Spy vs. Spy: Der Kampf um Informationen und Know-how – mit nicht immer legalen Methoden

Viele ausländische Unternehmen, aber auch Länder wie Frankreich, China und die USA, haben die Bedeutung der Globalisierung und der internationalen Weltwirtschaft verstanden. Sie haben verstanden, dass hier ein Krieg tobt und es letzten Endes nur Gewinner und Verlierer geben kann. Dabei entscheidet nicht zwingend die Leistungsfähigkeit der jeweiligen Ökonomie bzw. die Wettbewerbsfähigkeit eines Unternehmens oder Standortes über Sieg oder Niederlage, wie uns die meisten Ökonomen glauben machen wollen, sondern die Entschlossenheit der jeweiligen Kriegsgegner. Im Vordergrund steht vor allem der Umgang mit „Wissen". In Zukunft wird Wissen Informationen und Know-how als Ressource noch weiter in den Vordergrund treten und als wirtschaftlicher Machtfaktor vor allem im Rahmen der fortschreitenden Globalisierung der Märkte an Bedeutung gewinnen.

Das Wissen Ihres Unternehmens ist in den eigenen Händen ein nützliches und wertvolles Instrument, in fremden Händen kann es sich in eine schädliche Waffe gegen Ihr Unternehmen verwandeln. Informationen können von Fremden sehr unterschiedlich verwendet werden, zum Beispiel für Produktpiraterie oder um den Unternehmen gezielt zu schaden, zum Beispiel durch Erpressung oder Bestechung. Die Gründung der École de Guerre Économique (Schule für den Wirtschaftkrieg) im Jahre 1997 verdeutlich, dass zum Beispiel die französische Wirtschaft sich für diesen Krieg wappnet. Hier lernen Frankreichs Manager, wie man sich unter anderem gegen Gerüchte, Desinformation, Destabilisierung und dynamische Marktabschottungen wehrt und wie man angreift. Militärische Taktiken werden mit ökonomischen Konzepten vereint und zu Strategien weiterentwickelt.

Der Einsatz elektronischer Abhörtechniken ist ein wesentlicher Bestandteil dieser Vorgehensweise und gehört nicht in die Abteilung Science Fiction. Die Schlagzeilen vor kurzem publizierter Tageszeitungen mit Titeln wie „Hakkerangriffe aus Fernost" verdeutlichen

Carsten Baeck, Geschäftsführer DRB Deutsche Risikoberatung GmbH und Vorsitzender des AKUS Berlin-Brandenburg: Deutschland im Know-hor-Schutz nur bedingt abwehrbereit.

die Relevanz sowie Aktualität dieser Thematik. Die Verschmelzung von hervorragend ausgebildeten Informatikern und Nachrichtentechnikern mit kriminellen Netzwerken generiert eine schlagfertige Armee von Informationssöldnern manch einer würde auch von Informationsverkäufern (Informationtrader) sprechen die nur darauf warten mit dem Diebstahl von Wissen Geld zu verdienen. Im Gegensatz dazu zeigt sich, wie provinziell zum Teil die deutsche Politik und allen voran der deutsche Mittelstand denken und handeln. Egal ob „Hacker" oder „Produktfälscher" aus China, „Lauschangriffe" aus den USA bzw. Russland, politische Manöver aus Frankreich oder die „halblegale" Informationsgewinnung durch die Konkurrenz: die Welt ist nicht perfekt und wer sich nicht „intelligent" wehrt, der geht unter.

Aber was ist intelligente Prävention und Gegenwehr? Sicherlich nicht ein starres Konzept mit Geheimhaltungsvereinbarungen, Zugangsregelungen und Firewalls meint Peter Mnich von den Wissensschützern. „So wie Wissen entsteht und sich entwickelt, so sollte auch eine Wissensschutzarchitektur

AKUS

Arbeitskreis für Unternehmenssicherheit
Berlin-Brandenburg, www.akus.org
Geschäftsstelle IHK Berlin, Fasanenstr. 85,
10623 Berlin, Tel. (030) 31510-829,
Fax 31510-172, E-Mail: akus@berlin.ihk.de
Geschäftsstelle IHK Frankfurt (Oder), Puschkinstr. 12b, 15236 Frankfurt (Oder), Tel. (0335) 5621233,
Fax: 5621242, E-Mail: thiel@ffo.ihk24.de
V.i.S.d.P.: Christoph Irrgang, Geschäftsführer Berlin und Dr. Knut Thiel, Geschäftsführer Frankfurt (Oder)

entstehen flexibel, lernend und immer an den Beteiligten und den Prozessen orientiert." Unser Kommunikationsverhalten ist von Offenheit, permanenter Erreichbarkeit und schnellem Datentransfer geprägt weniger von Sicherheit und Schutz für das vertrauliche Gespräch. Ziel möglicher „Angriffe" auf schützenswerte Informationen kann jeder Ort der Kommunikation sein. Die Methoden reichen vom einfachen Mithören bis hin zum umfassenden Lauschangriff. Teuer erworbenes Know-how fließt binnen weniger Sekunden und beinahe spurlos an unberechtigte Nutzer ab.

Das „Abschöpfen" von Informationen und Know-how gehört heute zu den „normalen Geschäftspraktiken" weltweit. Die Anzahl bekannt gewordener Delikte gegen das Know-how deutscher Unternehmen (Verletzung geistigen Eigentums / Patente) stieg in den vergangenen drei Jahren um knapp 40% an,

„Der Mensch ist das wichtigste Glied in der Sicherheitskette. Alle technischen Maßnahmen und Sicherheitsregeln nutzen nichts, wenn die Menschen sie nicht umsetzen. Es gilt somit jeden einzelnen Mitarbeiter für die Sicherheit im Unternehmen zu sensibilisieren. Neben technischen Angriffen, die teilweise mit Tools wie Firewalls und Virenscannern abgewehrt werden können, gibt es auch eine Reihe von Angriffsarten, die gezielt menschliche Schwächen ausnutzen."

Klaus Schimmer, SAP

Wirtschaftsspionage um über 20%. Das Vorgehen der Angreifer variiert, aber es lässt sich in zwei wesentliche Felder kategorisieren, das legale der Competitive Intelligence (CI) und das nicht-legale der Spionage. Wo genau die Grenze verläuft, dürfte umstritten sein, denn was in einem Land noch erlaubt ist, ist in einem anderem schon verboten, jedoch wird in der Spionage verstärkt auf elektronische Abhörtechniken gesetzt.

Bei solchen Zuständen, die nicht nur Zyniker an die Praktiken der beiden Protagonisten der berühmten Comicserie „Spy vs. Spy" des berüchtigten MAD Magazins erinnern, muss die Frage gestellt werden, wie man sein Hab und Gut schützen kann, genauer gesagt sein Know-how. Die Deutsche Risikoberatung propagiert ein wissensbasiertes Risikomanagement. Haben Sie schon einmal eine Wissens- und Know-how-Schutzinventur gemacht? Wenn nicht, dann ist es höchste Zeit aktiv zu werden. Neben dem zu empfehlenden Schutz vor elektronischer Ausspähung durch eine entsprechende architektonische Gestaltung und den Einsatz von Lauschabwehrteams (Sweep-Team) sollten zum Beispiel die Möglichkeiten der Sicherung von impliziten (im Kopf vorhandenen) und expliziten (mit Hilfe von Technologien) Wissens durch organisatorische, rechtliche und technische Maßnahmen in Betracht gezogen werden, auch gegen das so genannte Socail Engineering. Letztlich ist, um sich konkret gegen Competitive Intelligence und Spionage zu schützen, der Aufbau eigener Counter-Intelligence Einheiten ratsam.

Die Brisanz dieses Themas wird auch in Zukunft seine Aktualität bewahren. Als Anstoß für neue Lösungen und Denkansätze soll auch die Veranstaltung des Arbeitskreis für Unternehmenssicherheit (AKUS) „Informations- und Know-how-Schutz in Unternehmen" dienen, die am 14. Mai 2007 in Berlin stattfindet. Hier wird Interessenten die Möglichkeit geboten, sich ausgiebig mit dieser Thematik zu beschäftigen. Die geladenen Sprecher referieren zu folgenden Themen:

- Die Bedeutung von Know-how für die Berliner Wirtschaft
Volkmar Strauch, Staatssekretär in der Senatsverwaltung für Wirtschaft, Technologie und Frauen

- Aktuelle Entwicklungen im Bereich Informationsschutz
Maxim Worcester, Geschäftsführer Control Risks Deutschland GmbH;

- Aktueller Stand von Wissenschaft und Technik bei der Abwehr von Lauschangriffen
Peter Mnich, Die Wissensschützer;

- Wie verhindert man den Missbrauch von Informationen?
Carsten Baeck, Geschäftsführer DRB Deutsche Risikoberatung GmbH

- Know-how als geistiges Schutzrecht?
Katja Schubert, FORGS Forum für geistige Schutzrechte

- Social Engineering – was Mitarbeiter Wissen müssen, um solche Angriffe auf das Unternehmen zu erkennen und abwehren zu können.
Klaus Schimmer, Security Marketing Manager SAP AG

- Erfahrungen aus einer Informationssicherheits-Zertifizierung nach ISO 27001 und BSI-Grundschutz
Timo Kob, Vorstand HiSolutions AG

Carsten Baeck, Geschäftsführer DRB Deutsche Risikoberatung GmbH und Vorsitzender des AKUS Berlin-Brandenburg

AKTUELLE TERMINE

14.5.	Informations- und Know-how-Schutz in Unternehmen	Berlin