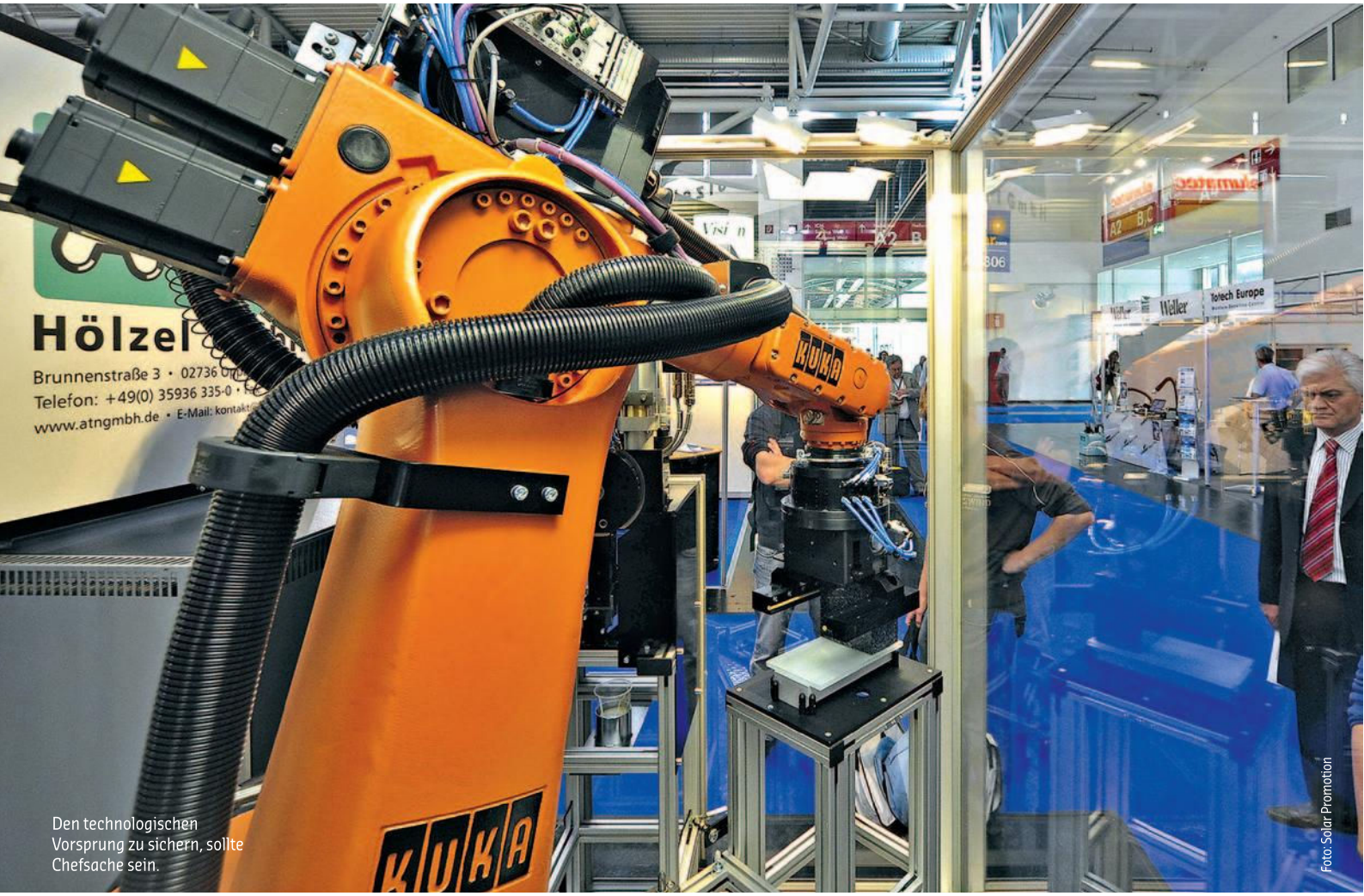

Den technologischen Vorsprung zu sichern, sollte Chefsache sein.

Foto: Solar Promotion

Das Kind am Brunnen

Die Solarbranche wird durch Innovationen getrieben. Sie vor der Konkurrenz zu schützen, ist für die Unternehmen daher essenziell.

Der effektive Schutz von Erfindungen und Wissen ist ein wichtiges Thema für deutsche Hersteller regenerativer Energietechnik, denn die Innovation in dieser jungen Industrie kommt weiterhin zum großen Teil aus Europa. Angesichts wachsender Konkurrenz können hier Unternehmen vor allem mit ihrem Vorsprung in der Technologie punkten. Doch oft wird ausgerechnet der Schutz geistigen Eigentums sträflich vernachlässigt. Die Gefahr besteht dabei nicht nur theoretisch: So warnt beispielsweise der Verfassungsschutz in seinem Jahresbericht von 2009 ausdrücklich vor internationaler Wirtschaftsspionage, etwa durch russische Nachrichtendienste. Auch dürfte die besondere Gefährdungslage bei Geschäften mit Partnern im Ausland und auf internationalen Messen zwischenzeitlich hinlänglich bekannt sein. Doch völlig unterschätzt wird die größte Gefahr: In etwa 80 Prozent der Fälle erfolgt der Geheimnisverrat durch (ehemalige) Mitarbeiter.

Vor diesem Hintergrund muss die deutsche Solarindustrie ihren Know-how-Schutz auf seine Wirksamkeit überprüfen, will sie ihre Marktposition auch in Zukunft halten und ausbauen. Für die meist mittelständischen Unternehmen ist dies eine besondere Herausforderung, weil es in ihnen nicht selten an der nötigen Sensibilität für dieses Thema fehlt. Der kollegiale Umgang der Unternehmen untereinander – ein Relikt gemeinsamer Gründerzeiten – verstellt allzu leicht den Blick für die wirtschaftlichen Konsequenzen, die aus dem Diebstahl von geistigem Eigentum drohen. Häufig fehlt es zudem an Patenten und anderen gewerblichen Schutzrechten, um das technische Know-how abzusichern.

Dabei geht es nicht nur darum, technische Erfindungen zu hüten, sondern auch Kundenbeziehungen oder Serviceleistungen sind gegen die Konkurrenz abzusichern. Vorrangiges Ziel muss es sein, Geheimnisverrat präventiv auszuschließen. In der Praxis hat es sich bewährt, betriebsintern Schutzprogramme zu etablieren, die im Außenverhältnis für externe Mitarbeiter, Zulieferer oder Partner durch individualisierte Vereinbarungen zur Geheimhaltung ergänzt werden. Entscheidend für die Wirksamkeit solcher Schutzstrategien ist das Zusammenspiel von technischem mit juristischem Sachverstand.

Was ist eigentlich Know-how?

Eine saubere Definition von Know-how gibt es nicht. Im deutschen Recht wird vielmehr insoweit synonym von Betriebs- und Geschäftsgeheimnissen gesprochen, ohne dass dabei eine klare gesetzliche Regelung bestünde. In der Rechtsprechung haben sich jedoch einige wichtige Auslegungskriterien herausgebildet. Ein juristisch relevantes Geheimnis liegt vor, wenn es sich um Tatsachen handelt, die

- im Zusammenhang mit einem wirtschaftlichen Geschäftsbetrieb stehen,
- nur einem begrenzten Personenkreis bekannt und damit nicht offenkundig sind,
- (subjektiv) nach dem erkennbaren Willen des Unternehmens und
- (objektiv) nach dessen berechtigten und schutzwürdigen wirtschaftlichen Interessen geheim gehalten werden sollen (insbesondere, wenn bei Offenbarung ein Schaden eintritt).

In der Praxis sind diese vier Gruppen von Unternehmensgeheimnissen besonders gefährdet: Konstruktionspläne, Fertigungsmethoden und Herstellungsverfahren; Kundenkarteien und Geschäftsunterlagen, insbesondere Kalkulationsunterlagen; Computerprogramme und EDV-Technik sowie Unterlagen über Serviceleistungen, insbesondere Wartungsarbeiten.

Know-how ist von gewerblichen Schutzrechten abzugrenzen. Schutzrechte gewähren dem Inhaber exklusive Rechte an der Nutzung und Verwertung einer Idee, einer Marke oder eines Produkts. Zum Schutz von technischem Wissen sind vor allem Patente geeignet. Sie begründen insbesondere Unterlassungsansprüche gegen unbefugte Verwender geschützter Techniken. Sie gewähren umfassenden Schutz vor Missbrauch, etwa durch unzulässiges Reverse Engineering. Aber nicht sämtliches Know-how kann durch Patente geschützt werden. So ist etwa Software als solche (bislang) patentrechtlich überhaupt nicht schutzfähig. Weiterhin kann es an der für die Patentierbarkeit erforderlichen Neuheit fehlen, etwa wenn Montagesysteme auf der Grundlage eingeführter Modelle fortlaufend weiterentwickelt werden.

Allerdings reichen Patente und sonstige gewerbliche Schutzrechte bei Weitem nicht aus, um Know-how umfassend zu schützen. Wirklich effektiver Geheimnisschutz setzt vielmehr voraus, dass Unternehmen intern entsprechende Programme etablieren und extern sensitive Vertragsbeziehungen durch Geheimhaltungsvereinbarungen ergänzen.

Das deutsche Recht sieht einen umfassenden Schutz von Know-how vor. Es erfasst sämtliche Tatsachen, die dem gewerblichen Rechtsschutz mangels Schutzfähigkeit nicht zugänglich sind, sowie dem Grunde nach schutzfähige Informationen, die jedoch nach dem Willen ihres Inhabers nicht durch gewerbliche Schutzrechte geschützt werden sollen. Der gesetzliche Geheimnisschutz erfolgt dabei im Wesentlichen durch das Strafrecht und das Zivilrecht.

Schadensersatz kommt zu spät

Die wichtigsten Normen des strafrechtlichen Geheimnisschutzes sind im Gesetz gegen den unlauteren Wettbewerb (UWG), im Strafgesetzbuch sowie im GmbH-Gesetz beziehungsweise Aktiengesetz festgelegt. Sie stellen den Geheimnisverrat, die Betriebsspionage und die Hehlerei von Geheimnissen unter Strafe. Zwar nimmt das Strafrecht in der Praxis allein eine untergeordnete Rolle ein, seine Regelungen sollten jedoch nicht unterschätzt werden. Denn zivilrechtliche Schadensersatzansprüche stützen sich häufig auf die Verletzung von Normen des UWG.

Die Bedeutung der strafrechtlichen Geheimhaltungspflichten ergibt sich damit aus ihren zivil- und arbeitsrechtlichen Folgen. Die gesetzliche Grundlage bieten das Delikts- und Wettbewerbsrecht. Haben die Parteien eine Vertraulichkeitsvereinbarung getroffen, bestehen bei ihrer Verletzung daneben (vertragliche) Unterlassungs- und Schadensersatzansprüche. Die Unternehmen sollten sich nicht ausschließlich auf den gesetzlichen Geheimnisschutz verlassen. Greift dieser doch erst,

Foto: Solar Promotion

Heutzutage sind die Besucher von Fachmessen mit Fotohandys, iPhones und schnellen Notebooks ausgerüstet. Blitzschnell gehen Produktneuheiten um die Welt. Deshalb müssen die Aussteller genau darauf achten, wie viel sie preisgeben.

Foto: H. Schwarzburger

Aufgeschraubt: Dieser in München ausgestellte Zentralwechselrichter lässt tief blicken. Allerdings sind die wirklich sensiblen Details unsichtbar: die Leistungselektronik im Innern.

wenn das Kind bereits in den Brunnen gefallen ist, also nach der missbräuchlichen Weitergabe von Informationen.

Effektiver Schutz setzt also weit vor dem Geheimnisverrat an. Dazu gehören ein betriebsinternes Schutzprogramm zur Prävention von Verrat, entsprechende Geheimhaltungsklauseln in jedem Arbeitsvertrag und Vertraulichkeitserklärungen mit Partnern, bevor sensible Daten ausgetauscht werden. Der Schutz von Know-how ist Chefsache. Und der beginnt damit, innerhalb des Unternehmens genau zu definieren, was schutzwürdig ist. Zunächst ist sensibles Wissen zu klassifizieren und zu dokumentieren. Dies ist ein fortlaufender Prozess, etwa durch periodische Audits. Je nach den Auswirkungen einer missbräuchlichen Weitergabe von Daten kann man eine Information klassifizieren als unternehmensvernichtend (streng geheim), schädigend (geheim), gefährdend (streng vertraulich) und beeinträchtigend (vertraulich). Diese Daten und ihre Klassifizierung gehören in den Safe des Chefs oder in den geschützten Kern des Computersystems.

Weiterhin ist zu klären, welche Mitarbeiter welche Informationen wirklich benötigen. Je größer der Personenkreis mit Zugang zu sensiblen Daten, desto schwieriger ist es, Verrat zu verhindern. Zugangsrechte sind genau zu prüfen. Es ist zudem eine weit verbreitete Unsitte, vertrauliche Kalkulationsgrundlagen oder Konstruktionszeichnungen in E-Mails zu versenden. Schnell landen diese Sendungen bei der Konkurrenz, einfach per Tastendruck.

Jede Menge Lecks

Auch der gesamte Außenauftritt des Unternehmens auf Messen oder Tagungen ist juristisch und technisch unter die Lupe zu nehmen. Im Vorfeld einer Messe müssen Unternehmen etwa bedenken: Was wird gezeigt, was bleibt unter Verschluss? Welches Gerät wird aufgeschraubt und präsentiert, welches nicht? Für Fachkonferenzen stellt sich die Frage: Welche Informationen werden im wissenschaftlichen Vortrag preisgegeben, welche nicht? Es genügt dabei nicht, auf schriftliche Unterlagen (Hand-outs) zu verzichten. Im Vortrag präsentierte Charts lassen sich problemlos mit dem Handy abfotografieren. Sie liegen auf dem Tisch der Konkurrenz, bevor der Referent seinen Vortrag beendet hat. Wer die technologische Innovation anführt, sollte sich generell in Zurückhaltung üben. Denn die vorschnelle Veröffentlichung auf einem Kongress oder im Internet kann unter Umständen dazu führen, dass die Patentbehörde einen Antrag auf Schutz ablehnt. Der Grund: Mit der Publikation ist die Erfindung nicht mehr neu und damit nicht mehr patentierbar.

Riskant: unzufriedene Mitarbeiter

Eingangs wurde gesagt, dass vier Fünftel aller Fälle von Geheimnisverrat auf (ehemalige) Mitarbeiter zurückgehen. Man kann Mitarbeiter allerdings nicht permanent überwachen und kontrollieren. Das ist aus Gründen des Arbeitnehmerdatenschutzes unzulässig und steht außerdem im Widerspruch zum Grundsatz der Verhältnismäßigkeit. Macht der Geheimnisschutz bestimmte Maßnahmen erforderlich, kann im Einzelfall die Einwilligung der betroffenen Mitarbeiter oder der Abschluss einer entsprechenden Betriebsvereinbarung erforderlich sein. Die Geheimhaltung sollte auch mit Zeitarbeitsfirmen und ihren Arbeitskräften abgesichert sein. Die hohe Fluktuation von Zeitarbeitern erhöht das Risiko, dass sensible Informationen nach draußen gelangen. Deshalb sollten besonders wichtige Informationen nur der Stammbelegschaft oder gar Führungskräften vorbehalten sein.

Freund, Feind oder Partner?

Zwar verpflichtet das arbeitsrechtliche Loyalitätsgebot alle Mitarbeiter, Stillschweigen über Betriebsinterna zu wahren. Aus Gründen der Rechtssicherheit sollte der Geheimnisschutz jedoch vertraglich konkretisiert werden. Die meisten Unternehmen haben dafür Klauseln in ihren Arbeitsverträgen. Was aber oft fehlt, sind Klauseln für den Fall, dass ein Mitarbeiter aus dem Unternehmen ausscheidet. Denn dann entfällt dessen Rücksichtnahmepflicht. Ob und inwieweit das genannte Loyalitätsgebot nach einer Entlassung oder einem Unternehmenswechsel weiter besteht, ist zwischen dem Bundesgerichtshof und dem Bundesarbeitsgericht jedoch strittig. Ein Arbeitgeber ist daher gut beraten, wenn er entsprechende Verschwiegenheitsverpflichtungen vereinbart, nötigenfalls unter Einschluss von Karenzentschädigungen.

Ebenso ist Sorgfalt beim Umgang mit externen Partnern angesagt: Dienstleistern, Zulieferern oder auch Kunden. Wer sein Know-how schützen will, muss auch mit seinen Partnern individuelle vertragliche Regelungen treffen. Am Anfang jeder (neuen) Geschäftsbeziehung steht daher der Abschluss einer entsprechenden Vertraulichkeitserklärung. In der Praxis sind die Geheimhaltungsregelungen häufig Gegenstand sonstiger Verträge, etwa von Kooperationsvereinbarungen oder Jointventure-Verträgen. Dasselbe gilt für Absichtserklärungen (Letter of Intent) im Vorfeld von Transaktionen oder Finanzierungen. Man sollte solche Vertraulichkeitsvereinbarungen niemals ungeprüft übernehmen. Das gilt sowohl für den Geber von Know-how wie für den Empfänger. Beide Seiten sollten die Vertragsmuster

kritisch prüfen, ob und inwieweit das Know-how geschützt wird, und wann der Verrat beginnt. Ein Unternehmen, das Know-how übernimmt, muss genau klären, welche Haftungsrisiken sich aus der Vertraulichkeitserklärung ergeben.

Unangenehme Überraschungen

Die Wirksamkeit von Vertraulichkeitsvereinbarungen hängt davon ab, ob die Parteien Regelungen getroffen haben, die ihr Schutzbedürfnis und die Bedeutung des betroffenen Know-how tatsächlich abbilden. Checklisten allein reichen nicht. So kommen in der Praxis häufig Vertraulichkeitsvereinbarungen zum Einsatz, in denen die Überschriften nicht unbedingt die tatsächlichen Regelungsinhalte spiegeln. Auf diese Weise wird den Vertragspartnern ein Schutzniveau suggeriert, das gar nicht gegeben ist. Im Konfliktfall kommt das zu unangenehmen Überraschungen. Gleichzeitig ist es sinnvoll, in einer musterhaften Vertraulichkeitserklärung unternehmensinterne Standards als Prüfungsgrundlage festzulegen. Ein solches Muster sollte mit einem erfahrenen Juristen erstellt und als Anfang eines fortlaufenden Lernprozesses betrachtet werden. Eine ordentliche Vertraulichkeitserklärung regelt insbesondere folgende Punkte:

- Definition des geschützten Know-how,
- erfasster Personenkreis,
- sachliche und personelle Ausnahmen vom Know-how-Schutz,
- Verpflichtung zum Schutze im Einzelnen,
- Zweckbestimmung für die Nutzung des überlassenen Know-how,
- Folgen einer Vertragsverletzung,
- Vertragsstrafe,
- Pflichten bei Vertragsbeendigung,
- Abwerbeverbot von Mitarbeitern,
- Gerichtsstand oder Schiedsklausel.

Häufig ist es in der Praxis erforderlich, die vertraulichen Informationen weiteren Personen zur Verfügung zu stellen, seien es externe Berater (etwa im Rahmen einer Due Diligence), seien es finanzierende Banken oder freie Mitarbeiter. Dann ist die unerlaubte Weitergabe der Daten zu beschränken, beispielsweise durch das Erfordernis einer expliziten Einwilligung.

Aufgrund anderer rechtlicher und kultureller Rahmenbedingungen ist der Schutz von Know-how im Auslandsgeschäft eine besondere Herausforderung. Wegen der territorialen Begrenztheit des Patentschutzes gewinnen Vereinbarungen oder Klauseln zur Vertraulichkeit (Non Disclosure Agreements, Confidentiality Clauses) an Bedeutung. Bei ihrem Entwurf sind grundsätzliche Fragen zu klären. Dazu gehören die Schutzfähigkeit bestimmter Daten im internationalen Rechtsverkehr, die Durchsetzbarkeit von Ersatzansprüchen im Verletzungsfall oder die kartellrechtliche Wirksamkeit. Die Begeisterung über einen Geschäftsabschluss im Ausland sollte dabei nicht blind dafür machen, dass aus dem ausländischen Geschäftspartner schnell ein Konkurrent werden kann. Hat er sich das Know-how erst einmal verschafft, ist der Weg frei zum Reverse Engineering.

Zusammenfassend kann man sagen: Der Schutz von Know-how wird immer wichtiger. Deutsche Unternehmen können im internationalen Wettbewerb nur dann bestehen, wenn sie ihren technologischen Vorsprung weiter ausbauen. Der Patentschutz allein reicht nicht aus. Vielmehr sind alle Betriebs- und Geschäftsgeheimnisse vor unbefugter Weitergabe zu schützen. Die Prävention durch betriebsinterne Schutzprogramme hat Vorrang. Ergänzt werden sie durch individuelle Vertraulichkeitserklärungen. ■

Rechtsanwalt Dr.
Christian Pisani
Müller & Pisani – Rechtsanwälte
www.muellerpisani.com

Foto: H. Schwarzburger

Die klare Botschaft ist oft wichtiger als Einblicke in die Technik.

Suntech bekämpft Piraten

Suntech verstärkt seinen Kampf gegen Plagiate. In den letzten Monaten wurde versucht, gefälschte Solarmodule nach Europa einzuführen. Sie werden unter sehr ähnlichem Markennamen vertrieben, garantieren aber weder die Leistung noch die Gewährleistung wie die Originalprodukte des chinesischen Herstellers. „Mithilfe einer professionellen Task Force arbeiten wir erfolgreich für den Schutz unserer Kunden und autorisierten Partner“, sagt Vedat Gürgeli, Vertriebschef bei Suntech in Europa. „Unsere Null-Toleranz-Strategie in Bezug auf Produktfälschungen hat sich bereits im Jahr 2010 als sehr erfolgreich erwiesen.“ Darüber hinaus nutzt Suntech die Dienste von Capip-EU, der europäischen „Koalition gegen Piraterie“. Ihr gehören 23 Anwaltskanzleien sowie Vertretungen in 29 europäischen Ländern und gerichtlichen Zuständigkeitsgebieten an. Die Organisation unterstützt Eigentümer von Marken und andere Betroffene mit Rechtsdienstleistungen und durch Spezialisten mit lokaler Expertise. Capip-EU arbeitet eng mit den nationalen Zollbehörden zusammen. Suntech geht gegen Produktfälscher gerichtlich vor. Bisher hat der weltgrößte Modulhersteller schon sechs Gerichtsverfahren in Europa und China gewonnen. Weitere Fälle befinden sich in laufenden Verfahren. Mehr als 40 Unternehmen erhielten offizielle Abmahnungen beziehungsweise Unterlassungserklärungen. Insgesamt wurden 28 Container mit gefälschter Ware von den europäischen Zollbehörden sichergestellt. (hs)