Chinesische Industriespionage wirksam bekämpfen

Viele deutsche Unternehmen unterschätzen die Möglichkeiten, in China erfolgreich gegen den Know-how-Diebstahl durch Marken- und Produktpiraten vorzugehen. Die Praxis zeigt, dass sich der Kampf gegen Industriespionage für die Hersteller lohnt.

HANS JOACHIM FUCHS

Die chinesische Marken- und Produktpiraterie im Maschinenbau hat zunehmend den Charakter der systematischen Industriespionage. Hinter den illegalen Nachbauten chinesischer Wettbewerber steckt oft kein Reverse Engineering, also die Rekonstruktion eines Originals durch Auseinanderbauen und Analysieren der Komponenten, sondern der gezielte Diebstahl des technischen Know-hows. Zum Einsatz kommen dabei Professoren, Mitarbeiter der eigenen Kunden und geschäftstüchtige Hacker. Oft verkaufen chinesische Kunden deutscher Maschinenbauer die mitgelieferten Dokumente an Wettbewerber weiter – trotz strenger Geheimhaltungsklauseln in den Verträgen.

Durch diesen permanenten Abfluss von Betriebsgeheimnissen entstehen globale Zweitmärkte mit billigen Maschinen, die auf die Margen der Originalhersteller drücken. So mancher deutsche Maschinenbauer sah sich schon gezwungen, die Preise seiner Originalprodukte aufgrund chinesischer Fälschungen um 25% zu senken. Es sind diese konkurrierenden Billigangebote, die den Absatz der deutschen Hersteller auf den globalen Exportmärkten untergraben. Das Problem ist also nicht nur der Umsatzverlust im laufenden Geschäftsjahr durch konkurrierende Fälschungen. Es ist auch der künftige Verlust von Marktanteilen durch illegale Nachbauten, der das eigene Geschäft systematisch schädigt.

Dr. Hans Joachim Fuchs ist geschäftsführender Gesellschafter von Chinabrand Consulting mit Büros in München, Boston und Shanghai, Tel. (0 89) 1 41 71 55, drhjfuchs@chinabrand.de

Bild: MM-Archiv

Oft kommt es zum gezielten Ausspionieren deutscher Unternehmen durch Hack-Aufträge chinesischer Konkurrenten. In vielen Fällen beschaffen Hacker aber auch auf eigene Faust Wissen, um es dann auf dem Markt zu verkaufen.

Diebstahl von Know-how durch verdeckte Ermittlungen nachweisen

Die Herausforderung für Originalhersteller ist es, den Diebstahl des Know-hows gerichtsfest zu beweisen. Dazu sind professionelle Ermittlungen und Beweissicherungen durch IP-Detektive erforderlich, die gerichtlich verwertbare Ergebnisse liefern und den Auftraggeber nicht täuschen. Wir kennen Fälle, in denen deutsche Auftraggeber von dubiosen chinesischen Ermittlern regelrecht hinters Licht geführt wurden. Ergebnisse waren konstruiert und mit den Plagiatoren wurde gemeinsame Sache gemacht. Bei der Bekämpfung der Industriespionage sind Professionalität, Zuverlässigkeit und Vertrauenswürdigkeit der eingeschalteten Dienstleister deshalb ein kritischer Erfolgsfaktor. Der Diebstahl von Know-how wird durch verdeckte Ermittlungen nachgewiesen. Es wird versucht, die gestohlenen Know-how-Träger wie Konstruktionszeichnungen, CD-ROM mit Datensätzen oder technologietragende Originalteile in den fälschenden Unternehmen zu entdecken. In manchen Fällen können sogar beim Plagiator eingeholte An-

Die Gesetzeslage in China

Wie das chinesisches Recht ausländische Produzenten schützt

Wer das geschützte Know-how (Betriebs-, Branchengeheimnisse) eines anderen stiehlt, macht sich in der Volksrepublik China auch dann strafbar, wenn er dabei keine Patente, Geschmacks- und Gebrauchsmuster oder industrielle Urheberrechte verletzt. Das Betriebsgeheimnis ist rechtlich geschützt. Industriespionage wird inzwischen konsequent verfolgt und hart bestraft, die Erfolgsaussichten für Prozesse sind bei sorgfältiger Vorbereitung und professioneller Durchführung gut. Die rechtliche Basis sind das Strafgesetz (§ 219), das Gesetz gegen unlauteren Wettbewerb (§§ 10, 25), das Vertragsgesetz (§ 43), das Arbeitsgesetz (§§ 23, 24) und die verwaltungsrechtlichen Bestimmungen für das Verbot von Verletzungshandlungen bei Geschäftsgeheimnissen.

Bei Industriespionage hat ein ausländisches Unternehmen die Möglichkeiten, den Angreifer verwaltungsrechtlich und strafrechtlich zu verfolgen sowie zivilrechtlich Schadensersatz zu verlangen. Es empfiehlt sich grundsätzlich der straf- und zivilrechtliche Weg, weil beim Verwaltungsverfahren das Risiko besteht, dass Geschäftsgeheimnisse bei Behörden dem lokalen Protektionismus und Patriotismus geopfert werden. Eine Voraussetzung für die erfolgreiche Bekämpfung der Industriespionage ist, dass das Know-how des Originalherstellers nachweisbar geschützt ist, einen Handelswert besitzt und öffentlich nicht zugänglich und bekannt ist. Bei einer Klage muss das bestohlene Unternehmen nicht nur beweisen, dass das geschützte Know-how vom Beklagten illegal beschafft wurde, es muss auch auf Behauptungen des Reverse Engineering seitens der Chinesen vorbereitet sein. In China ist es nicht strafbar, Know-how durch Reverse Engineering zu beschaffen. Diese Methode gilt in der Volksrepublik als eigene Forschung und Entwicklung. Der Fälscher muss jedoch beweisen, dass und wie er das Reverse Engineering durchgeführt hat.

gebote mit technischen Details Hinweise auf Know-how-Diebstahl geben. Gefälschte Maschinenteile werden über Test-Bestellungen angefordert, die dann einem staatlich zugelassenen Prüfunternehmen zur Begutachtung vorgelegt werden. Dieser Prüfer erstellt ein notarisiertes Gutachten. Auch eidesstattliche Erklärungen von Zeugen, die sich mit der Technik und den Prozessen auskennen, können vor Gericht als Beweis eingebracht werden.

Eine wirkungsvolle Methode ist, im Rahmen eines Tarngeschäftes als vermeintlicher Interessent des Know-hows aufzutreten und viel Geld für das gesuchte Wissen anzubieten. Verkaufsgespräche, technische Diskussionen und das Vorzeigen von Unterlagen und Teilen werden dabei verdeckt mitgeschnitten und gefilmt. Da solche Beweise in China beglaubigt sein müssen, ist auch ein chinesischer Notar anwesend, der unter der vorgetäuschten Identität des vermeintlichen Einkäufers agiert. Durch professionelle verdeckte Ermittlungen können Originalhersteller dem Gericht eine Fülle von Beweisen liefern: Fotos, Ton- und Filmaufnahmen, Muster, Zeugenaussagen, Beschreibungen des Know-hows und Gutachten – alles notariell beglaubigt. Das Gericht fordert unter Umständen weitere Beweise, beispielsweise weitere Gutachten einheimischer Experten. Sind die Beweise ausreichend, wird es zu einer Verurteilung des Fälschers kommen, wobei die sofortige Einstellung des Kopierens und in der Regel Schadensersatz verfügt wird.

Abnehmer vor riskanten Einkäufen und rechtlichen Konsequenzen warnen

Der Vorteil von Prozessen in China ist, dass der Originalhersteller schon während des laufenden Verfahrens im globalen Markt schlagkräftig kontern kann. So kann der Vertrieb des deutschen Maschinenbauers einen potenziellen Neukunden in Brasilien im Verkaufsgespräch warnend darauf hinweisen, dass der billige Wettbewerber in China vor Gericht steht und sich dort wegen Know-how-Diebstahls verantworten muss. Im Falle einer Verurteilung könnten dem brasilianischen Käufer der chinesischen Maschine massive Nachteile wie hohe Schadensersatzforderungen entstehen. Die Taktik des Vertriebs ist klar: Wer kauft schon ein Auto, das womöglich gestohlen ist? Bei laufenden Verfahren und gewonnenen Prozessen kann der internationale Handel abgemahnt werden. Breite Veröffentlichungen in der chinesischen Fachpresse warnen die gesamte Abnehmerbranche vor riskanten Einkäufen und rechtlichen Konsequenzen und der informierte Zoll der Volksrepublik kann auf Basis eines Urteils den Export gefälschter Maschinen ins Ausland verhindern.

Was chinesische Hackerangriffe betrifft, ist es falsch, anzunehmen, dass dahinter das Ministry of State Security (MSS) steckt. Hackerangriffe des chinesischen Geheimdienstes zielen in Deutschland in den meisten Fällen auf politische Einrichtungen, während private Unternehmen in der Regel von Wettbewerbern oder Computerspezialisten ausgeforscht werden. Oft kommt es zum Ausspionieren deutscher Unternehmen durch Hack-Aufträge chinesischer Konkurrenten oder Hacker beschaffen Wissen auf eigene Faust, um es dann zu verkaufen. In wenigen Fällen dringen ehrgeizige Technikfreaks in westliche IT-Systeme ein, um ihr Können zu beweisen.

Eine informationstechnische Rückverfolgung von Hackerattacken ist kaum möglich, weil die Angreifer keine technischen Spuren hinterlassen. Chinesische Hacker werden durch Profiling ermittelt. Das Zielunternehmen, die Art der ausspionierten Informationen und die Methoden weisen auf bestimmte Angreifer hin, die meist lokal konzentriert sind. Es kommt darauf an, Expertenwissen und Insiderkenntnisse über die chinesische Hackerszene zu nutzen. Man kennt verdächtige Auftraggeber, Gruppen und Personen. Informanten liefern weitere Erkenntnisse. Spezifische Industriecluster werden durchleuchtet und Ermittler treten als fiktive Einkäufer auf, um in der chinesischen Hackerszene nach einem spezifischen Know-how oder nach Experten mit bestimmten Fähigkeiten zu fragen. Die Antworten kommen meist sehr schnell. MM

MM-Serie

Strategien gegen Produktpiraterie

Diese und weitere Beiträge zum Thema Produktpiraterie finden Sie schon jetzt online unter www.maschinenmarkt.de/produktpiraterie