



## KEINE CHANCE DEN PRODUKTPIRATEN!

Innerbetriebliche Präventivmaßnahmen für Unternehmen gegen Fälschungen und Know-how-Abzug

---

Es gibt viele Möglichkeiten, sich vor Produktpiraterie zu schützen: juristische Vorgehensweisen, technische Lösungen, politische Einflussnahme. Darüber gibt es auch eine Fülle an Literatur. Unbekannt und oft unterschätzt hingegen sind die wirksamsten Maßnahmen: Die im eigenen Betrieb.

Will man größere Barrieren gegen die Fälscherindustrie errichten, muss man die betrieblichen Abläufe des Unternehmens und deren Schnittstellen zum Markt sicher machen. Dieser Ansatz erfordert die Zerlegung der gesamten Lieferkette des Unternehmens – vom Zulieferer bis zum Endkunden. Im Folgenden erhalten Sie einige wertvolle Tipps:

### Marktbeobachtung

- Markt beobachten: Plötzliche Rückgänge von Marktanteilen oder Umsätzen sowie die Häufung unberechtigter Reklamationen weisen auf Fälschungen hin.
- Zusammenarbeit mit Wettbewerbern und externen Dienstleistern prüfen, um gemeinsam gegen Produktpiraten vorzugehen.
- Eigene Mitarbeiter und Partner in der Distributionskette als Informationsquelle nutzen. Besonders Handelsvertreter und Einzelhändler im Ausland kennen sich im dortigen Markt aus.
- Messestände beobachten, im Internet recherchieren, Kataloge nach marktunüblichen Preisen durchsehen. Eventuell Testkäufe (ggfs. durch externen Dienstleister) machen.

## **Einkauf**

### Überprüfung der Lieferanten:

- Plausibilität prüfen: Preis, Vertriebsweg, Qualität. Vorsicht: Realistischer Preis kein Ausschlusskriterium!
- Verletzt die Lieferantenware Schutzrechte? Bei Ähnlichkeiten mit bekannten Markenprodukten z.B. überprüfen, ob tatsächlich IP-Verletzung vorliegt – v.a. Dingen Design ([www.dpma.org](http://www.dpma.org), [www.epo.org](http://www.epo.org)).
- Lieferanten auf Fälschungsaktivitäten und –potenziale hin überprüfen.
- „Paper Due Diligence“ beim Einkauf: Richtigkeit von Zertifizierungen, Qualitätsbescheinigungen etc. grundsätzlich bei der ausstellenden Institution überprüfen (SGS, TÜV, LGA etc.). Inhaltsangaben und Produktzusammensetzungen ggfs. mit unabhängigem Prüfinstitut gegenchecken.
- Unternehmen des Lieferanten besichtigen; Produktproben direkt aus der Produktion entnehmen und zu Hause in aller Ruhe prüfen.
- Auch Zulieferer von Verpackungsmaterial überprüfen, da viele Fälschungen in Originalverpackungen verkauft werden.
- Faustregel: Nur mit solchen Lieferanten zusammenarbeiten, die selber einen guten Ruf, Kunden und Investitionen zu verlieren haben. Eine Überprüfung des Geschäftspartners durch die deutschen Auslandshandelskammern ([www.ahk.de](http://www.ahk.de)) oder Wirtschaftsauskunfteien (z.B. Creditreform, Coface, Dun & Bradstreet) ist zu empfehlen.
- Beim Lieferanten auf die Gewährleistung eines Sicherheitsniveaus achten, das dem des eigenen Unternehmens entspricht.
- Neben betriebswirtschaftlicher Bewertung des Lieferanten (Bonität, Qualität etc.) auch weiche Faktoren bewerten:  
Bereitschaft zur gemeinsamen Planung und Problemlösung, Vertrauen, Offenheit, Kommunikationsfähigkeit, Informationsaustausch, Verhandlungsmacht, Wettbewerbskontakt, Ruf hinsichtlich Counterfeiting, Beziehungsgeflecht.
- Vergabe von Teilaufträgen an unterschiedliche externe Zulieferer, die sich nicht kennen und räumlich ausreichend voneinander entfernt sind.

### Vertragsgestaltung:

- Durch eine professionelle Vertragsgestaltung können Fälschungsrisiken zum Teil auf Lieferanten abgewälzt werden. Ein Lieferant kann z. B. dazu verpflichtet werden, ein Qualitätsmanagementsystem nach DIN EN ISO 9001:2008 einzuführen und zu unterhalten, das auch Fälschungen in Materialien, Teilen, Produktionsmitteln, Dienstleistungen, Software oder sonstigen Vorlieferungen von Unterlieferanten einbezieht. Der Auftraggeber kann auch vom Lieferanten einen Nachweis verlangen, dass er sich von der Echtheit aller ihm zugelieferten Produkte und Leistungen überzeugt hat und für Schäden aufkommt, die aus Fälschungen resultieren, die in seinem Unternehmen nicht erkannt wurden.
- Der Vertrag sollte den Lieferanten auch dazu verpflichten, die Rückverfolgbarkeit der von ihm gelieferten Produkte sicherzustellen.
- Grundsätzlich ist vom Lieferanten eine schriftliche Stellungnahme über die Ursachen der fälschungsbehafteten Lieferungen und Gegenmaßnahmen abzugeben.
- Zulieferer müssen vertraglich zusichern, dass sie die Produkte nicht an Dritte verkaufen.

### **Logistik**

- Lieferkette dicht machen, z.B. durch Tracking & Tracing (durch Einscannen eines Barcodes oder das Einlesen eines Chips wird überprüft, wo sich wann welche Ware befindet), durch Radio Frequency Identification (RFID) und durch Überprüfung der Routenführungen mittels Navigationssystemen, damit kein LKW in einem illegalen Lager Originalteile gegen Plagiate austauscht.
- Wareneingangskontrolle durch zuverlässige Prüfer durchführen. Achtung: Oft sind Originale und Plagiate in ein und derselben Lieferung vermischt!
- Speditionsverträge sollten immer Sondervorgaben für Logistikdienstleister enthalten, die z. B. vorsehen, dass der Spediteur keine Aushilfsfahrer beschäftigt, feste Routen einhält, keine Bedarfstouren durchführt oder Stichproben durch den Auftraggeber ermöglicht.
- Waren bereits endkundengerecht zusammenstellen, so dass fälschungskritisches Neu- und Umverpacken entfällt.
- Zur Nachverfolgung der Waren ist die Erfassung von Seriennummern ein bewährtes Mittel.

- Grenzbeschlagnahmeantrag stellen: Die Zentralstelle Gewerblicher Rechtsschutz (ZGR) mit bundesweiter und europaweiter Zuständigkeit kann Ware zurückhalten, wenn der Verdacht besteht, dass Ware das Recht geistigen Eigentums verletzt. Das Verfahren ist kostenlos, es muss nur ein Antrag vorliegen. Weitere Informationen unter [www.ipr.zoll.de](http://www.ipr.zoll.de).

## **Personal**

- Einen Ansprechpartner für den Schutz des geistigen Eigentums im Betrieb benennen.
- Fluktuation der Mitarbeiter eindämmen, denn mit jedem Mitarbeiter verlässt ein Stück Wissen das Haus. Besonders enttäuschte und unzufriedene Mitarbeiter, die möglicherweise zur Konkurrenz wechseln, stellen ein Sicherheitsrisiko dar.
- Mitarbeiter speziell schulen, wie sie Fälschungen erkennen; Anreize schaffen, Fälschungen aufzudecken; versicherungs-, straf- und personalrechtliche Konsequenzen erläutern.
- Heikles Wissen auf mehrere Mitarbeiter verteilen.
- In Arbeitsverträge mit Know-how-Trägern Geheimhaltungsklauseln aufnehmen. Dabei Begriff des zu schützenden Wissens (Geschäftsgeheimnis und die Geltungsdauer des Schutzes) so genau wie möglich definieren.
- Korruptionsbekämpfung, da Fälscher (besonders langjährige) Mitarbeiter bestechen, vertrauliche Informationen, Teile oder Werkzeuge zu beschaffen.

## **Forschung & Entwicklung**

- Einsatz von Aushilfen, Praktikanten und Doktoranden unbedingt erforderlich?
- Für F&E-Personal Arbeitsverträge mit Geheimhaltungsklauseln und Wettbewerbsverboten versehen.
- Bei Zusammenarbeit mit wissenschaftlichen Instituten und Universitäten darauf achten, dass es nicht über diese zum Know-how-Abfluss kommt (z.B. durch Gastwissenschaftler und bilaterale Kooperationen).
- F&E-Bereiche abspalten und als Insellösungen organisieren, in denen isolierte Teams nur Module entwickeln. Keines dieser Teams kennt alle Einzelheiten der Gesamtlösung.
- Schlüsselfunktionen in Komponenten bündeln, die nur im Stammhaus entwickelt, gefertigt und an die eigene Systemintegration geliefert werden.

- Aufspaltung von Entwicklungsaufgaben und Vergabe von Teilaufträgen an unterschiedliche externe Zulieferer, die sich nicht kennen und räumlich ausreichend voneinander entfernt sind.
- Integration der Module und Test des Gesamtsystems nur im Stammhaus vornehmen.
- Bei technischen Zeichnungen das Logo entfernen. Keine Zeichnungen herumschicken, vor allem nicht mit unverschlüsselten Mails.
- Nicht nur Datenbestände und Dokumente, sondern auch materielle Komponenten wie mechanische Teile oder Platinen verschlossen aufbewahren, z. B. in Tresoren. Das IT-System der F&E-Abteilung sollte von den Computersystemen des Unternehmens (Internet und Intranet) getrennt sein und als Insellösung betrieben werden, um ein Eindringen durch Unbefugte unmöglich zu machen.
- Vorsicht bei Zertifizierungen wie CCC in China oder GOST in Russland: Vorher zu prüfendes Produkt durch Schutzrechte schützen, da für die Zertifizierungen technische Details offenbart werden müssen! Zudem nicht jede Frage nach technischen Produktdetails, die das ureigene Firmen-Know-how betreffen, ungeprüft beantworten, sondern klären, ob sie zum Nachweis der Normeinhaltung nötig ist und gegebenenfalls mit der Zertifizierungsstelle darüber verhandeln; im Zweifel auf Markteintritt in Drittstaat verzichten!
- Übrigens: Ein Gerichtsprozess gegen Fälscher, in dem für die Beweisführung technische Details offengelegt werden müssen, kann größeren Schaden als Nutzen bringen.
- Mit der bewussten Verkomplizierung eines Produkts – z. B. durch aufwändige Details, eine komplexe Zusammensetzung, die Verwendung besonders hochwertiger Materialien oder durch hohen Anteil an Handarbeit – kann manchmal eine adäquate Nachahmung verhindert werden. Umgekehrt kann der Originalhersteller auch einfache Materialien verwenden und durch Massenproduktion niedrige Stückkosten realisieren. Die Nachahmung wird dadurch wirtschaftlich unattraktiv.

## **Produktion**

- Benennung von Personen, die für die einzelnen Teilprozesse für das Counterfeiting verantwortlich zeichnen.
- Rezepturen, Pläne oder Maschinenspezifikationen sind sicher aufzubewahren, z. B. in Tresoren.

- Um Schwund durch Diebstahl erkennen zu können, sollte die Zahl der beschafften Teile permanent mit der Zahl der gefertigten Produkte verglichen werden. Auch die Bestände des Lagers und des Ersatzteilbereichs sollten regelmäßig auf Schwund überprüft werden.
- Ausschuss kontrolliert entsorgen, unkenntlich machen oder vernichten! Denn viele Fälscher finden Kopiervorlagen auf dem Müll. Dies gilt auch für Verpackungen, Garantiekarten oder Bedienungsanleitungen.
- Stillstandszeiten der Fertigung ermitteln, protokollieren und auswerten, da sie Hinweise auf Fälschereingriffe geben.
- Generell: Sensible Bereiche eines Unternehmens durch bauliche, mechanische oder elektronische Absicherung (Zutrittskontrollen) unzugänglich machen
- Zusammenbau des Gesamtsystems in rechtssicherem Staat vornehmen.
- Informations- und Kommunikationstechnik:  
Computersysteme sind ein primäres Ziel von Wirtschaftsspionen. Doch so zahlreich die Instrumente des Angriffs sind, so vielfältig sind die Schutztechnologien, die Unternehmen beim Schutz ihrer I&K-Systeme zur Verfügung stehen. Siehe [www.ihk-muenchen.de](http://www.ihk-muenchen.de) > Innovation und Umwelt > E-Business und IuK Wirtschaft > IT-Sicherheit > Rechner und Computer Netzwerke absichern.

## **Outsourcing**

- Die Vergabe von Entwicklungsaufträgen an lokale Zulieferer, der Einsatz von Sicherheitsdiensten oder die Übertragung von EDV-Aufgaben an externe Fachleute sollten im Hinblick auf Piraterie überdacht werden. Grundsätzlich sollten Teilaufgaben an verschiedene Unternehmen vergeben werden, damit kein Zulieferer oder Dienstleister das Gesamtergebnis kennt und kopieren kann.
- Auch das Outsourcen von technischen Übersetzungen an lokale Übersetzer kann in sensiblen Ländern ein Sicherheitsrisiko sein.

## **Vertrieb**

- Aufklärungskampagnen gegenüber Kunden hinsichtlich Schäden und Gefahren, die aus Fälschungen resultieren.

- Sichtbare Sicherungskennzeichen gegenüber Kunden kommunizieren. Falls Produkte noch keine Sicherungskennzeichnungen haben, sollten sie unbedingt aufgebracht werden (Hologramme, Mehrfachcodes o.ä.).
- Kundenhotline einrichten.
- Messebeschlagnahmen in Deutschland/Europa durchführen.
- Zahl der Verkaufsstellen im Ausland übersichtlich halten, so dass Zuverlässigkeit und persönlicher, regelmäßiger Kontakt gewährleistet ist. Überprüfung durch Stichproben.
- Schulungen und Aufklärungsarbeit bei allen Vertriebsmitarbeitern als permanentes Instrument einführen.
- Stichprobenkontrollen bei Kunden durchführen.
- Bargeld oder teure Geschenke sind häufig ein wirksamer Schlüssel zum Öffnen der Vertriebsketten.
- Wirksamstes Mittel gegen die Korruption ist die Bildung von Vertriebsteams, in denen sich die Mitglieder gegenseitig kontrollieren. Teams machen es für den einzelnen Vertriebsmitarbeiter schwierig, Bestechungsgeld anzunehmen. Eine andere Maßnahme wäre, Vertriebsmitarbeiter zwischen verschiedenen Produktgruppen oder Kunden rotieren zu lassen, so dass keine allzu persönlichen Beziehungen entstehen.
- Transparentes und kontrollierbares Vertriebssystem aufbauen, in dem Verkaufsquoten, Routen und Besuchshäufigkeit festgelegt sind.
- Selektiver Vertrieb: Durch diese Auswahl wird für jeden Käufer offensichtlich, dass Produkte, die außerhalb dieses selektiven Vertriebssystems angeboten werden, Fälschungen sein müssen.
- In Händlerverträgen sollte grundsätzlich eine Vereinbarung zum Schutz des geistigen Eigentums enthalten sein. Diese kann den Absatzvermittler verpflichten, die Rechte des Herstellers am geistigen Eigentum zu schützen und sich nach besten Kräften für die Echtheit der gehandelten Ware einzusetzen. Die Vereinbarung kann z. B. genau festlegen,
  - wie der Händler seine Versorgungskette sicher zu machen und zu kontrollieren hat,
  - welche technischen Schutzmaßnahmen er installieren muss,
  - wann er bei Pirateriefällen Schadenersatz zu leisten hat,
  - wie genau der Händler seine Verkäufe zu dokumentieren hat,
  - welche Nachweise er über die Vertriebswege vorzulegen hat und
  - dass er Hinweise auf Plagiate sofort an den Hersteller weiterzuleiten hat.
- Der Weiterverkauf an Zwischenhändler sollte ausgeschlossen werden.

## **Auf Auslandsreisen**

Gerade im Ausland sind sowohl Konkurrenzspionage als auch „Angriffe“ dortiger Nachrichtendienste u.a. gegen das „geistige Eigentum“ von deutschen Firmen gerichtet.

- Visaanträge unbedingt gründlich und korrekt ausfüllen.
- Auf örtliche Agenturen verzichten und stattdessen Hotel selbst buchen.
- Aufgrund der vielfältigen Überwachungsmöglichkeiten auf Gesprächsdisziplin achten.
- Nur eigene Kommunikationsmittel benutzen.
- Eigene Dolmetscher nutzen und deren Telefonnummern nicht an Verhandlungspartner herausgeben.
- Sichere Verschlüsselungstechnik verwenden und diese anmelden.
- Keine persönlichen und firmeninternen Angaben offenlegen.
- Ungenutzte Schnittstellen an Kommunikations- und IT-Geräten deaktivieren.
- Bei Kontakten mit ausländischen Konsulaten möglichst wenig firmenspezifische Informationen angeben.
- Im Gastland die Landesgesetze unbedingt beachten und einhalten.
- Im Gastland bei längeren Aufenthalten ggf. wechselnde Hotels benutzen.
- Wichtige Informationen und Datenträger niemals im Hotelsafe aufbewahren. In den meisten Hotels der Gastländer sind die Codierungen der Hotelsafes dem Geheimdienst bekannt und zugänglich.
- Vorsicht bei Dienstleistungsunternehmen, die z. B. Installationen vornehmen. Es kann sich um Tarnfirmen handeln, die Abhörungsanlagen installieren.
- Bei allen Besprechungen mit sensiblen Inhalten sollten Mobiltelefone nicht zugelassen werden, da sie leicht als Aufzeichnungsgeräte umgebaut werden können.
- Ausländische Geschäftspartner nur gezielt nach Bayern einladen und darauf achten, dass auch nur die Personen nach Bayern kommen, die wirklich eingeladen wurden.

## **Quellen:**

CHINABRAND CONSULTING LTD. (Hrsg.)  
Piraten, Fälscher und Kopierer. Strategien und Instrumente zum Schutz geistigen Eigentums  
in der Volksrepublik China,  
Wiesbaden 2006

Blume, Andreas,  
Effiziente Bekämpfung der Produkt- und Markenpiraterie in und aus der VR China  
Vortrag am 21. April 2005 in der IHK München  
Produkt- und Markenpiraterie verhindern.

Präventionsstrategien der deutschen Wirtschaft.  
u.a. zum Download unter [www.ihk-muenchen.de](http://www.ihk-muenchen.de) > Recht und Fair Play > Markenrecht / Urheberrecht > Produkt- und Markenpiraterie > Strategiepapier dt. Wirtschaft gegen Produkt- und Markenpiraterie

Bayerisches Landesamt für Verfassungsschutz,  
Sicherheit für Unternehmen bei Auslandsgeschäften. Prävention durch Eigenschutz  
im Internet unter [www.verfassungsschutz.bayern.de](http://www.verfassungsschutz.bayern.de), abgerufen am 23.03.2007

Mit freundlicher Genehmigung der IHK für München und Oberbayern.