste. URL: http://www.verfassungsschutz-bw.de/spio/spio_praev_schutz-infoverl_druck.htm (Stand: 2008, Zugriff: 22.09.2008)

Landesamt für Verfassungsschutz Baden-Württemberg (Hrsg., 2008b): Prävention. Unternehmenssicherheit – Personelle Maßnahmen. URL: http://www.verfassungsschutz-bw.de/spio/spio_praev_plakat.htm (Stand: 2008, Zugriff: 22.09.2008)

Landesamt für Verfassungsschutz Baden-Württemberg und Bayern (Hrsg., 2006): Wirtschaftsspionage in Baden-Württemberg und Bayern. Daten – Fakten – Hintergründe. E. Kurz & Co., Stuttgart 2006.

Lux, Ch./Peske, Th. (2002a): Competitive Intelligence und Wirtschaftsspionage. Analyse, Praxis, Strategie. 1. Auflage, Gabler Verlag, Wiesbaden 2002.

Lux, Ch./Peske, Th. (2002b): Competitive Intelligence. Zwischen Anspruch und Wirklichkeit. In: WIK Zeitschrift für die Sicherheit der Wirtschaft, 2/2002.

Mangstl, H. (2005a): Schutz vor illegalen Lauschangriffen. So bleiben Daten und Gespräche vertraulich. Teil 1. In: GIT Sicherheit + Management, 9/2005.

Mangstl, H. (2005b): Schutz vor illegalen Lauschangriffen. So bleiben Daten und Gespräche vertraulich. Teil 2. In: GIT Sicherheit + Management, 10/2005.

Marwehe, Fr./Weißbach, H.-J. (2000): Der Wissenszyklus. Vom individuellen Wissen zur kollektiven Wissensbasis. URL: http://www.wiper.de/wzyklus.html (Stand: April 2000, Zugriff: 3.09.2008)

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

Ministerium des Innern und für Sport Rheinland-Pfalz (Hrsg., 1997): Spionage heute. Märkte, Macht und Militär. 1. Auflage, Mainz 1997.

Ministerium des Innern und für Sport Rheinland-Pfalz (Hrsg., 2008): Informationsschutz in der gewerblichen Wirtschaft – mit Sicherheit ein Gewinn. 1. Auflage, Mainz 2008.

Ministerium für Innovation, Wissenschaft, Forschung und Technologie des Landes Nordrhein-Westfalen (Hrsg., 2006): Secure-it in NRW. Mitarbeiter sensibilisieren für IT-Sicherheit und Datenschutz. Maßnahmen und Handlungsempfehlungen. Medienpool Köln GmbH, Köln 2006.

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

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

Osterrieth, Ch. (2007): Patentrecht. 3. Auflage, Verlag C.H. Beck, München 2007.

Patent- und Musterrecht (2008): 9., überarbeitete Auflage, Stand: 1. Januar 2008, DVT Beck-Texte, München 2008.

Picot, A. (1990): Der Produktionsfaktor Information in der Unternehmensführung. In: Information Management, 1/1990.

Picot, A./Reichwald, R./Wigand, R. T. (2003): Die grenzenlose Unternehmung. Information, Organisation und Management. 5., aktualisierte Auflage, Gabler Verlag, Wiesbaden 2003.

Porter, M. E. (1999): Wettbewerbsvorteile. Spitzenleistungen erreichen und behaupten. 5., durchgesehene und erweiterte Auflage. Campus Verlag, Frankfurt/Main 1999.

Prange, Ch. (2002): Organisationales Lernen und Wissensmanagement. Fallbeispiele aus der Unternehmenspraxis. 1. Auflage, Gabler Verlag, Wiesbaden 2002.

Probst, G./Raub, St./Romhardt, K. (1999): Wissen managen. Wie Unternehmen ihrer wertvollste Ressource optimal nutzen. 3. Auflage, Gabler Verlag, Wiesbaden 1999.

Rehäuser, J./Krcmar, H. (1996): Wissensmanagement im Unternehmen. In: Schreyögg, Georg/Conrad, Peter (Hrsg., 1996): Wissensmanagement. 1. Auflage, Gabler Verlag, Berlin-New York 1996.

Sack, D. K. (2008): Das integrierte Informationsschutzkonzept (I). In: WIK Zeitschrift für die Sicherheit der Wirtschaft, 1/2008.

Schärges, H. (2008): Christian Schaaf. Die Spionagegefahr kommt auch von Innen. In: WIK Zeitschrift für die Sicherheit der Wirtschaft, 1/2008.

Schönsleben, P. (2001): Integrales Informationsmanagement. Informationssystem für Geschäftsprozesse – Management, Modellierung, Lebenszyklus und Technologie. 2., vollständig überarbeitete und erweiterte Auflage, Springer Verlag, Berlin-Heidelberg 2001.

securitymanager.de (Hrsg., 2006): Sicherheitskultur im Unternehmen. Feig & Partner, Leipzig 2006.

Sicherheitsforum Baden-Württemberg (Hrsg., 2005): Mit Sicherheit erfolgreich. Erfolgsfaktor Know-how-Schutz. Information und Prävention. Wilhelm Stober GmbH, Eggenstein 2005.

Staudt, E. (2002): Kompetenzentwicklung und Innovation. Die Rolle der Kompetenz bei Organisations-, Unternehmens- und Regionalentwicklung. 1. Auflage, Waxmann Verlag, Münster 2002.

Thommen, J.-P. (2004): Managementorientierte Betriebswirtschaftslehre. 7., aktualisierte und ergänzte Auflage, Versus Verlag, Zürich 2004.

Werner, M. (2004): Einflussfaktoren des Wissenstransfers in wissensintensiven Dienstleistungsunternehmen. Eine explanativ-empirische Untersuchung bei Unternehmensberatungen. 1. Auflage, Deutscher Universitätsverlag, Wiesbaden 2006.

WKWI (1994): Profil der Wirtschaftsinformatik. Ausführungen der Wirtschaftlichen Kommission der Wirtschaftsinformatik. In: Wirtschaftsinformatik, 36(1).

Anhang: Übersicht Managementempfehlungen

Wertaktivität	Wissensformen	Spionagemethoden	Schutzmaßnahmen
EINGANGS-LOGISTIK	*kollektiv-explizit*[1]: Transport-, Lager- und Konservierungstechnologien (Logistiksysteme); Produktinformationen; Liefer- und Lieferantendaten	Diebstahl physischer Datenträger (Prüfprotokolle, Lieferpapiere…), Informationsabfluss durch illoyale Mitarbeiter und Lieferanten, Social Engineering, Eindringen in IT-Systeme, Verwendung technischer Hilfsmittel (u.a. Kopien…)	sorgfältige Auswahl von Mitarbeitern und Lieferanten (datenschutzrechtliche Verpflichtungen), Sensibilisierung der Mitarbeiter, Aufsichtspflicht für kurzzeitig eingesetzte Kräfte (Bsp. Reparaturdienste), Festsetzung von Sicherheitsstandards zur Aufbewahrung, Zugangs- und Zugriffsbeschränkungen (bautechnische Absicherung), regelmäßige Updates der IT-Software
	kollektiv-implizit[3]: Koordination von Lagerhaltungs- und Materialtransportsystemen	Informationsabfluss durch Mitarbeiter (bewusst, unbewusst), Einsatz von Spionen (Bsp. Praktikant)	sorgfältige Auswahl der Mitarbeiter (auch bei Fremdfirmen), Sensibilisierung der Mitarbeiter
OPERATIONEN	*kollektiv-explizit*[1]: Informationen über Herstellungsverfahren und Produktmerkmale, Fach- und Detailwissen	Diebstahl physischer Datenträger (u.a. Produkte, Konstruktionsunterlagen), Einsatz technischer Hilfsmittel (Bsp. Fotos bei Rundgang), Social Engineering/Gesprächsabschöpfung, bewusster Informationsabfluss durch Mitarbeiter	sorgfältige Auswahl von Mitarbeitern (Geheimhaltungsvereinbarungen), Sensibilisierung der Mitarbeiter, Aufsichtspflicht für kurzzeitig eingesetzte Kräfte, Festsetzung von Sicherheitsstandards, Zugangs- und Zugriffsbeschränkungen (bautechnische Absicherung)
	individuell-implizit[1/2]: körperliche Fähigkeiten, Kombinationsgabe, technisches Verständnis…	An- bzw. Abwerben von Mitarbeitern, unbewusster Informationsabfluss durch eigene Mitarbeiter	Sensibilisierung der Mitarbeiter, Abwehr von Head-Hunter-Anrufen

Wertaktivität	Wissensformen	Spionagemethoden	Schutzmaßnahmen
AUSGANGS-LOGISTIK	*kollektiv-explizit*[1]*:* Informationen über Ausgangslogistiksysteme; Kundendaten, Informationen über deren Produkte	Diebstahl physischer Datenträger (z.B. Lieferverträge, Lieferpläne…), Hacking von Logistiksysteme (IT); Gesprächsabschöpfung, Social Engineering, Datenverlust durch illoyale Mitarbeiter	sorgfältige Auswahl von Mitarbeitern und Partner (datenschutzrechtliche Verpflichtungen), Sensibilisierung der Mitarbeiter, Aufsichtspflicht für kurzzeitig eingesetzte Kräfte, Zugangs- und Zugriffsbeschränkungen (bautechnische Absicherung)
	kollektiv- und individuell-implizit[2]*:* Koordination der Lieferaufträge und Transportlogistik	Informationsabfluss durch eigene Mitarbeiter	sorgfältige Auswahl der Mitarbeiter (auch bei Fremdfirmen), Sensibilisierung der Mitarbeiter
MARKETING/ VERTRIEB	*kollektiv-explizit*[1]*:* Informationen über Kunden- und Vertreternetzwerke, Vertriebswege, Distributionskanäle, Produktangebote; Hintergrundwissen über Kunden- und Marktanforderungen; Vertriebs- und Marketingkonzepte; Fachwissen	Informationsabfluss durch illoyale Mitarbeiter, Diebstahl von Datenträgern (z.B. externalisiertes Wissen auf Notizen, Skizzen…), Hacking von Projektdatenbanken; Social Enginering/Gesprächsabschöpfung im Vertrieb	sorgfältige Auswahl von Mitarbeitern (Geheimhaltungsvereinbarungen), Sensibilisierung der Mitarbeiter, Vergabe von Zugangs- und Zutrittsrechten, bautechnische Absicherung (z.B. Räume, Schränke…), Schutz der IT durch Sicherheitsstandards (Passwörter, Accounts…), Aufsicht bei fremden Personal, regelmäßige IT-Überprüfung, Verschlüsselung gefährdeten Wissens
	kollektiv- und individuell-implizit[1]*:* Kreativität bei der Entwicklung von Marketingkonzepten; Unternehmensleitlinien im Umgang mit Kunden (Kundenbetreuung)	Gesprächsabschöpfung (u.a. technisches Verständnis); Abwerben der Mitarbeiter (meist in Zusammenhang mit Spionageaktivitäten im Personalbereich)	Sensibilisierung der Mitarbeiter, Wettbewerbsverbote; Abwehr von Head-Hunter-Anrufen

Wertaktivität	Wissensformen	Spionagemethoden	Schutzmaßnahmen
KUNDENDIENST	*kollektiv-explizit*[1]*:* Informationen über Produkte, Angebote und Zusatzleistungen; Fachwissen über Produkte	überwiegend personelle Spionagemethoden (durch natürliche Wissensträger): Gesprächsabschöpfung, Social Engineering, Informationsabfluss durch illoyale Mitarbeiter; Diebstahl physischer Datenträger	Sensibilisierung der Mitarbeiter, datenschutzrechtliche Verpflichtungen; Festsetzung von Sicherheitsstandards (Bsp. Umgang mit mobilen Wissensträgern), Verschlüsselung gefährdeten Wissens (Bsp. auf Laptops)
	kollektiv- und individuell-implizit[2]*:* Kombinationsgabe (bzgl. Problemlösungen), Leitlinien im Umgang mit Kunden (Kundenbetreuung)	Abwerben der Mitarbeiter (meist in Zusammenhang mit Spionageaktivitäten im Personalbereich; Head-Hunter), Gesprächsabschöpfung	Sensibilisierung der Mitarbeiter (Bsp. unbewusster Wissenstransfer durch detailliertes Ausfragen bei „Kundengesprächen“)
UNTERNEHMENS-INFRASTRUKTUR	*„individuell“-explizit*[1]*:* marktbezogene Angaben, Gewinn, Umsatz, Finanz- und Vermögenslage, Verkaufszahlen, Unternehmensplanung, sonstige interne Daten…	Informationsverluste durch illoyale Mitarbeiter und Führungskräfte, Social Engineering, Hacking von IT-Systemen, Diebstahl von Unterlagen, Einsatz technischer Hilfsmittel (Bsp. Lauschangriff bei Versammlungen)	sorgfältige Auswahl von Mitarbeitern (Geheimhaltungsvereinbarung), Sensibilisierung der Mitarbeiter, Aufsichtspflicht für kurzzeitig eingesetzte Kräfte, Zugangs- und Zugriffsbeschränkungen, bautechnische Absicherung, regelmäßige Updates der IT-Software
	kollektiv- und individuell-implizit[1/2]*:* Unternehmenskultur und -philosophie, Führungsstil/-verhalten/-stärke, Normen, Richtlinien; Koordination der Geschäftstätigkeit	Abwerben von Mitarbeitern in höheren Positionen (Führungskräfte), Gesprächsabschöpfung/Social Engineering (u.a. Informationen zur Führung)	Sensibilisierung der Mitarbeiter, Abwehr von Head-Hunter-Anrufen

Wertaktivität	Wissensformen	Spionagemethoden	Schutzmaßnahmen
PERSONALWIRTSCHAFT	*individuell- und kollektiv-explizit*[1]*:* Informationen zur Personalentwicklung und -beschaffung; Personaldaten; Lohn- und Gehaltsabrechnungssysteme…	Hacking von Systemen, physischer Diebstahl von Unterlagen (Bsp. Personalakten) und Personaldaten, soziale Manipulation, Gesprächsabschöpfung, Informationsabfluss durch illoyale Mitarbeiter	Sicherheitsstandards für Passwortvergabe und Verhalten im Internet, Vergabe von Zugangs- und Zutrittsrechten, regelmäßige Updates zur IT-Sicherheit, Sensibilisierung von Mitarbeitern, Geheimhaltungsvereinbarungen, Aufsicht bei kurzzeitig eingesetzter Kräfte, bautechnische Absicherung
	kollektiv-implizit[3]*:* Unternehmensgrundsätze, Werte, Normen, Betriebsklima	Gesprächsabschöpfung (z.B. zu Einstellungskriterien, die über die Hard- und Soft-Skills hinausgehen)	Sensibilisierung der Mitarbeiter
TECHNOLOGIE-ENTWICKLUNG	*individuell- und kollektiv-explizit*[1]*:* Neu- und Weiterentwicklungen jeder Art (Logistiksysteme, Produkte, Produktionsprozesse), Maßnahmen zur Optimierung der Geschäftstätigkeit	Informationsabfluss durch illoyale Mitarbeiter, Gesprächsabschöpfung, Social Engineering, Hacking von Systemen und neue Technologien, Diebstahl von Datenträgern, Verwendung technischer Hilfsmittel	Bautechnische Absicherung, Vergabe von Zugangs- und Zutrittsrechten, Sensibilisierung der Mitarbeiter, Geheimhaltungsvereinbarungen, IT-Sicherung durch Passwörter und regelmäßige Updates, Aufsicht kurzzeitig eingesetzter Kräfte, Verschlüsselung
	individuell-implizit[1/2]*:* Kreativität der Wissenschaftler, Entwickler, Konstrukteure und Mitarbeiter; Kombinationsgabe	Abwerben der Mitarbeiter (meist in Zusammenhang mit Spionageaktivitäten im Personalbereich; Head-Hunter)	Sensibilisierung der Mitarbeiter, Abwehr von Head-Hunter-Anrufen

Wertaktivität	Wissensformen	Spionagemethoden	Schutzmaßnahmen
BESCHAFFUNG	*kollektiv-explizit*[1]*:* Lieferantendaten, Vertragskonditionen, Bewertungen, Reklamationsquoten, Beschaffungswege; Produktmerkmale, Informationen zur Unternehmensplanung	Diebstahl von Speichermedien, Hacking von IT-Systemen, Informationsverlust durch illoyale Mitarbeiter, Social Engineering	sorgfältige Auswahl von Mitarbeitern und Lieferanten (Vertraulichkeitsvereinbarungen), Sensibilisierung der Mitarbeiter, Aufsichtspflicht für kurzzeitig eingesetzte Kräfte, Zugangs- und Zugriffsbeschränkungen, bautechnische Absicherung, regelmäßige Updates der IT-Software
	kollektiv-implizit[2/3]*:* Verhaltensregeln im Umgang mit Lieferanten (Unternehmensleitlinien)	Gesprächsabschöpfung, Social Engineering	Sensibilisierung der Mitarbeiter

Quelle: eigene Darstellung.

Legende: [1] stark spionagegefährdet

[2] spionagegefährdet

[3] weniger spionagegefährdet

Die Autoren

Prof. Dr. Carsten Fussan studierte Wirtschaftswissenschaften an der Freien Universität Berlin und promovierte ebendort über die Thematik der Entstehung von Wettbewerbsvorteilen in innovativen Unternehmen. Zu Beginn seiner beruflichen Tätigkeit arbeitete Prof. Dr. Fussan zwischen 1993 und 1999 u.a. als Abteilungsleiter Vorstandsstab einer Investmentbank. Im Laufe seines weiteren Berufslebens nahm er verschiedene Management-Positionen bei IBM sowie Tätigkeiten als Managementberater u.a. bei der Top-5 US-Beratungsgesellschaft Deloitte Consulting wahr. Inhaltliche Schwerpunkte dieser Positionen waren insbesondere strategisches Wachstumsmanagement und die Entwicklung von Wagnisunternehmen (Spin-offs, Neugründungen, Ausgründungen). Bei IBM oblag Prof. Dr. Fussan u.a. die Leitung eines innovativen Produktbereiches für die Region EMEA (Europe, Middle East, Africa).
Der Wechsel in die wissenschaftliche Laufbahn erfolgte 2005/2006 durch Erstberufung an die Ohm Hochschule Nürnberg. 2007 wechselte Prof. Dr. Fussan an die Hochschule Anhalt und vertritt hier das Lehr- und Forschungsgebiet „Entrepreneurship“ (Unternehmensgründungen). Prof. Dr. Fussan ist Gründungsbeauftragter der Hochschule Anhalt und Koordinator des Masterstudienganges „Betriebswirtschaft und Unternehmensführung“.

Christina Maren Witte, Diplom Betriebswirtin (FH). Studium International Business an der Ohm Hochschule in Nürnberg von 2001 bis 2006. Thema der Diplomarbeit: Krisenpräventionsmanagement am Beispiel Produkt- und Markenpiraterie in China (ausgezeichnet mit dem Förderpreis der Ohm Hochschule). Seit Oktober 2007 bei der s.Oliver Bernd Freier GmbH&Co.KG in Rottendorf, Senior Country Merchandiser.

Selina C. W. Rehn, Diplombetriebswirtin (FH), studierte in Nürnberg an der Ohm Hochschule Betriebswirtschaft. Während ihres Studiums arbeitete sie als wissenschaftliche Mitarbeiterin am Forschungsprojekt „Produktpiraterie“ unter der Leitung von Prof. Dr. C. Fussan. Frau Rehn engagierte sich neben dem Studium als Studentenvertreterin, Tutorin für Studienanfänger sowie als Mitglied im studentischen Konvent. Seit Mitte 2008 ist Frau Rehn bei Highland Opportunity Limited in Schottland als Business Services Officer tätig. Dort liegen ihre Schwerpunkte in der Förderung und Beratung von Jung- bzw. Wachstumsunternehmen in den schottischen Highlands.

Marion Fricke, Diplombetriebswirtin (FH), Studium der Betriebswirtschaft an der Hochschule Anhalt (FH) in Bernburg von 2003 bis 2008. Forschungsthema: Maßnahmen gegen Produktpiraterie im Bereich Logistik. Seit 2008 bei der Licht & Ton Union e.K. in Magdeburg, Assistentin der Geschäftsleitung. Seit 2009 nebenberuflich Gesellschafterin des Reitbetriebes Fricke GbR in Heyrothsberge sowie Vorstandsmitglied des Reitsportzentrums Heyrothsberge e.V.

Gundula Warnecke, Betriebswirtin (BA), studierte von 2005 bis 2008 Betriebswirtschaft an der Hochschule Anhalt (FH). Ihre Bachelorarbeit befasste sich mit möglichen Schwachstellen der Porter'schen Wertschöpfungskette, die im Rahmen eines Industriespionageangriffs ausgenutzt werden können, sowie deren präventive Beseitigung. Seit Oktober 2008 studiert sie Unternehmensführung (MA) an der Hochschule Anhalt (FH), mit Schwerpunkt Strategisches Management. Zudem ist sie seit 2009 als wissenschaftliche Mitarbeiterin im Forschungsteam „Produktpiraterie" unter Leitung von Prof. Dr. Fussan tätig.