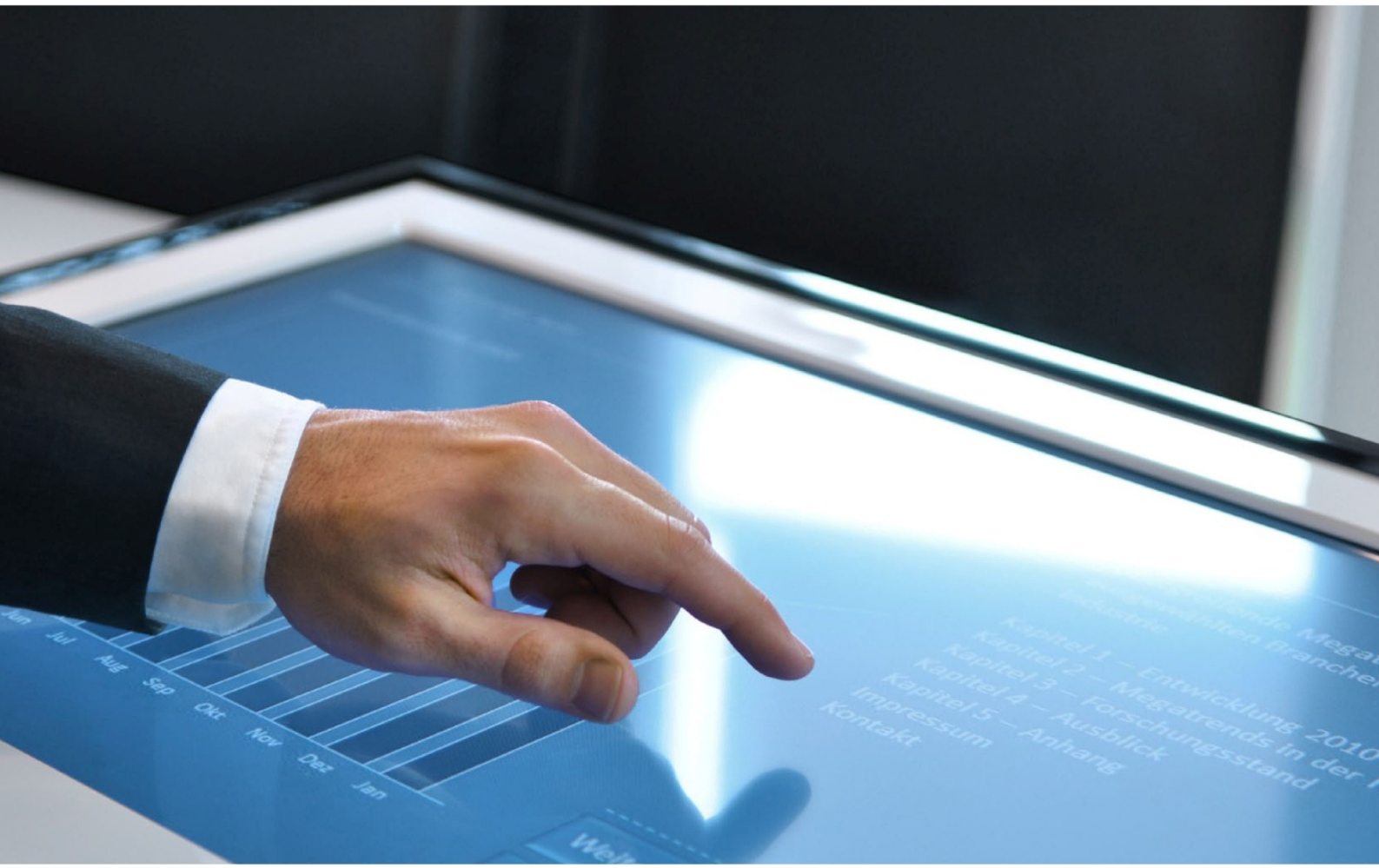
bayme vbm

Die bayerischen Metall- und Elektro-Arbeitgeber



Forschungsbericht

Strategien zur Piraterieabwehr

Stand: Januar 2011
www.baymevbm.de/pirateriesschutz

Vorwort

Umsetzungsorientierte Strategien zum Schutz Ihrer Innovationen

---

Internationalisierung ist einer der Erfolgsfaktoren, den auch kleine und mittelständische Unternehmen für sich nutzen. Die innovativen Produkte unserer bayerischen Unternehmen sind weltweit gefragt.

Doch die Globalisierung der Weltwirtschaft bringt auch neue Herausforderungen für die Unternehmen mit sich. Die Sicherung des technologischen Vorsprungs unserer Unternehmen wird zu einem wesentlichen Faktor im internationalen Wettbewerb. Innovative Technologien, Prozesse und Verfahren müssen für die eigenen Produkte genutzt und vor dem Zugriff durch Produktpiraterie geschützt werden. Nur so wird es unseren Unternehmen gelingen, ihren Spitzenplatz in der Welt zu erhalten.

Effektiver und effizienter Technologieschutz spielt dabei eine wesentliche Rolle. In der KME – Kompetenzzentrum Mittelstand GmbH haben wir dieses Thema aufgegriffen und beim Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum der Technischen Universität München ein Forschungsprojekt mit dem Thema „Strategien zur Piraterieabwehr für den Mittelstand“ in Auftrag gegeben. Die KME – Kompetenzzentrum Mittelstand GmbH wurde vom vbm – Verband der Bayerischen Metall- und Elektroindustrie e. V., zusammen mit der Technischen Universität München gegründet, um für Mitgliedsunternehmen relevante Forschungsprojekte durchzuführen.

Die Studie zeigt Ihnen auf, welche Felder insbesondere für mittelständische Unternehmen wichtig sind. Best-Practice-Beispiele und Handlungsempfehlungen unterstützen Sie, die für Ihr Unternehmen richtige Strategie zum Technologieschutz zu finden.

Bertram Brossardt
Januar 2011

Inhalt

1 Technologieschutz bayerischer KMU in der Metall- und Elektroindustrie

Globalisierung erfordert Anpassung des Technologieschutzes

Die Globalisierung der Weltwirtschaft betrifft schon lange nicht nur Großunternehmen, sondern längst auch mittelständische Unternehmen der bayerischen Metall- und Elektroindustrie. Durch die Erstreckung ihrer Geschäfte ins Ausland profitieren sie einerseits von neuen, stark wachsenden Absatzmärkten und stellen Nähe zu den Großkunden wieder her, die schon früh ins Ausland abgewandert waren. Andererseits stellt diese Globalisierung deutsche Unternehmen jedoch vor große Herausforderungen, denn der globale Wettbewerb ist geprägt von Konkurrenz aus Niedriglohnländern, von Produktpiraterie, von marktmächtigen Großkunden und von kürzer werdenden Technologiezyklen. Herausragende Qualität allein („Made in Germany“) ist dagegen immer weniger ein Mittel, denn Wettbewerber aus Schwellenländern holen auch hier auf und erreichen mittlerweile vielfach ähnliche Qualitätsstandards zu günstigeren Preisen. Über den Erfolg und das Überleben unserer mittelständischen Wirtschaft entscheiden werden damit mehr noch als früher Innovationskraft und Kosteneffizienz. Nur sie sichern nachhaltig Wettbewerbsfähigkeit auf den globalen Märkten. *Effektiver Technologieschutz ist hier nicht nur eine wesentliche Voraussetzung, sondern ein Kernaspekt*. Jedes technologiegetriebene KMU der bayerischen Metall- und Elektroindustrie steht damit vor der Aufgabe, seine Innovationen wirksam zu konkurrenzfähigen Kosten zu schützen, denn nur so lassen sich die Chancen der Globalisierung effektiv nutzen.

Dieser Bericht stellt aktuelle Probleme und Risiken des Technologieschutzes für die zahlreichen innovativen und technologieintensiven Unternehmen der bayerischen Metall- und Elektroindustrie (M+E Industrie) vor. Anhaltspunkte, inwieweit auch KMU der bayerischen M+E Industrie von diesen Risiken betroffen sind und inwieweit diese Risiken dort auch gesehen werden, wurden durch Workshops und Interviews mit bayme vbm Mitgliedsunternehmen gewonnen. Analysiert wurde auch der dort konkret praktizierte Technologieschutz. Um Schwächen und Optimierungspotentiale von Schutzkonzepten zu verdeutlichen, die bayerische KMU derzeit praktizieren, werden diesen empirischen Befunden die Methoden des Technologieschutzes gegenübergestellt, die in der Wissenschaft erarbeitet worden sind und diskutiert werden. Umgesetzt und für die bayme vbm Mitgliedsunternehmen handhabbar gemacht werden die erzielten Befunde durch *Orientierungshilfen in Form von Checklisten sowie durch Handlungsempfehlungen*, deren Umsetzung die Effektivität von Technologieschutz steigert – vielfach bei reduzierten Kosten.

Dass es *keine allgemeingültige „Best-Practice“-Lösung im Sinne eines „One Size Fits All“* gibt, versteht sich dabei von selbst. Zu sehr ist die Schlagkraft der unterschiedlichen Schutzmaßnahmen individuell bestimmt und hängt diese von verschiedenen Faktoren ab, z. B. dem Schutzgegenstand sowie der Größe, dem Wettbewerbsumfeld und der Ziele des Unternehmens. Unsere Handlungsempfehlungen sollen darum primär als

Anregungen dienen, um für jedes Unternehmen individuell zu prüfen, inwieweit die vorgeschlagene Maßnahmen konkret Verbesserungspotential für den eigenen Technologieschutz bieten.

Abbildung 1
Vorgehensweise

Bild: Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum

2 Verschärfung des Wettbewerbs

Wettbewerbsvorteile sichern durch effektiven und kosteneffizienten Technologieschutz

Der Wettbewerb, dem bayerische Unternehmen weltweit ausgesetzt sind, gewinnt weiter an Härte. Im Technologieschutz äußert sich diese zunehmende Wettbewerbsintensität unter anderem durch das Auftreten von Produktpiraterie. Oder anders gewendet: Produktpiraterie ist Teil der neuen Herausforderungen für Unternehmen und ihren Technologieschutz. Um ihr zu begegnen, bedarf es (auch) eines effektiveren Technologieschutzes, um den eigenen technologischen Vorsprung und die damit verbundenen Wettbewerbsvorteile auf den Märkten der globalen Welt zu sichern.

Schon jetzt werden steigende Anteile des F+E Budgets von Unternehmen für den Erwerb gewerblicher Schutzrechte verwendet, v. a. für Patente, Gebrauchsmuster, Geschmacksmuster und Marken. In technologieintensiven Branchen fließen bis zu fünf Prozent der F+E Budgets in die Erlangung und den Erhalt von Schutzrechten – ohne Durchsetzungs- und Verteidigungskosten, die diesen Anteil noch erheblich steigern können.[1] *Technologieschutz muss damit auch kosteneffizient sein*, damit er F+E Budgets nicht unnötig belastet und am Ende die Innovationskraft der betroffenen Unternehmen mindert.

2.1 Wie begegnen bayerische KMU dieser Herausforderung?

Unsere Gespräche mit bayerischen KMU der Metall- und Elektroindustrie haben ergeben, dass sowohl Patentschutz als auch Geheimhaltung besonderer Stellenwert beim Technologieschutz zukommt. Während Patente in der Regel für Erfindungen in Technologiebereichen angemeldet werden, bei denen die Möglichkeit zum Reverse Engineering besteht, werden namentlich Herstellungsverfahren und Materialbehandlungen häufig nicht durch Patentierung geschützt, sondern durch Geheimhaltung.

2.1.1 Patentmanagement

Patente melden Unternehmen meist in Staaten an, in denen Sie F+E betreiben, die geschützte Erfindung an Produktionsstandorten auswerten oder die so hergestellten Produkte anbieten wollen. Angemeldet werden vorwiegend Technologien, die Anwen-

[1] *Bader,* in: Gassmann / Kobe Management von Innovation und Risiko: Quantensprünge in der Entwicklung erfolgreich managen, S. 469f.

dung in Produkten finden sollen. Gelegentlich werden vielversprechende Technologien aber auch abstrakt durch sog. Vorratspatente geschützt. Andere strategische Ziele einer Patentanmeldung als die eigene kommerzielle Verwertung einer Technologie, wie z. B. die Generierung von Lizenzeinnahmen, scheinen von Unternehmen der M+E Industrie selten verfolgt zu werden, sind beispielsweise für Startups aber durchaus vorstellbar.

Entschieden wird über den angestrebten Schutz und den Schutzansatz (Patentanmeldung oder Geheimhaltung) meist von einem feststehenden Personenkreis, also einem Gremium. In manchen Unternehmen entscheiden auch nur Einzelpersonen über den richtigen Technologieschutz und müssen diese Personen lediglich bei Überschreitung eines bestimmten Betrags eine Genehmigung einholen.

Wenig etabliert scheinen Prozesse für ein regelmäßiges Controlling von Patentportfolios, obwohl dies zur Entscheidung über die Aufrechterhaltung von Patenten nützlich wäre, deren Jahresgebühren (Annuitäten) mit zunehmendem Alter progressiv ansteigen.

Einige Unternehmen werden durch eingeschränkte Budgets für den Technologieschutz zu strategischen Entscheidungen gezwungen. Steigender Kostendruck, in 2008 / 2009 forciert durch die Wirtschaftskrise, veranlasste diese Unternehmen, stärker auf die Wirtschaftlichkeit ihres Patentwesens zu achten und Patentanmeldungen stärker als früher auch wirtschaftlich zu betrachten. Auch die Länderauswahl bei der Patentanmeldung wird so – zu Recht – stärker strategisch betrachtet. Technologien werden nur noch für traditionelle Schlüsselmärkten patentiert. Abgedeckt werden soll ein Anteil des Gesamtmarkts, der so groß ist, dass das Auftreten als Wettbewerber in den übrigen, unbedeutenden Märkten sich nicht lohnt. Soweit Wachstumsmärkte wie China bei der Länderauswahl nach wie vor ignoriert werden, scheint noch an der überkommenen Unternehmensvision festgehalten zu werden, das Kerngeschäft nur in den traditionellen Märkten des Unternehmens zu schützen. Ob diese Entscheidung heute noch strategisch sinnvoll ist, erscheint fraglich (s. a. unten *Kapitel 4 Technologieschutz in China*).

Nur wenige der befragten bayerischen KMU verfügen über ein strategisches Patentmanagement und verfolgen mit Patentanmeldungen andere strategische Ziele als die Sicherung der eigenen Technologieverwertung. Unternehmen, die über ein strategisches Patentmanagement verfügen, melden beispielsweise auch Sperrpatente für Substitutionstechnologien zu selbstgenutzten Technologien an. Eingesetzt werden vereinzelt auch „Verwirrungspatente“ mit dem Ziel, die Konkurrenzbeobachtung von Wettbewerbern in der Weise zu behindern, dass diesen Entwicklungstrends vorgetäuscht werden, die die Anmelder in Wahrheit gar nicht weiter verfolgen. Die betreffenden Anmelder wollen sich so Zeitvorteile in der Produktentwicklung verschaffen. Jährlich lassen diese Unternehmen ihre Schutzrechte von definierten Gremien daraufhin analysieren, ob die Schutzrechte ihren Zweck erfüllen und ob sie mit Blick auf die Lebenszyklen der von ihnen betroffenen Produkte aufrechterhalten oder fallengelassen

werden sollen. Ähnlich verfahren diese Unternehmen bei der Anmeldung neuer Patente.

2.1.2 Geheimhaltung

Unsere Gespräche mit bayerischen KMU zeigen, dass Know-how namentlich für Herstellungsverfahren sowie Materialbehandlungen häufig durch Geheimhaltung gesichert wird, dass Technologieschutz hier also nicht *rechtlich* durch Patentanmeldung realisiert wird, sondern *faktisch* durch Geheimhaltung (Know-how-Schutz). Einige der befragten Unternehmen sehen in ihrem geheimen Know-how einen deutlichen Wettbewerbsvorteil, weil sie dadurch zu geringen Kosten nachhaltig eine hohe Produktqualität erzielen können, die nicht imitierbar ist, weil Unternehmensgeheimnisse gegen widerrechtliche Aneignung auch ohne die Offenlegung geschützt sind, die das Patentrecht für die Patenterteilung erfordert. Gleichwohl stehen auch für Unternehmen, die bewusst auf Know-how-Schutz setzen, Know-how-Schutz und Patentschutz nebeneinander. Nicht alle technischen Innovationen sind geheimschutzfähig. Unverzichtbar sind Patente vielfach gerade für den Schutz des Ersatzteilgeschäfts, in dem meist Unternehmensfremde die eigenen Produkte einbauen oder anderweitig verwenden.

2.2 Maßnahmen eines wirksamen und kosteneffizienten Technologieschutzes (Patentschutz vs. Know-how-Schutz)

Im Ergebnis sind sowohl Patentschutz als auch Know-how-Schutz wirksame Methoden des Technologieschutzes. Welche der beiden im Einzelfall besser geeignet ist, kann nicht pauschal, sondern nur mit Blick auf den Einzelfall beantwortet werden. Stets zu beachten ist freilich, dass Know-how-Schutz nur für geheimschutzfähige Informationen eine Alternative zum Patentschutz darstellt.

Abbildung 2
Technologieschutz

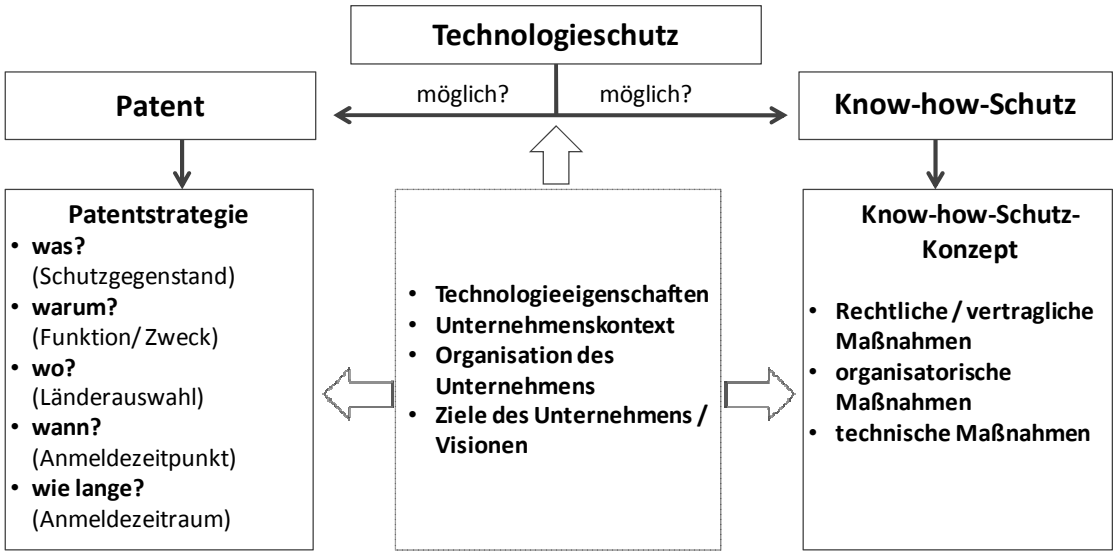


Bild: Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum

2.2.1 Unterschiedliche Schutzvoraussetzungen

Der Begriff Know-how ist im deutschen Recht nicht definiert. Das deutsche Rechts spricht stattdessen von Betriebs- und Geschäftsgeheimnissen, was insofern treffender ist, also die Geheimnisqualität deutlich wird, die eine Information aufweisen muss, damit Schutz besteht. Betriebsgeheimnisse sind Geheimnisse technischen Inhalts, Geschäftsgeheimnisse sind nicht-technische Geheimnisse, vorwiegend kaufmännische, wie z. B. Kundendaten.[2] Um Schutz als *Betriebs- und Geschäftsgeheimnis* zu genießen, muss eine Information jede der folgenden *vier Voraussetzungen* erfüllen:

– Nichtoffenkundigkeit,
– Unternehmensbezogenheit,
– Geheimhaltungsinteresse des Unternehmers,
– Geheimhaltungswille des Unternehmers.[3]

[2] *Kraßer,* Der Schutz des Know-how nach deutschem Recht, GRUR 1970, 587.
[3] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 20.

Nach dieser Definition fallen Innovationen nicht unter den gesetzlichen Know-how-Schutz, die durch Reverse Engineering nachgeahmt werden können, denn hier fehlt die Voraussetzung der Nichtoffenkundigkeit. Anders als Patentschutz schützt Know-how-Schutz nicht eine Information als solche, sondern lediglich den Zugang zu ihr.[4]

Die *materiellen Patenterteilungsvoraussetzungen* nach § 1 Abs. 1 PatG setzen anders an. Hier geht es um den Schutz einer technischen Informationen als solcher. Er erfordert, dass eine Information technisch, neu, erfinderisch und gewerblich anwendbar ist. Das erlaubt den Schutz von Technologien, die sich nicht geheim halten lassen, wie im Maschinenbau nicht selten der Fall. Umgekehrt eignet sich Know-how-Schutz für Technologien, die beispielsweise nicht technisch sind oder die für ein Patent zu wenig Erfindungshöhe aufweisen. Trotz Patentfähigkeit häufig nicht patentiert bleiben Verfahren, weil die Verletzung von Verfahrenspatenten häufig schwer nachweisbar ist. Hier ist Know-how-Schutz häufig die zielführendere Alternative.[5]

2.2.2 Vor- und Nachteile

Weil beide Schutzansätze spezifische Vor- und Nachteile mit sich bringen, sind keine pauschalen Aussagen darüber möglich, welche der beiden Schutzansätze allgemein vorzugswürdig ist. Stattdessen kommt es auf den Einzelfall an, z. B. auf die Art der zu schützenden Information, auf die Wettbewerbssituation des Unternehmens, dessen Unternehmensziele und -organisation, Bedrohung durch Piraterie etc.

Ein wesentlicher Nachteil des Patentschutzes ist sein Offenlegungserfordernis, denn es kann das Problem Produktpiraterie verschärfen. Insbesondere in Ländern mit einer fragwürdigen Rechtsdurchsetzung verdient dieser Aspekt besondere Beachtung (*s. Kapitel 4*). Weltweit kann vorhandenes technologisches Wissen über Patentdatenbanken ohne nennenswerte Kosten abgerufen werden, was Produktpiraten ab Veröffentlichung von Patentanmeldungen (spätestens 18 Monate nach Erteilung) zum Nachbau befähigen kann, also nicht selten noch vor Patenterteilung.[6] Problematisch ist auch die komplette Schutzlosigkeit von Erfindungen, deren Patentanmeldung das Patentamt zurückgewiesen hat. Weil sie im Erteilungsverfahren offengelegt worden sind, besteht für sie auch kein Know-how-Schutz.[7] Ein weiterer Nachteil des Patentschutzes ist seine auf 20 Jahre begrenzte Laufzeit (§ 16 Abs. 1 PatG), der vor allem für Grundlagenpatente ein Problem sein kann, also für Erfindungen, die nicht rasch veralten. Auch aus Kostensicht spricht einiges für Know-how-Schutz, also für Geheimhaltung. Während

---

[4] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 23.
[5] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 404.
[6] *Ann / Grüneis,* Herausforderung, Produktpiraterie - Sind Patente heute noch sinnvoll oder stärken Sie nur die Piraten?, Industrie Management 2008, 61.
[7] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 394.

die Amtsgebühren zur Erlangung und Aufrechterhaltung einer Patentfamilie in Europa bei einem breiteren Länderportfolio über zehn Jahre ca. 25.000 Euro kostet,[8] sind die Kosten des Know-how-Schutzes schwerer zu quantifizieren, weil viele der hier zu berücksichtigen Kosten Teil des Overheads sind und als solcher weniger leicht zuordenbar sind als Patentkosten. Kostenfaktoren des Patentschutzes sind Patentanwaltsgebühren, interne Personalkosten (Patentingenieure), Amtsgebühren und bei ausländischen Patentanmeldungen Übersetzungskosten.[9] Kostenrisiken birgt darüber hinaus die Durchsetzung des Patentschutzes vor Gericht (Verletzungsprozesse) sowie die Verteidigung des Patents vor dem Bundespatentgericht (BPatG).

Freilich birgt der Patentschutz auch Vorteile gegenüber dem Know-how-Schutz. Beispielsweise wird ein Patent regelmäßig die Unternehmensfinanzierung erleichtern. Viele Kapitalgeber sind patentfixiert, und nicht patentgeschützte Erfindungen sind aus naheliegenden Gründen erheblich schwerer zu kommunizieren als solche, für die Patentschutz besteht.[10] Zusätzlich besteht stets die Gefahr, dass Know-how von Wissensträgern, v. a. Arbeitnehmern und Kunden verraten wird oder dass es auf unlauterem Weg aufgedeckt wird. Diese Problematik wird später in den *Kapiteln 6.3 und 6.4* nochmals aufgegriffen werden.

Ganz grundsätzlich besteht beim Know-how-Schutz generell das Risiko, dass Dritte eine Parallelerfindung machen und zum Patent anmelden. Zwar kann der Ersterfinder seine Erfindung dann nach § 12 PatG weiterhin für eigene Zwecke nutzen. Die interessantere kommerzielle Auswertung seiner Erfindung ist ihm dann jedoch versperrt. Ein Mittel zur Verhinderung der Patentierbarkeit von Parallelerfindungen sind sogenannte Defensivpublikationen, durch die ein neuheitsschädlicher Stand der Technik geschaffen wird.[11]

Durch eine geschickte Patentstrategie sind andererseits Wettbewerbsvorteile zu erzielen. Effizienzgewinne ermöglicht beispielsweise eine geschickte Länderauswahl. In einigen Branchen ist eine Beschränkung des Schutzes auf wichtige Schlüsselmärkte oder sogar nur einen Kernmarkt ausreichend. Der ermöglicht Kosteneinsparungen, ohne Wirksamkeitsverluste für den Technologieschutz.[12] Schlüsselmärkte müssen nicht zwangsläufig durch ihre aktuelle Bedeutung definiert sein. Vielmehr sollten Entscheidungen die gesamte Patentlaufzeit von maximal 20 Jahren im Auge behalten[13] und sollte ein regelmäßiges Patentcontrolling Schutzrechte identifizieren, die keinen

---

[8] *Gassmann / Bader*, Patentmanagement: Innovationen erfolgreich nutzen und schützen, S. 44.
[9] *Ann* in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 51.
[10] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 57f.
[11] *Henn,* Defensive Publishing, S. 11 ff; *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 63.
[12] *Harhoff / Reitzig,* Strategien zur Gewinnmaximierung bei der Anmeldung von Patenten, S. 21.
[13] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 440.

Nutzen mehr bieten oder versprechen, denn die Aufgabe derartiger Patente ermöglicht Kosteneinsparungen.

Von den weiteren Zielen, deren Verfolgung Patente über die Nutzung für eigene Fertigungen oder Vertriebe hinaus ermöglichen, war eingangs bereits die Rede. Spätestens seit Mitte der 80er Jahre haben spektakuläre Patentverletzungsklagen, wie z. B. zwischen Polaroid und Kodak, gezeigt, dass Patentschutz zu einem strategischen Instrument im Kampf um Märkte und Marktpositionen geworden ist.[14]

So werden beispielsweise *Sperrpatente* mit dem Ziel angemeldet, die Handlungsfreiheit (*Freedom to Operate*) von Wettbewerbern einzuschränken. *Sperrpatente* können aber auch eigene Technologien schützen, wenn diese Technologien substituierbar sind. Von strategischer Bedeutung können auch Patente sein, die *eigene Handlungsfreiheit* sichern und Abhängigkeiten von Schutzrechten Dritter vorbeugen.[15] Ferner kann durch eigene Schutzrechtanmeldungen Verhandlungsmasse für den Zugang zu anderen Technologien geschaffen werden *(Kreuzlizenzen)*.[16] Eine weitere strategische Maßnahme ist der Einsatz von *Verwirrungspatenten*, die von Ziel und Richtung eigener F+E ablenken sollen.[17] Schließlich lassen sich durch Patente auch schlichtweg Deckungsbeiträge in Form von *Lizenzeinnahmen* erwirtschaften oder lassen sich Patente für *Marketingzwecke* verwenden – auch im Hinblick auf Kapitalgeber.[18]

In summa sind die Möglichkeiten der Patentverwertung vielfältig – auch für KMU. Unsere Gesprächspartner nutzten diese Chance überwiegend nicht, sondern verfolgten fast durchgehend sehr konservative um nicht zu sagen „traditionelle“ Patentstrategien. Gleichzeitig fehlten vielfach definierte Prozesse zum Patentportfolio-Controlling, was vermuten lässt, dass mit Blick sowohl auf Kosten als auch auf Patentverwertung Verbesserungspotentiale bestehen. Bemerkenswert war stattdessen die vielfach wenig systematische Art der Entscheidungsfindung im Patentwesen. Weder waren Potentiale und Probleme der unterschiedlichen Schutzansätze (IP-Schutz – Know-how-Schutz) umfassend bekannt, noch wurden diese für jeden Schutzgegenstand systematisch geprüft. Stattdessen beobachteten wir die gewisse Beliebigkeit eines Vertrauens auf eigene Erfahrungen aus der Vergangenheit.

---

[14] *Harhoff / Reitzig,* Strategien zur Gewinnmaximierung bei der Anmeldung von Patenten, S. 3.
[15] *Gassmann / Bader*, Patentmanagement: Innovationen erfolgreich nutzen und schützen, S. 26; *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 436.
[16] Gassmann / Bader, Patentmanagement: Innovationen erfolgreich nutzen und schützen, S. 26.
[17] *Reitzig,* Politik der Zäune, in: Wirtschaftswoche, 29 / 2004 (http://www.wiwo.de/unternehmen-maerkte/politik-der-zaeune-352046/) (Stand: 29.01.2011).
[18] *Gassmann/Bader*, Patentmanagement: Innovationen erfolgreich nutzen und schützen, S. 26.

Abbildung 3
Checkliste – Schutzstrategie

Checkliste – Schutzstrategie

- Prüfen, welche Schutzansätze sinnvoll sind
- Entscheidung für einen Schutzansatz treffen – auch unter Kostenaspekten
- Patentanmeldungen
  - Länderauswahl (Fertigungen/Märkte/Wettbewerber)
  - Strategische Ziele (Schutz eigener Fertigung, Lizenzeinnahmen, Marktsperrung, Verwirrung von Wettbewerbern etc.)
- Patent-Controlling
  - Aufrechterhaltung von Patenten nach konkretem Mehrwert
  - anderweitige Verwertung ungenutzter Patente (durch Verkauf, Lizenzierung) oder Aufgabe

Bild: Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum

3 Auslaufen des Patentschutzes

Technologieschutz durch Patente ist zeitlich begrenzt

Nach § 16 Abs. 1 S. 1 PatG beträgt die Schutzdauer für Patente maximal 20 Jahre ab prioritätsbegründender Anmeldung beim Patentamt. In der Pharmaindustrie und im Pflanzenschutz kann dieser Schutz aufgrund der langen Zulassungsverfahren durch sog. ergänzende Schutzzertifikate um fünf Jahre verlängert werden (§ 16 a Abs. 1 PatG).

Durch die Laufzeitbegrenzung des Patentschutzes können daraus keine langfristigen Wettbewerbsvorteile entstehen. Das zeigt insbesondere die Pharmabranche. Wie groß der Nutzen vieler Patente bis zum Auslaufen des Schutzes gleichwohl noch ist, zeigt die Dimension des Generikamarkts.[19] In den meisten Industrien werden für Patente aufgrund kürzerer Technologiezyklen gleichwohl nicht einmal die möglichen 20 Jahre ausgenutzt, sondern liegt die durchschnittliche Schutzdauer für deutsche Patente bei rund 13 Jahren.[20] Gleichwohl sind auch in der M+E Industrie wertvolle Grundlagenerfindungen betroffen, die als Teil der grundsätzlich bestehenden *Nachahmungsfreiheit* nach Ablauf der Schutzdauer von jedermann legal kopiert werden dürfen. Das kann starke Umsatzeinbrüche nach sich ziehen, sofern die bis dato geschützten Technologie wirtschaftlich noch Bedeutung besitzt.

3.1 Wie bereiten sich bayerische KMU auf das Auslaufen von Patenten vor?

Die meisten unserer Gesprächspartner scheinen die Beschränkung des Patentschutzes auf 20 Jahre nicht als Problem zu empfinden. Hauptgrund dafür sind die branchentypischen Technologielebenszyklen in der M+E Industrie. In den meisten Fällen erfordern sie nicht die Aufrechterhaltung von Patenten bis zum Ablauf der maximalen Schutzdauer. Auch beim Technologieschutz scheint das Thema kaum Schwierigkeiten zu bereiten, denn es wurde nur selten erwähnt.

Aufgefangen wird das Problem wegfallender Exklusivität durch gezielt eingesetzten Markenschutz. Nach Auslaufen des Patentschutzes soll Mitbewerbern der Markteintritt

[19] Nach einer Studie von Accenture erwirtschafteten Generika 2004 rund zehn Prozent (47,9 Mrd. Euro) der weltweiten Arzneimittelumsätze zu Herstellerabgabepreisen. *Accenture*, Die Bedeutung der Generikaindustrie für die Gesundheitsversorgung in Deutschland (http://www.accenture.com/NR/rdonlyres/C55589E4-D171-42DE-8DD0-9ACABD5B3851/0/Generika_in_D_2005_Accenture.pdf) (Stand: 12.1.2011).

[20] Nach zehn Jahren ist nur noch die Hälfte der Patente vor dem EPA aufrecht erhalten. *EPO, JPO, KIPO and USPTO*, Four Office Statistics Report 2009, S. 47 (http://www.trilateral.net/statistics/tsr/fosr2009/report.pdf) (Stand: 29.01.2011).

dadurch erschwert werden, dass bekannte Marken, die für die Qualität vormals patentgeschützter Produkte stehen, die bestehenden Absatzkanäle gefestigt haben.

3.2 Produktschutz nach Auslaufen des Patentschutzes

Schon vor Auslaufen ihrer Patente sollten Unternehmen daher auf *komplementären Patent- und Markenschutz* setzen. Während Patente die Technologie selbst schützen, zielt Markenschutz vorrangig auf die Kundenschnittstelle ab.[21] Durch den Aufbau einer starken Marke während der Patentlaufzeit wird beim Kunden eine starke Assoziation zwischen Marke und den Produkten erzeugt, die die patentgeschützte Technologie enthalten. Dies ist vorteilhaft, wenn der Patentschutz ausläuft. Studien aus der Arzneimittelindustrie zeigen, dass der Wert des Produktes nach Auslaufen des Patents stark vom Marketing des Produkts während der Patentlaufzeit abhängt. Trotz der Konkurrenz durch Generika lassen sich nach Auslaufen des Patentschutzes noch erhebliche und in diesem Umfang erstaunliche Umsatzerlöse aus Arzneimitteln erzielen, wenn diese konsequent unter einem Markennamen vertrieben wurden. Das prominenteste Beispiel dafür ist die Marke Aspirin für den aus reinsynthetischer Acetylsalicylsäure bestehenden Schmerzhemmer der Firma Bayer AG (nun Bayer-Schering). Das zugehörige Patent lief schon zu Beginn des vorigen Jahrhunderts aus, doch wegen des starken Markennamens ist das Produkt nach wie vor verbreitet und profitabel. Gut positionierte Marken können als *Marktzutrittssperren* für Konkurrenten fungieren.[22] Kann so erreicht werden, dass der Markt vor Nachahmungen geschützt wird, hat der Markenschutz ähnliche Wirkungen wie der Patentschutz. Auch nach Ablauf des Patentschutzes muss eine Marke durch zielgruppenspezifisches Marketing weiter gepflegt werden. Dies ist möglich und sinnvoll, weil Markenschutz zeitlich unbegrenzt aufrecht erhalten werden und daher langfristig Schutz bieten kann.

Selbstredend darf die Marke nicht nur bekannt sein, sondern muss darüber hinaus auch *Qualität* mit ihr in Verbindung gebracht werden. Idealerweise erzeugt ein Unternehmen noch während der Patentlaufzeit ein derartiges *Markenimage*. Beispielsweise können durch den Patentschutz einer Erfindung *werbliche Vorteile* generiert werden, indem dieser Schutz ins Marketing eingebunden wird, z. B. durch Sichtbarmachung der Patente auf der Web-Site des Unternehmens.[23]

Neben dem Einsatz von Marken kann auch der komplementäre Gebrauch anderer Schutzrechte, wie z. B. *komplementärer Patentschutz*, den Schutz einer Technologie

---

[21] *Gassmann / Bader*, Patentmanagement: Innovationen erfolgreich nutzen und schützen, S. 253.
[22] *Reitzig,* Politik der Zäune, in: Wirtschaftswoche, 29 / 2004 (http://www.wiwo.de/unternehmen-maerkte/politik-der-zaeune-352046/) (Stand: 29.01.2011).
[23] *Reitzig,* Politik der Zäune, in: Wirtschaftswoche, 29 / 2004 (http://www.wiwo.de/unternehmen-maerkte/politik-der-zaeune-352046/) (Stand: 29.01.2011).

nach Auslaufen früher erlangter Patente sichern. Kann der betreffende Schutzgegenstand beispielsweise mit einer weiteren Technologie gebündelt oder gekoppelt werden, deren Schutzrecht noch länger besteht, kann dies den Absatz einer ungeschützten Technologie sichern helfen. In der Pharmaindustrie profitiert beispielsweise das dänische Pharmaunternehmen Leo Pharma von dieser Strategie. Durch Bündelung zweier Mittel zu einem therapeutischen Ansatz kann der Absatz des Mittels, dessen Patentschutz als erstes auslaufen wird, durch den Patentschutz des anderen Mittels kompensiert werden.[24] Wenngleich sich diese Methode im Gegensatz zum komplementären Gebrauch von Marken nur in Einzelfällen eignet, ist sie prinzipiell auch in der M+E Industrie anwendbar.

Eine gängige Methode im Maschinen- und Anlagenbau ist die Kopplung eines Produkts mit produktbegleitenden Dienstleistungen. Als dem Produkterwerb nachgelagerte Leistungen, die überdies dauerhaften Kundenkontakt erfordern, steigern diese Leistungen die Kundenbindung.[25] So können nicht nur zusätzliche Umsätze und Deckungsbeiträge erzielt werden, sondern wird nach Auslaufen des Patentschutzes auch der Marktzutritt für Wettbewerber erschwert. Hauptsächlich bietet sich dieses Geschäftsmodell für Maschinen- und Anlagenhersteller an und bietet die beschriebene Kundenorientierung prinzipiell eine Maßnahme zur Absatzsicherung sowie Schutz gegen Produktpiraten und legale Nachahmer.

In summa kann durch die Kombination juristischer Maßnahmen (z. B. Markenschutz) mit anderen Maßnahmen (z. B. Marketing oder Serviceangeboten) der Verlust einer Monopolstellung kompensiert werden, die während seiner Laufzeit ein Patent geboten hatte. Freilich müssen entsprechende Vorkehrungen frühzeitig vorbereitet und getroffen werden, denn nach Auslaufen des Patentschutzes ist es zu spät. Auch hier zeigt sich mithin die *Notwendigkeit eines strategischen Schutzrechtsmanagements*.

---

[24] *Reitzig,* Politik der Zäune, in: Wirtschaftswoche, 29/2004 (http://www.wiwo.de/unternehmen-maerkte/politik-der-zaeune-352046/) (Stand: 29.01.2011).
[25] *Lay / Jung Erceg,* in: Lay / Jung Erceg Produktbegleitende Dienstleistungen: Konzepte und Beispiele erfolgreicher Strategieentwicklung, S. 43.

Abbildung 4
Checkliste – Auslaufen des Patentschutzes

Checkliste – Auslaufen des Patentschutzes

- Komplementären Markenschutz vor Auslaufen des Patentschutzes aufbauen
- Sofern möglich komplementäre Patente anmelden
- Marketingfokus auf jahrelange Technologieerfahrung als Erfinder richten
- Durch produktbegleitende Dienstleistungen Kundenzufriedenheit und Kundenbindung schaffen

Bild: Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum

4 Technologieschutz in China

Produktpiraterie und schwache Schutzrechtsdurchsetzung in China erschweren effektiven Technologieschutz

Schon länger wird insbesondere die VR China mit Produktpiraterie und den daraus resultierenden wirtschaftlichen Schäden in Verbindung gebracht. Nach einer aktuellen VDMA Umfrage ist die Volksrepublik auch weiterhin unangefochten „Plagiatweltmeister". 79 Prozent der teilnehmenden VDMA-Mitglieder gaben an, von illegalen Imitationen aus China betroffen zu sein.[26] Auch alle Unternehmen der M+E Industrie sind gefordert, den Schutz ihres Geistigen Eigentums auf diese Herausforderung abzustimmen. Allerdings gestaltet sich das nicht einfach, da die Sinnhaftigkeit von Schutzrechtsanmeldungen in der VR China aufgrund der unsicheren Schutzrechtsdurchsetzung nach wie vor umstritten ist.

Patentanmeldungen erfordern die Offenlegung der Erfindung, für die Schutz begehrt wird. Allein dieser Umstand stellt schon ein Imitationsrisiko dar. Durch die Entwicklung der Informationstechnologie ist die Recherche von Patentanmeldungen und Patentdatenbanken von jedem Ort der Welt aus möglich, also auch aus Pirateriehochburgen. Da chinesische Unternehmen bekanntermaßen akribisch in außerchinesischen Patentdatenbanken nach technischem Know-how mit wirtschaftlicher Perspektive suchen, verzichten inzwischen viele Unternehmen darauf, ihre Erfindungen zum Patent anzumelden.[27] Zudem erweist sich die Durchsetzung von Schutzrechten in China als schwierig und teuer. Lokaler Protektionismus, Korruption und das Erfordernis der notariellen Beurkundung sämtlicher ausländischer Beweismittel für gewerbepolizeiliche Verfahren sowie Verletzungsprozesse behindern die effektive Schutzrechtsdurchsetzung. Da langwierige Prozesse für den Mittelstand häufig erfolglos oder von vornherein nicht finanzierbar sind,[28] hatte VDMA 2008 kurzzeitig sogar einmal von Patentanmeldungen in der VR China abgeraten, wenn die Produkte kein sehr komplexes technisches Know-how voraussetzen. Zu gering wurden die Chancen eingeschätzt, sich vor chinesischen Gerichten gegen chinesische Produktpiraten zur Wehr zu setzen.[29]

---

[26] VDMA-Umfrage zur Produkt- und Markenpiraterie 2010, S. 10 (http://www.pro-protect.de/1/fileadmin/downloads/VDMA%20Umfrage%20Produkt-%20und%20Markenpiraterie%202010.pdf) (Stand: 29.01.2011).

[27] *Ann / Grüneis,* Herausforderung, Produktpiraterie - Sind Patente heute noch sinnvoll oder stärken Sie nur die Piraten?, Industrie Management 2008, 61.

[28] *Ann / Grüneis,* Herausforderung, Produktpiraterie - Sind Patente heute noch sinnvoll oder stärken Sie nur die Piraten?, Industrie Management 2008, 60.

[29] Patent-Verzicht schützt vor China-Plagiaten, welt online 02.01.2008 (http://www.welt.de/wirtschaft/article1510484/Patent_Verzicht_schuetzt_vor_China_Plagiaten.html) (Stand: 29.01.2011).

Mittlerweile gibt es freilich Anlass zur Hoffnung, dass die Probleme bei der Schutzrechtsdurchsetzung in der VR China künftig beseitigt werden könnten. Auch chinesische Unternehmen melden inzwischen weltweit Patente an, beim EPA als sechstgrößte Nation von Antragstellern. Auch im eigenen Land steigt die Anzahl der Patentanmeldungen chinesischer Unternehmen und werden chinesische Rechteinhaber zunehmend von Piraterie betroffen. 2009 stiegen die Patentanmeldungen beim chinesischen Staatsamt für Geistiges Eigentum (SIPO) trotz Wirtschaftskrise um 15 Prozent an, während ausländische Unternehmen neun Prozent weniger Neuanmeldungen tätigten als im Vorjahr.[30] Folglich steigt auch das Eigeninteresse chinesischer Unternehmen an einer effektiven Rechtsdurchsetzung zum Schutze ihres Geistigen Eigentums.

Für die schon mittelfristige Behebung der Mängel bei der Schutzrechtsdurchsetzung in der VR China spricht zudem, dass der Gewerbliche Rechtsschutz in der VR China im Vergleich zu Deutschland noch relativ jung ist. Binnen weniger als 30 Jahren wurde ein Schutzrechtssystem zum Schutz und zur Durchsetzung von Rechten des Geistigen Eigentums geschaffen, das hinsichtlich institutioneller und gesetzlicher Ausgestaltung internationalem Standard weitgehend entspricht. Bei allen praktischen Schwierigkeiten und Problemen sind die Fortschritte Chinas beim Schutz Geistigen Eigentums also erheblich.[31] Und wie schwierig es ist, eine flächendeckende kundige und schlagkräftige Verletzungsgerichtsbarkeit aufzubauen, zeigt selbst das Beispiel des europaweit führenden Patentstreitstandorts Deutschland, wo Patentstreitverfahren praktisch nur in Düsseldorf, Mannheim und – mit weitem Abstand – München durchgeführt werden, nicht aber am verbleibenden Dutzend anderer möglicher Gerichtsstände. Der Aufbau einer landesweit effektiven Verletzungsgerichtsbarkeit in einem Staat von der Größe Chinas, ist von einer ganz anderen Dimension,[32] so dass selbst wenn von einzelnen Gerichten in Shanghai oder Beijing schon Urteile auf internationalem Niveau zu erwarten sind,[33] die Vollstreckung in den Provinzen nach wie vor und sicher noch einige Zeit problematisch bleiben wird. Nach wie vor umstritten ist auch, ob die Zentralregierung in Beijing nicht überall durchgreifen kann oder ob sie nicht durchgreifen will.[34]

Obwohl bislang keineswegs alle Probleme des Schutzes Geistiger Eigentumsrechte in China gelöst sind, deuten sowohl das Eigeninteresse chinesischer Unternehmen als auch die bisherigen Verbesserungen des Schutzrechtssystems der letzten Jahre auf eine weitergehende positive Entwicklung hin. Unter diesem Gesichtspunkt und unter Berücksichtigung einer maximal zwanzigjährigen Lebensdauer von Patenten, scheint

---

[30] China holt im Patent-Wettrennen auf (http://www.wirtschaftsblatt.at/home/international/wirtschaftspolitik/china-holt-im-patent-wettrennen-auf-450418/index.do) (Stand: 29.01.2011).
[31] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 10 Rn. 87f.
[32] *Ann*, Verletzungsgerichtsbarkeit - zentral für jedes Patentsystem und doch häufig unterschätzt, GRUR 2009, 205, 207.
[33] *Nack*, Rechtsschutz in China möglich, in A&D week digitale Zeitung für industrielle Automation 09.11.2010 Ausgabe 22, S. 4 (http://www.aud24.net/pi/index.php?StoryID=388) (Stand: 29.01.2011).
[34] *Ann*, Festschrift Schilling, S. 6.

zweifelhaft, ob der Verzicht auf Patentschutz in der VR China zum gegenwärtigen Zeitpunkt immer noch empfohlen werden kann. Eher scheint das Gegenteil der Fall, sollte Patentschutz in der VR China also jedenfalls dann angestrebt werden, wenn Know-how-Schutz, also Geheimhaltung aus technischen Gründen keine Option darstellt.

Wichtig ist auch, dass *nur die planmäßige Verletzung von Schutzrechten als Geschäftsmodell Piraterie darstellt*,[35] nicht aber die bloße Nachahmung als solche. Grundfalsch wäre es in jedem Fall, aus Angst vor Know-how-Verlust ganz auf den Wachstumsmarkt China zu verzichten. *Überreaktionen dieser Art stiften mehr Schaden als Nutzen!*

4.1 Inwiefern beeinflusst die Rechtsunsicherheit in China den Technologieschutz bayerischer KMU?

Aus unseren Gesprächen folgt, dass Unsicherheit über die Rechtsdurchsetzung in China einige Unternehmen in ihrer Entscheidungsfindung hinsichtlich angemessener Technologieschutzmaßnahmen und sogar in ihrer Geschäftsstrategie insgesamt beeinflusst. Freilich sind die Ansätze sehr unterschiedlich. Zum einen wird ganz auf geschäftliche Aktivitäten in China verzichtet, weil entweder das Risiko im Vergleich zum Nutzen als zu hoch eingeschätzt wird oder weil das Unternehmensleitbild Geschäfte in traditionellen Märkten vorsieht statt Expansion. Andere Unternehmen betreiben in China nicht nur Fertigungen, sondern auch F+E, stehen Patentanmeldungen dort aber gleichwohl sehr skeptisch gegenüber. Im Gegensatz zu anderen Ländern stellt Patentschutz für China nicht die bevorzugte Schutzmethode dar, sondern werden Investitionen in Patentschutz für die Volksrepublik als Geldverschwendung angesehen, weil die Rechtsdurchsetzung zu hohe finanzielle Risiken mit sich bringe und wenig erfolgversprechend sei. Produktnachahmungen seien auch mit Schutzrechten nicht zu verhindern.

Die meisten Unternehmen berücksichtigen die Rechtssituation in China dagegen nicht bei ihrer Entscheidungsfindung zu Technologieschutz oder Geschäftsstrategie.

Einige der befragten Unternehmen betreiben Patentanmeldungen in China aufgrund verstärkter eigener wirtschaftlicher Aktivitäten sowie des starken Wirtschaftswachstums vor Ort. Zutreffend wird China als Markt bewertet, der geschützt werden muss, um künftig wettbewerbsfähig zu sein. Sich dort gegen den Branchentrend keine günstige Wettbewerbsposition zu sichern, wird als riskant angesehen.

---

[35] *Ann / Hauck / Maute*, Auskunftsanspruch und Geheimnisschutz im Verletzungsprozess, S. 27 ff.

Nur Gesprächspartner mit rein regionaler Unternehmensausrichtung ohne globale Wachstumsziele betrachten den chinesischen Markt als irrelevant und ignorierten ihn deshalb bei der Schutzrechtanmeldung.

4.2 Strategien zum Technologieschutz in China

Universelle Lösung für effektiven Technologieschutz gegen Produktnachahmungen gibt es nicht. Vielmehr *muss jedes Unternehmen individuell eine auf die eigene Wettbewerbssituation, Unternehmensziele und nicht zuletzt die zu schützende Technologie zugeschnittene Schutzstrategie festlegen*. Ebenso kann nicht pauschal beantwortet werden, welche Schutzansätze im Besonderen geeignet sind, Schutzrechtsverletzungen in China zu verhindern und zu unterbinden. Die Unsicherheit bei der dortigen Rechtsdurchsetzung ist ein wesentlicher Aspekt, der bei der Wahl der Schutzmaßnahmen zu berücksichtigen ist. Juristischer Schutz reicht alleine nicht aus. Zusätzlich bedarf es faktischer Schutzmaßnahmen. Da es kaum möglich sein wird, Produktpiraterie vollständig zu unterbinden, sind auch Maßnahmen von Bedeutung, um Pirateriewaren zu identifizieren und auf Schutzrechtsverletzungen angemessen zu reagieren.

4.2.1 Geheimhaltung

Als kostengünstiger und zeitlich unbegrenzter Schutzansatz wird Know-how-Schutz häufig eine Alternative zur Patentanmeldung darstellen.[36] Zusätzlich eignet sich diese Schutzmethode als effektive Vorkehrung gegen Produktpiraterie, da sie keine Offenlegung des Schutzgegenstandes erfordert. Allerdings ist Geheimhaltung von Know-how nur sinnvoll, wenn sichergestellt werden kann, dass das Know-how auch tatsächlich geheim bleibt.[37] Pauschalweisungen, Schutzrechte grundsätzlich durch Geheimhaltung zu ersetzen, um Offenlegung als Piraterievorlage zu vermeiden, sind nicht zielführend, sondern kontraproduktiv. Das Nachahmungsproblem würde so nur verstärkt, da offenkundig gewordene Technologie, für die kein Schutzrecht besteht, von allen Wettbewerbern legal kopiert werden darf, ohne dass von „Produktpiraterie“ gesprochen werden könnte. Wie oben bereits gesagt, eigenen sich darum Schutzgegenstände nicht für Know-how-Schutz, die leicht durch Reverse Engineering erschlossen werden können oder bei denen Parallelerfindungen absehbar sind.[38]

---

[36] *Ann*, Know-how-Schutz – Stiefkind des Geistigen Eigentums?, GRUR 2007, 40.
[37] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 10 Rn. 126.
[38] *Ann / Grüneis,* Herausforderung, Produktpiraterie - Sind Patente heute noch sinnvoll oder stärken Sie nur die Piraten?, Industrie Management 2008, 61f.

4.2.2 Chinesische Geschäftspartner

Bei einer Produktionsverlagerung nach China ist es oftmals unvermeidbar, Geschäftsbeziehungen mit Externen vor Ort einzugehen, die ein Risiko für internes Know-how darstellen. Obwohl ohne ein gewisses Vertrauen keine erfolgreiche Geschäftsbeziehung zu Lizenznehmern, Vertriebspartnern und Zulieferern aufgebaut werden kann, sollten diese doch stets kritisch beobachtet werden. *Sorgfältige Vertragsgestaltungen, die auch Auskunftsrechte und die Befugnis zu stichprobenhaften Überprüfungen der Partner vorsehen* sollten, sind dafür unabdingbare Voraussetzung[39] – im Übrigen keineswegs nur für chinesische Geschäftspartner, sondern für alle Geschäftspartner, die mit kritischem Know-how in Berührung kommen.

4.2.3 Technologiespaltung

Reduzieren lässt sich das Risiko, dass Dritte Zugang zu dem für die Beherrschung einer Technologie erforderlichen Know-how gewinnen zum einen durch Technologiespaltung, also die Etablierung von Produktlinien unterschiedlicher technischer Komplexität für „sichere“ Staaten und für „Pirateriestaaten“. Ein anderer Weg besteht im Zurückbehalt technologiekritischer Fertigungsschritte mit dem Ziel, Pirateriestandorten den Zugang zu „cutting-edge“-Technologien zu erschweren. So können beispielsweise verschiedene Schritte eines Herstellungsprozesses räumlich getrennt werden, indem der gesamte Produktionsprozess auf verschiedene Orte aufgeteilt wird – in China ebenso wie in anderen Staaten. Allerdings ist dieses Vorgehen kostspielig,[40] und wird die Erschließung verschiedener Standorte in China nicht wenige KMU finanziell überfordern.

Sinnvoller ist in diesen Fällen die Abkürzung der Wertschöpfungskette am Auslandsstandort auf wenige Produktionsschritte. Werden Schlüsselkomponenten an einem anderen Standort produziert (beispielsweise in Deutschland) als am Standort der Endmontage (beispielsweise China), erschwert auch dies den Zugang von Piraten zu „cutting-edge“-Technologien.[41]

In summa eignet sich Technologiespaltung so freilich nur für Produkte einer gewissen Komplexität. Mindestvoraussetzung ist die Teilbarkeit der entsprechenden Produktionsprozesse.

---

[39] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 10 Rn. 122f.
[40] *Ganea*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 12 Rn. 70.
[41] *Ann*, Festschrift Schilling S. 8.

4.2.4 First Mover Strategie

Ein probates Mittel zum Technologieschutz stellen können auch verkürzte Technologiezyklen darstellen,[42] denn für Technologien mit kurzen Lebenszyklen ist der Verzicht auf Schutzrechte selbst dann eine Option, wenn sie sich durch Reverse Engineering erschließen lassen. Hier bietet bereits der Zeitvorsprung im Markt hinreichend Schutz. Führt ein Wettbewerber seine Kopie in den Markt ein, kann der Technologieentwickler bereits eine Verbesserung oder Weiterentwicklung des Ausgangsprodukts anbieten. Besonders geeignet ist diese Schutzstrategie daher, wenn die Kompetenzniveaus der Wettbewerber sich stark unterscheiden. In diesem Fall können sie fremde Technologien nicht rasch adaptieren. Anders gewendet: je schneller die Technologie fortentwickelt oder ersetzt wird und je größer der Wissensvorsprung des First Movers ist, desto höher die Hürden für die Adaption einer Technologie und desto weniger aussichtsreich und wahrscheinlich die Kopie einer Technologie.

4.2.5 Komplexitätssteigerung

In zahlreichen Industrien sind Produkte und Komponenten mittlerweile sehr komplex und enthalten eine Vielzahl geschützter Technologien, z. B. embedded Software. Derartige Produkte können durch eine Kombination aus Schutzrechten und geheimem Know-how effektiv geschützt werden.[43] Je komplexer ein Produkt gestaltet werden kann, desto besser ist es gegen unerwünschte Nachahmungen zu schützen. In Ländern, in denen verlässlicher juristischer Schutz nicht flächendeckend erreichbar ist, kann Piraterie durch eine Kombination aus Geheimhaltung und Schutzrechten deutlich erschwert werden.

Diese Tatsache bestätigen einige unserer Gesprächspartner. Sie sehen sich von den Folgen der Piraterie weniger betroffen, da ihre Produkte auf Grund geheimer Herstellungsverfahren nicht in gleicher Qualität kopiert werden können. Freilich ist es riskant, sich auf derartige Qualitätsvorsprünge langfristig zu verlassen, denn wie eingangs gesagt: Schwellenländer holen auf und können mittlerweile Produkte in ähnlicher Qualität erzeugen wie einheimische Hersteller – zu deutlich günstigeren Preisen.

---

[42] *Addor, Li-Treyer*, Vorsichtsmaßnahmen sind der effektivste Kopierschutz, io new management 5 / 09, S. 14.
[43] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 407f.; *Ann*, Festschrift Schilling S. 8.

4.2.6 Patentschutz

Wie eingangs erwähnt, gibt es Schutzgegenstände, die sich schlichtweg nicht zur Geheimhaltung eignen oder die nicht auf anderem Weg ausreichend geschützt werden können, z. B. durch die obern erwähnte Verkürzung von Technologiezyklen. Ohne juristischen IP-Schutz können über das Wettbewerbsrecht nur sklavische Nachahmungen, bekämpft werden – abhängig von der Rechtslage im jeweiligen Staat.[44] Ohne Schutzrechte sind solche Technologien folglich weitgehend schutzlos.

Sollte Patentschutz insofern ohne sinnvolle Alternative sein, sollte heute auch in der VR China Patentschutz anstrebt werden. Dies gilt ungeachtet der nach wie vor bestehenden Durchsetzungsmängel, denn eine Patentanmeldung kann nicht nachgeholt werden, wenn die zu erwartenden Verbesserungen der Patentrechtsdurchsetzung eingetreten ist. Nicht vor dem Chinesischen Staatsamt für Geistiges Eigentum (SIPO) zu patentieren, würde bedeuten, dass die Auswertung einer in Europa, den USA und Japan geschützten Erfindung auf dem bedeutenden Absatzmarkt China kaum möglich sein wird. Die Technologie könnte dann in China völlig legal nachgeahmt und vertrieben werden.[45]

Nur eine Anmeldung in der VR China kann dem entgegenwirken, denn die maximale Patentlaufzeit beträgt 20 Jahre. Was sich in 20 Jahren verändern kann, zeigt die dynamische Entwicklung Chinas und seiner Wirtschaft.[46] Selbst wenn die Situation in China derzeit noch keinen Patentschutz erzwingen mag oder die Patentdurchsetzung dort nach wie vor zu unsicher erscheint, muss dies nicht zwangsläufig auch für die nächsten 20 Jahre gelten, also für die gesamte Laufzeit eines chinesischen Patents, das heute angemeldet wird. Erfindungen, die künftig möglicherweise von strategischer und damit wirtschaftlicher Relevanz in China sein können, sollten dort deshalb auch schon heute geschützt werden.[47] Insbesondere für Grundlagenpatente, die häufig über die gesamte Patentlaufzeit von großem Wert sind, könnte sich ein Verzicht später negativ auswirken, weil dort, wo es keine Schutzrechte gibt, in keinem Fall etwas durchgesetzt werden kann, auch nicht in Zukunft.[48] Umgekehrt, können Unternehmen, die jetzt in China Schutzrechte anmelden und den Markt erschließen, schwer aufholbare Wettbewerbsvorteile etablieren, wenn Schutzrechte ihre Wirkung entfalten.[49] Geduld und Kampf, die für den Erwerb von Schutzrechten heute noch nötig sein mögen, könnte für die Zukunft also eine lohnende Investition darstellen. Für die Zukunft profitieren

---

[44] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 409.
[45] *Ann / Grüneis,* Herausforderung, Produktpiraterie - Sind Patente heute noch sinnvoll oder stärken Sie nur die Piraten?, Industrie Management 2008, 61f.
[46] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 413.
[47] *Gassmann / Bader*, Patentmanagement: Innovationen erfolgreich nutzen und schützen, S. 174.
[48] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 10 Rn. 94.
[49] *Gassmann / Bader*, Patentmanagement: Innovationen erfolgreich nutzen und schützen, S. 177.

könnten davon auch bayerische KMU, denn *in summa* wird eher die Vernachlässigung des Wachstumsmarktes China ein Risiko darstellen als Patentanmeldungen dort.

4.2.7 Patentdurchsetzung in China

Seit ihrem WTO-Beitritt hat die VR China eine Reihe von Gesetzen zum Schutz Geistigen Eigentums in Kraft gesetzt und bietet ein vergleichsweise vielgestaltiges System zur Durchsetzung von Rechten und Ansprüchen auf dem Gebiet des Geistigen Eigentums an. Es umfasst neben den zivilrechtlichen Verfahren und Strafverfahren auch (gewerbepolizeiliche) Verwaltungsverfahren.[50] Die Schwächen in der Durchsetzung der Rechte werden langfristig behoben werden, wenn Gerichte und Behörden die nötige Erfahrung haben und der Mangel des Unrechtbewusstseins in der Bevölkerung behoben ist.[51] Wann dieser Prozess abgeschlossen sein wird, ist nur sehr schwer vorhersagbar.

Für KMU bieten auf den ersten Blick die *Verwaltungsverfahren* des chinesischen Rechts gute Möglichkeiten zur Schutzrechtsdurchsetzung, denn diese Verfahren sind schnell und preisgünstig.[52] Problematisch erweist sich jedoch häufig, dass die zuständigen Behörden sich lokalprotektionistisch verhalten und nicht gegen Rechtsverletzer vorgehen, eingeleitete Verfahren behindern oder diese nicht an die Strafverfolgungsbehörden abgeben wollen. Ferner sind die Verwaltungsverfahren nicht-öffentlich und wenig transparent.[53] Insbesondere KMU haben geringe Chancen, ihre Rechte wirksam durchzusetzen. Große Konzerne können auf Grund der lokalen wirtschaftlichen Bedeutung mehr Macht ausüben können. Sie schaffen wichtige Arbeitsplätze und tragen zur wirtschaftlichen Entwicklung bei. Daher werden ihre Bedürfnisse von lokalen Entscheidungsträgern und Behörden stärker berücksichtigt.[54]

Erfolgversprechender für KMU könnten *zivilrechtliche oder strafrechtliche Klagen bei den Volksgerichten* in Peking oder Shanghai sein, an denen mittlerweile gut ausgebildete Richter tätig sind.[55] Diese Verfahren haben den Nachteil, dass sie deutlich länger dauern als in Deutschland und kostenaufwendiger sind. Immerhin kann der Geschädigte Schadenersatzansprüche geltend machen. Andererseits werden Entschädigungssummen sowie Strafen für Schutzrechtsverletzungen als zu niedrig angesehen, dass sie abschreckende Wirkung hätten. Das Risiko, dass Kläger auf Kosten sitzen-

---

[50] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 10 Rn. 91.
[51] *Gassmann / Bader,* Patentmanagement: Innovationen erfolgreich nutzen und schützen, S. 177.
[52] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 10 Rn. 91.
[53] *Holtbrügge / Puck,* Geschäftserfolg in China: Strategien für den größten Markt der Welt, S. 233.
[54] *Gassmann / Bader,* Patentmanagement: Innovationen erfolgreich nutzen und schützen, S.175f.
[55] *Holtbrügge / Puck,* Geschäftserfolg in China: Strategien für den größten Markt der Welt, S. 233.

bleiben, ist also auch im Erfolgsfall hoch.[56] Für KMU ist das ein Problem, weil auch ein positives Gerichtsurteil noch nicht bedeutet, dass diese in der Provinz auch wirklich vollstreckt werden können. Die Wahrscheinlichkeit, dass Verfolgungsorgane den Forderungen lokaler politischer Entscheidungsträger nachgeben, ist hoch.[57]

Der Transport von Piraterieware ins Ausland kann mit Hilfe *zollrechtlicher Verfahren* unterbunden werden. Unternehmen können Anträge stellen, dass bestimmte für den Export vorgesehene Produkte vom chinesischen Zoll untersucht und wenn nötig beschlagnahmt werden.[58] Auf diese Weise wird zwar nicht der chinesische Absatzmarkt geschützt, verhindert werden kann aber immerhin der Transport von Piraterieware in andere Märkte außerhalb Chinas.

In summa ist die Schutzrechtsdurchsetzung in China prinzipiell möglich und verspricht auch in Zukunft immer besser zu werden. Dennoch ist sie gegenwärtig insbesondere für KMU immer noch schwierig und nicht immer erfolgversprechend. Das große Unternehmen sich positiver äußern, ist nachvollziehbar. Anders als KMU verfügen sie meist über Marktmacht und können sie durch ein gezieltes *Beziehungsmanagement* mit der chinesischen Regierung Patentrechte leichter durchsetzen. Auch in den Provinzen hilft diese Marktmacht. Großunternehmen treiben die wirtschaftliche Entwicklung voran und schaffen Arbeitsplätze, so dass es ihnen leicht fällt, auch lokal gute Beziehungen zu Entscheidungsträgern und Behörden aufzubauen.[59]

Bei der Durchsetzung von Schutzrechten ist es sinnvoll, kompetente *fachliche Beratung* in Anspruch zu nehmen. Es gibt eine Vielzahl spezialisierter Anwaltskanzleien (auch in China), die über Erfahrung auf dem Gebiet des Gewerblichen Rechtschutzes in China verfügen.[60] Freilich sind auch hier KMU gegenüber Großunternehmen benachteiligt, weil sie in der Regel finanziell limitiert sind.

4.2.8 Technische Schutzmaßnahmen zur Produktidentifikation

Für die Rechtsdurchsetzung unabdingbar ist die *Erkennung von Schutzrechtsverletzungen*. Verschiedene Techniken erlauben die eindeutige Kennzeichnung von Originalprodukte und deren zweifelsfreie Unterscheidung von Produktfälschungen. Die Identifikation von Produkten als Originalen ist nicht nur für den Originalhersteller und

---

[56] *Cox / Sepetys*, in: Leonard / Stiroh Economic Approaches To Intellectual Property Policy, Litigation,and Management, S. 293, 300.
[57] *Ganea*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 12 Rn. 90.
[58] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 10 Rn. 92, 112-15.
[59] *Gassmann / Bader*, Patentmanagement: Innovationen erfolgreich nutzen und schützen, S. 175f.
[60] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 10 Rn. 131.

die Kunden zum Schutz vor Fälschungen wichtig, sondern auch für die Zollbeamten, denn sie sollen den Umlauf illegaler Nachahmungen unterbinden.[61]

Gängige *Produktkennzeichnungen* zum Originalitätsbeweis sind beispielsweise Hologramme, Farbcodes, RFID-Tags, besondere Schriften, spezielle Klebstoffe oder Codenummern. Die Verwendung mehrerer dieser Merkmale kann die Sicherheit steigern. Eingeschränkt geeignet ist der Einsatz allerdings bei niedrigpreisigen Produkten. Hier könnte auch eine geringe Erhöhung der Produktionskosten dazu führen, dass diese Produkte nicht mehr wettbewerbsfähig angeboten werden könnten.[62] Freilich werden mittlerweile auch schon technische Produktkennzeichnungen kopiert, was die Unterscheidung zwischen Fälschung und Original weiter erschwert.

Abbildung 5
Checkliste – Technologieschutz in China

Checkliste – Technologieschutz in China

- Schutzrechte nach Möglichkeit durch Geheimhaltung ersetzen
- Komplexität steigern und verschiedene Schutzansätze kombinieren
- Schlüsseltechnologien aus China fernhalten (Technologiespaltung)
- bei kurzlebigen Technologien ggf. auf Schutzrechte verzichten (*First Mover Advantage*)
- Grundlagenerfindungen durch Patente schützen
- Patente konsequent anmelden, nicht nur in „sicheren" Systemen
- kulturelle Unterschiede berücksichtigen
- Regionale Behördenkontakte pflegen
- Geschäftspartner vorsichtig auswählen
- Geschäftspartner beobachten und kontrollieren (Stichproben)
- konsequentes Durchsetzungsimage schaffen
- fachanwaltliche Beratung suchen und sichern

Bild: Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum

[61] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 10 Rn. 114.
[62] *Ann,* Festschrift Schilling S. 8.

5 Transparenzverlangen

Einschränkungen der Möglichkeit zum Schutz kritischen Know-hows

Fordern Aufsichtsbehörden, etwa für Luftfahrzeuge, Transparenz in Produktionsprozessen sowie die Standardisierung von Bauteilen, schafft dies für Unternehmen Probleme bei der Differenzierung im Wettbewerb. Diese Entwicklung betrifft auch den Technologieschutz.

Wie eingangs erläutert sind die Möglichkeiten zum Einsatz von Know-how-Schutz im Technologieschutz strukturell begrenzt, denn Know-how-Schutz setzt anders an als technische Schutzrechte. Für den Technologieschutz ist Know-how-Schutz darum nur praktikabel für Schutzgegenstände, die ihrer Natur nach geheimschutzfähig sind. Nicht greifen kann Know-how-Schutz, wenn die Technologien offen zutage liegen, wie z. B. in der hier beschriebenen Situation branchenspezifischer Transparenzgebote. Denn wenn Know-how preisgegeben werden muss, verliert es entweder sogleich seinen Schutz oder steigt die Wahrscheinlichkeit eines Schutzverlusts durch Informationslecks.[63]

5.1 Wie begegnen bayerische KMU dieser Situation?

Auch bayerische KMU sind von Transparenzgeboten betroffen und werden gezwungen, Geheimhaltungsstrategien für Prozesse und Technologien zu überdenken, die offengelegt werden müssen. Als Folge steigt das Interesse an Patentschutz, weil technologische Vorsprünge in einer Situation erzwungener Offenlegung nur so gesichert werden können.

5.2 Alternativschutz zu Geheimhaltung

Wenngleich der Erwerb technischer Schutzrechte, v. a. von Patenten, Gebrauchsmustern und Topographieschutzrechten, vielfach eine Alternative zur Geheimhaltung darstellen wird, ist doch zu beachten, dass diese Alternative nicht für alle geheimschutzfähigen Informationen besteht. Beschränkungen ergeben sich zum einen aus den Einschränkungen der dem Patentschutz zugänglichen Gegenstände in §§ 1 III, 1a, 2, 2aPatG. Beschränkungen folgen darüber hinaus aber auch aus § 1 Abs. 1 PatG, der

[63] *Ann/Kalbfus*, Gesetzlicher Schutz für geheimes Know-how – nur gerecht oder auch wirtschaftlich sinnvoll?, in Iurratio, 133.

die Patentierbarkeit einer Erfindung an deren Neuheit, Erfindungshöhe und gewerbliche Anwendbarkeit knüpft. Diese Voraussetzungen sind erheblich enger als diejenigen für Know-how-Schutz. Hier genügt, dass die betreffende Information nicht offenkundig ist und aus diesem Grund wirtschaftlichen Wert besitzt und dass ihre rechtmäßigen Inhaber nach den Umständen angemessene Geheimschutzmaßnahmen treffen.[64]

Auf Grund der enger gefassten Erteilungsvoraussetzungen für Patentschutz bildet dieser nur teilweise eine Alternative zum Know-how-Schutz. Für den Schutz von Prozess-Know-how durch Verfahrenspatente, ist darum stets zu prüfen, ob Patentschutz überhaupt erreichbar sein wird. Mit Blick auf die Patenterteilungsvoraussetzungen Technizität oder Erfindungshöhe wird dies nicht immer der Fall und nur durch die Beiziehung qualifizierten patentanwaltlichen Rechtsrats zu ermitteln sein.

Bei Verfahrenspatenten zu beachten ist ferner das Beweisproblem im Verletzungsfall.[65] Ungeachtet der praktischen Relevanz dieses Themas ist es immerhin insofern kein Argument gegen die Anmeldung von Verfahrenspatenten, weil auch alle Wettbewerber von den hier gegenständlichen Transparenzvorschriften zur Offenlegung ihrer Herstellungsverfahren gezwungen sein werden.

Abschließend sind freilich auch ökonomische Aspekte zu beachten. Kostenintensiver Patentschutz bietet sich nur an, wenn er konkrete Wettbewerbsvorteile bietet. Während die Kosten des Know-how-Schutzes nahezu unabhängig von der Menge des geheim gehaltenen Wissens sind, fallen die keineswegs geringen Patentkosten[66] anmeldungs- und später schutzrechtsspezifisch an. Der Ersatz von Know-how-Schutz durch Verfahrenspatente kann daher seriös nur auf Basis umfassender Kosten-Nutzen-Rechnungen erfolgen. Gelegentlich wird es sinnvoller sein, auf Schutz ganz zu verzichten und die ersparten Mittel an anderer Stelle zur Gewinnung konkreter Wettbewerbsvorteile einzusetzen.

---

[64] *Ann*, Know-how-Schutz – Stiefkind des Geistigen Eigentums?, in GRUR 2007, 41.
[65] *Huber* in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 404.
[66] Allein die Amtsgebühren für ein deutsches Patent betragen bezogen auf die Patentlaufzeit ca. 14.000 Euro.

Abbildung 6
Checkliste – Technologieschutz für transparente Verfahren

Checkliste – Technologieschutz für transparente Verfahren

- Prüfen, welches Know-how sich noch geheim halten lässt
- Know-how hinsichtlich des strategischen Werts und Nutzens bewerten und festlegen, was alternativ geschützt werden muss
- Alternative Schutzansätze prüfen, z. B. Verfahrenspatente
    - Erfüllung der Patenterteilungsvoraussetzung
    - Nachweisbarkeit einer Schutzrechtsverletzung
    - Kosten-Nutzen-Abwägung

Bild: Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum

6 Bedrohungen durch Know-how-Verlust

Vielfältige Möglichkeiten des Know-how-Verlusts

Die Ursachen des Know-how-Verlusts sind vielfältig. Beispielsweise kann anvertrautes Know-how durch Mitarbeiter oder Kooperationspartner, v. a. Kunden und Geschäftspartner verraten werden. Auch können Unternehmensgeheimnisse gestohlen oder anders auf unlautere Art abhanden kommen. Täter kann prinzipiell jeder sein – auch ein Mitarbeiter, sogar wenn ihm sein Wissen nicht als Teil seiner Beschäftigung bekannt gemacht wurde.

Abbildung 7
Tätergruppen für Know-how-Verletzungen

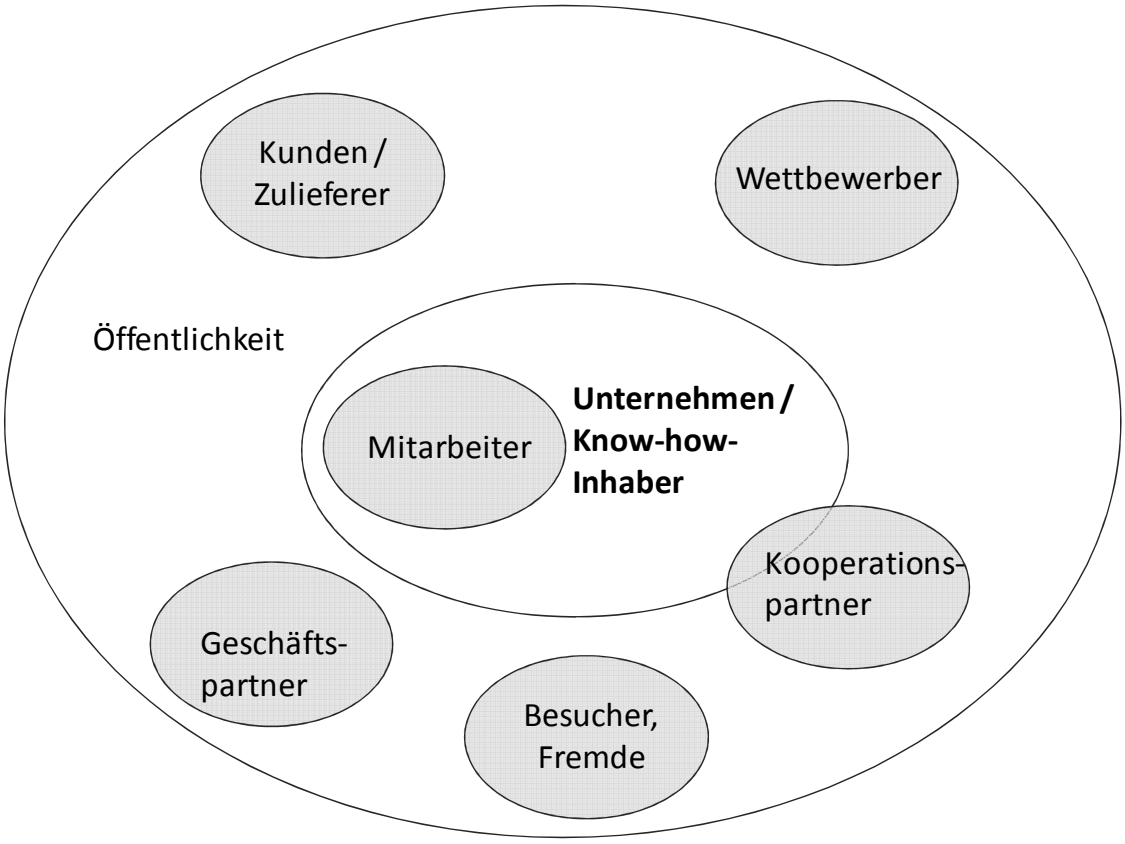


Bild: Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum

6.1 Know-how-Verlust durch Kunden

Durch die Sättigung der Märkte sind diese von Anbietermärkten zu Käufermärkten geworden. Unternehmen stehen vor der Herausforderung, schneller und besser zu sein als ihre Mitwettbewerber und ihre Aktivitäten flexibel an Bedarfslage und Kundenwünschen auszurichten.[67] Nach einer Untersuchung von Kienbaum sind lediglich 0,6 Prozent aller Innovationsideen kommerziell erfolgreich.[68] Eine hohe Marktorientierung durch Einbindung von Kunden in die Innovationsphase wird inzwischen von zahlreichen Unternehmen als notwendig anerkannt zur Sicherung und zum Ausbau von Marktposition und Wettbewerbsfähigkeit.[69] Vorteile einer derartigen Zusammenarbeit äußern sich in einer stärkeren Kundenbindung, einem besseren Verständnis von Marktbedürfnissen, Fehlervermeidung in der frühen Innovationsphase und einer besseren Produktqualität. Kunden teilen ihre Bedürfnisse mit und geben Ideen für neue Produkte. Ebenso geben sie Feedback zu Innovationen im Entwicklungsstadium.[70] Kunden entwickeln sich dabei vom passiven Empfänger zum Wertschöpfungspartner der Unternehmen.[71]

Während verstärkte Kundenorientierung und Kundenintegration geeignete Problemlösungen darzustellen scheinen, um eigene Marktpositionen in wettbewerbsintensiven Märkten zu festigen, birgt dieser Ansatz auch neue Risiken und Probleme. Wie in der Literatur ausführlich diskutiert, wird der Technologieschutz vor neue Herausforderungen gestellt. Die Einbindung von Kunden ins Innovationsgeschehen schafft Potentiale für eine ungewollte Know-how-Diffusion, denn geheimes technologisches Know-how muss Kunden im Rahmen kooperativer Entwicklungsaktivitäten offengelegt werden. Auch drohen Streitigkeiten, wer welches Know-how in die gemeinsame Arbeit eingebracht hat. Schließlich ergeben sich durch starke Kundenorientierung auch indirekt Schwierigkeiten für den Technologieschutz. Unternehmen können in Abhängigkeiten zu ihren Großkunden geraten, z. B. wenn sie Nischenmärkte bedienen. Auch werden auf Anregung von Kunden häufig nur inkrementelle Verbesserungen verfolgt und eigene, vielversprechende Innovationen zur Bedienung anderer Märkte vernachlässigt. Schließlich gewinnen Kunden an Verhandlungsmacht und können Abhängigkeitsverhältnisse weiter verschärfen, indem sie Exklusivität fordern.[72] Das macht es zum einen schwerer für die Unternehmen, ihren Kundenstamm zu erweitern. Zum anderen können sie eigene Technologien nicht mehr durch Geheimhaltung schützen. Ihre Ver-

---

[67] *Wildemann,* Produktionssysteme mit Zukunft am Standort Deutschland, S. 5.
[68] *Bader,* in: Gassmann/Kobe Management von Innovation und Risiko: Quantensprünge in der Entwicklung erfolgreich managen, S. 469.
[69] *Gassmann/Kausch/Enkel,* Einbeziehung des Kunden in die frühe Phase des Innovationsprozesses, Thexis 2005 Nr. 2, 9.
[70] *Enkel,* in: Gassmann/Kobe Management von Innovation und Risiko: Quantensprünge in der Entwicklung erfolgreich managen, S. 171.
[71] *Reichwald/Piller*, Interaktive Wertschöpfung, S. 1.
[72] *Gassmann/Kausch/Enkel,* Einbeziehung des Kunden in die frühe Phase des Innovationsprozesses, Thexis 2005 Nr. 2, 11.

handlungsmacht zur Durchsetzung eines vertraglichen Know-how-Schutzes ist schwach diese Durchsetzung bei Vertragsverletzung kann durch unternehmensstrategische Erwägungen gefährdet werden. Geheimhaltung des Know-how würde sich wiederum nachteilig auf die Kundenbeziehung oder gemeinsame Entwicklungsarbeiten auswirken.

Bayerische mittelständische Unternehmen scheinen stark von diesen Problemen betroffen, denn die Mehrzahl unserer Gesprächspartner zählen große OEMs zu ihren Kunden, die sie mit kundenorientierten Problemlösungen an sich binden. Im Rahmen gemeinsamer F+E Aktivitäten haben diese Mittelständler vielfach geheimes Know-how mit ihren Kunden geteilt – mit schlechten Erfahrungen.

6.1.1 Welche Probleme bereiten gemeinsame F+E Arbeiten mit Kunden bayerischen KMU?

Für die Mehrzahl unserer Gesprächspartner bedeutet Kundenorientierung die Einbindung von Kunden in F+E Aktivitäten. Dabei ergaben sich zwei verschiedene Ausprägungsformen dieser gemeinsamen F+E Arbeit mit Kunden: eine frühe Einbindung der Kunden in Forschungs- und Entwicklungsprojekte in Form vertikaler F+E Kooperationen und eine späte Integration des Kunden, bei der fertig entwickelte Produkte an Kundenbedürfnisse angepasst werden. Dieses sog. *Customizing* umfasst beispielsweise das Anpassen von Maschinen und deren Prozessparametern an Produktionsprozesse und Produkte von Kunden im Rahmen von Laborversuchen und dient vor allem der Absatzförderung.

Als Hauptgrund für Entwicklungspartnerschaften mit dem Kunden wurden uns Kundenbindung und Absatzsicherung durch marktnahe Innovationen genannt. Kosteneinsparungen wurden demgegenüber nicht als bedeutsames Ziel hervorgehoben.

Wurde Kunden während der Zusammenarbeit geheimes Know-how offenbart, das nicht durch Vertraulichkeitsvereinbarungen geschützt war, wurde diese Offenbarung verschiedentlich von Kunden ausgenutzt, indem sie dieses Know-how entweder weitergaben oder Patente anmeldeten, die auf dem Know-how ihrer Lieferanten basierten. Diese konnten dann nicht mehr über ihre eigene Technologie frei verfügen und standen vor der Frage, ob sie zumindest ihre Vorbenutzung beweisen konnten. In anderen Fällen war es aus Gründen der Marktmacht unmöglich, rechtlich gegen Kunden vorzugehen und erzwangen diese Kunden damit eine Form von Technologieexklusivität. Beobachtet wurden auch Fälle, in denen Kunden zwar nicht fremde Technologien patentieren, wohl aber nach abgeschlossener gemeinsamer F+E Arbeit die entwickelten Produkte selbst herstellten. Auch damit wurde das Ziel der Absatzförderung durch Kundeneinbindung in F+E nicht erreicht, sondern wurde geheimes Know-how ohne Gegenwert schlichtweg verschenkt.

Die Praxis bayerischer KMU verfügt für diese Probleme offensichtlich nicht über Lösungsansätze. Vielmehr sind die Unternehmen in der Regel nicht bereit, zum Schutz ihres geheimen Know-hows gegen Kunden vorzugehen. Auch meinen sie, nicht auf

Kundenbindung verzichten zu können, selbst wenn dies auf Kosten ihres Know-hows geht. Als einzige gezielte Schutzmethode genannt wurde die Anmeldung von Verfahrenspatenten – unter Hinnahme der Probleme, die diese Patente auswerfen.

6.1.2 Schutzmaßnahmen gegen den Know-how-Verlust durch F+E Partnerschaften mit den Kunden

Die Probleme unserer Gesprächspartner aus der bayerischen Metall- und Elektroindustrie decken sich mit den in der einschlägigen Literatur genannten Problemen. Auch dort werden als Probleme der Verlust geheimen Know-how bzw. die missbräuchliche Verwendung dieses anvertrauten Wissens von Kundenseite sowie die steigende Kundenabhängigkeit beschrieben, die kundenfokussierte Entwicklungsaktivitäten mit sich bringen.

Begegnet werden kann diesem Problem mit verschiedenen Schutzansätzen. Eine Maßnahme sind auch hier klare vertragliche Regelungen zum Umgang mit für die gemeinsame Arbeit relevanten Unternehmensgeheimnissen. Das umfasst die Geheimhaltungspflicht der Projektpartner bezüglich des gegenseitig zur Verfügung gestellten Know-hows sowie dessen zweckgebundene Nutzung sowohl während der Zusammenarbeit als auch nach Vertragsende. Hiervon zu trennen ist die Behandlung des im Rahmen der Kooperation generierten neuen Know-hows, dessen Geheimhaltung, Schutzrechte und Verwertung gleichfalls geregelt werden sollten.[73] Für echte F+E Kooperationen sollten F+E Verträge verwendet werden, die Schutzrechts- und Know-how-Vereinbarungen enthalten müssen.[74]

Häufig berichteten unsere Gesprächspartner über einfache Customizing-Aktivitäten mit Kunden, also die Anpassung fertig entwickelter Produkt auf Kundenproduktionsprozesse und -produkte. Teils haben diese Arbeiten eher den Charakter produktbegleitender Services als einer Entwicklungspartnerschaft. Überdies sind sie von so kurzer Dauer, dass der Abschluss einfacher Vertraulichkeitsvereinbarungen ausreichend erscheint. Da das Customizing – auch wenn die Probleme sehr individuell sein können – einer Standardleistung gleicht, könnte es ratsam sein, eine Vorlage für Vertraulichkeitsvereinbarungen zu entwerfen, die nach Anpassung durch einen fachkundigen Rechtsanwalt auf den Einzelfall für alle Produktanpassungen mit Kunden verwendet werden kann.

Besonders bedeutsam sind Vertraulichkeitsvereinbarungen für Entwicklungspartner-

---

[73] *Maume*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 4 Rn. 12.; *Gassmann / Kausch / Enkel,* Einbeziehung des Kunden in die frühe Phase des Innovationsprozesses, Thexis 2005 Nr. 2, 11.
[74] *Maume* in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 4 Rn. 29.

schaften, da hier der gesetzliche Geheimnisschutz nicht greift. Der strafrechtliche Know-how-Schutz nach § 17 UWG sanktioniert Geheimnisverrat, Industriespionage und Geheimnishehlerei. Im Fall eines Geheimnisverrats kann nicht gegen die begünstigten Konkurrenten strafrechtlich vorgegangen werden, sondern nur gegen die Mitarbeiter des Know-how-Trägers als Täter. Überdies fehlt bei freiwilliger Offenbarung von Know-how im Rahmen von Vertragsverhandlungen meist das erforderliche „Verschaffen" oder „Sichern" des Know-how und scheitert ein Vorgehen vielfach an der Nachweisbarkeit von Tathandlungen oder Schäden. Wurden Verträge geschlossen, kann zumindest der vertragliche Know-how-Schutz noch greifen, freilich nur, wenn der Vertrag spezifische Geheimhaltungsvereinbarung enthält. Zwar anerkennt die Rechtsprechung vereinzelt Pflichten zur Loyalität und zur wechselseitigen Rücksichtsnahme der Vertragspartner gemäß §§ 241 Abs. 2, 242 BGB, jedoch ist der Umfang derartiger Pflichten nicht klar definiert, so dass fraglich bleibt, ob und welches Know-how *in casu* geschützt ist. Schutz besteht zudem grundsätzlich nur bis zum Vertragsende. Nur Geheimschutzvereinbarungen mit auch nach Umfang und Dauer klar definierten Geheimhaltungspflichten können diese Mängel beheben.[75]

Ob Mittelständler sich in Verhandlungspositionen befinden, die den Abschluss von Vertraulichkeitsvereinbarungen mit OEMs erlaubt, mag nicht immer unzweifelhaft sein. Gleichwohl sollte im Verletzungsfall auch gegen Kunden rechtlich vorgegangen werden – gegen wichtige Großkunden von denen Abhängigkeit besteht freilich mit Fingerspitzengefühl. Ein weiterer Ansatz zur Vermeidung von Know-how Abflüssen ist die Auswahl des richtigen Kooperationspartners. Beispielsweise kann die Kooperation zum Vertrauensaufbau mit kleinen gemeinsamen Innovationsvorhaben begonnen werden, bevor für den Fall positiver Erfahrungen Folgeprojekte geplant werden. Langfristige Allianzen sollten ausschließlich mit bewährten Kunden eingegangen werden.[76]

Für den Know-how-Schutz im Rahmen des Produkt-Customizing bietet sich dieses Vorgehen freilich nicht besonders an. Derartige Aktivitäten stehen in der Regel im direkten Zusammenhang mit dem Verkauf eines Produkts, und entsprechend wenig Interesse hat der Kunde an anderen „Probeprojekten". Auch könnte sich eine Ablehnung negativ auf den Absatz auswirken. *In summa* fühlen sich viele Unternehmen aufgrund starker Abhängigkeiten von verhandlungsstarken OEMs gezwungen, den Bedürfnissen ihrer Kunden auch in Forschung und Entwicklung entgegen zu kommen.

Immerhin haben die Unternehmen ein hohes Maß an Flexibilität, welches Know-how, sie ihren Kunden offenbaren. Auch wenn jedes Unternehmen bestrebt sein wird, sich seinen Kunden als besonders kompetenter und innovativer Partner zu präsentieren, um diese Kunden an sich zu binden, kann das Risiko des Know-how-Verlusts dadurch

---

[75] *Müller,* Effektiver Know-how-Schutz durch Geheimhaltungsverträge, in DZKF 1 / 2 2009, 70.
[76] *Gassmann / Kausch / Enkel,* Einbeziehung des Kunden in die frühe Phase des Innovationsprozesses, Thexis 2005 Nr. 2, 11.

minimiert werden, dass bei jeder Offenbarung von geheimem Know-how sorgfältige Risiko-Nutzen-Abwägungen durchgeführt werden. Eine systematische Erfassung aller Unternehmensgeheimnisse und deren Unterteilung in verschiedene Sensibilitätsgruppen kann auch dabei hilfreich sein.[77] Sie ist auch nützlich, wenn der Kunde dasselbe oder ähnliches Know-how mit in das Projekt einbringt, um beweisen zu können, dass dieses Know-how bereits vorher im Unternehmen vorlag. Sonst bestünde die Gefahr, dass eigenes Know-how im Unternehmen nicht mehr verwendet werden dürfte.

Generell sollte nach dem Prinzip *need to know* vorgegangen werden: Kunden sollten nur erfahren, was zur Erarbeitung ihrer Beiträge in der gemeinsamen F+E zwingend erforderlich ist. Auch sollten Entwicklungspartnerschaften auf das Nötigste reduziert werden, um Know-how-Abflüsse zu verhindern. Um ihren Mehrwert zu optimieren, ist überdies die Wahl des richtigen Zeitpunkts für die Einbindung des Kunden in den Innovationsprozess wichtig.[78]

Wesentlich zur Reduzierung von Know-how Abflüssen beitragen können ferner organisatorische Maßnahmen im eigenen Unternehmen. Zum Schutz geheimen Know-hows, das nichts mit dem gemeinsamen Forschungs- und Entwicklungsprojekt mit dem Kunden zu tun hat, ist beispielsweise die räumliche Trennung der Projektgruppe von anderen Bereichen der F+E Abteilung wichtig. Klare Schnittstellen zwischen den Abteilungen des eigenen Unternehmens helfen, nicht-kooperationsrelevante Abteilungen von kooperierenden Teilen abzugrenzen und so Einblicke in die Unternehmung zu beschränken. Während der Zusammenarbeit reduziert dies die Gefahr eines unerwünschten Informationsaustausches deutlich.[79]

Der Königsweg zum Schutz firmeninternen Know-hows ist die Anmeldung von Schutzrechten. Von unseren Gesprächspartnern in Erwägung gezogen und auch angemeldet werden beispielsweise Verfahrenspatente, sofern Know-how-Schutz durch Geheimhaltung nicht möglich ist. Voraussetzung für diesen Schutz ist allerdings die Patentfähigkeit der Technologie. Entsprechend ist dies keine Universallösung für die Problembewältigung im Know-how-Schutz.

In summa erweist sich der auf Kunden abzielende Know-how-Schutz sich als Kompromiss. Die Minimierung des Risikos ungewollter Know-how-Verluste wirkt sich meist negativ auf die Kundenbeziehung oder die Effektivität des gemeinsamen Forschungs- und Entwicklungsprojektes aus. Andererseits kann ein kompletter Verzicht auf Know-

---

[77] *Wildemann*, Konzeptwettbewerb und Know-how-Schutz in der Automobil- und Zulieferindustrie (http://www.industrielle-dienstleistungen.de/uploads/html/publikationen/aufsatz/files/weissenberger_Konzeptwettbewerb.pdf) (Stand: 21.01.2011); *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 10 Rn. 25.

[78] *Gassmann / Kausch / Enkel,* Einbeziehung des Kunden in die frühe Phase des Innovationsprozesses, Thexis 2005 Nr. 2, 11.

[79] *Michel,* Management von Kooperationen im Bereich Forschung und Entwicklung, Konstanzer Managementschriften Band 7 / 2009, S. 64f.

how-Schutz dazu führen, dass sämtliche Wettbewerbsvorteile, basierend auf geheimem Know-how, verloren gehen, was die Marktposition des Unternehmens schwächt. Die Herausforderung besteht darin, den bestmöglichen Mittelweg zu finden. Durch die Verhandlungsmacht von OEMs ist der Spielraum mittelständischer Zulieferer allerdings begrenzt. Daher sollte jede Zusammenarbeit zu Beginn kritisch analysiert werden und sollte eine Einschätzung stattfinden, wie hoch das Risiko des Know-how-Verlusts ist, welche Tragweite dieser hätte und welche Chancen und Bedeutung die Partnerschaft birgt. Auch sollten Entscheidungsoptionen vorliegen, notfalls auch gegen die allgemeine Unternehmensphilosophie der Kundenorientierung ein gemeinsames Forschungs- und Entwicklungsvorhaben jedenfalls dann auszuschlagen, wenn Risiko und Mehrwert nicht in angemessenem Verhältnis zueinander stehen.[80]

Abbildung 8
Checkliste – F+E Partnerschaften

Checkliste – F+E Partnerschaften

- Sensibilität projektrelevanten Know-hows bewerten
- Eingebrachtes Know-how durch Vertraulichkeitsvereinbarungen schützen (ggf. im Rahmen des F+E Vertrags)
- Klare Regelungen bezüglich der Verwertung der Projektergebnisse (Zufallserfindungen, Schutzrechte, Geheimhaltung, Zweckbindung)
- Zur Beweisführung im Notfall (Verletzung) systematisch eigenes Know-hows erfassen und auf Vertraulichkeit hinweisen
- Partner und einzubringendes Know-how nach Nutzen- und Risikokriterien bewerten
- F+E Partnerschaft und übrige F+E räumlich trennen
- Sensibles Know-how ggf. zum Schutzrecht anmelden

Bild: Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum

[80] *Michel,* Management von Kooperationen im Bereich Forschung und Entwicklung, Konstanzer Managementschriften Band 7 / 2009, S. 64f.

6.1.3 Welche Probleme bereiten bayerischen KMU Konzeptwettbewerbe?

Eine neue Form von Entwicklungspartnerschaften bilden sogenannte Konzeptwettbewerbe oder Innovationstage. Sie vermittelten mehreren unserer Gesprächspartner die steigenden Anforderungen und die Verhandlungsmacht ihrer Kunden. Durch die Ausschreibung solcher Konzeptwettbewerbe oder Innovationstage geben diese Kunden, beispielsweise in der Automobilindustrie, eigenen Kosten- und Innovationsdruck an Zulieferer weiter, die möglichst innovative und den Kundenanforderungen entsprechende Lösungen zu günstigen Preisen präsentieren müssen. Zur Herausstellung ihrer Innovativität und Technologiekompetenz und zur Unterscheidung von Mitwettbewerbern, geben Unternehmen bei derartigen „Beauty Contests“ immer wieder auch geheimes Know-how preis. Auch wenn Vertraulichkeit zugesichert wurde, sammelten unsere Gesprächspartner hier immer wieder schlechte Erfahrungen. In einem besonders krassen Fall gaben Kunden eingereichte Unterlagen abredewidrig an Mitbieter weiter und offenbarten so Unternehmensgeheimnisse unserer Gesprächspartner gegenüber deren Konkurrenten.

Auch wenn sich dies nicht bestätigen lässt, stellt sich die Frage, ob dieses Kundenverhalten nur auf Irrtümern oder Fehlleistungen subalterner Stellen beruht. Angesichts eindeutiger Interessen ist nicht auszuschließen, dass Einkäufer hier den Hebel ihrer Marktmacht rücksichtslos zu Lasten ihrer Zulieferer einsetzen und deren Know-how im eigenen Kosteninteresse bewusst gefährden oder solche Gefährdungen hinnehmen. Besagte Zulieferer, mit denen wir sprachen, sehen keine Möglichkeit, sich gegen solche Praktiken rechtlich zu wehren, weil sie die Beziehung zu wichtigen Großkunden nicht gefährden wollen. Wir halten diese Verhaltensmuster für kurzsichtig und meinen, dass jedenfalls im Verbandskontext zu einem Umgang gefunden werden sollte, der machtgetriebene Rechtsbrüche gegenüber marktschwächeren Unternehmen ächtet, weil durch Rechtsbrüche begründete Wettbewerbspositionen nicht nachhaltig sind.

6.1.4 Maßnahmen zum Know-how-Schutz bei Teilnahme an Konzeptwettbewerben

Aus juristischer Sicht gibt es verschiedene Ansätze, um dem Problem zu begegnen. An Macht- und Abhängigkeitsverhältnissen, die der Nutzung solcher Ansätze entgegenstehen, führt juristisch jedoch kein Weg vorbei. Diese Nutzung erfordert auf beiden Seiten einen Mentalitätswechsel und die Einsicht, dass sich Geschäftsbeziehungen langfristig nur entwickeln lassen, wenn beide Seiten davon Vorteile haben.

Aus juristischer Perspektive wird sich als Problemlösung insbesondere der Abschluss von Vertraulichkeitsvereinbarungen anbieten. Durch solche individuellen Vereinbarungen kann umfassender, auf die Bedürfnisse des Know-how-Inhabers im Einzelfall abgestimmter Schutz erreicht werden. Detailliert geregelt werden sollten in Vertraulichkeitsvereinbarungen namentlich der Umgang mit Unterlagen und deren Rückgabe. Die Vereinbarung von Vertragsstrafen ist ein denkbares Sicherungsmittel, doch hängt der Einsatz dieser Option naturgemäß stark an der Marktposition des Verwenders.[81] Ob mittelständische Unternehmen OEMs zur Unterzeichnung von Geheimhaltungsvereinbarungen bewegen können, ohne dadurch ihre Ausgangssituation im Kompetenzwettbewerb zu verschlechtern, ist derzeit bedauerlicherweise zweifelhaft, auch wenn dort nichts anderes vereinbart werden würde als ohnehin geltendes Recht ist.

Bei Konzeptwettbewerben greift überdies häufig der gesetzliche Know-how-Schutz, v. a. nach § 18 UWG, der die unbefugte Verwertung von im geschäftlichen Verkehr anvertrauten Vorlagen oder Vorschriften technischer Art, insbesondere Zeichnungen, Modelle, Schablonen, Schnitte, Rezepte unter Strafe stellt. Kalkulationen eines Projektes, detaillierte Leistungsbeschreibungen, Ausführungsvorschläge fallen unter den weit zu fassenden Begriff der „Vorlagen oder Vorschriften technischer Art“, so dass die Anwendbarkeit von § 18 UWG nur selten zweifelhaft sein dürfte. Einzelne Konstruktionszeichnungen oder Herstellungsanweisungen sind ebenfalls und schon für sich genommen durch § 18 UWG geschützt. Da Angebote dem Auftraggeber konkludent nur mit der Verpflichtung überlassen werden, diese allein in einer Ausschreibung zu verwenden, gelten sie im Sinne des § 18 UWG als „anvertraut“.

Um Unsicherheiten vorzubeugen, sollten alle individuell ausgearbeiteten Angebote durch einen ausdrücklichen Vertraulichkeitsvermerk gekennzeichnet sein, denn dieser Vermerk wird in aller Regel zur Erfüllung des Merkmals des »Anvertrautseins« aus § 18 UWG führen.[82] Auch könnte der Zulieferer, dessen Know-how durch Verschulden des Kunden, offenbart wurde, Ansprüche wegen der Verletzung vorvertraglicher Pflichten (sog. c.i.c.) geltend machen, wenn der Kunde in einem solchen Fall Obhutspflichten im Sinne des § 311 Abs. 2 Nr. 3 BGB nicht erfüllt hat.

Ausschreibungen können ein Vertragsanbahnungsverhältnis (§ 311 Abs. 2 Nr. 2 BGB) darstellen, dessen Verletzung ebenfalls Schadenersatzansprüche des geschädigten Know-how-Inhabers auslösen kann.[83] Auch hier ist allerdings fraglich, ob ein als Zulieferer betroffenes KMU rechtlich gegen einen bedeutenden Kunden vorzugehen würde und sich so auch für andere Kunden als „schwierig“ erweisen könnte. Immerhin kann die Kennzeichnung von Unterlagen als vertraulich die Hemmschwelle beim Kunden erhöhen, diese Unterlagen weiterzureichen.

---

[81] *Maaßen*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 3 Rn. 65.
[82] *Maaßen*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 3 Rn. 69f.
[83] *Maaßen*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 3 Rn. 71.

Bekannt geworden sind andererseits auch bereits Fälle, in denen sich große OEMs bereits in Allgemeinen Geschäftsbedingungen (AGB) sämtliche Nutzungsrechte an dem in Angebotsunterlagen verkörperten Know-how (einschließlich einschlägiger Schutzrechte) haben einräumen lassen. Damit waren diese Kunden zur Nutzung dieser Informationen berechtigt, auch wenn keine Auftragserteilung versprochen wurde.[84]

Ausschreibungsunterlagen samt AGB sollten daher eingehend studiert werden, denn auch wenn einseitige AGB einmal nicht wirksam sein sollten, vermeidet das rechtzeitige Ansprechen von Problemen späteren Ärger.

Neben rechtlichen Schutzmaßnahmen, die insbesondere gegenüber Kunden mit starken Verhandlungs- und Marktpositionen aus Furcht um Aufträge nur eingeschränkt eingesetzt werden, gibt es auch Wege für einen faktischen Informationsschutz. So ist denkbar die Einreichung von 80 Prozent-Lösungen oder die Modifikation von Konstruktionszeichnungen oder Mustern.[85] Allerdings kann schon eine besondere technologische Problemlösung den Wettbewerbsvorteil ausmachen, dessen Vertraulichkeit vor der Konkurrenz bewahrt werden soll. Für Unternehmen, die in Konzeptwettbewerben als besonders kreative, innovative und kompetente Partner dastehen wollen, birgt die Zurückhaltung wichtiger Details das Risiko des Verlusts eines Auftrags, weil der potenzielle Kunde nicht überzeugt werden konnte. Auch dieser Ansatz funktioniert darum nicht in jeder Situation und für jedes Unternehmen.

In summa stehen Unternehmen damit vor der Abwägung, wie wichtig ihnen ein konkreter Auftrag ist und welchen Wettbewerbsvorteil das dafür relevante Know-how tatsächlich verkörpert. Für diese Abwägung sollte das eigene Know-how systematisch erfasst und nach Sensibilitätsklassen geordnet werden,[86] denn so wird das Risiko der Teilnahme an einem Konzeptwettbewerb und der vollständigen Offenlegung kritischen Know-hows besser einschätzbar. Strategisch wird es gelegentlich sinnvoll sein, auch einmal auf einen Auftrag zu verzichten und stattdessen sein Geistiges Eigentum konsequent zu schützen, frei nach dem Motto, dass der Krieg gewonnen werden muss, nicht nur eine einzelne Schlacht.

---

[84] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 4 Rn. 117.
[85] *Wildemann*, Konzeptwettbewerb und Know-how-Schutz in der Automobil- und Zulieferindustrie (http://www.industrielle-dienstleistungen.de/uploads/html/publikationen/aufsatz/files/weissenberger_Konzeptwettbewerb.pdf**)** (Stand: 21.01.2011)
[86] *Wildemann,* Konzeptwettbewerb und Know-how-Schutz in der Automobil- und Zulieferindustrie (http://www.industrielle-dienstleistungen.de/uploads/html/publikationen/aufsatz/files/weissenberger_Konzeptwettbewerb.pdf) (Stand: 21.01.2011); *Huber,* in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 10 Rn. 25ff.

Abbildung 9
Checkliste – Konzeptwettbewerbe

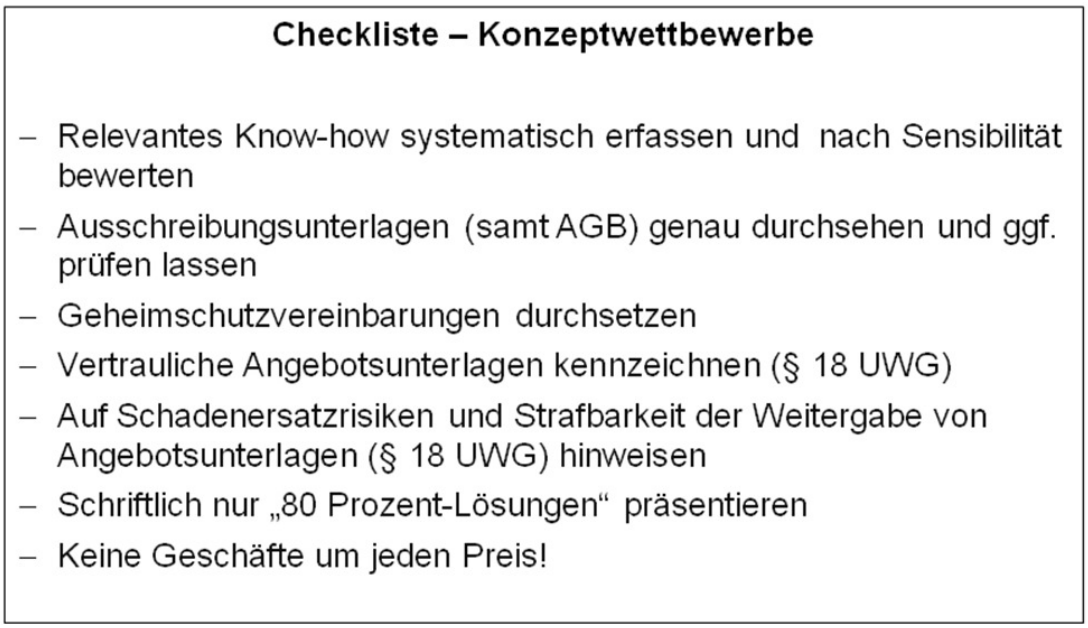


Bild: Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum

6.2 Know-how-Verlust durch Outsourcing

In den letzten Jahrzehnten war die Wirtschaft stark von einem Trend zur Arbeitsteilung gekennzeichnet. Die Wertschöpfungstiefe der Unternehmen sank, immer mehr Leistungen wurden zugekauft und Prozesse ausgelagert. Netzwerkproduktionen, Outsourcing, virtuelle Fabriken, kapitalarmes Wachstum und Betreibermodelle wurden als „Königsweg für eine schlanke Produktion und höchste Rendite“ betrachtet. Mittlerweile zeigt sich in vielen Branchen jedoch wieder ein konträrer Trend. Das Outsourcing zentraler Bauteile verursacht Abstimmungsprobleme in komplexen Produkten. Koordinationsaufwand, Kosten und das Streben nach Identität zwischen Produkt und Unternehmen (Beispiel: Mercedes-Benz) lassen Unternehmen wieder auf höhere Fertigungstiefen setzen, um ihre Rendite zu erhöhen.[87] Aus Sicht des Technologieschutzes ist dieser Trend positiv zu werten. Ein produzierendes Unternehmen kann sein Know-how

[87] *Wildemann*, Produktion hat goldenen Boden - Selbermachen ist gesund, S. 1, 3 (http://www.tcw.de/uploads/html/publikationen/aufsatz/files/Produktion_hat_goldenen_Boden.pdf) (Stand: 29.01.2011);

erheblich besser schützen als ein Unternehmen, das nur noch eine Vielzahl von Wertschöpfungspartnern koordiniert. Audi-Vorstand Jochem Heizmann warnt darum zu Recht, dass eine Senkung der Wertschöpfungstiefe die große Gefahr mit sich bringt, unverzichtbares Kern-Know-how zu verlieren und damit Qualität.[88]

Freilich ist trotz dieser positiven Entwicklung das Problemfeld aus dem Betrachtungswinkel des Technologiesschutzes nicht komplett bereinigt. Laut „SiFo-Studie 2009 / 2010“ sind *16 Prozent aller Wirtschaftsstraftäter Subunternehmer*.[89] Da Unternehmen zahlreiche Dienstleistungen über Unternehmensgrenze hinweg in Anspruch nehmen, bestehen zahlreiche Schnittstellen nach außen, und diese bilden stets eine Gefahr für ungewollten Know-how-Verlust. Letztendlich ergeben sich beim Outsourcing ähnliche Probleme und Risiken wie bei der Zusammenarbeit mit anderen Dritten,[90] wenngleich nicht alle extern bezogenen Leistungen die Mitteilung sensiblen Know-hows oder Einblicke in geheime Unternehmensbereiche erfordern.

6.2.1 Wie stark ist die Bedrohung für bayerische KMU?

Auch unsere Gesprächspartner nahmen externe Dienstleister in Anspruch, vorrangig in den Bereichen IT, Raumpflege, Mitarbeiterverpflegung, Werksicherheit, Instandhaltung von Produktionsanlagen. Die Auslagerung von Kernprozessen der Wertschöpfung, etwa der Produktion, scheint hingegen die Ausnahme zu sein. Probleme durch den Fremdbezug von Leistungen wurden selten wahrgenommen. Die Geschäftsbeziehungen beschrieben unsere Gesprächspartner hinsichtlich des Know-how-Schutzes als unbedenklich und störungsfrei.

6.2.2 Maßnahmen zum Schutz von Know-how beim Outsourcing

Hauptproblem und Hauptrisiko des Know-how-Schutzes im Rahmen von Outsourcing liegt in der Weitergabe vertraulicher, für den externen Leistungsbezug notwendiger Informationen.[91] Wird Kern-Know-how outgesourct und mit Partnern kooperiert, die gleichzeitig mit Wettbewerbern zusammenarbeiten, steigt die Gefahr von Know-how-Verlusten und drohen Abhängigkeitsverhältnisse sowie der Verlust von Wettbewerbs-

---

[88] *Wildemann*, Produktion hat goldenen Boden - Selbermachen ist gesund, S. 2 (http://www.tcw.de/uploads/html/publikationen/aufsatz/files/Produktion_hat_goldenen_Boden.pdf) (Stand: 29.01.2011).
[89] *Sicherheitsforum Baden-Württemberg (Hrsg.),* SiFo-Studie 2009 / 2010 – Know-how-Schutz in Baden-Württemberg, 2010, S. 67 (http://www.sicherheitsforum-bw.de/x_loads/SiFo-Studie.pdf) (Stand: 29.01.2011).
[90] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 4 Rn. 78.
[91] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 4 Rn. 94f.

vorsprüngen. Schutzmaßnahme der Wahl bei der Weitergabe vertraulicher Informationen sind vertragliche Regelungen, die Geheimhaltung, eingebundene Personenkreise, Wettbewerbsverbote, Erfüllungsort, Rechte an Verbesserungen etc. klären.[92]

Generell scheinen Unternehmen der bayerischen M+E Industrie die Risiken des Know-how-Verlusts durch externe Geschäftspartner besser zu bewältigen als durch Kundenintegration in Forschung und Entwicklung. Dies mag damit zusammenhängen, dass gegenüber Outsourcingpartnern stärkere Verhandlungspositionen bestehen als gegenüber OEMs, denen gegenüber angemessene vertragliche Vereinbarungen zum Schutz geheimen Know-hows nur schwer durchsetzbar sind.

Zum Schutz gegen Know-how-Abfluss durch Outsourcing bietet sich der Aufbau eines internen Know-how-Schutz-Systems an. Notwendig sind aufgrund des Kontakts zu Unternehmensangehörigen vor allem personelle Maßnahmen, ferner Maßnahmen im technischen und organisatorischen Bereich. Diese Maßnahmen zum betriebsinternen Know-how-Schutz werden später *in den Kapiteln 6.3 und 6.4* dargestellt.

Abbildung 10
Checkliste – Outsourcing

Checkliste – Outsourcing

- Vertragliche Regelung treffen (Vertraulichkeitsvereinbarungen, Wettbewerbsverbote, Erfüllungsortes etc.)
- Relevantes Know-how systematisch erfassen und nach Sensibilität bewerten
- Know-how nur nach „Need-to-Know“ weitergeben
- Partner bewusst nach Vertrauenswürdigkeit und Kompetenz auswählen

Bild: Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum

[92] *Huber*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 4 Rn. 106ff.

6.3 Know-how-Verlust durch Mitarbeiter

Laut „SiFo-Studie 2009 / 2010“ sind *für Know-how-Verletzungen meist eigene Mitarbeiter verantwortlich*. Über 70 Prozent der Täter, nach anderen Quellen sogar 80 Prozent[93], kommen aus dem geschädigten Unternehmen selbst, obwohl zwei Drittel aller Unternehmen, also ein etwa gleich hoher Prozentsatz eben dies für unwahrscheinlich halten.[94] Derartige Fehleinschätzungen lassen vermuten, dass erstens unzureichende Schutzmaßnahmen getroffen werden und dass sich dieses zweitens nicht ändern wird, solange Unternehmen das Problem nicht zur Kenntnis nehmen.

Die „SiFo-Studie 2009 / 2010“zeigt darüber hinaus, dass *in allen Unternehmenspositionen mit Tätern gerechnet werden muss*. Besonders hoch ist gemessen an ihrer Personalstärke der Anteil von Führungskräften, wie beim kürzlich bekannt gewordenen Verrat von Know-how zur Elektromobilität, das leitende Mitarbeiter von Renault-Nissan an chinesische Empfänger weitergaben. An fast jedem fünften Fall sind Topmanager zumindest beteiligt.[95] Die Ursachen für derart illoyales Handeln sind vielfältig. Häufig spielt mangelndes Werte- oder Unrechtsbewusstsein eine Rolle, doch es liegen auch eigennützige Beweggründe vor, wie z. B. finanzielle Anreize oder berufliche Enttäuschung. Bekannt sind auch Fälle, in denen Mitarbeiter von Externen erpresst worden sind.[96]

Mitarbeiter sind die größte Schwachstelle beim Schutz kritischer Unternehmensgeheimnisse. Sie sind sowohl innerbetrieblich als auch im Verhältnis zu Unternehmensexternen, Kooperationspartnern, Wettbewerbern, Geschäftspartnern etc., Schnittstellen und nutzen diese Stellung – beabsichtigt oder unbeabsichtigt, fremdnützig oder eigennützig – zum Know-how-Verrat.[97] Know-how-Verletzungen durch Mitarbeiter sind vielgestaltig. Sie reichen vom Diebstahl oder der unerlaubten Vervielfältigung von Dokumenten bis zum Verrat anvertrauten oder widerrechtlich beschafften Wissens. Diese Vielfalt und Varianz an Ausprägungsformen verdeutlicht, dass es keine Pauschallösung für das Problem gibt, sondern nur Bausteine, aus denen jedes Unternehmen die seinen Gegebenheiten und Erfordernissen entsprechende Lösung aufbauen kann. Auch zur Reduktion der Gefahr des Know-how-Verlusts durch die eigenen Mitarbeiter sind verschiedene Maßnahmen nötig – dazu sogleich.

---

[93] *Pisani,* Strategien beim Know-how-Schutz, Medizinprodukte Journal 2009 Nr. 4, 263.
[94] *Sicherheitsforum Baden-Württemberg (Hrsg.)*, SiFo-Studie 2009 / 2010 – Know-how-Schutz in Baden-Württemberg, 2010, S. 15 (http://www.sicherheitsforum-bw.de/x_loads/SiFo-Studie.pdf) (Stand: 29.01.2011).
[95] *Sicherheitsforum Baden-Württemberg (Hrsg.)*, SiFo-Studie 2009 / 2010 – Know-how-Schutz in Baden-Württemberg, 2010, S. 67 (http://www.sicherheitsforum-bw.de/x_loads/SiFo-Studie.pdf) (Stand: 29.01.2011).
[96] *Sicherheitsforum Baden-Württemberg (Hrsg.)*, SiFo-Studie 2009 / 2010 – Know-how-Schutz in Baden-Württemberg, 2010, S. 70f (http://www.sicherheitsforum-bw.de/x_loads/SiFo-Studie.pdf) (Stand: 29.01.2011).
[97] *Michel,* Management von Kooperationen im Bereich Forschung und Entwicklung, Konstanzer Managementschriften Band 7 / 2009, S. 63.

Ein wesentliches Problem des betrieblichen Know-how-Schutzes bildet die *Mitarbeiterfluktuation*. Wechseln Mitarbeiter zu einem Wettbewerber, besteht das signifikante Risiko eines ungewollten Know-how-Transfers. Dies belegt die „SiFo-Studie 2009 / 2010“, nach der 25 Prozent aller einschlägigen Taten durch abgeworbene Mitarbeiter und Manager begangen wurden.[98]

Maßnahmen zum Know-how-Schutz im Unternehmen müssen die Loyalität der Mitarbeiter im Auge haben, ferner die Sensibilisierung für die Bedeutung kritischen Know-hows für das Unternehmen sowie möglichen Know-how-Verrat durch Mitarbeiter.

6.3.1 Wie begegnen bayerische KMU dieser Gefahr?

Bayerische KMU der M+E Industrie unterschätzen das Risiko eines Know-how-Verrats durch Mitarbeiter, denn sie halten diesen schlichtweg für unwahrscheinlich. Zwar sind Maßnahmen, die den Geheimnisverrat durch Mitarbeiter unterbinden sollen, theoretisch bekannt. Doch werden diese häufig nicht konsequent umgesetzt. In der uns bekannt gewordenen Praxis ist ein strategisches Wissensmanagements eher die Ausnahme als die Regel.

So beschränken sich beispielsweise Geheimhaltungsvereinbarungen mit Mitarbeitern in der Regel auf Standardvereinbarungen im Rahmen des Arbeitsvertrags. Nur selten werden verschärfte Geheimhaltungsvereinbarungen mit Mitarbeitern getroffen, die mit besonders sensiblem Know-how umgehen.

Obwohl das Problem der Mitarbeiterfluktuation bekannt ist und gesehen wird, werden nachvertragliche Wettbewerbsverbote kaum je verwendet. Aus Kostengründen wird darauf meist gänzlich verzichtet. Immerhin hörten wir von ihrem vereinzelten Einsatz für Mitarbeiter in Schlüsselpositionen.

Die Erfassung und systematische Kategorisierung kritischer Unternehmensgeheimnisse erfolgte bei keinem unserer Gesprächspartner. Immerhin wurden in Einzelfällen F+E und Teile der Produktion geschützt, was Überlegungen zur Sensibilität des dort erzeugten oder eingesetzten Know-hows stattfinden. Weil Know-how nicht bewertet wurde und weil damit unsystematisch oder informell umgegangen wurde, erfolgte auch die Verteilung von Know-how auf Mitarbeiter ohne die unter dem Aspekt eines nachhaltigen Know-how-Schutzes wünschenswerte Strategie.

---

[98] *Sicherheitsforum Baden-Württemberg (Hrsg.)*, SiFo-Studie 2009 / 2010 – Know-how-Schutz in Baden-Württemberg, 2010, S. 63, 67 (http://www.sicherheitsforum-bw.de/x_loads/SiFo-Studie.pdf) (Stand: 29.01.2011).

Zum Know-how-Zugang für Mitarbeiter gibt es in den meisten Unternehmen Bestimmungen, die im IT-System durch Zuweisung individueller Zugangsberechtigungen umgesetzt werden. Dennoch fehlen in zahlreichen Unternehmen physische Zugangsbeschränkungen zu know-how-kritischen Arbeitsbereiche. Auch schutzbedürftige Dokumente werden so leicht allgemein zugänglich.

Vereinzelt wird Wissen auf Mitarbeiter nach dem aus dem Geheimschutz geläufigen Prinzip *„Need-to-Know“* verteilt. Diese Maßnahme ist vorbildlich, denn sie hält den Personenkreis klein, der im Unternehmen Zugang zu kritischen Unternehmensgeheimnissen hat. In einem Fall wurde kritisches Know-how sogar bewusst segmentiert an verschiedene Mitarbeitergruppen weitergegeben mit dem Ziel, die Konzentration von Know-how bei einzelnen Mitarbeitern zu verhindern.

Schulungen zum Know-how-Schutz werden kaum durchgeführt. Immerhin finden in einigen Unternehmen, wenn auch unregelmäßig, informelle Mitarbeiterunterrichtungen zum Thema Know-how-Schutz statt.

6.3.2 Schutzmaßnahmen gegen den Know-how Verlust durch Mitarbeiter

Unsere Beobachtungen entsprechen dem Befund der SiFo-Studie 2009 / 2010, es werde das *Risiko des Know-how-Verlusts durch Mitarbeiter nicht stark genug wahrgenommen.* Dementsprechend mangelt es in den Unternehmen an Präventionsmaßnahmen oder an deren konsequenter Umsetzung.

Die unlautere Aneignung von Unternehmensgeheimnissen ist nicht Teil dieses Abschnitts. Sie wird in *Kapitel 6.4* behandelt. Gleichwohl im Bereich der Prävention gegen Industriespionage keine Differenzierung zwischen unternehmensinternen und externen Tätern erforderlich.

6.3.3 Rechtlicher Schutz

Grundnorm des gesetzlichen Know-how-Schutzes ist § 17 UWG. *Geheimnisverrat begeht nach § 17 Abs. 1 UWG*, wer als eine bei einem Unternehmen beschäftigte Person ein ihr im Rahmen ihres Dienstverhältnisses anvertrautes oder zugänglich gewordenes Geschäfts- oder Betriebsgeheimnis während der Geltungsdauer ihres Dienstverhältnisses Dritten mitteilt. *§ 17 Abs. 2 Nr. 1 UWG* stellt *Industriespionage* unter Strafe. Danach ist es verboten, sich ein Geschäfts- oder Betriebsgeheimnis zu beschaffen oder zu sichern unter Verwendung technischer Mittel durch Herstellung einer verkörperten Wiedergabe des Geheimnisses oder durch Wegnahme einer Sache, in der das

Geheimnis verkörpert ist. Das umfasst die unbefugte Kopie geheimer Unterlagen, die Speicherung und Mitnahme geheimer Daten auf Datenträgern oder die Erlangung fremder Unternehmensgeheimnisse durch technische Aufklärung, wie etwa das Anzapfen von IT-Wartungszugängen oder das Abhören mittels versteckter Mikrofone.[99]

Prinzipiell sind Mitarbeiter im Rahmen eines bestehenden Arbeitsverhältnisses zwar verpflichtet, über Betriebsinterna, insbesondere Betriebs- und Geschäftsgeheimnisse, Stillschweigen zu bewahren. Dies ergibt sich aus dem allgemeinen arbeitsrechtlichen Loyalitätsgebot. Aus Gründen der Rechtssicherheit sollte der Geheimnisschutz jedoch vertraglich weiter konkretisiert werden.[100] Sichereren Schutz als Arbeitsverträge bieten *individuelle Vertraulichkeitsvereinbarungen*, die für den Einzelfall geschütztes Know-how definieren, konkrete Verpflichtung zum Know-how-Schutz normieren und die Nutzung überlassenen Know-hows auf bestimmte Zwecke beschränken.[101]

Inwieweit das allgemeine arbeitsrechtliche Loyalitätsgebot auch zu *nachvertraglicher Verschwiegenheit* verpflichtet, ist umstritten. Die Rechtssprechungen des BAG und BGH divergieren in diesem Punkt erheblich. Während das BAG diese Frage tendenziell im Sinne der schutzgeneigten Arbeitgeber entscheidet, geht der BGH von der grundsätzlichen Freiheit des Arbeitnehmers aus, beruflich erworbene Kenntnisse zu nutzen, solange er diese redlich erworben hat.[102] Auf Grund dieser uneinheitlichen Rechtssprechung auch der obersten Bundesgerichte muss jedes Unternehmen damit rechnen, dass Betriebs- und Geschäftsgeheimnisse im Zuge der Mitarbeiterfluktuation zur Konkurrenz abwandern.

Die Vereinbarung nachvertraglicher Verschwiegenheitspflichten ist im Grundsatz möglich, freilich nur solange der Arbeitnehmer in seiner Berufsausübung nicht unzumutbar beschränkt wird. Unzumutbarkeit wird nicht angenommen, wenn konkret bezeichnete Geschäftsgeheimnisse auch nachvertraglich geheim gehalten werden müssen, wohl aber wenn die Geheimhaltungspflicht sämtliche dem Arbeitnehmer bekannt gewordenen geschäftlichen und betrieblichen Tatsachen umfasst. Derart weitgehende nachvertragliche Geheimhaltungsverpflichtungen sind nichtig,[103] weil Arbeitnehmer sonst fast keine Möglichkeit hätten, gewonnenen Berufserfahrungen in einem neuen Arbeitsverhältnis einzusetzen. In ihrer Wirkung kämen solche Klauseln einem *Wettbewerbsverbot* gleich, das freilich nur für einen Zeitraum bis maximal zwei Jahren und nur gegen Zahlung einer sog. Karenzentschädigung (>50 Prozent des letzten Bruttomonatsgehalts) zulässig ist (§§ 74 ff. HGB). Arbeitsrechtlich ist der Totalschutz von Know-how-Schutz wegen der auf zwei Jahre begrenzten Laufzeit von Wettbewerbsverboten

---

[99] *Loschelder*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 99ff.
[100] *Pisani,* Strategien beim Know-how-Schutz, Medizinprodukte Journal 2009 Nr. 4, 263; *Loschelder*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 208.
[101] *Pisani,* Strategien beim Know-how-Schutz, Medizinprodukte Journal 2009 Nr. 4, 263f.
[102] *Loschelder*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 209.
[103] *Brock*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 2 Rn. 55ff.

nur für diesen Zeitraum möglich.[104] Auch sind Wettbewerbsverbote relativ teuer. Besonders in technologisch schnelllebigen Branchen lässt sich auf diesem Weg gleichwohl einiges erreichen.

6.3.4 Organisatorische Maßnahmen

Nach einer grundlegenden Daumenregel im Geheimschutz steigt das Risiko des Bekanntwerdens einer Information exponentiell zum Grad ihrer Verbreitung.[105] Die Geheimhaltung einer Information wird durch eine große Zahl von Mitwissern also überproportional erschwert. Andererseits ist eine gewisse Verteilung von Know-how im Unternehmen unvermeidlich, denn Mitarbeiter müssen auch arbeiten können.

Reduziert werden kann Gefahr des Bekanntwerdens von Unternehmensgeheimnissen, indem dieses Wissen allein nach dem Prinzip *„Need-to-Know"* je nach Funktion und Zuständigkeit des jeweiligen Mitarbeiters weitergegeben wird.[106] Kritisches Know-how wird so nur Mitarbeitern zur Verfügung gestellt wird, die es zur Verrichtung ihrer Arbeit zwingend benötigen.

Zusätzlich kann Know-how strategisch so verteilt werden, dass niemand das gesamte Know-how seines Unternehmens kennt und verraten kann. Das verringert die von der Mitarbeiterfluktuation ausgehende Gefahr. Umgesetzt werden kann dies beispielsweise durch Kompartimentalisierung, also durch die *Isolierung von Betriebsabläufen und Funktionen innerhalb des Betriebes*.[107] Träger von Schlüssel-Know-how haben so einerseits weniger Kontakt und Möglichkeit zum Informationsaustausch. Zu beachten ist andererseits jedoch, dass sich Kompartimentalisierung in der Regel negativ auf die in den meisten Unternehmen erstrebte freie Unternehmenskommunikation auswirkt.

Besondere Regelungen zur Know-how-Weitergabe sind für Praktikanten, Werkstudenten, Diplomanden und Doktoranden notwendig. Hier ist schon zu Beginn des Beschäftigungsverhältnisses bekannt, dass diese Personen nur für kurze Zeit im Unternehmen tätig sein werden. Ferner ist wahrscheinlich, dass sie kurze Zeit später ein neues Beschäftigungsverhältnis bei einem anderen Unternehmen beginnen werden – häufig im gleichen Geschäftsfeld bei einem Mitbewerber. Auf beides ist bei der Entscheidung zu achten, wie viel und welchen Einblick dieser Personenkreis erhalten soll.

---

[104] *Brock*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 2 Rn. 82, 90; *Ann* in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 59.
[105] *Ann / Kalbfus*, Gesetzlicher Schutz für geheimes Know-how – nur gerecht oder auch wirtschaftlich sinnvoll?, in Iurratio, 133.
[106] *Pisani,* Strategien beim Know-how-Schutz, Medizinprodukte Journal 2009 Nr. 4, 262.
[107] *Michel,* Management von Kooperationen im Bereich Forschung und Entwicklung, Konstanzer Managementschriften Band 7 / 2009, S. 64.

Damit bei der Know-how-Verteilung nur das zu schützende sensible Know-how nach dem „Need-to-Know-Prinzip“ behandelt wird und nicht das gesamte unternehmensinterne Wissen, ist unabdingbar, dass *kritische Informationen identifiziert und nach Geheimschutzbedürftigkeit klassifiziert werden*.[108] Der bayerische Verfassungsschutz empfiehlt eine Grobeinteilung in die Kategorien offen, firmenintern, streng vertraulich, und geheim.[109] Dieses Vorgehen erleichtert auch ein systematisches Vorgehen beim rechtlichen Schutz durch individuelle Vertraulichkeitsvereinbarungen.

Natürlich kann die organisatorische Aufteilung und Verteilung von Wissen für sich noch keinen Know-how-Schutz bewirkt, sondern diesen nur insofern vorbereiten, als sie Schutzobjekte identifizieren hilft. Zusätzlich müssen für die Zugänglichkeit des Know-how technische Vorkehrungen getroffen werden. Sicherheitskritische Unternehmensbereiche sind durch *Zutrittsbeschränkungen* zu sichern, für die Unternehmens-IT müssen *Zugriffsregelungen* vorhanden sein (s. a. unten *Kapitel 6.4)*.

Bereits erwähnt wurde oben der Widerspruch zwischen einer solchen Reorganisation als breit eingesetzte universelle Schutzmethode und dem Idealbild eines möglichst effizienten Informationsflusses. Stets abzuwägen ist deshalb, ob der Sicherheitsgewinn einer Sicherungsmaßnahme überwiegt oder deren (negative) wirtschaftlichen Folgen durch Einschränkung des Informationsflusses.[110]

Ferner ist der Einsatz dieser Maßnahmen nur eingeschränkt für KMU möglich. Zwar kann das „Need-to-Know-Prinzip“ Anwendung finden, jedoch lassen sich Produktion und F+E erst ab einer gewissen Unternehmensgröße sinnvoll kompartimentieren.

6.3.5 Maßnahmen zur Erhöhung der Mitarbeiterloyalität

Wie oben beschrieben eignen sich arbeitsrechtliche Maßnahmen nur bedingt für einen nachvertraglichen Know-how-Schutz. Das Problem der steigenden Mitarbeiterfluktuation hat daher gewichtige Bedeutung auch für den Know-how-Schutz.[111] Während deutsche Arbeitnehmer früher häufig ihr gesamtes Berufsleben bei nur einem Arbeitgeber verbrachten oder sich dies zumindest vorstellen konnten, weil wechselseitige Loyalität zwischen Unternehmen und Arbeitnehmern in der Unternehmenskultur verankert war, ist gegenwärtig genau das Gegenteil der Fall.[112] Die Mitarbeiterzufriedenheit in Deutschland ist gering und sie sinkt stetig. Nach einer Studie des Marktforschungsin-

---

[108] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 61.
[109] *Bayerisches Landesamt für Verfassungsschutz* (http://www.wirtschaftsschutz-bayern.de/App.aspx?EditionViewID=3a5ebacf-5178-4f28-b47e-161d8d5d9fd5) (Stand: 29.01.2011).
[110] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 61; *Ann / Kalbfus,* Geheimnisse sind schützenswert, FAZ v. 15.06.2009, S. 12.
[111] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 59.
[112] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 60.

stituts IFAK fühlen sich nur zwölf Prozent aller Beschäftigten (drei Prozent weniger als im Vorjahr) ihrem Arbeitgeber gegenüber verpflichtet und engagieren sich im Job. Ein Viertel hat innerlich bereits gekündigt. Unmotivierte Mitarbeiter mit schwacher Unternehmensbindung leisten weniger, verbreiten keine positive Mund-zu-Mund-Propaganda und kündigen schneller.[113] Auch ohne Rekurs auf das Ethos eines „Siemensianers", „Zeissianers" oder „Kruppianers" vergangener Tage lässt sich also bis heute empirisch belegen, dass eine Steigerung der Mitarbeiterzufriedenheit die Loyalität zum Arbeitgeber fördert und sich damit gleichzeitig positiv auf den Know-how-Schutz jedes Unternehmens auswirkt. Hinzu kommen Kosteneinsparungen, die zufriedene Mitarbeiter in den Bereichen Recruiting, Unternehmensimage und Arbeitsleistung bewirken.

Eine gesteigerte Mitarbeiterloyalität beschränkt jedoch nicht nur den Know-how-Verlust durch weniger Mitarbeiterfluktuation. Sie verringert auch die Wahrscheinlichkeit des Geheimnisverrates während des Beschäftigtenverhältnisses. Laut SiFo-Studie 2009 / 2010 ist *berufliche Enttäuschung eines der zentralen Tatmotive für Geheimnisverrat*. Maßnahmen zur Mitarbeiterzufriedenheit können diese Gefahr einschränken.[114]

6.3.6 Maßnahmen zur Sensibilisierung für die Wichtigkeit von Know-how

Laut der SiFo-Studie 2009 / 2010 ist die am häufigsten genannte Ursache einer Know-how-Verletzung durch Mitarbeiter mangelndes Unrechtbewusstsein.[115] Vielfach geben Mitarbeiter geheimes Wissen preis, ohne sich dessen bewusst zu sein. In anderen Fällen werden sie durch Dritte "abgeschöpft", ohne es zu bemerken („Social Engineering").[116] Es ist daher notwendig, sämtliche Mitarbeiter für die Rechtlage und die Relevanz effektiven Know-how-Schutzes zu sensibilisieren – durch Schulungen oder durch Sicherheitstrainings. Auch der Außenauftritt auf Messen oder Tagungen sowie in wissenschaftlichen Beiträgen von Mitarbeitern kann technisch und juristisch geübt werden. Zurückhaltung auch bei der Kommunikation technischer Innovationen gegenüber der (Fach-)Öffentlichkeit ist häufig der richtige Weg. Das sollte jeder F+E Mitarbeiter wissen![117]

---

[113] Arbeitsklima-Barometer 2008 des IFAK Instituts aus Taunusstein (http://www.t-online-business.de/arbeitsklima-barometer-2008-zu-wenig-engagement-in-deutschen-firmen-/id_16895016/index) (Stand: 29.01.2011).
[114] *Sicherheitsforum Baden-Württemberg (Hrsg.)*, SiFo-Studie 2009 / 2010 – Know-how-Schutz in Baden-Württemberg, 2010, S. 68ff (http://www.sicherheitsforum-bw.de/x_loads/SiFo-Studie.pdf) (Stand: 29.01.2011).
[115] *Sicherheitsforum Baden-Württemberg (Hrsg.)*, SiFo-Studie 2009 / 2010 – Know-how-Schutz in Baden-Württemberg, 2010, S. 68ff (http://www.sicherheitsforum-bw.de/x_loads/SiFo-Studie.pdf) (Stand: 29.01.2011).
[116] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 31.
[117] *Pisani,* Strategien beim Know-how-Schutz, Medizinprodukte Journal 2009 Nr. 4, 262; *Senze*, Schutz vor ungewolltem Abfluss von Know-how, S. 20 (http://www.luther-lawfirm.com/download_vortraege_de/252.pdf) (Stand: 29.01.2011).

Zu beachten ist schließlich, dass das Risiko des „Social Engineering“ durch die Verbreitung sozialer Netzwerke deutlich gesteigert wird. Jede veröffentlichte Information kann als Grundlage für eine gezielte Kontaktanbahnung dienen.[118]

Abbildung 11
Checkliste – Mitarbeiter

Checkliste – Mitarbeiter

- Individuelle Geheimschutzabreden mit Mitarbeitern treffen (keine Internet-Muster, sondern Maßarbeit!)
- Wettbewerbsverbote vereinbaren, wenn kostenseitig vertretbar
- schutzbedürftiges Know-how vom übrigen unternehmensinternen Wissen trennen
- Know-how-Verteilung nach Prinzip „Need-to-Know “
- Know-how-Konzentration bei einzelnen Mitarbeitern vermeiden
- Technische Zutritts- und Zugriffsbeschränkungen im Unternehmen gemäß Know-how-Verteilung einrichten und regelmäßig überprüfen
- Auf Mitarbeiterzufriedenheit achten
- Mitarbeiter für Unternehmensgeheimnisse sensibilisieren
- Klare Richtlinien zum Umgang mit geheimen Informationen, Daten und Dokumenten schaffen und bekannt machen

Bild: Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum

6.4 Know-how-Verlust durch Industriespionage

Als Bedrohung geschützten Know-hows steht an zweiter Stelle hinter dem Geheimnisverrat durch Mitarbeiter, bei dem Beschäftigte ihnen anvertraute Unternehmensgeheimnisse unbefugt weitergeben oder zu eigenen Zwecken verwenden, die unlautere

[118] *Bayerisches Landesamt für Verfassungsschutz* (http://www.wirtschaftsschutz-bayern.de/App.aspx?EditionViewID=3a5ebacf-5178-4f28-b47e-161d8d5d9fd5) (Stand: 29.01.2011).

Aneignung von Know-how – sowohl durch *Wirtschaftsspionage* fremder Staaten bzw. ihrer Geheimdienste als auch durch *Konkurrenzspionage* von Mitbewerbern. Bei der Wirtschaftsspionage geht es Staaten mit Technologierückständen hauptsächlich um wirtschaftsnahe Forschungsergebnisse und konkrete Produkte, während hoch industrialisierte Länder in erster Linie an strategischen Informationen interessiert sind. Konkurrenten spähen in der Regel wettbewerbsrelevante Informationen über Märkte, Technologien oder Kunden, aktuelles Know-how zur Produktentwicklung und Produktionstechnik, Preise, Kalkulationen oder Designstudien aus.[119] Laut der Corporate Trust Sudie 2007 dürfte etwa jedes fünfte Unternehmen schon einmal von Industriespionage betroffen gewesen sein.[120]

Potenzielle *Täter sind sowohl Unternehmenszugehörige als auch Externe aus dem Geschäftsumfeld*. Auch mit Angreifern ohne direkten Unternehmensbezug muss gerechnet werden. Laut „SiFo-Studie 2009 / 2010“ spielen ausländische Nachrichtendienste mit nur sechs Prozent der berichteten, aufgeklärten und vermuteten Fälle zwar nur eine untergeordnete Rolle. Es ist jedoch davon auszugehen, dass dieses Risiko bei forschungsintensiven Großunternehmen deutlich höher ist, als es die überwiegend zu KMU durchgeführte Studie zeigt. Grund ist die hohe Professionalität von Nachrichtendiensten, deren illegale Informationsbeschaffung häufig unbemerkt bleibt.[121] Täter aus dem näheren Umfeld können Mitbewerber, Kunden, Zulieferer, Dienstleister und Besucher sein, ferner Mitarbeiter, denen im Rahmen ihrer Tätigkeit nicht die betreffenden Unternehmensgeheimnisse anvertraut wurden, sondern die sich diese unlauter beschafft haben. Diese Arbeitnehmer fallen nicht selten durch ausgedehnte Nachtarbeit auf, denn nachts besteht wenig soziale Kontrolle durch Kollegen und Vorgesetzte.[122]

Die *Arten der Tatbegehung, eingesetzte technische Mittel und Tätergruppen sind vielfältig.* Informationsbeschaffung findet unter anderem statt durch den klassisch-kriminellen *(Einbruchs)Diebstahl* von Daten oder Datenträgern. Er kann sowohl Arbeitsplatz als auch private Wohnräume des Know-how-Inhabers betreffen, ferner Fahrzeuge.[123]

Eine andere Form von Know-how-Diebstahl bildet das Ausspähen von Daten oder Informationen. Dabei wird häufig *von technischen Mitteln der IT oder Fernmeldung Gebrauch gemacht*, wie z. B.:

---

[119] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 28; *Bundesamt für Verfassungsschutz für die Verfassungsschutzbehörden in Bund und Ländern (Hrsg.)*, Wirtschaftsspionage – Risiko für Ihr Unternehmen, S. 6f (http://www.wirtschaftsschutz-bayern.de/content/al_library/_ext_files/broschuere_0608_wirtschaftsspionage.pdf) (Stand: 29.01.2011).

[120] *Corporate Trust*, Studie: Industriespionage - Die Schäden durch Spionage in der deutschen Wirtschaft, 2007, S. 13 (http://www.corporate-trust.de/pdf/STUDIE_191107.pdf) (Stand: 29.01.2011).

[121] *Sicherheitsforum Baden-Württemberg (Hrsg.)*, SiFo-Studie 2009 / 2010 – Know-how-Schutz in Baden-Württemberg, 2010, S. 67f (http://www.sicherheitsforum-bw.de/x_loads/SiFo-Studie.pdf) (Stand: 29.01.2011).

[122] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 32.

[123] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 34.

- Einsatz von Trojanern,
- Hacker-Angriffe,
- Missbrauch von Fernwartungszugängen, Benutzerrechten oder Administratorrechten,
- Abhören oder Umleiten von Telefon-, Telefax- oder Datenverbindungen,
- Durchführung von Verkehrsflussanalysen (z. B. über ISDND-Kanal),
- Abhören von Räumen mittels Richtmikrofonen, mobilen Endgeräten oder Rechnern mit Mikrofon,
- Foto- und Filmaufnahmen mit mobilen Endgeräten,
- Angriffe auf W-LANs.[124]

Ferner werden auch menschliche Schwächen von Know-how-Inhabern ausgenutzt, indem sie durch sogenanntes *„Social Engineering"* teils auch ohne eigenes Wissen „abgeschöpft" werden. In anderen Fällen werden Mitarbeiter mit gezielt erarbeiteten Kompromaten erpresst oder bestochen.[125]

Ein weiteres Risiko sind *Dienstreisen* der Mitarbeiter, die in Zeiten globaler Vernetzung auch international stark zugenommen haben. Dabei ist mitgeführtes Firmen-Know-how anderen und größeren Gefahren ausgesetzt als innerhalb des Unternehmens. Öffentliches Arbeiten am Laptop, wie z. B. im ICE, am Flughafen oder in Seminaren, sowie Telefonate in der Öffentlichkeit erhöhen die Gefahr des ungewollten Know-how-Verlusts. Durch gezieltes Mitlesen oder Mithören können dabei vertrauliche Informationen unbemerkt verloren gehen. Auch die Gefahr des Diebstahls oder Verlusts von Datenträgern wird erhöht. Hotelzimmer und Hotelzimmersafes sind kein sicherer Aufbewahrungsort für hochsensibles Unternehmens-Know-how.[126] Besonders problematisch ist die Wirtschaftsspionage bei Auslandreisen in bestimmte Länder. Durch die Visaerteilung ist bekannt, wer wann und wo einreisen wird, und an den Grenzübertrittsstellen bestehen definierte Punkte, an denen Dienste eines Staats auf eigenem Gebiet frei agieren können. Reisende lassen sich dort leicht von ihrem Gepäck trennen.[127] Die VR China ist in dieser Hinsicht ein besonderer Problemfall. Der Einsatz von Verschlüsselungstechnik auf Firmenrechnern ist in China nach wie vor genehmigungspflichtig, und Verschlüsselungsverfahren haben nur dann eine Chance auf Zulassung, wenn sie von chinesischen Sicherheitsbehörden mitgelesen werden können. Wer sich nicht daran hält, fällt spätestens im großen Datenstrom aus der Masse heraus und muss mit Strafe und der Beschlagnahmung seiner Geräte rechnen.[128]

---

[124] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 33.
[125] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 31.
[126] *Bayerisches Landesamt für Verfassungsschutz* (http://www.wirtschaftsschutz-bayern.de/App.aspx?EditionViewID=3a5ebacf-5178-4f28-b47e-161d8d5d9fd5) (Stand: 29.01.2011).
[127] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 35.
[128] *Bayerisches Landesamt für Verfassungsschutz (Hrsg.)*, Nutzung von Laptops in der VR China (http://www.wirtschaftsschutz-bayern.de/content/al_library/_ext_files/Verschl%FCsselung%20China.pdf) (Stand: 29.01.2011).

Die Arten des Know-how-Verlusts durch Industriespionage sind vielfältig. Aus diesem Grund bedarf es eines umfangreichen Know-how-Schutz-Konzepts, welches möglichst viele Facetten berücksichtigt und ständig der Bedrohung angepasst wird. Insbesondere das professionelle Vorgehen von Wirtschaftsspionen erfordert hochentwickelten Know-how-Schutz.

6.4.1 Wie schützen sich bayerische mittelständische Unternehmen gegen diese Gefahr?

Unsere Gesprächspartner trafen großteils mehr als eine Maßnahme zum Schutz ihrer Unternehmensgeheimnisse, verwendeten meist jedoch kein ganzheitliches und durchdachtes Schutzkonzept. *Vor allem mangelte es an der Systematik des Know-how-Schutzes, mit der Folge teils erheblicher Sicherheitslücken*.

Signifikante Sicherheitslücken sehen wir beispielsweise beim Objektschutz. Zugangsbeschränkungen für know-how-sensible Bereiche, wie z. B. F+E oder kritische Fertigungen fehlen vielfach. Damit hat im Prinzip jeder Mitarbeiter Zutritt auch zu Orten, an denen er nichts zu tun hat und denen geheime Dokumente aufbewahrt oder kritische Fertigungsschritte vollzogen werden.

IT-Abteilungen sind häufig besser geschützt, pikanterweise auch Personalabteilungen, was darauf schließen lässt, dass Unternehmensleitungen dem Datenschutz ihrer Mitarbeiter mehr Aufmerksamkeit schenken als der Sicherheit der Unternehmensgeheimnisse, von denen die Existenz des Unternehmens abhängen kann. Die Ergebnisse der „SiFo-Studie 2009 / 2010“ unterstützt die Beobachtung, dass F+E- sowie Produktionsbereiche – obwohl bei forschungsintensiven Unternehmen häufiger von Know-how-Verletzungen betroffen – schwach oder zumindest schwächer als andere Abteilungen im Unternehmen geschützt werden.[129] Teilweise ist der mangelhafte Schutz darauf zurück zu führen, dass die Notwendigkeit der Installation technischer Zugangssicherungen nicht gesehen wird oder Schutzmaßnahmen nicht gewünscht werden auf Grund negativer Auswirkungen auf die Arbeitsatmosphäre. Beim Besuch eines unserer Gesprächspartner hätten wir das Unternehmen statt durch den Empfang auch durch eine offenstehende Tür in den Keller des Unternehmens betreten und wieder verlassen können. Im Monteursoverall eines Sanitärbetriebs und mit einem Werkzeugkasten in der Hand hätten wir uns im Unternehmen vermutlich weitgehend frei bewegen können.

Derartige Mängel entstehen aus dem bereits mehrfach angesprochenen Grund, dass zahlreiche Unternehmen ihr kritisches Know-how weder definieren, noch hinsichtlich

---

[129] *Sicherheitsforum Baden-Württemberg (Hrsg.)*, SiFo-Studie 2009 / 2010 – Know-how-Schutz in Baden-Württemberg, 2010, S. 73f (http://www.sicherheitsforum-bw.de/x_loads/SiFo-Studie.pdf) (Stand: 29.01.2011).

seines Geheimschutzbedürfnisses kategorisieren. Dadurch ist schwer zu erkennen, welche Unternehmensbereiche schützenswert sind und daher auch für eigene Mitarbeiter nur beschränkt zugänglich sein sollten. Dabei wäre ein Zugangsschutz heute technisch einfach und zu geringen Kosten einzurichten. Zugangsrechte lassen sich beispielsweise elektronisch auf *Firmenausweisen* speichern. Dadurch können Firmenausweise für zutrittsbeschränkte Bereiche als elektrische Türöffner fungieren. Gleichzeitig signalisiert das Tragen von Betriebsausweisen auch, ob sich Personen berechtigt im Unternehmen oder sogar bestimmten Unternehmensbereichen aufhalten und dient damit als zusätzliche Zugangskontrolle.[130] Insbesondere bei größeren Firmen ist das offene Tragen von Betriebsausweisen „am Mann" wichtig, weil dort eine fremde Person weniger auffällt.

Vergleichsweise gut organisiert ist immerhin der Umgang mit Unternehmensbesuchern. Nach den uns erteilten Auskünften kommen sie mit geheimem Know-how nicht in Berührung. Vielmehr sind Besucherausweise als Verschärfung der Zutrittskontrolle sichtbar zu tragen und gilt vielfach ein Fotografier- und Handyverbot. Damit kommen sie den Empfehlungen des Bayer. Landesamts für Verfassungsschutz nach.[131] Dennoch ist trotz angemessener Schutzmaßnahmen die Notwendigkeit jeder Betriebsbesichtigung kritisch zu überprüfen unter Berücksichtigung der jeweiligen Werksteile und Besucher.[132] Freilich ist es gerade angesichts des Auseinanderfallens des Umgangs mit Besuchern einerseits und Mitarbeiter und Praktikanten andererseits fraglich, ob Angreifer tatsächlich als Besucher firmieren und nicht eher als Praktikanten, Diplomanden etc. versuchen werden, Zugang zu Unternehmensgeheimnissen zu gewinnen.

IT-Sicherheit ist mittlerweile zentraler Bestandteil jeden Know-how-Schutz-Konzepts, Dokumente und Informationen in Unternehmen heute überwiegend elektronisch vorliegen. Spionageangriffe erfolgen daher häufig aus der Ferne auf die IT-Systeme dieser Unternehmen. Werden know-how-kritische Daten im IT-System gespeichert, ist ein umfangreiches Sicherheitskonzept zum Schutz des IT-Systems unverzichtbar. Der Schutz der unternehmenseigenen IT-Systeme scheint überwiegend gut und sicher organisiert. Es werden individuelle Zugangsberechtigungen für Mitarbeiter hinsichtlich ihrer Tätigkeit vergeben und von der IT-Abteilung eingerichtet. Angemessener Passwortschutz, aktuell gehaltene Virenschutzprogramme und Firewalls sind vorhanden. In einigen Unternehmen werden auch weitergehende Maßnahmen eingesetzt, wie z. B. die Verschlüsselung des E-Mailverkehrs oder Kopiersperren gegen heimliche Datentransfers auf Speichermedien, wie z. B. USB-Sticks oder das Brennen von CDs. Vielfach wird auch die private Nutzung des Internets untersagt und zum privaten Surfen in

---

[130] *Bayerisches Landesamt für Verfassungsschutz* (http://www.wirtschaftsschutz-bayern.de/App.aspx?EditionViewID=3a5ebacf-5178-4f28-b47e-161d8d5d9fd5) (Stand: 29.01.2011).
[131] *Bayerisches Landesamt für Verfassungsschutz* (http://www.wirtschaftsschutz-bayern.de/App.aspx?EditionViewID=3a5ebacf-5178-4f28-b47e-161d8d5d9fd5) (Stand: 29.01.2011).
[132] *Pisani,* Strategien beim Know-how-Schutz, Medizinprodukte Journal 2009 Nr. 4, 262.

den Pausen ein Rechner zur Verfügung gestellt, der nicht ins Unternehmensnetz integriert ist.

Manche Unternehmen kennzeichnen geheim zu haltende Dokumente nicht, sondern verbieten Vertraulichkeitskennzeichnungen sogar, um Angreifern keine Relevanzhinweise zu geben. Auch dies kann ein guter Weg sein, schon weil er zeigt, dass zum Umgang mit kritischem Know-how Überlegungen angestellt werden. Der Umgang mit vertraulichen Dokumenten umfasst auch deren Entsorgung. Ob die Mehrzahl der KMU zwischen schutzwürdigen Papierdokumenten und Restmüll unterscheidet, erscheint fraglich. Sicherheitslücken in diesem Bereich können leicht behoben werden durch die Entsorgung vertraulicher Dokumente durch Vernichtung. Das gleiche gilt für elektronische Dokumente. Nicht mehr benötigten Dateien auf Datenträgern, wie z. B. Festplatten, Laufwerken sollten gezielt und regelmäßig gelöscht werden,[133] insbesondere vor der Entsorgung, Reparatur oder Weitergabe von IT-Geräten (z. B. Computer, Handys und sogar Drucker, Scanner oder Kopierer). Dazu ist häufig professionelle Hilfe erforderlich.[134]

6.4.2 Maßnahmen gegen die unlautere Verschaffung von geschütztem Know-how?

Industriespionage ist nach § 17 Abs. 2 Nr. 1 UWG strafbar. Diese Vorschrift erfasst schon Verhaltensweisen, die noch vor der Mitteilung der Betriebsgeheimnisse liegen, etwa die unbefugte Verschaffung oder Sicherung von Unternehmensgeheimnissen unter Anwendung technischer Mittel, durch Herstellung einer verkörperten Wiedergabe oder durch Wegnahme einer Sache (Speichermediums!), in der das Geheimnis verkörpert ist.[135]

Dieser gesetzliche Know-how-Schutz ist keine beliebige Maßnahme des Strafgesetzgebers, sondern rechtfertigt sich volkswirtschaftlich. Ohne diesen Schutz würden Konkurrenzausspähungen intensiviert, was zur Erhöhung betrieblicher Sicherheitsmaßnahmen führen würde, weil „Interessenten“ und Inhaber immer mehr Aufwand treiben würde, einerseits die Zugangsbarrieren zum Know-how zu überwinden bzw. diese andererseits zu erhöhen. Die dadurch entstehenden Kosten (von Spionage und Spionageabwehr) müssten weitergereicht werden. Auch würde sich individueller Know-how-Schutz negativ auf den Informationsfluss und die Wissensbasis im Unternehmen aus-

---

[133] *Senze,* Schutz vor ungewolltem Abfluss von Know-how, S. 17 (http://www.luther-lawfirm.com/download_vortraege_de/252.pdf) (Stand: 29.01.2011).
[134] *Bayerisches Landesamt für Verfassungsschutz* (http://www.wirtschaftsschutz-bayern.de/App.aspx?EditionViewID=3a5ebacf-5178-4f28-b47e-161d8d5d9fd5) (Stand: 29.01.2011).
[135] *Loschelder*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 109f.

wirken, was in Ansätzen freilich auch heute schon gilt. Beides ginge letztendlich zu Lasten der Allgemeinheit.[136]

Gleichwohl ist der gesetzliche Know-how-Schutz kein Grund dafür, individuellen Know-how-Schutz zu vernachlässigen, denn § 17 UWG gilt nur für Geschäfts- und Betriebsgeheimnisse, was die Betätigung von Geheimhaltungswillen erfordert. Werden keine angemessenen Maßnahmen zum Schutz dieser Geheimnisse unternommen, greift der gesetzliche Know-how-Schutz nicht, weil der Schutzgegenstand dann nicht als Geschäfts- oder Betriebsgeheimnis gilt. Darüber hinaus ist Industriespionage häufig schwer nachweisbar. Auch darum muss jedes Unternehmen sein geheimes Know-how aktiv eigenverantwortlich schützen. Bei der Ausgestaltung dieses Know-how-Schutzes sind die einzelnen Maßnahmen an den Wert des zu schützenden Know-how anzupassen. Unverhältnismäßig teure Maßnahmen sind ebenso zu vermeiden wie Sicherheitslücken. *Know-how-Schutz ist daher definitionsgemäß Maßarbeit!*

6.4.3 Ganzheitliches Schutzkonzept

Wie schon zuvor beschrieben, ist dringend zu empfehlen, *unternehmensinternes Know-how in verschiedene Geheimhaltungskategorien zu klassifizieren*, um auf dieser Grundlage Zugangsberechtigungen zu erteilen und Vertraulichkeitsvereinbarungen für die einzelnen Mitarbeiter zu erstellen (s. *Kapitel 6.3).* Auch über die Berechtigung zum Umgang mit Dokumenten, Daten und Informationen, z. B. hinsichtlich der Aufbewahrung und Entsorgung sollten die Geheimhaltungskategorie entscheiden. Selbstredend muss diese Kategorisierung von Know-how regelmäßigen überprüft und erneuert werden. Dies kann im Rahmen periodischer Know-how-Audits geschehen, die Teil eines umfassenden IP-Controlling sein sollten.[137]

Ein systematischer und effektiver Know-how-Schutz erfolgt durch ein umfassendes Schutzkonzept auf Basis des klassifizierten Know-hows. Es besteht aus einer Vielzahl von Maßnahmen, die von den KMU bereits eingesetzt werden. Teilweise sind Sicherheitslücken wie zuvor dargestellt durch ergänzende Maßnahmen zu schließen.

6.4.4 Dienstreisen

Nicht thematisiert in unseren Gesprächen wurde der Know-how-Schutz auf Dienstreisen. Er soll hier dennoch nicht unerwähnt bleiben, da er Bestandteil eines umfassenden Know-how-Schutz-Programms ist. Auf Dienstreisen besteht ein erhöhtes Risiko des Know-how-Verlusts, wenn in der Öffentlichkeit am Laptop gearbeitet oder telefo-

---

[136] *Ann / Kalbfus,* Geheimnisse sind schützenswert, FAZ v. 15.06.2009, S. 12.
[137] *Pisani,* Strategien beim Know-how-Schutz, Medizinprodukte Journal 2009 Nr. 4, 262.

niert wird. Das bedeutet, dass besonders darauf geachtet werden muss, ob eventuelle Mitleser oder Mithörer in der Nähe sind.

Bei Reiseziel in problematische Gebiete, kann die Gefahr des Datenverlusts minimiert werden, indem auf die Mitnahme des eigenen Laptops mit sensiblen Daten verzichtet wird.[138] Verwendet werden können spezielle „Reise-Notebooks“, die keine know-how-sensiblen Daten enthalten. Schützenswerte Daten sind sicherer auf einen verschlüsselten USB-Stick aufgehoben.[139] Bezüglich Reisen nach China warnt der bayerische Verfassungsschutz vor der staatlichen Verschlüsselung der W-LAN Netze. Auffälligen Nutzern drohe eine Überwachung durch die chinesischen Geheimdienste. Durch eine vollständige Internetrestriktion mache man sich aber genauso verdächtig.[140]

6.4.5 Audit

Regelmäßige Auditierungen des Know-how-Schutz-Programms können dazu beitragen, dessen Effektivität zum Geheimnisschutz zu verbessern, zur Vermeidung von „Betriebsblindheit“ auch durch externe Sachverständige.[141]

---

[138] *Ann*, in: Ann / Loschelder / Grosch Praxishandbuch Know-how-Schutz, Kap. 1 Rn. 35f.
[139] *Bayerisches Landesamt für Verfassungsschutz* (http://www.wirtschaftsschutz-bayern.de/App.aspx?EditionViewID=3a5ebacf-5178-4f28-b47e-161d8d5d9fd5) (Stand: 29.01.2011).
[140] *Bayerisches Landesamt für Verfassungsschutz (Hrsg.)*, Nutzung von Laptops in der VR China (http://www.wirtschaftsschutz-bayern.de/content/al_library/_ext_files/Verschl%FCsselung%20China.pdf) (Stand: 29.01.2011).
[141] *Pisani,* Strategien beim Know-how-Schutz, Medizinprodukte Journal 2009 Nr. 4, 263.

Abbildung 12
Checkliste – Industriespionage

Checkliste – Industriespionage

- Relevantes Know-how systematisch erfassen und know-how-kritische Unternehmensbereiche definieren
- Physischen Zutrittsschutz für Betriebsgelände sowie know-how-kritische Unternehmensbereiche schaffen
- Tragen von Mitarbeiter- und Besucherausweisen anordnen
- Fotografierverbot und Handyverbot anordnen und durchsetzen
- Schutzbedürftige Dokumente durch Vernichtung entsorgen
- Schutzbedürftige Daten regelmäßig von Datenträgern löschen
- Schutzbedürftige Daten aus Speichern alter oder defekter IT-Geräte entfernen
- IT-Sicherheitskonzept umsetzen (Passwortschutz, Virenschutz, Firewall, Verschlüsselung, Gebrauch fremder Endgeräte)
- auf Dienstreisen spezielle „Reise-Notebooks“ sowie verschlüsselte USB-Sticks verwenden
- Know-how-Schutz-Programm regelmäßig auditieren, ggf. durch zuverlässige(!) externe Sachverständige

Bild: Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum

7 Handlungsempfehlungen

Notwendigkeit eines ganzheitlichen Schutzkonzepts

7.1 Zusammenfassung

Die von uns geführten Gespräche mit Verbandsunternehmen zeigen, dass der *Technologieschutz im Mittelstand der bayerischen M+E Industrie verschiedene, teils gravierende Schwächen aufweist.* Vielfach fehlt eine Strategie, was wie geschützt werden soll. Auch fehlen Strukturen und Prozesse bei Entscheidungsfindung. Dies weckt Zweifel, ob in jedem Fall der richtige Schutzansatz gewählt wird und ob alternative Schutzmöglichkeiten bei dieser Wahl in Betracht gezogen werden. Viel zu wenig beachtet wird die Notwendigkeit, auch einmal erteilte Schutzrechte systematisch einem begleitenden IP-Controlling zu unterziehen mit dem Ziel, nicht mehr benötigte Schutzrechte fallenzulassen und damit Jahresgebühren und vor allem Monitoringaufwand einzusparen.

Auffallend im *Patentwesen ist das Fehlen definierter Prozesse für ein Controlling des Patentportfolios*. Das birgt die Gefahr, dass ungenutzte Schutzrechte die eingangs erwähnten Kosten verursachen. Doch bereits bei der Entscheidung über Patentanmeldungen scheint teils wenig strategisch vorgegangen zu werden. Dabei sollten gerade KMU sehr kritisch prüfen, ob Kosten im Hinblick auf die Länderauswahl (geographischer Schutzbereich) gesenkt werden können und ob mit Patenten auf die Ergebnisse eigener F+E möglicherweise auch andere Ziele erreicht werden können als deren exklusive Nutzung in eigenen Produkten.

Deutliche *Sicherheitslücken bestehen beim betriebsinternen Know-how-Schutz*. Offenbar unterschätzen insbesondere KMU die Gefahr der Industriespionage sowie des Geheimnisverrats durch Kunden oder eigene Mitarbeiter. Der Know-how-Schutz unserer Gesprächspartner erfolgte überwiegend unsystematisch, was sich beispielsweise in Unklarheiten darüber äußerte, was im Unternehmen als geheim zu haltendes Know-how zu betrachten war. Vielfach glich der Schutz betriebsinternen Know-hows weniger einem Konzept als einzelnen Schutzmaßnahmen, die nur wenig aufeinander abgestimmt waren. Obwohl vielen Unternehmen die Bedeutung ihres Know-how, z. B. in der Fertigung oder Materialbehandlung, in Form von langjähriger Erfahrung bewusst ist, wird der Schutz dieses Wettbewerbsvorteils oftmals nur halbherzig durchgeführt. Das spricht dafür, dass KMU die Gefahrensituation des Know-how-Verlusts nicht wahrnehmen und für die Risiken stärker sensibilisiert werden müssen.

7.2 Geheimhaltung vs. Patentschutz

Die Geheimhaltung kritischer Information ist kostengünstiger als deren Patentschutz. Während Patentschutz hohe Anwalts- und Übersetzungskosten sowie interne Kosten und Amtsgebühren sowohl bei der Anmeldung als auch bei der Aufrechterhaltung mit sich bringt, verursacht auch ein ausgebauter Know-how-Schutz deutlich geringere Zusatzkosten. Unternehmen sollten darum vor jeder Patentanmeldung prüfen, ob die zur Anmeldung heran stehende Technologie durch Geheimhaltung bei gleicher Schlagkraft kosteneffizienter geschützt werden kann als durch Patentierung und ob Geheimhaltung darum eine Alternative zum Patentschutz darstellt.

Freilich kann die Auswahl zwischen beiden Schutzarten durch den Schutzgegenstand eingeschränkt sein. So eignet sich Know-how-Schutz nicht für Technologien, die durch Reverse Engineering zugänglich sind. Dann fehlt die wesentliche Bedingung der Geheimschutzfähigkeit. Andererseits ist auch Patentschutz nur beschränkt einsetzbar, denn patentiert werden nur technische Erfindungen, die neu, erfinderisch und gewerblich anwendbar sind. Insbesondere sollte von einer Patentanmeldung abgesehen werden, wenn begründete Zweifel daran bestehen, dass das Patent auch erteilt wird, denn auch bei Nicht-Erteilung werden Anmeldung und Information offengelegt.

Auch die erwartete Technologielebensdauer sollte bei der Auswahl des Schutzansatzes berücksichtigt werden. Grundlagenerfindungen sollten auf Grund ihres Werts und ihrer Lebensdauer patentiert werden, denn dadurch werden alle darauf basierenden Anwendungen durch ein einziges Patent geschützt. Wird der wirtschaftliche Nutzen über die maximale Patentlaufzeit hinausgehen, sollten frühzeitig unterstützende Schutzmaßnahmen für die betroffenen Produkte ergriffen werden, z. B. komplementärer Markenschutz oder das Angebot produktbegleitender Dienstleistungen. Die Festigung von Absatzkanälen erschwert Wettbewerbern den Marktzutritt. Bei kurzen Technologielebenszyklen kann der Schutz des Erstanbieters (First Mover Advantage) hinreichend sein – selbst wenn die Technologie durch Reverse Engineering nachgeahmt werden kann.

Ratsam ist generell ein Mix verschiedener Schutzmaßansätze. Produkte hoher Komplexität können gleichzeitig durch Geheimhaltung und mehrere Schutzrechte geschützt werden. Neben Geheimhaltung und Patenten können auch Marken Exklusivität unterstützen. Software genießt (automatisch) Urheberrechtsschutz.

Aber nicht nur der Schutzgegenstand beeinflusst die Wahl der optimalen Schutzmethode. Auch Eigenschaften des Unternehmens selbst, wie z. B. die Größe, Strategie und Ziele des Unternehmens oder das Wettbewerbsumfeld sind entscheidend beim Technologieschutz.

Schutzrechte sind unverzichtbar, wenn Unternehmen gezwungen sind, Know-how zu teilen, z. B. in der Luftfahrtbranche, wo transparente Herstellungsprozesse gefordert werden. Hier können Verfahrenspatente ein Schutzansatz sein. Auch bei gemeinsa-

men Forschungsvorhaben, z. B. mit Kunden, kann ein Schutzrecht die sicherere Schutzmethode darstellen. Stets zu beachten ist jedoch, dass eine Patentanmeldung nur sinnvoll ist, wenn eine Schutzrechtsverletzung später auch nachgewiesen werden kann. Insbesondere bei Verfahren ist dies nicht immer der Fall. In manchen asiatischen Staaten bestehen Probleme bei der Schutzrechtsdurchsetzung (Enforcement). Nicht nur weil sich dies noch vor dem Auslaufen der 20-jährigen Schutzdauer ändern wird, sollte dort gleichwohl patentiert werden, wenn das Land, wie vielfach die VR China, als Fertigungsstandort oder Markt wichtig ist.

7.3 Patentstrategie

Kosteneffizienter Patentschutz setzt voraus, dass jedes Schutzrecht im Patentportfolio einen seinen Kosten angemessenen Nutzen erbringt, selbst wenn es zunächst nur strategischen Wert bietet, wie z. B. eine vielversprechende Option für die Zukunft. Über jede Patentanmeldung und –aufrechterhaltung muss unter Kosten-Nutzen-Aspekten mit Blick auf die Strategie des Unternehmens entschieden werden.

Bei der Länderauswahl ist darauf zu achten, ob Schlüsselmärkte und Fertigungsstandorte identifiziert werden können. Gelegentlich kann schon der Schutz eines zentralen Markts oder weniger Märkte ausreichen, um die Nachahmung einer Technologie für Konkurrenten nicht lohnend zu machen. Unter Berücksichtigung des Produktlebenszyklus' müssen bei der Länderauswahl gegebenenfalls auch Wachstumsmärkte einbezogen werden, die aktuell noch unbedeutend sind, aber für die Zukunft Potential bieten.

Gesteigert werden kann die Effizienz von Patentschutz, wenn dadurch zusätzliche Ziele neben der eigenen Technologieverwertung durch marktfähige Produkte verfolgt werden. Geprüft werden sollte, ob Lizenzierung möglich ist oder das Patent zu Marketingzwecken vor Verbrauchern und Kapitalgebern genutzt werden kann. Auch ein Einsatz zur Erzielung spezieller Wettbewerbsvorteile ohne die kommerzielle Verwertung der Technologie kann erwägenswert sein. So sollte überlegt werden, ob Verwirrungs- oder Sperrpatente geeignete Mittel zur Sicherung eigener Märkte und Aktivitäten sein können.

Ungenutzte Patente verursachen nur Kosten und sollten im Zuge eines systematischen IP-Controlling identifiziert und aufgegeben werden.

7.4 Know-how-Schutz

Nur systematischer Know-how-Schutz kann effektiv schützen. Einzelmaßnahmen sind für einen lückenlosen Schutz unzureichend. Erfolg versprechen nur ganzheitliche Schutzkonzepte aus maßgeschneiderten rechtlichen / vertraglichen, organisatorischen und technischen Maßnahmen. *Know-how-Schutz ist Maßarbeit!*

Grundlage jedes nachhaltigen Know-how-Schutzes ist die Definition von schützenswertem Know-how im Unternehmen sowie dessen Klassifizierung in verschiedene Sensibilitätsstufen.

7.4.1 Rechtliche Maßnahmen

Für Mitarbeiter, die im Rahmen ihrer Arbeitstätigkeit mit vertraulichem Know-how umgehen, sollten individuelle Geheimhaltungsvereinbarungen getroffen werden, die nicht nur Schutz anordnen, sondern auch genau erfassen, welche Informationen geheimschutzbedürftig sind.

Um nachvertraglichen Geheimschutz zu erzielen, können Wettbewerbsverbote eingesetzt werden. Diese sind jedoch nur wirksam bei Zahlung einer Karenzentschädigung (> 50 Prozent der zuletzt bezogenen und für eine Laufzeit von zwei Jahren). Wegen ihrer erheblichen Kosten sollten *Wettbewerbsverbote nur nach gründlicher Kosten-Nutzen-Analyse eingesetzt werden.*

Auch Geschäftspartnern, z. B. Kunden, sollte schutzbedürftiges Know-how stets nur nach Abschluss einer Geheimschutzvereinbarung mitgeteilt werden. Dabei sollten keine Ausnahmen gemacht werden, weil nur so eine als solche nach außen kommunizierbare „Policy“ etabliert werden kann. Sollte der Abschluss einer Geheimschutzvereinbarung (gegen Kunden) nicht durchsetzbar sein, kann der Verzicht auf ein Geschäft die bessere Alternative sein als das Risiko eines Know-how-Verlusts.

Die Gestaltung von Vertraulichkeitsvereinbarungen ist Sache des Fachanwalts.

7.4.2 Organisatorische Maßnahmen

Zugang zu schutzbedürftigen Unternehmensgeheimnissen sollte Mitarbeitern nur nach dem Prinzip *„Need-to-Know“* gewährt werden. Um Zugangsberechtigungen technisch umsetzen zu können, müssen know-how-kritische Bereiche definiert werden.

Sofern nach Unternehmensorganisation und -größe möglich, kann eine strategische Verteilung geheimen Know-hows den Geheimschutz verbessern. In keinem Fall sollten einzelne Mitarbeiter Kenntnis vom gesamten geheimen Know-how für die Herstellung eines Produkts besitzen, dessen Wegfall die Existenz des Unternehmens bedrohen würde. Die *Kompartimentierung von Know-how* senkt das Verlustrisiko im Zuge der unvermeidlichen Mitarbeiterfluktuation.

Zur Vorbeugung gegen Geheimnisverrat durch Mitarbeiter sollte in Mitarbeiterschulungen die Notwendigkeit von Know-how-Schutz und dessen Zusammenhang mit der Sicherung der Arbeitsplätze im Unternehmen („Ast, auf dem wir sitzen!“) vermittelt werden. Dies senkt das Risiko fahrlässigen Geheimnisverrats. Auch die Erhöhung der Mitarbeiterzufriedenheit steigert die Mitarbeiterloyalität. Zufriedene Mitarbeiter sollten deshalb auch aus Perspektive des Technologieschutzes Ziel jeder Geschäftsleitung sein,

weil dies sowohl Know-how-Verlust durch Mitarbeiterfluktuation entgegenwirkt als auch vorsätzlichem Verrat.

Der Umgang mit schutzbedürftigen Informationen und Dokumenten erfordert Richtlinien. Was schutzbedürftig ist, sollte jedem Mitarbeiter bekannt oder erkennbar sein, durch Einweisung oder durch Kennzeichnung. Besondere Aufmerksamkeit verdient die Entsorgung von Papierdokumenten und Datenträgern. Sensible Unternehmensdokumente sollten bei der Entsorgung vernichtet werden, z. B. durch Aktenvernichter. Schutzbedürftige Daten müssen von Datenträgern alter oder defekter Geräte professionell gelöscht werden, denn es besteht gerade bei Technologieführern das nicht unerhebliche Risiko, dass aussortierte Datenträger gezielt nach sensiblen Daten durchsucht werden. Schließlich empfiehlt sich, das offene Tragen von *Mitarbeiter- und Besucherausweise* anzuordnen und das Arbeitsgebiet auf Personen zu prüfen, die das Betriebsgelände auffallend häufig abends oder an Wochenenden betreten. Ein allgemeines *Fotografierverbot* in know-how-kritischen Bereichen ist selbstverständlich, wird aber weitgehend bereits praktiziert.

7.4.3 Technische Maßnahmen

Technische Maßnahmen sollen vor allem die Wirksamkeit organisatorischer Maßnahmen gewährleisten. Sowohl im IT-System als auch auf dem Unternehmensgelände sollten know-how-kritische Bereiche nur für Personen zugänglich sein, denen eine entsprechende Berechtigung zuerkannt wurde.

Die Verschlusssicherheit know-how-kritischer Bereiche und Dokumente sollte durch technische Sicherungen wie z. B. Zahlencodes oder sonstige Schlösser gewährleistet werden. So kann verhindert werden, dass unberechtigte Personen Zugriff auf geschütztes Know-how haben.

IT-Schutz ist ein komplexer Bereich des Know-how-Schutzes. Es ist empfehlenswert Richtlinien zur IT-Sicherheit in einer *IT-Policy* zusammenzufassen. Diese beinhaltet u. a.:

- Effektiven Passwortschutz,
- Schutz vor Viren und Hackerangriffen,
- Zugangsberechtigungskonzepte,
- Regelungen zur Benutzung unternehmensfremder IT-Geräte im Unternehmensnetzwerk und
- Sicherheit bei der Internetnutzung (z. B. Datenverschlüsselung).

Der Schutz von IT-Systemen bedarf fachkundiger Beratung!

Für Dienstreisen empfehlenswert ist die Mitnahme sog. „Reise-Notebooks“, die keine sensiblen Unternehmensdaten enthalten. Als Datenträger sind verschlüsselte USB-Sticks geeignet. Dadurch kann der Gefahr des Know-how-Verlusts, z. B. durch Diebstahl, außerhalb des Unternehmens, vorgebeugt werden. Namentlich bei Reisen in

kritische Staaten wie China ist größte Vorsicht geboten. Grenzübertritte erfolgen nur an definierten Stellen und meist in Zeiträumen, die in Visaanträgen offengelegt wurden. Zudem lassen sich beim Grenzübertritt Reisende und Gepäck ohne weiteres trennen. Dass IT-Geräte ausländischer Besucher durch Nachrichtendienste systematisch ausspioniert werden, ist bekannt.

7.5 Auditierung

Betriebsinterne Know-how-Schutz-Programme müssen regelmäßig überprüft und fortentwickelt werden. Empfehlenswert ist die Durchführung von Audits, ggf. durch (sorgfältig ausgewählte!) externe Sachverständige.

Autoren

Christoph Ann
Univ.-Prof. Dr. LL.M (Duke Univ.)
Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum
Technische Universität München
Munich Intellectual Property Law Center (MIPLC)

Kelvin W. Willoughby
Univ. Prof. Dr. Dr. LL.M. (MIPLC)
Lehrstuhl für Entrepreneurship and Intellectual Property
Direktor das MBA-Programms der Curtin Graduate School of Business
Curtin University , Perth, Australien

Stephanie Bergmann
Dipl.-Ing., MBA
Lehrstuhl für Wirtschaftsrecht und Geistiges Eigentum
Technische Universität München

Literaturverzeichnis

Accenture	Die Bedeutung der Generikaindustrie für die Gesundheitsversorgung in Deutschland (http://www.accenture.com/NR/rdonlyres/C55589E4-D171-42DE-8DD0-9ACABD5B3851/0/Generika_in_D_2005_Accenture.pdf) (Stand: 12.01.2011)
Addor / **Li-Treyer**	Vorsichtsmaßnahmen sind der effektivste Kopierschutz, io new management 5 / 2009, S. 12-14
Ann	Know-how – Stiefkind des Geistigen Eigentums?, GRUR 2007, 39-43
Ann	Produktpiraterie – Bloße Verletzung individueller Rechte oder Bedrohung des Systems gewerblicher Schutzrechte insgesamt?, S. 1–12, in Gewerbliche Schutzrechte und ihre Durchsetzung, Festschrift für Tilman Schilling zum 70. Geburtstag am 29.07.2007, Köln 2007
Ann / **Grüneis**	Herausforderung Produktpiraterie - Sind Patente heute noch sinnvoll oder stärken sie nur die Piraten?, Industrie Management 2008, S. 59-62
Ann	Verletzungsgerichtsbarkeit - zentral für jedes Patentsystem und doch häufig unterschätzt, GRUR 2009, 205-209 (gleichzeitig Festschrift für Klaus-Jürgen Melullis)
Ann / **Kalbfus**	Geheimnisse sind schützenswert, FAZ v. 15.06.2009, S. 12
Ann / **Kalbfus**	Gesetzlicher Schutz für geheimes Know-how – nur gerecht oder auch wirtschaftlich sinnvoll?, Iurratio 2009, 133-136
Ann / **Loschelder** / **Grosch (Hrsg.)**	Praxishandbuch Know-how-Schutz, Köln 2010
Ann / **Hauck** / **Maute**	Auskunftsanspruch und Geheimnisschutz im Verletzungsprozess, Köln 2011
Bayer. Landesamt für Verfassungsschutz	Nutzung von Laptops in der VR China (http://www.wirtschaftsschutz-bayern.de/content/al_library/_ext_files/Verschl%FCsselung%20China.pdf) (Stand: 29.01.2011)
Bayer. Landesamt für Verfassungsschutz	(http://www.wirtschaftsschutz-bayern.de/App.aspx?EditionViewID=3a5ebacf-5178-4f28-b47e-161d8d5d9fd5) (Stand: 29.01.2011)
Bundesamt für Verfassungs-schutz für die Verfassungs-schutzbehörden in Bund und Ländern (Hrsg.)	Wirtschaftsspionage – Risiko für Ihr Unternehmen (http://www.wirtschaftsschutz-bayern.de/content/al_library/_ext_files/broschuere_0608_wirtschaftsspionage.pdf) (Stand: 29.01.2011)
Corporate Trust	Studie: Industriespionage – Die Schäden durch Spionage in der deutschen Wirtschaft, 2007 (http://www.corporate-trust.de/pdf/STUDIE_191107.pdf) (Stand: 29.01.2011)

EPO, JPO, KIPO and USPTO	Four Office Statistics Report 2009 (http://www.trilateral.net/statistics/tsr/fosr2009/report.pdf) (Stand: 29.01.2011)
Gassmann / **Kausch** / **Enkel**	Einbeziehung des Kunden in die frühe Phase des Innovationsprozesses, Thexis 2005 Nr. 2, 9-12
Gassmann / **Kobe (Hrsg.)**	Management von Innovation und Risiko: Quantensprünge in der Entwicklung erfolgreich managen, 2. Aufl., Berlin, Heidelberg 2007
Gassmann / **Bader**	Patentmanagement: Innovationen erfolgreich nutzen und schützen, Berlin, Heidelberg, New York 2007
Harhoff / **Reitzig**	Strategien zur Gewinnmaximierung bei der Anmeldung von Patenten, (http://www.inno-tec.bwl.uni-muenchen.de/files/forschung/publikationen/harhoff/zfb1999.pdf) (Stand: 29.01.2011)
Henn	Defensive Publishing, Köln 2010
Holtbrügge / **Puck**	Geschäftserfolg in China – Strategien für den größten Markt der Welt, 2. Aufl., Berlin, Heidelberg 2008
Lay / **Jung Erceg (Hrsg.)**	Produktbegleitende Dienstleistungen: Konzepte und Beispiele erfolgreicher Strategieentwicklung, Berlin, Heidelberg 2002
Kraßer	Der Schutz des Know-how nach deutschem Recht, GRUR 1970, 587-597
Leonard / **Stiroh (Hrsg.)**	Economic Approaches To Intellectual Property Policy, Litigation, and Management, 2005
Michel	Management von Kooperationen im Bereich Forschung und Entwicklung, Konstanzer Managementschriften Band 7, 2009
Müller	Effektiver Know-how-Schutz durch Geheimhaltungsverträge, DZKF 1 / 2 2009, 69-76
Nack	Rechtsschutz in China möglich, in A&D week digitale Zeitung für industrielle Automation 09.11.2010 Ausgabe 22, S. 4 (http://www.aud24.net/pi/index.php?StoryID=388) (Stand: 29.01.2011)
Pisani	Strategien beim Know-how-Schutz, Medizinprodukte Journal 2009 Nr. 4, 261-264
Reichwald / **Piller**	Interaktive Wertschöpfung – Open Innovation, Individualisierung und neue Formen der Arbeitsteilung, 2. Aufl., Wiesbaden 2009
Reitzig	Politik der Zäune, Wirtschaftswoche, 29 / 2004 (http://www.wiwo.de/unternehmen-maerkte/politik-der-zaeune-352046/) (Stand: 29.01.2011)
Senze	Schutz vor ungewolltem Abfluss von Know-how, 2009 (http://www.luther-lawfirm.com/download_vortraege_de/252.pdf) (Stand: 29.01.2011)

Sicherheitsforum Baden-Württemberg (Hrsg.) SiFo-Studie 2009 / 2010 – Know-how-Schutz in Baden-Württemberg, 2010 (http://www.sicherheitsforum-bw.de/x_loads/SiFo-Studie.pdf) (Stand: 29.01.2011)

VDMA VDMA-Umfrage zur Produkt- und Markenpiraterie 2010 (http://www.pro-protect.de/1/fileadmin/downloads/VDMA%20Umfrage%20Produkt-%20und%20Markenpiraterie%202010.pdf) (Stand: 29.01.2011)

Wildemann Konzeptwettbewerb und Know-how-Schutz in der Automobil- und Zulieferindustrie, (http://www.industrielle-dienstleistungen.de/uploads/html/publikationen/aufsatz/files/weissenberger_Konzeptwettbewerb.pdf) (Stand: 21.01.2011)

Wildemann Produktion hat goldenen Boden - Selbermachen ist gesund (http://www.tcw.de/uploads/html/publikationen/aufsatz/files/Produktion_hat_goldenen_Boden.pdf) (Stand: 29.01.2011)

Wildemann bayme vbm Forschungsbericht, Produktionssysteme mit Zukunft am Standort Deutschland, 2010

Abbildungsverzeichnis

Ansprechpartner

Dirk Pollert
stv. Hauptgeschäftsführer

Telefon 089-551 78-314
Telefax 089-551 78-315
dirk.pollert@baymevbm.de

Dr. Georg Liedl
KME – Kompetenzzentrum Mittelstand GmbH

Telefon 089-54 84-21 40
Telefax 089-54 84-21 49
georg.liedl@kme-mittelstand.de

Impressum

Herausgeber:

bayme
Bayerischer Unternehmensverband
Metall und Elektro e. V.

vbm
Verband der Bayerischen Metall-
und Elektro-Industrie e. V.

Max-Joseph-Straße 5
80333 München

www.baymevbm.de

Verfasser:

Prof. Dr. jur. Christoph Ann LL. M.
Technische Universität München
Lehrstuhl für Wirtschaftsrecht und
Geistiges Eigentum

Arcisstraße 21
80333 München

www.jura.wi.tum.de