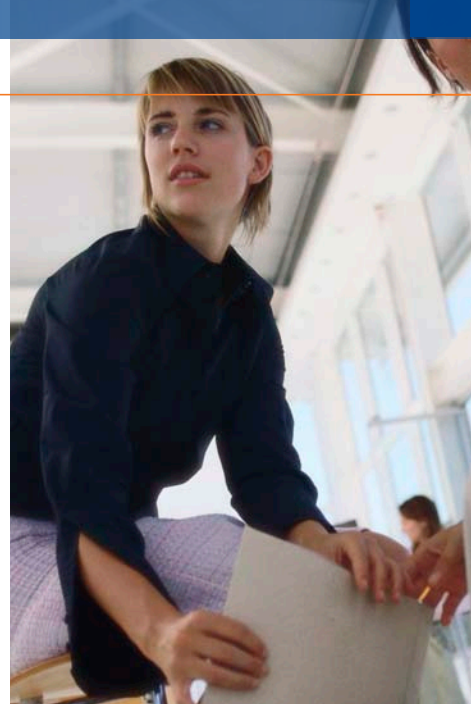


KONKURRENZSPIONAGE

Wenn der Mitbewerber zu viel weiss

Zum dritten Mal in Folge geht ein Auftrag an den gleichen direkten Mitbewerber, weil er offenbar mit dem Preis geringfügig tiefer lag. Man wird misstrauisch und fragt: Weiss die Konkurrenz mehr, als sie eigentlich dürfte? Wie man Antworten findet und vor allem wie man sich proaktiv schützt, erklärt Dr. Dr. Christof Müller, Experte für Wirtschaftskriminalität.



Herr Müller, was sagt Ihre Erfahrung: Wo schlagen Spione am häufigsten zu?

Müller: Man muss sich das zugrunde liegende Bedürfnis genauer ansehen: Der Wettbewerb findet heute auf globaler Ebene statt, enorm grosse Kontrakte werden international ausgeschrieben, mit einer entsprechenden Anzahl an Interessenten. Wenn beispielsweise eine staatliche Organisation mit einem neuen Funksystem ausgerüstet werden soll oder Aufträge für öffentliche Transportsysteme zu vergeben sind, geht es um riesige Summen. Daraus entsteht ein Interesse daran, Geheimnisse der Konkurrenz zu erfahren: Hat sie in einem bestimmten Bereich Vorteile, die mir im Wege stehen, diesen Auftrag zu bekommen? Wie sieht die Preisstruktur aus? Kann ich mehr über die Offertstellung herausfinden? In einer rigiden internationalen Ausschreibung haben

Sie eine einzige Möglichkeit zu bieten. Da will man wissen, wo man mit den eigenen Preisvorstellungen steht. Und Unternehmen kommen ins Grübeln, ob sie Kanäle besitzen oder öffnen können, die ihnen hier weiterhelfen. Damit sind wir im illegalen Bereich der Konkurrenzspionage angekommen.

Öffentliche Informationen

Im «illegalen Bereich» der Konkurrenzspionage – also gibt es auch eine «legale Spionage»?

Müller: Ja, wir sprechen dann von «Open Source Intelligence», also eine Konkurrenzanalyse aufgrund der öffentlich verfügbaren Informationen. Ein Beispiel: Ein Maschinenindustrieller möchte die Kapazität und die interne Preisstruktur seiner Konkurrenz kennen. Er beauftragt einen speziellen Dienstleister in diesem Bereich, der alles zugängliche Material zusammenträgt. Dazu

gehört vielleicht der Firmenprospekt, in dem die neue Fertigungsstrasse abgebildet ist. Dann fragt man beim Hersteller nach, was das Gerät leisten kann, und mit einer Hochrechnung ermittelt man beispielsweise die Investitionskosten, den Output und sogar den Break-even. Die Möglichkeiten solcher Dienstleister sowohl auf der technischen wie auch der betriebswirtschaftlichen Seite sind erstaunlich. Eventuell wird sogar versucht über eine Strohfirma eine Offerte einzuholen oder es werden Medienauftritte angeboten, welche vorgängig vor Ort besprochen werden müssen, um den Hintergrund und das Business der Firma besser kennenzulernen.

Womit ich einen beinahe schon gläsernen Mitbewerber vor mir habe, mit offen liegenden Schwachstellen...

Müller: Er fragt sich dann, wie er genau an dem Punkt getroffen werden kann, wo es am meisten schmerzt – und vermutet schnell, dass illegale Mittel im Spiel gewesen sein müssen, vielleicht eine Quelle aus seinen eigenen Reihen. Die meisten Unternehmen sind sich nicht bewusst, wie viel öffentliche Informationen sie preisgeben und wie diese ausgewertet werden können. Dass jemand akribisch hinter alle veröffentlichten Fotos geht, darauf ausmisst, beim Hersteller nachfragt und daraus verwertbare Schlüsse zieht, scheint den meisten noch unvorstellbar. Kein Zweifel: Wenn jemand laut «Geschäftsgeheimnisverrat» schreit, ist recht sicher etwas vorgefallen. Nur ob es legal oder illegal abgelaufen ist, bleibt die Gretchenfrage.

IM INTERVIEW



Christof Müller (Tel.: 071 245 04 66), Dr. oec. HSG und Dr. iur. HSG, war unter anderem Lehrbeauftragter für Interne Revision und Vollamtlicher Dozent Wirtschaftskriminalistik an der Universität St. Gallen (HSG) und führte bei PricewaterhouseCoopers die Abteilung Forensic Investigation. Heute ist er als Anwalt und Certified Fraud Examiner (CFE) in St. Gallen tätig. Dabei vertritt er als Krisenmanager in Fällen von Wirtschaftskriminalität geschädigte Unternehmen nicht nur vor Gericht, er übernimmt auch die «Spurensuche» und Beweissicherung – und erlebt so die gesamte Bandbreite der Konkurrenzspionage. www.acm-law.ch

Falls es sich tatsächlich um einen illegalen Vorgang handelt – wie läuft dieser ab? Gibt es «den typischen Fall»?

Müller: Illegal wird es, wenn jemand an eine Information kommen will, für die ein besonderer Geheimnisschutz besteht, wie es das Gesetz formuliert. Um diesen Sachverhalt überhaupt zu erfüllen, müssen bestimmte Massnahmen getroffen worden sein. Wer seine Offerte für eine Ausschreibung offen herumliegen lässt, kann sich später nicht über eine Verletzung des Fabrikations- und Geschäftsgeheimnisses beschweren. Ein Mitarbeiter, der solche Informationen weitergibt, kommt allenfalls mit dem Arbeitsrecht in Konflikt, nicht aber mit dem Strafrecht. Wurde ein solcher Schutzbereich aufgebaut, muss sich ein Angreifer fragen, wie er diesen durchbrechen kann. Nachrichtendienstlich unterscheidet man zwei Möglichkeiten – die menschliche und die technische, wobei noch immer gilt, dass der Weg über den Menschen einfacher funktioniert. Es wird ausgekund-

schaftet, wer Zugriff hat und bei wem es offene Flanken gibt. Zur tatsächlichen «Bearbeitung» des Komplizen in spe bestehen dann die klassischen zwei Möglichkeiten: Zuckerbrot oder Peitsche.

Der menschliche Faktor

Also muss man sich das tatsächlich wie in einem Spionage-Thriller vorstellen?

Müller: Nehmen wir das Bankgeheimnis – es gibt ja immer wieder einmal Vorwürfe, dass dieses verletzt wurde und Informationen nach aussen gedrungen sind. Wer wissen möchte, wie viel Geld sich auf einem bestimmten Konto befindet, kann versuchen, die Rechneranlage einer Bank zu knacken. Ein enorm hoher Aufwand, und bisher selten erfolgreich. Auch der französische Geheimdienst hat sich vor Jahrzehnten an der Verschlüsselung von Datenbändern einer Schweizer Bank die Zähne ausgebissen. Deswegen landet man schnell beim Personenansatz. Die Sonntagszeitung hat vor einiger Zeit

«Wer seine Offerte für eine Ausschreibung offen herumliegen lässt, kann sich später nicht über eine Verletzung des Fabrikations- und Geschäftsgeheimnisses beschweren.»

Ihr Ziel:

Führungsfachfrau/-mann mit eidg. Fachausweis

Wir öffnen Ihnen den Zugang in die Führungsetage. Gemeinsam mit erfahrenen Experten reflektieren und optimieren Sie Ihre fachlichen und sozialen Kompetenzen. Erlernen Sie die Kunst des Selbstmanagements und steigern Sie Ihre Leadership-Qualitäten!

Informieren Sie sich auch über unsere anerkannten Lehrgänge in den Bereichen:

- Führung und Organisation
- Marketing und Verkauf
- Kaufmännische Aus- und Weiterbildungen
- Informatik
- Sprachen
- Ausbildung für Auszubildende
- Wellness & Fitness Fachausbildungen

Melden Sie sich noch heute zu einer Informationsveranstaltung in Ihrer Nähe an und lassen Sie sich kompetent beraten – eine Ausbildung bei der Klubschule Business eröffnet Ihnen neue berufliche Perspektiven.

Schärfen Sie Ihr Profil.

Tel. 0844 373 654 oder
www.klubschule.ch/business

business



einmal eruiert, wie ein Zürcher Privatdetektiv Bankinformationen beschafft und dafür – in einem konkreten Fall – einen Bankmitarbeiter mit 100 Franken bestochen hat.

Wie finden Angreifer diese Informanten?

Müller: Bleiben wir bei den Bankern: Wenn nicht schon Beziehungen zu einem Mitarbeiter bestehen, wird ein Angreifer sich in den Bars rund um den Paradeplatz in Zürich tummeln. Dort sucht er denjenigen mit der dicksten Cohiba, der sich lautstark darüber beschwert, dass er so gut und gleichzeitig unterbezahlt ist. Wenn der Alkoholpegel steigt, wird der Angreifer Geschichten hören, anschliessend kann er den Mann verfolgen, um herauszufinden, wo genau er arbeitet, wo er wohnt, ob er ins Casino oder Bordell geht. Es werden Bedürfnisse erfasst, die man später vielleicht erfüllen kann. Die bittere Erkenntnis: Die Schwierigkeit für den Angreifer besteht eher darin herauszufinden, welche geheime Information er genau möchte, wo diese zu finden ist und wer darauf Zugriff hat. Ist dieser Teil einmal abgehakt, hat er die grösste Hürde wohl bereits überwunden.

Gibt es auch tatsächliche physische Einbrüche – oder sind diese Zeiten vorbei?

Müller: Wir alle haben Hollywood-Filme mit Einbrüchen in Hochsicherheitstrakte gesehen. Doch eben: Die meisten Unternehmen schützen sich gut, die technischen Möglichkeiten dazu sind heute vorhanden, warum sollte man also das Risiko auf sich nehmen, irgendwo einzusteigen? Viel eleganter und vor allem gefahrloser ist es für einen Angreifer, bei Tag durch die Vordertür zu laufen oder noch besser, sich das gewünschte Teil herauszutragen zu lassen. Das vergessen die Unternehmen leider allzu oft: Sie vertrauen ihren Mitarbeitern recht vorbehaltlos, ohne viel über sie zu wissen. Verstehen Sie mich nicht falsch, ich propagiere keine Misstrauenskultur. Doch ich halte es für keinen Fehler, sich die ganz normalen, bekannten Fakten über seine Mitarbeiter öfter mal anzusehen, etwa wer wie oft abgemahnt wurde oder beispielsweise auch, welche Hobbys die Leute haben.

Gibt es den typischen «Risiko-Mitarbeiter»?

Müller: So würde ich das nicht sagen – doch die Unternehmen verlieren hier manchmal das Mass. Während man sich sehr wohl überlegt, wen man am Abend mit der Geldkassette zur Bank schickt, geht man bei der Vergabe von Zugriffsrechten im Firmennetzwerk völlig sorglos um.

Auf Spurensuche ...

Wenn ein Unternehmen befürchtet, Opfer von Konkurrenzspionage geworden zu sein – wie geht es weiter vor?

Müller: Man geht schnell davon aus, von einem Mitarbeiter verraten worden oder Opfer eines Hacker-Angriffs geworden zu sein, wenn man das Gefühl hat, dass der Mitbewerber zu viel weiss. In dieser Situation braucht man ein Ziel: Will ich wissen, ob tatsächlich Informationen abgeflossen sind? Oder will ich mich proaktiv darum kümmern, dieses Gefühl künftig nicht mehr haben zu müssen, und mein System entsprechend verbessern? Wer sich für den Rückblick entscheidet und Antworten sucht, muss Beweise finden. Und das gestaltet sich schwierig, wenn sich der Täter nicht in irgendeiner Form selbst verrät.

Das klingt desillusionierend...

Müller: Richtig, doch ohne ein Geständnis oder einen Zufallstreffer läuft nur sehr, sehr selten etwas. Die Erfahrung zeigt: Eine kleine Chance bleibt, wenn man einen Anfangsverdacht hat und weiss, wohin man schauen muss. Wenn die Information nicht an einem zentralen Ort geschützt war, sondern beispielsweise auf mehreren Servern – mit den dazugehörigen ungeschützt aufbewahrten Backup-Medien – zur Verfügung stand, können sie schlichtweg gleich aufgeben.

Also sollte ein betroffenes Unternehmen vor allem dafür sorgen, nicht noch einmal betroffen zu sein...

Müller: Es sollte eine Risikosensibilisierung für die Zukunft stattfinden. Bestehende Schwachstellen im System sind zu erkennen und schnell zu beheben. Sonst sieht man, bildlich gesprochen, bei der Suche nach dem Übeltäter dem Badewasser beim Auslaufen zu, statt den Stöpsel in den Abfluss zu stecken. Man sollte das «Need-to-

know»-Prinzip einführen, also fragen, wer auf welche Informationen Zugriff braucht. Digitale Daten sind oft an mehreren Orten abgelegt, solche Redundanzen sollten wenn möglich eliminiert werden. Grundsätzlich müssen die Gebäudesicherung und die IT-Security auf dem neuesten Stand sein. Auch Backups müssen zwingend ins Konzept einbezogen werden: Alle Sicherheit ist dahin, wenn das Backup-Tape mit den sensiblen Daten frei zugänglich ist.

Auch KMU betroffen

Gibt es Branchen, die besonders betroffen sind?

Müller: Dort, wo das Geld liegt, findet man auch das Risiko. Man kann das kaum von der Branche abhängig machen, ausgeprägtes technisches Know-how ist für die Konkurrenz immer von Interesse. Nehmen Sie unsere Textil-Industrie in der Ostschweiz, die unter anderem Hochleistungssegele für die Alinghi herstellt – plötzlich muss man sich auch auf absolutem KMU-Niveau Gedanken darüber machen, ob man sich ausreichend geschützt hat. Deswegen gebe ich allen Verantwortlichen den Rat: Sie kennen Ihren Betrieb, denken Sie doch einmal sozusagen mit einer schwarzen Seele, wo Sie angreifen würden. Und schon wissen Sie, wo Sie den grössten Handlungsbedarf haben.

Lässt sich der Schaden beziffern, der in der Schweiz durch Konkurrenzspionage entsteht?

Müller: Nein. Selbst wenn ein Fall aufgedeckt wird, wird er wohlweislich unter Verschluss gehalten. Erstens ist es oft schwer, strafrechtlich etwas durchzupeitschen, und zweitens scheut man die damit verbundene Öffentlichkeit. Meistens gibt es sogar noch eine ordentliche, keine fristlose Kündigung des Mitarbeiters, und dann eben die Freistellung, um allen möglichen PR-Desastern aus dem Weg zu gehen. Betroffene Unternehmen neigen leider dazu, ein bis zwei Jahre viel Geld in Sicherheit zu investieren, um sich dann so geschützt zu fühlen, dass sie alle Vorsicht wieder vergessen. Doch solche Investitionen müssen kontinuierlich erfolgen, Sicherheit als Thema tritt nicht zyklisch auf.

Herr Dr. Dr. Müller, herzlichen Dank für dieses spannende Gespräch!

tw ◆