

## 8 Verbergen und Verhindern: Counterintelligence

*Wirtschafts- und Industriespionage zielen auf die illegale Beschaffung von Informationen über ein Unternehmen*

*Counterintelligence bezeichnet die Abwehr von legaler und illegaler Ausforschung*

*Wer die Grenzen zwischen Legalität und Illegalität verwischt, bringt die Branche in Misskredit*

Zunächst eine begriffliche Unterscheidung. Von Wirtschaftsspionage spricht man, wenn die Akteure fremde Nachrichtendienste sind, Industriespionage geht von anderen Unternehmen aus. Beide Begriffe beschreiben die illegale Beschaffung von Informationen über ein Unternehmen, bei der unter anderem Abhörtechniken und Software-Angriffe genutzt werden. Mit der Abwehr von Wirtschaftsspionage sind in Deutschland die Verfassungsschutzbehörden befasst, gegen Industriespionage müssen sich die Unternehmen selbst schützen. Der Verfassungsschutz in Bund und Ländern bietet Beratung zu diesem Thema an und verspricht Vertraulichkeit – was er aufgrund des Opportunitätsprinzips im Umgang mit strafrechtlich relevanten Dingen auch darf (im Gegensatz zum Legalitätsprinzip, dem die Polizei verpflichtet ist und das sie dazu zwingt, jede Vermutung in Richtung einer Straftat zu verfolgen).

Counterintelligence bezeichnet die Regeln und Prozesse, die dazu dienen sollen, das Unternehmen vor Ausforschung mit legalen und mit illegalen Mitteln zu schützen. Diese liegen aber jenseits der klassischen Sicherheitsmaßnahmen – und werden von vielen Unternehmen sträflich vernachlässigt.

Leider gibt es eine Reihe von Dienstleistern der Sicherheitsbranche, die in ihrer Terminologie die Unterscheidung zwischen legal und illegal völlig verwischen. So wird z.B. auf der Website eines international tätigen Sicherheitsunternehmens Corporate Intelligence mit Wirtschaftsspionage und Business Intelligence mit Betriebsspionage gleichgesetzt und behauptet, dass es sich kein Unternehmen leisten könne, ohne Betriebsspionage auszukommen und Spionage im Grunde genommen nicht illegal sein müsse.

Mit Texten wie diesem, die eine diffuse Gefahr beschwören, zur „Spionage“ mit legalen Mitteln aufrufen und dabei sämtliche Begriffe durcheinander bringen, wird vielleicht der ein oder andere Kunde gewonnen, aber im großen Maßstab Glaubwürdigkeit verspielt und das legitime und ethisch einwandfreie Sammeln und Auswerten von Informationen aus öffentlichen Quellen in Misskredit gebracht. Was letztlich dazu führt, dass sich „anständige Unternehmer“ mit diesem Gewerbe nicht beschäftigen möchten und sie dadurch erstens Erkenntnisgewinne über und Schutz vor ihren Wettbewerbern verlieren.

Wie wenig CI mit Spionage zu tun haben muss und wie effektiv Recherche und Analyse sein können, wenn sie konsequent durchgeführt werden, hat kurz vor Fertigstellung dieses Buches die Chicago Tribune bewiesen – nur dass sie sich kein normales Unternehmen vorgenommen hatte, sondern ein besonders geschütztes. Das Traditionsblatt hat nämlich allein durch die Nutzung legaler und offen zugänglicher Sekundärinformationen die Identität von 2.653 CIA-Agenten und die Standorte von zwei Dutzend geheimen Niederlassungen herausgefunden, darunter des

sagenumwobenen Ausbildungslagers „The Farm“ in Virginia. Hinzu kommen Flugzeuge und auch Scheinfirmen der „Firma“, die wohl nach ihrer Entdeckung ziemlich schnell geschlossen werden dürften.

Wenn es gelingt, solche Informationen...

- ... selbst über einen Geheimdienst herauszufinden, wie steht es dann erst mit der Sicherheit Ihrer Informationen?
- ... mit legalen Mitteln herauszufinden, was kann man dann erst mit illegalen Mitteln tun?
- ... über eine Organisation herauszufinden, die sich der Risiken sicher völlig bewusst ist, was passiert erst mit Unternehmen, die über das Thema gar nicht nachdenken?

## 8.1 Die Lücken des Sicherheitsparadigmas

Der Begriff „Betriebsgeheimnisse“ wird oft als Sammelbezeichnung für alle Informationen über Verfahren, Materialien und Geschäftsprozesse verwendet, die einem Unternehmen einen Wettbewerbsvorteil verschaffen. Das Problem des vorherrschenden Sicherheitsparadigmas ist der Mythos, diese Informationen würden am besten und ausreichend mit den klassischen Mitteln des Werksschutzes vor fremdem Zugriff bewahrt, Geheimnisse seien in erster Linie mithilfe von Sicherheitspersonal, Zäunen, Zutrittskontrollen, Firewalls und möglicherweise auch durch die regelmäßige Überprüfung auf Wanzen zu schützen. Wenn man berücksichtigt, wie selten Verschlüsselungsprogramme wie Pretty Good Privacy für den E-Mail-Verkehr verwendet werden und in welcher unglaublichen Menge Betriebsgeheimnisse sozusagen auf einer elektronischen Postkarte versandt werden, während man auf der anderen Seite in vielen Werken nur auf umständliche Weise zu einem Besucher ausweis kommt, muss man sich ob dieses Missverhältnisses schon wundern.

In diesem Kapitel soll es aber nicht in erster Linie um klassische Sicherheitsfragen und deren technische Lösung gehen – das können Sie an anderer Stelle ausführlicher und kompetenter nachlesen. Hier möchte ich dagegen Ihre Aufmerksamkeit auf die Bereiche lenken, in denen das Sicherheitsparadigma versagt, weil den größten Informationslecks eben nicht technisch, sondern nur pädagogisch beizukommen ist.

Das herrschende Sicherheitsparadigma ignoriert weitgehend die in diesem Buch beschriebenen Methoden der primären und sekundären Recherche sowie der Intelligence-Analyse. Spätestens mit dem Erscheinen des Buches „Die Kunst der Täuschung“ von Kevin Mitnick sollte jedoch jedem Sicherheitsverantwortlichen eines Unternehmens klar geworden sein, dass ohne eine Schulung aller Mitarbeiter in Bezug auf die Weitergabe jeglicher Informationen über das Unternehmen, seine Mitarbeiter, seine Produkte, seine Pläne und seine Geschäftsbeziehungen ein riesiges Loch in der Schutzhülle um eine Firma klafft, durch das ungehindert unternehmenskritische Informationen entweichen.

*„Betriebsgeheimnisse“  
verschaffen Wettbewerbs-  
vorteile*

*Den größten Informations-  
lecks ist nicht technisch,  
sondern nur pädagogisch  
beizukommen*

Eine Risikoanalyse wird sich zunächst um drei Bereiche kümmern: um das zu schützende Wissen, um die handelnden Akteure sowie um die Prozeduren und Ereignisse, bei denen Informationen „verloren“ gehen können.

## 8.2 Risikoanalyse, Teil eins: Wissen

Wie bereits mehrfach erwähnt, lassen sich 90 Prozent aller Informationen, die Sie über einen Wettbewerber haben möchten, aus öffentlichen Quellen gewinnen. Das gilt auch für Ihr eigenes Unternehmen. Daher ist es sinnvoll, in einem ersten Schritt zunächst eine Inventur des zu schützenden Wissens vorzunehmen. Als Basis können die Checklisten aus Kapitel 3 dienen – setzen Sie sich also Ihre Sonnenbrille auf (bitte keinen Schlapphut, wir wollen ja nicht jedes Klischee bestätigen), fühlen Sie sich wie ein Industriespion und gehen Sie diese Checklisten noch einmal durch. Das Ergebnis ließe sich dann in eine solche Liste eintragen:

*Zunächst eine Inventur des zu schützenden Wissens vornehmen*

Bereiche	Welche Informationen sind zu schützen?	Wer verfügt über diese Informationen?	Auf welchen Wegen werden Informationen nach draußen gegeben?
Strategien			
F&E			
Lieferanten			
Produktion			
Marketing			
Werbung			
PR			
Sales			
Distribution			
Kunden			
Dienstleister			
...			

*Das Wissen eines Unternehmens bewegt sich in unterschiedlichen Sphären*

Dabei werden Sie feststellen, dass sich das Wissen Ihres Unternehmens in unterschiedlichen Sphären bewegt, von den verschiedensten Menschen bewegt wird und vielfältigen Zwecken folgt. Das klingt vielleicht etwas abstrakt, hilft aber hier, ein wenig Abstand zum Alltagsbetrieb und einen Überblick zu gewinnen.

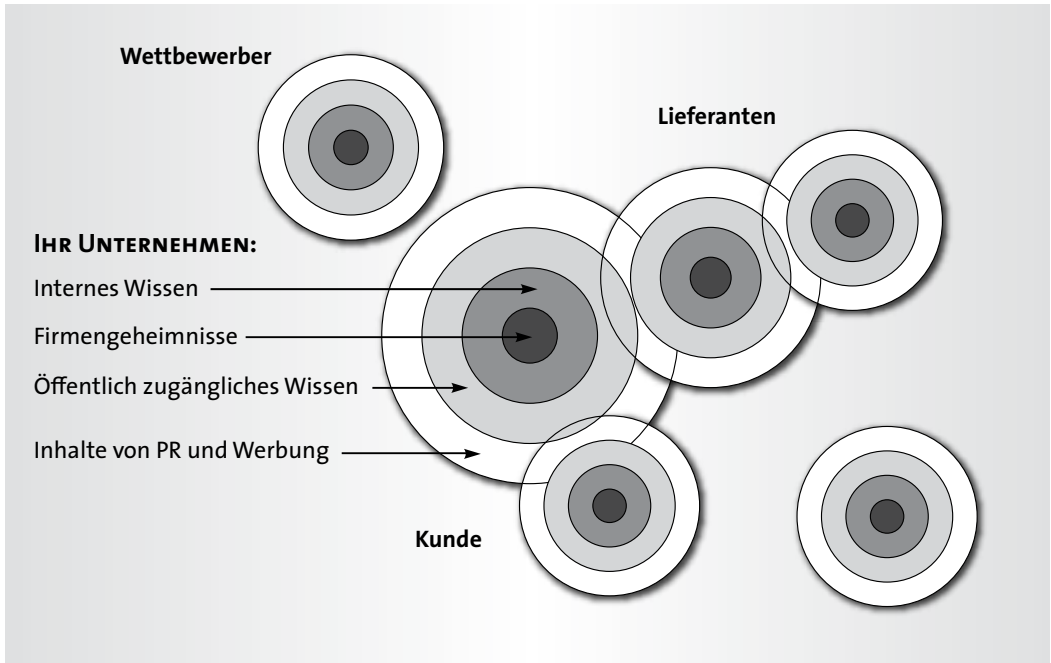


Abb. 8.1: Das Wissen eines Unternehmens bewegt sich in unterschiedlichen Sphären

Die Preisgabe von Informationen aus diesen unterschiedlichen Sphären hat jeweils verschiedene Konsequenzen:

Art der Information	Inhalt	Konsequenzen
<b>Betriebsgeheimnisse</b>	<ul style="list-style-type: none"> <li>Produktionsverfahren, Telefonverzeichnisse, Organisationscharts</li> <li>interne Finanzinformationen, Kundenlisten, Strategien, Entwicklungsergebnisse</li> <li>Kreditwürdigkeit, Warenbezugsquellen, Preislisten ...</li> </ul>	Finanzielle Verluste, Verlust von Wettbewerbsvorteilen, Verlust an Kreditwürdigkeit, Angreifbarkeit, Verlust von Kunden, Verlust von Lieferanten ...
<b>Internes Wissen</b>	Formelle und informelle Strukturen, Abläufe, Namen, Gewohnheiten, Bekanntschaften, Seilschaften, Loyalitäten ...	Kann als Hebel zur Erlangung von Betriebsgeheimnissen eingesetzt werden (durch Vortäuschen, Manipulation, Betrug ...)
<b>Öffentlich zugängliches Wissen</b>	Alle Inhalte, die über sekundäre und primäre Recherche zugänglich sind	Liefert das Rohmaterial für eine CI-Analyse und kann über diese zu ähnlichen Konsequenzen wie beim Verlust von Betriebsgeheimnissen führen
<b>Inhalte von PR, Werbung und vorgeschriebenen Investoreninformationen</b>	Alle Inhalte, die „vorsätzlich“ im Rahmen der Kommunikationspolitik veröffentlicht wurden	Liefert die Anlässe für sekundäre und primäre Recherche