Management

Martin Scholl Die ZKB hat einen neuen Chef – einen, der den Betrieb seit seiner Lehrlingszeit kennt. **Seite 25**

Geheimes wird zu Allgemeingut

WERKSPIONAGE Im globalen Wettbewerb wird die Konkurrenz zunehmend schärfer beobachtet. Mitunter mit unfeinen oder sogar kriminellen Methoden. Wie können Schweizer KMU ihre Geschäftsgeheimnisse besser schützen?

KATRIN PIAZZA

Wer genau wissen möchte, was seine Konkurrenten so treiben, wird in seiner Recherchierlust vom Gesetz beschränkt: Artikel 273 des Schweizerischen Strafgesetzbuches verbietet das Ausspionieren oder Weitergeben von Fabrikations- oder Geschäftsgeheimnissen ausdrücklich.

Trotzdem ist kriminelles Auskundschaften – speziell via Internet – geradezu en vogue. Diesen Eindruck vermitteln zumindest die Halbjahresberichte der Melde- und Analysestelle Informationssicherheit des Bundesamtes für Polizei: Im zweiten Halbjahr 2006 wurden – neben der fast schon als alltäglich erscheinenden Internetkriminalität – erstmals gezielte Spionagefälle gegen Schweizer Firmen registriert. Ziel der Attacken, so der Bericht, seien unter anderen Unternehmen, die mit Aufträgen der Regierung betraut waren, und solche der Rüstungsindustrie.

Risiko wird unterschätzt

«Und was geht mich das an?», mag sich der durchschnittliche Chef eines Schweizer KMU fragen. Studien von Ernst & Young und PriceWaterhouseCoopers haben kürzlich gezeigt, dass das Risiko Wirtschaftskriminalität in den Chefetagen generell unterschätzt wird. «Grundsätzlich kann jedes Unternehmen, das über einen Wissensvorsprung verfügt, zum Ziel nachrichtendienstlicher Aktivitäten werden», stellt Hansruedi Stadler klar, «unabhängig von Grösse, Branche oder Marktpräsenz.»

Bis zu seiner Pensionierung im letzten Dezember hat Stadler als Leiter Kommissariat Ost im Inlandnachrichtendienst die Aktivitäten fremder Offensivdienste beobachtet. Die meisten Länder forderten ihre Geheimdienste offiziell und ausdrücklich auf, auch zugunsten der heimischen Wirtschaft zu arbeiten. «Mit dem klar definierten Ziel, für einen bestimmten Industriebereich Informationen zu beschaffen.»

Für Nat Bächtold, Berater bei der Zürcher Kommunikationsagentur Richterich & Partner und erster Deutschschweizer Absolvent der französischen Wirtschaftsschule «École de guerre économique», ist klar, dass um wichtige Informationen längst mit harten Bandagen gekämpft wird. Wer sich auf fremde Märkte bewegen wolle, müsse sich bewusst sein, dass die Mitkonkurrenten dort möglicherweise andere Vorstellungen davon hätten, was im Wirtschaftsleben erlaubt und anständig sei.

BILDERBOX

Es muss nicht immer Hightech sein – findige Betriebsspione werden auch in Abfallsäcken fündig.

Konkurrenzanalyse wird mit mitunter unzimperlichen Methoden betrieben, wie der Schweizer Stefan Michel bestätigt, der auch Assistenzprofessor für Marketing an der Wirtschaftsuniversität Thunderbird in Gledale, Arizona, ist: «Einiges im Marketing lässt sich schwer überprüfen.» Bei den komplexen, vielschichtigen und von verschiedenen Interessen und Abhängigkeiten geprägten Beziehungen könne «von der höflichen Anfrage bis zur Bestechung» alles drin sein, weiss Michel.

Sträfliche Sorglosigkeit

Wie im Spionagekrimi muss es bei der Konkurrenzbeobachtung nicht gerade zugehen – vielfach sind die Unternehmen selbst im Umgang mit ihren sensiblen Daten geradezu sträflich arglos. Stadler und Michel zählen bekanntere Sünden auf, wie das unbekümmerte Telefongespräch im öffentlichen Raum, der mit Kundendaten vollgepackte Laptop im Hotelzimmer oder die leichtfertige Prahlerei unter vermeintlichen Kollegen an der Fachmesse.

Dass sich aber auch die Festplatte des Kopiergeräts, die im Schulungsraum zurückgelassene Flipchart oder der ausrangierte Geschäftscomputer in den richtigen – oder besser gesagt: falschen – Händen in wahre Fundgruben verwandeln können, dürfte noch nicht bis in jedes Sicherheitskonzept eingeflossen sein.

Zwar macht sich ebenso strafbar, wer in fremden Papierkörben wühlt oder falsche Tatsachen vorspiegelt, um an Informationen zu gelangen – Personen, die dieses Risiko gegen gutes Geld auf sich nehmen, lassen sich jedoch finden. Unnötiger Aufwand, meint Bächtold: «Mit genügend Akribie, Zeit und Finanzen lässt sich fast jede Information auf legalem Weg recherchieren.»

Schliesslich sind heute sehr viele Unternehmensinformationen frei zugänglich, teilweise zwar kostenpflichtig, etliche jedoch gratis: Medien- und Wirtschaftsdatenbanken, Homepages, branchenspezifische Publikationen, Newsletter, und Investorenbriefe sind offene, zugängliche Quellen. «Diese Instrumente werden noch viel zu wenig genutzt», glaubt Bächtold. Der Kommunikationsfachmann plädiert für einen bewussteren Umgang mit Informationen. «Viele, vor allem kleine Unternehmen, glauben noch immer, der Wettbewerb beschränke sich auf Preis und Qualität.»

FAKTEN

Spionageabwehr für den Hausgebrauch

Vorgehen Wie lässt sich aus der Masse das relevante Stückchen Wissen herausfiltern? Die heutige Informationsflut stellt auch Geheimdienste vor Probleme, bestätigt Hansruedi Stadler, der ehemalige Leiter Kommissariat Ost im Inlandnachrichtendienst: «Deshalb gehen die Akteure, die sich nachrichtendienstlicher Methoden bedienen, umso gezielter vor.» Das heisst: Sie lokalisieren Wissensträger und prüfen sie systematisch auf Schwachstellen. Diese müssen nicht immer materieller oder beruflicher Natur sein, sondern können auch in persönlichen Neigungen oder Hobbys der betreffenden Personen gefunden werden. «Gefährdet sind die Frustrierten», weiss Stadler. Wer unter Mangel an Anerkennung leide, sich ungerecht behandelt oder schlecht entlöhnt wähne, sei tendenziell anfällig für Aufmerksamkeit von aussen, weshalb Stadler ein gutes Unternehmensklima für eine wesentliche Grundlage eines effizienten Sicherheitskonzeptes hält.

Drei Punkte Wie ein effizientes Sicherheitskonzept erstellt wird:
1. Schützenswerte Informationen und deren Träger im Unternehmen definieren.
2. Mitarbeitende für Sicherheit sensibilisieren und verbindliche Verhaltensregeln aufstellen.
3. Eigene Schwachstellen regelmässig in Szenarien überprüfen. (Wie würde ich vorgehen, wenn ich mir selbst diese Information entlocken müsste?)

Bei Spionagverdacht: Dienst für Analyse und Prävention DAP, Bolligenstrasse 56, Bern, Tel. 031 322 45 11.

NACHGEFRAGT | **ANDRE JACOMET,** Managing Consultant Swiss Infosec, Bern

«Der Mensch ist das grösste Sicherheitsrisiko»

Sie spionieren im Auftrag von Firmenchefs die Sicherheitslücken in Betrieben aus. Wie viele KMU haben überhaupt ein effektives Sicherheitskonzept?
Andre Jacomet: Das ist je nach Branche unterschiedlich. In der Finanzbranche ist das Problem meist erkannt – in den meisten anderen Branchen tendiert das Bewusstsein gegen Null.

Wer ist besonders gefährdet?
Jacomet: Grundsätzlich jedes Unternehmen.Insbesondere die Biotechnologie und Hightech-Firmen, aber auch die Medizin, die Pharmabranche – alle, die Forschung betreiben – und dort werden die Informationen oft sogar geteilt anstatt geschützt, was den Missbrauch vereinfacht.

Muss denn jede Firma davon ausgehen, dass sie Daten besitzt, die andere interessieren?
Jacomet: Sie müssen sich fragen, was Ihren Unternehmenswert überhaupt ausmacht – und was Wert hat, kann gestohlen werden.

Einzelne Firmen haben schon stark in ihre IT-Sicherheit investiert. Reicht das?

ANDRE JACOMET

Jacomet: Es ist bekannt, dass Angriffe im so genannten Social Engineering-Bereich eine wesentlich höhere Erfolgschance haben als jeder Hackerangriff.

Das heisst, die Mitarbeitenden sind die Schwachstelle?
Jacomet: Der Mensch ist sicher das grösste Sicherheitsrisiko. Nicht einmal, weil er sich erpressen lässt oder böswillig ist, sondern weil er ungenügend geschult wurde, kein Problembewusstsein entwickelt hat und den Wert der Informationen nicht kennt.

Wie kann man vorbeugen?
Jacomet: Indem man Bewusstsein schafft – und das muss in der Unternehmensleitung beginnen. Danach durch Mitarbeiterschulung, neue Konzepte, computerbasiertes Lernen etc.

Was kann eine Firma tun, um die möglichen Lücken zu erkennen?
Jacomet: Oft herrscht Betriebsblindheit – dagegen kann ein externer Berater helfen, der innerhalb von ein paar wenigen Tagen das Unternehmen durchleuchtet und Sicherheitslücken eruiert.

Mit welchen Kosten muss ein 50-Personen-KMU rechnen für ein Grobkonzept eines externen Sicherheitsberaters?
Jacomet: Wenn man von Tagessätzen von etwa 1500 bis 2000 Fr. ausgeht, kostet eine erste Evaluation 4000 bis 8000 Fr.

INTERVIEW: THOMAS PFISTER

CHEFSACHE

Networking für Jungunternehmer


ADRIAN LIGGENSTORFER
Gründer und Präsident Pioneers' Club PCU, Zürich (www.pcunetwork.com).

Die Bedeutung sozialer Netze ist im Geschäftsleben traditionell gross. Früher bewegte man sich primär innerhalb eines natürlichen Netzwerks, in das man hineingeboren wurde. Im Zuge von Chancengleichheit und Anonymität erhöhte sich die soziale Mobilität zwischen den Schichten, und das Individuum tut gut daran, sein eigenes Netzwerk aufzubauen oder sich in bereits vorhandene Netzwerke einzugliedern. Was einst als Seilschaft und Nepotismus abqualifiziert wurde, erfährt unter der Bezeichnung «Networking» mittlerweile öffentliche Wertschätzung. Die Fähigkeit zum «Business Networking» gilt gar als Schlüsselkompetenz, und manche Experten schätzen das «Know-who» höher ein als das «Know-how». Erfolg beruht nie allein auf eigener Leistung; Bekanntheitsgrad und das entsprechende Image zählen zu den wichtigsten Faktoren.
Je nach Branche mangelt es Jung-

> «Vielen Jungunternehmern mangelt es weniger an Leistung als an Zeit und einem unterstützenden Netzwerk.»

unternehmern weniger an persönlicher Leistungsfähigkeit als an Zeit, finanziellen Mitteln und einem unterstützenden Netzwerk. Die Möglichkeiten der schnellen und zielgerichteten Kontaktaufnahme mit Experten, potenziellen Auftraggebern, Investoren, Mitarbeitern und Geschäftspartnern sind in den letzten Jahren immer vielfältiger geworden. Während sich früher in exklusiven Zirkeln beste Beziehungen knüpfen liessen, finden Jungunternehmer im Internet ein vielfältiges Angebot an virtuellen Businessclubs, die ohne weitere soziale Verpflichtungen die effiziente Aufgleisung eines Kontaktes bieten können, wohl aber kaum je ein persönliches Treffen ersetzen werden.

Für Jungunternehmer ist der Erfahrungsaustausch untereinander innerhalb eines Netzwerks von grossem Nutzen, denn niemand ist zum Unternehmer geboren und niemand kann sich zum Unternehmer ausbilden lassen, sondern ein jeder muss es mittels «learning by doing» erlernen. In einem Jungunternehmernetzwerk können Kooperationspartner gefunden und Synergien geschaffen werden, Projektteams branchenübergreifend zusammengestellt und Mentoren wie auch Türöffner getroffen werden.

Unabhängig welchen Netzwerks man sich bedient, erfolgreiche Akteure in sozialen Netzwerken gehen offen auf andere Menschen zu und investieren in jede einzelne Beziehung, denn Profiteure werden schnell entlarvt. «Man muss Menschen mögen» ist eine wichtige Grundhaltung. Anderseits kann ein allzu grosses Netzwerk kaum mehr in einem vernünftigen Zeitaufwand gepflegt werden und verkommt bald zu einem blossen Adressbuch ohne Beziehungen.