

Industriespionage – Schutz sensibler Unternehmensdaten

Kurzfassung

Wirtschaftsspionage und Competitive Intelligence stellen für Unternehmen zunehmend eine existenzielle Gefahr dar. Produktideen, Forschungsergebnisse oder proprietäres Know-how müssen vor dem unbefugten Zugriff durch Dritte wirkungsvoll geschützt werden. Gegenstand dieser Abhandlung ist die Entwicklung einer Methode zum Schutz sensibler Unternehmensdaten.

Folgende Fragen sollen dabei geklärt werden: Wie erkennt man, dass ein ungewollter Informationsabfluss stattfindet? Wo befinden sich Schwachstellen und Sicherheitslücken in den Prozessen eines Unternehmens? Wie kann sich ein Unternehmen vor der Ausspähung durch Konkurrenten schützen?

Der adäquate Umgang mit Wirtschaftsspionage und Competitive Intelligence trägt mit wachsender Bedeutung zum Erfolg oder Misserfolg eines Unternehmens bei. Mit dem „CI Kompass“ wird eine Methode vorgestellt, welche die Kernfragen hierzu adressiert. Ein effektiver Schutz von Unternehmens-Know-how ist unabdingbar, um zukünftig in globalisierenden Märkten erfolgreich in Wettbewerb treten zu können.

Abstract

Industrial espionage and Competitive Intelligence increasingly pose a significant threat to organizations. Product ideas, R&D results or proprietary know-how must be protected from the unauthorized access through third-parties. The purpose of this paper is to develop a method to safeguard confidential company information.

The following key questions will be addressed: Which methods are available to detect unintentional data leakage? Where are weaknesses and security gaps in business processes? Which methods help to effectively protect a company from espionage?

Appropriately handling industrial espionage and Competitive Intelligence will increasingly make a major contribution towards the success or failure of a company. The “CI Compass” introduces a method which addresses the key questions hereunto. In the future, effectively safeguarding company know-how will be essential to compete successfully in globalizing markets.

Schlüsselbegriffe

Wirtschaftsspionage,
Competitive Intelligence

Key words

Industrial espionage,
Competitive Intelligence,
data protection



Prof. Dr.-Ing. Christian Seiter (MBA) verantwortet das Lehrgebiet International Marketing an der Hochschule Karlsruhe. Seine Forschungsschwerpunkte liegen in den Bereichen Competitive Intelligence, International Business und Strategie.

Kontakt: christian.seiter@hs-karlsruhe.de

Tobias Lippoth ist Absolvent des Studienganges International Management an der Hochschule Karlsruhe. In seiner Masterarbeit befasste sich Herr Lippoth mit der Abwehr von CI und Wirtschaftsspionage.



Einleitung

Die Konkurrenz schläft nicht.

In der heutigen vernetzten Welt ist dieses Sprichwort von großer Bedeutung, da Wirtschaftsspionage und Wettbewerbsbeobachtung für Unternehmen zunehmend problematisch und zu einer existenziellen Bedrohung werden können. Das Gefährdungspotenzial für Produktideen und Produktions-Know-how nimmt drastisch zu. Der bisher entstandene Schaden ist enorm. Eine Analyse von 400 technologieorientierten Unternehmen ergab, dass bereits zwei Drittel aller Unternehmen Opfer eines ungewollten Informationsabflusses waren.¹ Durch die aktuelle Wirtschaftskrise verstärkt sich das Problem der Spionage, da die Zeiten für Unternehmen härter geworden sind und Vorteile gegenüber der Konkurrenz von größerer Bedeutung werden als bisher.² Vor allem innovative deutsche Unternehmen, etwa aus der Wind- und Solarenergie-Branche, stehen im Fokus der Spione.³ Eine Schätzung des Innenministeriums ergab eine Schadenshöhe von 20 Milliarden Euro für das Jahr 2007, der der deutschen Wirtschaft dadurch entstanden ist, Tendenz steigend.⁴ Nicht nur der finanzielle Schaden ist enorm. Durch den Wissensdiebstahl sind in Deutschland bis zu 70.000 Arbeitsplätze gefährdet. Dadurch ergeben sich weitere Konsequenzen.⁵ Die Problematik der legalen Wettbewerbsbeobachtung, auch Competitive Intelligence genannt, und der illegalen Wirtschaftsspionage zwingt Unternehmen dazu, sich mit Abwehrstrategien auseinanderzusetzen und Gegenmaßnahmen zu entwickeln, um auch zukünftig erfolgreich bleiben zu können.

Fast jedes Unternehmen ist in der Lage, mit Hilfe von Competitive Intelligence Methoden eine systematische, professionelle, entscheidungsorientierte sowie legale Recherche und Analyse der Wettbewerber durchzuführen. Die Voraussetzungen für die Umsetzung von Competitive Intelligence ist in der heutigen vernetzten Welt mit zunehmender Liberalisierung der Märkte immer einfacher. Competitive Intelligence Akteure setzen aus vielen Puzzleteilen ein schlüssiges Bild eines Unternehmens zusammen, welches aus Informationen von Märkten und Wettbewerbern stammt. „Als ‚Competitive Intelligence‘ (CI) wird einerseits der systematische Prozess der Informationserhebung und -analyse bezeichnet, durch den aus fragmentierten (Roh-)Informationen über Märkte, Wettbewerber und Technologien den Entscheidern ein plastisches Verständnis über sein Unternehmensumfeld entsteht. CI-Themen sind dabei meist zukunftsorientierte Aussagen zu Wettbewerberpositionierungen, -intentionen und -strategien. Andererseits ist ‚Intelligence‘ das Endresultat des Prozesses: Das benötigte Wissen über Markt und Wettbewerb. Insbesondere werden Aussagen über die erwarteten Auswirkungen für das eigene Unternehmen und darauf basierende Handlungsempfehlungen getroffen.“⁶

¹ vgl. Sicherheitsforum Baden-Württemberg: Mit Sicherheit erfolgreich, Erfolgsfaktor Know-how-Schutz, S.10

² vgl. Pressrelations: Konferenz über Industriespionage in der Wirtschaftskrise

³ vgl. Koenen, J.; Hottelet, U.: Tagesgeschäft Spionage

⁴ vgl. Deutsche Presse-Agentur: Innenministerium: 20 Milliarden Schaden durch Wirtschaftsspionage

⁵ vgl. Pelkmann, T.: China in der Leitung

⁶ Deutschen Competitive Intelligence Forum: Was ist Competitive Intelligence

CI beschreibt die legalen Methoden der Informationsbeschaffung und Informationsanalyse, wobei Wirtschaftsspionage alle illegalen Aktivitäten einschließt. Zu bedenken ist hierbei, dass zwischen diesen beiden Begrifflichkeiten eine Grauzone existiert, welche eine Reihe ethischer Aspekte beinhaltet. Ist es moralisch korrekt eine Informationserhebung durch fingierte Vorstellungsgespräche mit Mitarbeitern der Wettbewerber durchzuführen? Rechtlich ist dies nicht verboten, aber ist es moralisch einwandfrei? Eine rein kriminologische und juristische Abgrenzung der Begriffe reicht hierfür nicht aus. Die ethische Komponente erschwert die Definition der Begriffe. Um der wachsenden Bedeutung von CI in der heutigen Wirtschaftswelt moralisch gerecht zu werden hat die Society of Competitive Intelligence Professionals (SCIP) einen Verhaltenskodex entworfen, an den sich die CI-Akteure halten sollen. Dies ermöglicht, die Grauzone zu verringern und eine neue Managementdisziplin zu fördern.

Gehen ethische Grundsätze verloren?

Wer sind die Akteure?

Nicht nur Unternehmen aus dem In- und Ausland möchten mehr über die Konkurrenz wissen, auch Staaten setzen ihre Geheimdienste oder Regierungsstellen ein. Im Mittelpunkt der Ausspähungen stehen die Bereiche Wirtschaft, Wissenschaft und Technik. Je nach Abhängigkeit der Bedürfnisse und unter Berücksichtigung der zur Verfügung stehenden Ressourcen und Möglichkeiten, unterscheiden sich die in Frage kommenden CI und Wirtschaftsspionagemassnahmen.

Neue Aufgaben für James Bond? Im Auftrag ihrer Majestät.

Der immer stärkere Wettbewerbsdruck durch die Internationalisierung lässt das Interesse von Staaten erstarken, Schlüsselindustrien auszuspienieren. Es ist eine falsche Annahme, dass die Gefahren ausschließlich aus China, Russland und Nordkorea stammen. Fast jeder Staat ist aktiv, auch befreundete westliche Staaten. Dies ist für die zukünftige Entwicklung und Stabilität der Nationen von Bedeutung. Der Wohlstand der Nation sollte auch durch den Schutz und durch die Unterstützung seitens des Staates gewährleistet werden. Als Unterstützung kann hierbei die Versorgung mit Informationen als Maßnahme angesehen werden.⁷

Ein Trugschluss. Nicht nur China setzt auf Spionage.

Ein Beispiel ist die Bereitstellung von Informationen zu neu patentierten Verfahren von Wettbewerbern, die sich noch im Genehmigungsprozess des Patentamtes befinden.

Privatwirtschaftliche Akteure können mit eigenen CI-Abteilungen oder Partnerschaften auf diesem Gebiet aktiv werden. Heutzutage können auch externe Dienstleister diese Aufgaben wahrnehmen. In der Regel besteht das Personal der Dienstleister aus hoch qualifizierten Spezialisten.⁸

⁷ vgl. Lux, C.; Peske, T.: Competitive Intelligence und Wirtschaftsspionage: Analyse, Praxis, Strategie, S.36

⁸ vgl. Romppel, A.: Competitive Intelligence, Konkurrenzanalyse als Navigationssystem im Wettbewerb, S.11 ff.

Ursachen für CI und Wirtschaftsspionage

Kernkompetenzen repräsentieren die Wettbewerbsfähigkeit eines Unternehmens.

Das Know-how von Unternehmen basiert auf Kernkompetenzen, die sie für den Wettbewerb erfolgreich machen. Kernkompetenzen sind ein Verbund von Fähigkeiten und Technologien, die einen überlegenen und längerfristigen wahrgenommenen Kundennutzen schaffen und so einen nachhaltigen Wettbewerbsvorteil erzeugen. Diese verschiedenen Informationen sind absolut wichtig für die Wettbewerbsfähigkeit und sichern den Fortbestand eines Unternehmens in der Zukunft. Hieraus ergeben sich verschiedene Ursachen für CI und Wirtschaftsspionage:⁹

- Eine entscheidende Rolle für die Positionierung eines Staates oder eines Unternehmens ist die wirtschaftliche Stärke.
- Informationen sind das Wissenspotenzial, das die Handlungsfähigkeit und Leistungskraft von Staaten und Unternehmen wesentlich bestimmt. Informationen sind heutzutage in der komplexen und sich immer schneller verändernden Welt eine strategische Ressource.
- Wichtige und bedeutende Informationen werden von Staaten oder Unternehmen gezielt geheim gehalten, um eigene Vorteile zu generieren oder zu erhalten. Dies führt dazu, dass Dritte versuchen, sich diese legal oder illegal zu beschaffen.
- Durch CI oder Wirtschaftsspionage erhalten Unternehmen oder Staaten neue Möglichkeiten, sich schneller und einfacher Wettbewerbsvorteile zu beschaffen. Eigene F&E-Aktivitäten sind dann nicht mehr so enorm wichtig, um mit der Konkurrenz mitzuhalten.
- Eigene Interessen werden von Staaten und Unternehmen wahrgenommen, die auf unterschiedlichen Gebieten ihre konkrete Ausprägung erfährt. Diese eigenen Interessen führen letztendlich zu CI- oder Wirtschaftsspionage Maßnahmen.

Die Vorgehensweise bei CI und Wirtschaftsspionage

Gleiches Schema, großes Risiko für den Angegriffenen.

Zu Beginn muss der Bedarf ermittelt werden. Die Feststellung des Bedarfs wird mit Key Intelligence Topics (KITs) gewährleistet, aus diesen Schlüsselthemen werden Key Intelligence Questions (KIQs) abgeleitet. Man kann die KITs als Grundlage des gesamten CI-Zyklus ansehen.¹⁰ In der Literatur werden verschiedene CI-Zyklen beschrieben, die sich in ihrem Grundprinzip vereinzelt unterscheiden.¹¹ Für die Umsetzung des CI-Zyklus ist es nicht von Bedeutung, ob CI oder Wirtschaftsspionage betrieben wird. Zweitens muss der CI-Zyklus geplant, organisiert und gesteuert werden. Zu beachten ist dabei, dass genügend Informationen gesammelt werden, um die KIQs umfassend beantworten zu können.¹²

⁹ vgl. Landesamt für Verfassungsschutz Baden-Württemberg und Bayern: Wirtschaftsspionage in Baden-Württemberg und Bayern, S.13 ff.

¹⁰ vgl. Michaeli, R.: Competitive Intelligence, S.119 f.

¹¹ vgl. Michaeli, R.: Competitive Intelligence, S.118 sowie Romppel, A.: Competitive Intelligence, Konkurrenzanalyse als Navigationssystem im Wettbewerb, S.45

¹² vgl. Michaeli, R.: Competitive Intelligence, S.121 ff.

Drittens erfolgt die eigentliche Datenerhebung. Die gewonnenen Daten müssen auf Glaubwürdigkeit und Plausibilität überprüft werden, damit eine fundierte Analyse stattfinden kann.

Viertens werden die verschiedenen Daten in einen identischen und auswertbaren Zustand transformiert. Diese Datenbasis ist die Grundlage für die kommende Analyse. Dabei müssen vor der Analyse Fehlinformationen sowie unglaubwürdige Quellen erkannt und ausgeschlossen werden. Die eigentliche Analyse der Daten ist deren Interpretation unter dem Gesichtspunkt der KIQs.

Im fünften Schritt wird aufbauend auf der Analyse der Bericht erstellt. Wesentlich hierbei ist, dass die verschiedenen Hierarchiestufen im Unternehmen unterschiedliche Informationen benötigen. Je höher die Hierarchiestufe, desto strategischere Themen sind von Bedeutung.

Im finalen Schritt folgt die Bewertung des CI-Zyklus. Die gestellten Aufgaben sind abgearbeitet und die KITs und KIQs sind gelöst. Es erfolgt nun die Integration der gewonnenen Erkenntnisse in die tägliche Arbeit. Mit Hilfe der neuen Erkenntnisse und Einschätzungen ist es nun möglich eine effektive Strategie zu entwickeln und umzusetzen. Eine Reflektion des CI-Projektes ist zudem hilfreich, um zukünftige CI-Zyklen effektiver und effizienter zu durchlaufen.

Möglichkeiten der Datenerhebung

Observation

Ziel der Observation ist es, Informationen durch Beobachtung der direkten oder indirekten Wettbewerbsaktivitäten zu erheben und zu analysieren.¹³ Bei der Observation von Personen geht es nicht um deren Beschattung, sondern um Themen wie die Personaldichte (z.B. Anzahl der Vertriebsmitarbeiter), Nutzungsintensität von Räumen (z.B. Überstunden), Anzahl der Fremdfirmenmitarbeiter, Besuch von Unternehmensberatern, Besuche von bisherigen oder potenziellen Kunden.

Diese gesammelten Daten lassen sich nur schwer auf andere Weise besorgen. Dieses Verfahren ist personal- und arbeitsintensiv und daher eher einzusetzen, um sich erfolgskritische Erkenntnisse und fehlende Informationen zu besorgen.

Es gibt viele Möglichkeiten um Informationen zu gewinnen.

Human Intelligence

Human Intelligence (HUMINT) ist die Informationsgewinnung mittels menschlicher Quellen, und ein bedeutsamer Bestandteil der Datenerhebung. Die Nutzung Mensch als Informationsquelle ist unerlässlich bei der Recherchearbeit. Besonders der ethische Faktor ist hier von Bedeutung und erfordert unbedingt das Einhalten der SCIP Richtlinien.¹⁴ Der Umgang mit Menschen als Informationsquellen erfordert Geschick und Kenntnisse in der Gesprächsführung, da offene Dialoge viele neue und brauchbare Informationen hervorbringen, aber auch Fehleinschätzungen beinhalten können.

¹³ vgl. Michaeli, R.: Competitive Intelligence, S.177 ff.

¹⁴vgl. Lux, C.; Peske, T.: Competitive Intelligence und Wirtschaftsspionage: Analyse, Praxis, Strategie, S.84 f.

Der Schwerpunkt von HUMINT ist der zielbewusste Kontakt und Wissenstransfer mit Wissensträgern. Themen von HUMINT¹⁵ sind zukünftige Tendenzen, Strategien, Wahrnehmungen und Einschätzungen der Märkte und eigenen Produkte oder Dienstleistungen. Diese Wissensträger können von unterschiedlicher Herkunft und Bildungsniveau sein. Für HUMINT Aktivitäten bieten sich viele verschiedene örtliche Gegebenheiten an. Messen, Ausstellungen, Konferenzen, Hochschulen, Kundenbesuche, Institutionen, Verbände, Behörden und Reisen sind nur beispielhaft zu nennen.

Technical Intelligence

Technical Intelligence (TECHINT) ist als Obergriff der technischen Informationsbeschaffung zu verstehen, hinter dem sich mehrere technische Möglichkeiten verbergen. Die technischen Möglichkeiten haben in den letzten Jahren rasant zugenommen und werden auch zukünftig immer mehr Möglichkeiten aufweisen.¹⁶ Beispielsweise ist ein Themenschwerpunkt die Bildaufklärung über ein Zielobjekt. Dabei werden die Zielobjekte auf Bild oder Film festgehalten, um diese später zu analysieren. Verschiedene Typen von Sensoren (z.B. visuelle, radar-, infrarot-, laser-, elektrooptisch, usw.) ermöglichen ein breites Spektrum an Aufnahmen.

Darüber hinaus sind die Kommunikationsübertragungen, z.B. Sprachübertragung per Telefon, auch ein möglicher Bestandteil der Untersuchung.

Open Source Intelligence

Open Source Intelligence (OSINT) ist die Beschaffung interessanter Informationen aus frei zugänglichen Quellen.¹⁷ Internetdatenbanken, Diplomarbeiten, Forschungsberichte, Handbücher, Patent- und Lizenzunterlagen oder Qualitätszertifizierungen bieten hierfür viele Möglichkeiten. Diese Informationen sind im Normalfall frei zugänglich und können meistens legal beschafft werden.¹⁸ Aufgrund der Bereitschaft der Unternehmen zu kundenfreundlicher Transparenz oder dem offenen Verhalten gegenüber Kunden/Lieferanten ist dies ein idealer Ansatzpunkt für die Informationsbeschaffung. Die grundlegende Auswertung offener Quellen lässt wertvolle Rückschlüsse auf Know-how zu.

Das Internet ist dabei einer der wichtigsten Quellen für OSINT. Mit dem Internet lassen sich alle Arten von Datenbanken nach relevanten Informationen durchforsten. Das Internet als Suchinstrument ist interessant für das Monitoring von Wettbewerbern, Zulieferunternehmen und Kunden. Zudem ist die Identifikation neuer Websites oder Webportale wichtig, um in der Lage zu sein, neue Informationen aufzunehmen.

¹⁵ vgl. Michaeli, R.: Competitive Intelligence, S.199 ff.

¹⁶ vgl. McGonagle, J.; Vella, C.: Internet Age of Competitive Intelligence, S.7

¹⁷ vgl. Romppel, A.: Competitive Intelligence, Konkurrenzanalyse als Navigationssystem im Wettbewerb, S.51

¹⁸ vgl. Lux, C.; Peske, T.: Competitive Intelligence und Wirtschaftsspionage: Analyse, Praxis, Strategie, S.97 ff.

Abwehr von CI und Wirtschaftsspionage

Die bisher beschriebene Problematik macht deutlich, dass es unabdingbar ist, sich mit CI und Wirtschaftsspionage zu beschäftigen. Es gibt verschiedene Ansätze, sich gegenüber CI und Wirtschaftsspionage zu wappnen. Anzumerken ist, dass hier nur frei zugängliche Modelle aufgezählt werden.

Es gibt verschiedene Ansätze, sich zu schützen.

Der Intelligence Protection Kreislauf ist identisch mit dem CI-Kreislauf. Der Intelligence Protection Kreislauf wird nicht wie ursprünglich zur Informationssammlung, sondern zum Informationsschutz angewandt. Ziel ist die Neutralisierung des CI-Angriffes durch aktive, flexible und angepasste Maßnahmen.¹⁹

Operations Security (OPSEC) ist ein Informationsschutzkonzept und stammt aus dem Vietnamkrieg. OPSEC ist ein Prozess, der angewendet wird, um Gegner zu identifizieren und abzuwehren. Der OPSEC-Prozess ist mit Systemen, Drohungen, Verwundbarkeitsanalysen, Risikobewertungen, rentabler Gegenmaßnahme-Planungen und deren Durchführung verbunden.

Die Handlungsempfehlungen vom Landesamt für Verfassungsschutz Baden-Württemberg sollen Unternehmen in die Lage versetzen, sich gegen Wirtschaftsspionage zu wappnen. Die Methode basiert auf einer Checkliste sowie einem Stufenplan, der schrittweise vollzogen wird.²⁰ Zudem sind Mitarbeiter des Verfassungsschutzes bereit, unterstützend in der Beratung gegen Wirtschaftsspionage tätig zu werden.

Als weiteres Modell basiert der Know-how-Schutz auf fünf Grundsätzen. Diese fünf Grundsätze verhelfen dem Unternehmen die Abwehr intelligent und lernfähig zu gestalten, um zukünftige neue und abgewandelte Bedrohungen zu erkennen und abzuwehren. Die Hauptaufgabe besteht im Erkennen und der Reduktion von Risiken.

Als letztes Modell sind die neun Grundsätze von McGonagle zu nennen. Die Grundsätze von McGonagle sind eine Verhaltensrichtlinie für Unternehmen, die CI abwehren wollen. Durch diese Grundsätze kann ein Unternehmen eine Analyse vornehmen und sich seiner Schwachstellen bewusst werden. Die kritischen Informationen stehen im Mittelpunkt und werden in vier Bereiche untergliedert. Eine Unterscheidung in Strategie-, Operativ-, Ziel- und Technologie-orientiert hilft dabei die Schwerpunkte von CI und Wirtschaftsspionage zu identifizieren.

Aus den beschriebenen Modellen wurden die Stärken und Schwächen abgeleitet und ein neues Modell entwickelt, der sogenannte CI-Kompass.

¹⁹ vgl. Lux, C., Peske, T.: Competitive Intelligence und Wirtschaftsspionage: Analyse, Praxis, Strategie, S.151

²⁰ vgl. Landesamt für Verfassungsschutz Baden-Württemberg: Know-how-Schutz, S.9 f.

Know-how-Schutz ist absolut notwendig – Daher der CI-Kompass

Das bestehende Grundprinzip des CI-Kompass geht davon aus, dass ein Unternehmen von der Informationsseite und deren Bedeutung für das Unternehmen in konzentrischen Kreisen aufgebaut ist.

Im inneren Kreis befinden sich die Kernkompetenzen, welche das Know-how beinhalten, die Ideen und die Strategien. Da der innere Kern die kritischen Informationen beherbergt, ist dieser als das Zentrum des Unternehmens anzusehen. Um diesen Kern sind andere Informationen und Details positioniert, die den Kern schichtweise umgeben. Ganz außen liegen die freizugänglichen und nicht oder kaum schützenswerten Informationen des Unternehmens.

Im ersten Schritt müssen die Kernkompetenzen des Unternehmens eindeutig identifiziert und herausgearbeitet, danach die dazu gehörigen Geschäftsprozesse abgebildet werden. Wichtig bei der Identifikation der Geschäftsprozesse ist, nur die relevanten Prozesse zu den dazugehörigen Kernkompetenzen zu erfassen. Durch diese Prämisse wird eine zu große und unnötige Überprüfung des Know-how-Schutzes vermieden. Generell ist anzumerken, dass man sich bei der Überprüfung auf die wesentlichen Faktoren beschränken soll. Diese entscheidende Einschränkung findet über die Begrenzung der Geschäftsprozesse statt.

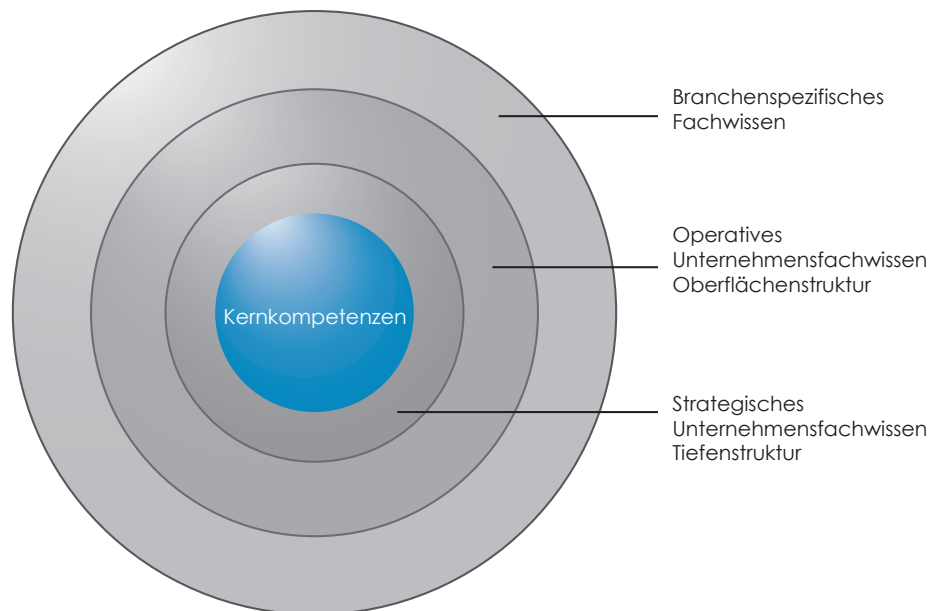
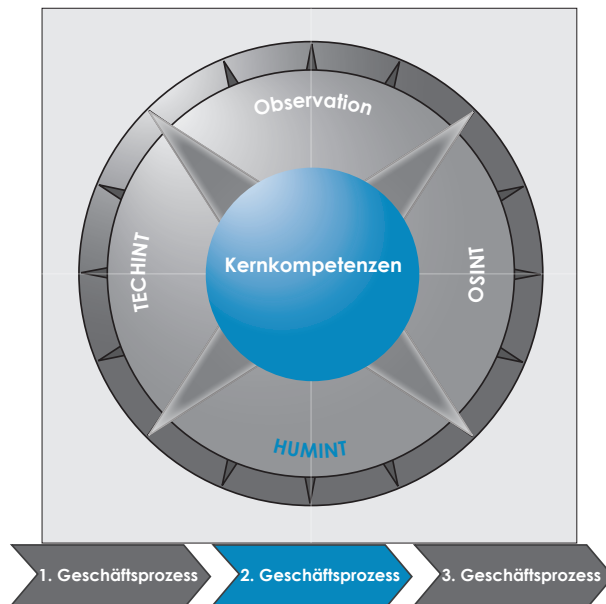


Abbildung 1: Das Grundprinzip des CI-Kompass.

Industriespionage – Schutz sensibler Unternehmensdaten

Die folgende Abbildung zeigt den CI-Kompass:



Der CI-Kompass koordiniert den Aufbau des Know-how-Schutzes.

Betrachtungshorizonte	Beschreibung der Einzelaspekte	Unternehmenskritisch	Angreifbarkeit
Einbezug des Unternehmens in die Wertkette		① ② ③ ④ ⑤	① ② ③ ④ ⑤
Fremdfirmenmitarbeiter			

Abbildung 2: CI-Kompass

Im Mittelpunkt des Modells stehen die Kernkompetenzen, welche innerhalb der Geschäftsprozesse umgesetzt werden. Die Geschäftsprozesse wiederum werden untersucht, um die Stärken und Schwächen zu ermitteln. Die Untersuchung nach Know-how-Abflüssen erfolgt anhand der verschiedenen Datenerhebungsschwerpunkte, die für die aktive CI verwendet werden. Die verschiedenen Einzelaspekte der Datenerhebung ermöglichen eine multidimensionale Analyse und können verschiedene Möglichkeiten eines ungewollten Know-how Abflusses aufzeigen. Die Aspekte werden jeweils separat auf den zu untersuchenden Geschäftsprozess ausgerichtet und analysieren die Stärken und Schwächen des Geschäftsprozesses in Bezug zu dem Einzelaspekt der Datenerhebung.

Die Aspekte sind:

- Technical Intelligence
- Human Intelligence
- Open Source Intelligence
- Observation

Die Ergebnisse werden für jeden Aspekt der Datenerhebung in einem Protokoll festgehalten. Jeder einzelne Punkt der Untersuchung wird in diesem Protokoll in zweierlei Hinsicht bewertet.

1. Unternehmenskritisch: Inwiefern ist der einzelne Punkt in der Untersuchung für die Kernkompetenz von Bedeutung?
2. Angreifbarkeit: Inwiefern kann ein möglicher Angreifer über diesen Aspekt versuchen, das Know-how abzuziehen? Wie schwer fällt es dem Angreifer Informationen zu erlangen? Wie hoch ist das Risiko entdeckt zu werden?

*Eine Bewertung schafft
Transparenz in der Daten-
erhebung.*

Eine Bewertungsskala schafft hierbei einen klaren Rahmen. Die Skala der Punktvergabe liegt zwischen eins und fünf, wobei eins die Minimalpunktzahl ist. Dieser Wert wird vergeben, wenn sich die daraus ergebenden Problemfelder als unkritisch für das Unternehmen erweisen oder die Angreifbarkeit des Unternehmens als sehr gering herausstellt. Deshalb ist die Vergabe der Minimalpunktzahl immer als das Maximalziel seitens des Unternehmens anzustreben. Diese Maßnahmen zeigen die Schwachstellen und Stärken des Unternehmens auf, und es lassen sich mögliche Know-how-Abflüsse sowie potenzielle Angriffsmöglichkeiten erkennen. Der erste Bewertungsaspekt „Unternehmenskritisch“ kann für alle Aspekte gleichermaßen definiert werden, da dieser für alle allgemeingültig ist. Die folgende Tabelle zeigt die Eingruppierungen für den Bewertungspunkt „Unternehmenskritisch“.

Vergebener Punkt	Zu erfüllendes Kriterium
1	Der Aspekt ist irrelevant für die Kernkompetenz.
2	Der Aspekt ist in geringem Umfang wichtig für die Kernkompetenz.
3	Der Aspekt ist relevant für die Kernkompetenz.
4	Der Aspekt ist sehr wichtig für die Kernkompetenz.
5	Der Aspekt ist die Schlüsselfunktion für die Kernkompetenz

Beispielsweise ist ein Aspekt im Datenerhebungspunkt HUMINT, ob Know-how-Träger im Unternehmen existieren und ob diese für Dritte identifizierbar sind. Sind die

Know-how-Träger ein wichtiger Bestandteil der Kernkompetenz, dann ist dies als ein kritischer Faktor anzusehen. Die Bewertung „Unternehmenskritisch“ würde dann mit „4“ oder „5“ erfolgen.

Der zweite Bewertungsaspekt „Angreifbarkeit“ bezieht sich auf einen möglichen Angreifer. Kann dieser den Aspekt nutzen, um das Know-how abzufangen? Im obigen Beispiel würde eine Bewertung der Know-how-Träger unter solchen Aspekten erfolgen. Üben die Know-how-Träger im Rahmen ihrer Tätigkeit eine Zusammenarbeit mit Kunden oder Lieferanten z.B. durch gemeinsame F&E-Aktivitäten aus, würde die Angreifbarkeit mit einer Bewertung von „4“ bis „5“ erfolgen. Ein Kunde oder Lieferant könnte diese Know-how-Träger ohne großes Risiko aushorchen oder abwerben.

Vergebener Punkt	Zu erfüllendes Kriterium
1	Der Aspekt ist für den Angreifer nicht identifizierbar.
2	Der Aspekt ist für den Angreifer schwer ermittelbar und mit einem hohen Risiko identifiziert zu werden verbunden.
3	Der Aspekt lässt sich identifizieren. Aufwand und Risiko erkannt zu werden ist vorhanden.
4	Der Aspekt lässt sich identifizieren. Risiko erkannt zu werden ist minimal.
5	Der Aspekt lässt sich leicht erkennen ohne das Risiko identifiziert zu werden.

In der Anwendung der Bewertungsskalen sollte jeder Einzelaspekt zuerst vollständig herausgearbeitet und dann mit den vergebenen Skalen verglichen werden, um die endgültige Einordnung zu vollziehen.

Aufbau des Unternehmensschutzes

Ist anschließend die Überprüfung der Kernkompetenzen anhand der Geschäftsprozesse mit Hilfe der verschiedenen Datenerhebungsaspekte und die dazugehörige Bewertung der beiden Faktoren „Unternehmenskritisch“ und „Angreifbarkeit“ erfolgt, kann die Auswertung der Ergebnisse folgen. Die Auswertungsergebnisse je Datenerhebungsaspekt sollten in einer Matrix grafisch dargestellt werden. Diese Möglichkeit bietet eine bessere Übersicht und Darstellung der einzelnen Punkte der Bewertung. Im Folgenden ist eine Beispielmatrix gezeigt. Auf der Abszisse wird die „Angreifbarkeit“ in den fünf Bewertungsschritten eingetragen, auf der Ordinate steht der Bewertungspunkt „Unternehmenskritisch“ mit den fünf Bewertungsschritten. Die drei Graustufen, die in der Matrix hinterlegt sind, zeigen die Wichtigkeit für das Unternehmen auf. Liegt ein Bewertungspunkt in einem dunkelgrauen Quadranten sollte das Unternehmen hier zuerst Abwehrmaßnahmen definieren und umsetzen. Gefolgt von den mittelgrauen Quadranten und den hellgrauen Quadranten in der Aktivitätendringlichkeit. Dies unterstützt die Rangfolge und Zielvorgabe beim Definieren von Abwehrmaßnahmen.

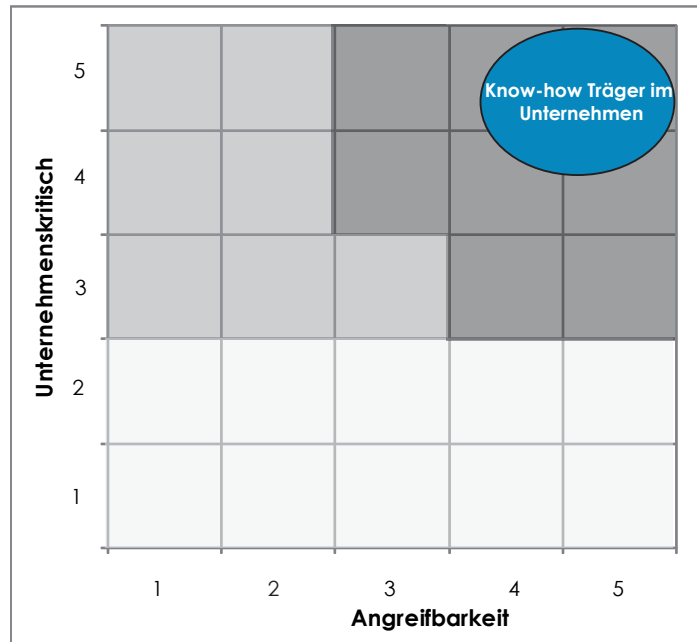


Abbildung 3: Beispielmatrix.

Das Beispiel der Bewertung des Aspektes „Sind Know-how-Träger vorhanden?“ gibt das Ergebnis in der Matrix wieder. Da dieser Aspekt als kritisch identifiziert wurde, befindet sich dieser im dunkelgrauen Bereich.

Aufgrund der vorliegenden Bewertungen der vier verschiedenen Datenerhebungsaspekte der Kernkompetenzen lassen sich individuelle Abwehrmaßnahmen generieren. Hierbei ist die Individualität von besonderer Bedeutung, da ein Unternehmen nicht standardisiert eingruppiert werden kann. Es gibt hierbei mehrere wesentliche Faktoren, die berücksichtigt werden müssen:

1. Unternehmenskultur und Unternehmensphilosophie.
2. Machbarkeit im Rahmen der Geschäftstätigkeit.
3. Finanzieller Aufwand für die Umsetzung und Aufrechterhaltung des Schutzes.

Ablaufprozess des CI-Kompass

In der folgenden Abbildung ist der Ablauf des CI-Kompass grafisch dargestellt. Zu erkennen ist, dass die Vorarbeiten im Rahmen der Identifizierung der Kernkompetenzen sowie der zugehörigen Geschäftsprozesse notwendig sind. Erst danach kann der CI-Kompass angewandt werden.

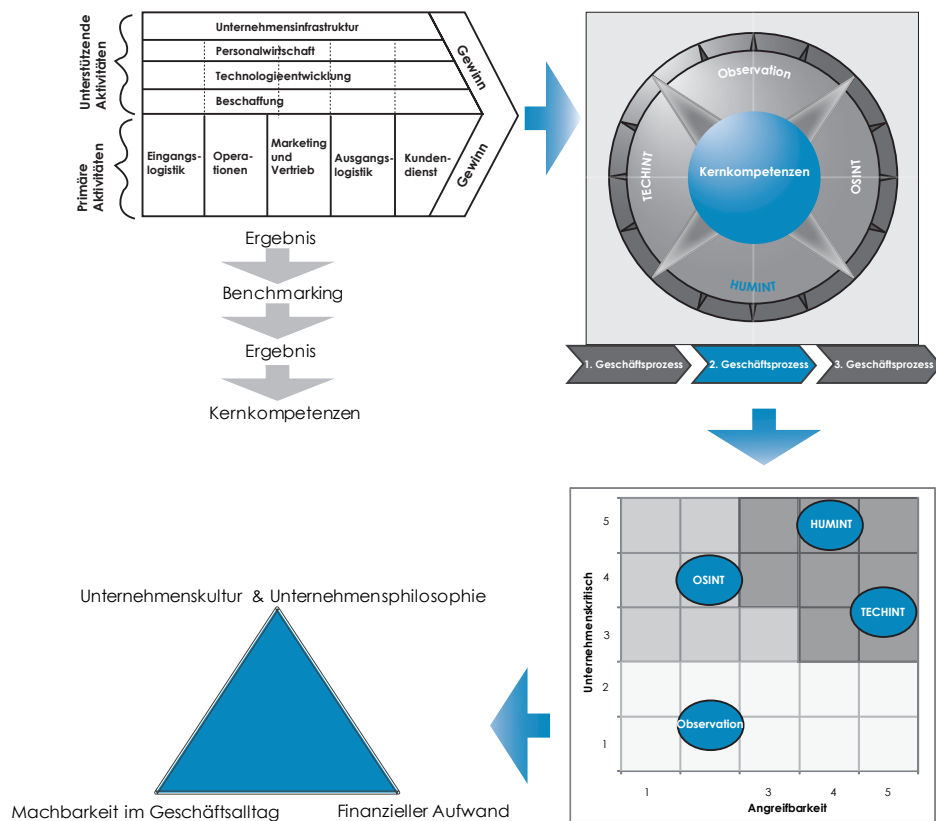


Abbildung 4: Ablauf CI-Kompass.

Praktischer Einsatz des CI-Kompass

Der CI-Kompass wurde in einem Unternehmen hinsichtlich Wirkungsweise und Effektivität getestet. Als Ergebnis ist vorweg zu nehmen, dass sich der CI-Kompass in der praktischen Anwendung als wirkungsvolles Hilfsmittel eignet. Durch die vier Datenerhebungsaspekte konnten die verschiedenen Möglichkeiten eines Angriffes untersucht und Stärken und Schwächen im Unternehmen identifiziert und analysiert werden.

Die Schwächen können als möglicher Angriffspunkt genutzt werden. Die Stärken wiederum helfen die Abwehr effektiv zu gestalten und den Schutz zu erhöhen. Als Stärke in diesem Unternehmen ist die Unternehmenskultur anzusehen. Durch gezielte Informationen der Belegschaft, durch Broschüren oder Newsletter, können die Mitarbeiter gegenüber CI und Wirtschaftsspionage sensibilisiert werden. Eine Möglichkeit hierzu wäre das Ansprechen von Fremden, die sich unbefugt auf dem Werksgelände aufhalten. Noch bedeutender ist es, das Verständnis zu fördern, dass Lieferanten, Kunden oder Fremde über die Mitarbeiter Know-how abgreifen möchten. Dadurch würden die Mitarbeiter

Der CI-Kompass ist ein praktikables Hilfsmittel.

von sich aus vorsichtiger bei der Preisgabe von Informationen sein. Auf Basis der Stärken des Unternehmens ist auch die Konzeption eines Projektteams entstanden, welches sich dem Know-how-Schutz verpflichtet fühlt. Dieses Team agiert abteilungsübergreifend und kann aufgrund der gesetzten Schwerpunkte effektiv eine Analyse von möglichen Problemen vornehmen und den nötigen Schutz umsetzen. Hierbei sind technische und wirtschaftliche Kooperationen, Aktivitäten von Headhuntern, die Datensicherheit im Netzwerk sowie der Mitarbeiter des Unternehmens Schwerpunkte des Teams.

Des Weiteren konnten Schwachstellen identifiziert werden, die einen möglichen Know-how-Abfluss bis jetzt ermöglichten. Darunter ist die Datensicherheit im Netzwerk anzusehen, die Speicherung von Druckseiten im Drucker oder Kopierer selber, die Verwendung von mobilen Speichermedien sowie die Nutzung von Kommunikationsanlagen. Erwähnenswert ist zudem die Entsorgung von Informationen und Materialien, welche bis jetzt nicht unter dem Gesichtspunkt des möglichen Know-how-Abflusses stattgefunden hat. Zudem konnte auch in diesem Unternehmen die größte Schwachstelle, der Mensch, nachgewiesen werden.

Aktuelle Untersuchungen belegen, dass der eigene Mitarbeiter im Unternehmen die größte Gefahr des Know-how-Schutzes darstellt. Die Wirtschaftswoche belegt mit ihrer Untersuchung, dass der Informationsabfluss durch eigene Mitarbeiter die häufigste Gefahrenquelle ist.²¹ Dargestellt werden die wichtigsten Angriffsziele auf Unternehmen in der folgenden Abbildung. Die blauen Balken kennzeichnen den Know-how-Abfluss durch Mitarbeiter, egal ob dieser gewollt oder ungewollt stattgefunden hat.

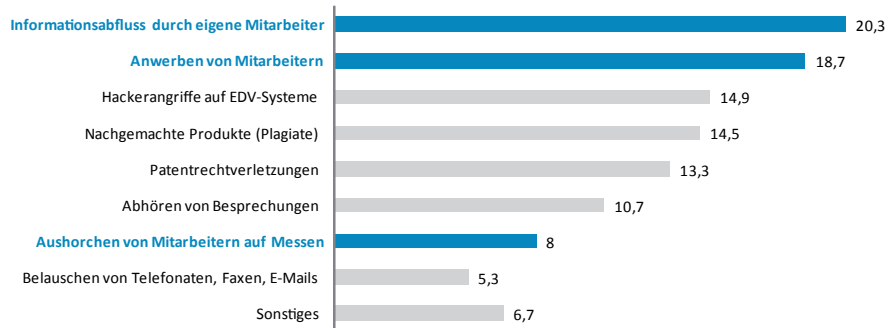


Abbildung 4: Die wichtigsten Angriffsziele auf Unternehmen.

Fazit

Unternehmen müssen sich der Möglichkeiten und Gefahren der Themengebiete CI und Industriespionage bewusst sein, um erfolgreich in ihren Märkten agieren zu können. Die Vernachlässigung der Gefahren durch CI und Industriespionage, vor allem bei deutschen Unternehmen, führt zu wirtschaftlichen Schäden und dem Verlust der Wettbewerbsfähigkeit.

²¹ vgl. Nuri, M.: Getarnte Kollegen, S.68 ff.

Der CI-Kompass ist eine neue Methode, um diese Problemstellung zu lösen. Dabei ist die Konzentration auf die Kernkompetenzen eine zielgerichtete Vorgehensweise, die schützenswerten Informationen zu erfassen und zu bewerten sowie unnötige Analysen zu vermeiden. Die Zusammenführung der legalen und illegalen Datenerhebung nach den vier Gesichtspunkten HUMINT, TECHINT, OSINT und Observation schaffen ein Modell, dass eine umfassende Analyse gewährleistet. Der Fokus auf die Kernkompetenzen und deren Geschäftsprozesse sowie die daraus abgeleiteten Möglichkeiten der Datenerhebung bauen einen wirkungsvollen Analyserahmen auf, in dem sämtliche Aspekte detailliert bearbeitet werden können. Die anschließende Bewertung der Ergebnisse durch zwei Bewertungskriterien fokussiert die Anstrengungen des Unternehmens auf die wesentlichen und kritischen Bereiche. Dadurch können die Ressourcen zur Abwehr von CI und Industriespionage effizient eingesetzt werden und ermöglichen einen schnellen Schutz für die als kritisch identifizierten Bereiche.

Ein Zitat von MARK TWAIN, das die gesamte Thematik in einem Satz zusammenfasst, hilft die Problemstellung zu verdeutlichen: „Man muss seine Überlegenheit mit ständiger Wachsamkeit erkaufen“. Wird dieses Zitat von Wirtschaftsunternehmen beachtet, ist die Sicherheit des Know-how in den Kernkompetenzen eine Selbstverständlichkeit und die Wettbewerbsfähigkeit bleibt erhalten.

Quellen

Deutschen Competitive Intelligence Forum: Was ist Competitive Intelligence, <http://www.dcif.de/was-ist-competitive-intelligence.html>, Abruf vom 30. November 2008.

Deutsche Presse-Agentur: Innenministerium: 20 Milliarden Schaden durch Wirtschaftsspionage, <http://www.finanznachrichten.de/nachrichten-2007-10/9218102-innenministerium-20-milliardenschaden-durch-wirtschaftsspionage-016.htm>, Abruf vom 22. September 2009.

Koenen, J.; Hottelet, U.: Tagesgeschäft Spionage, <http://www.handelsblatt.com/technologie/it-internet/tagesgeschaeft-spionage%3B1318834>, Abruf vom 21. September 2009.

Landesamt für Verfassungsschutz Baden-Württemberg: Know-how-Schutz, Handlungsempfehlungen für die gewerbliche Wirtschaft, Verlag Kurz & Co, Stuttgart, 2004.

Landesamt für Verfassungsschutz Baden-Württemberg und Bayern: Wirtschaftsspionage in Baden-Württemberg und Bayern, Daten – Fakten – Hintergründe, Verlag Kurz & Co., Stuttgart, 2006.

Lux, C.; Peske, T.: Competitive Intelligence und Wirtschaftsspionage: Analyse, Praxis, Strategie, Gabler-Verlag, Wiesbaden, 2002.

McGonagle, J.; Vella, C.: Internet Age of Competitive Intelligence, Greenwood Pub., Westport, 1999.

Michaeli, R.: Competitive Intelligence, Strategische Wettbewerbsvorteile erzielen durch systematische Konkurrenz-, Markt- und Technologienanalysen, Springer-Verlag, Berlin u.a., 2006.

Nuri, M.: Getarnte Kollegen, in: Wirtschaftswoche, Heft 8, 2008, S.68-72.

Pressrelations: Konferenz über Industriespionage in der Wirtschaftskrise, <http://www.pressrelations.de/new/standard/derefferrer.cfm?r=376688>, Abruf vom 21. September 2009.

Romppel, A.: Competitive Intelligence, Konkurrenzanalyse als Navigationssystem im Wettbewerb, Cornelsen Verlag, Berlin, 2006.

Sicherheitsforum Baden-Württemberg: Mit Sicherheit erfolgreich, Erfolgsfaktor Know-how-Schutz, Wilhelm Stober GmbH Eggenstein, 2007.