

Späher der Konkurrenz

Die Zahl der Fälle von Konkurrenzausspähung und nachrichtendienstlicher Aufklärung zum Schaden österreichischer Unternehmen hat zugenommen. Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung macht gefährdete Unternehmen auf diese Gefahren aufmerksam.

Die U-Bahn fährt in der Station. Die Türen öffnen sich, Leute steigen ein und aus, die Türen schließen sich wieder. Hunderte Male am Tag, 365 Tage im Jahr, viele Jahre hindurch. Funktioniert dies einmal nicht, sind Verkehrsverzögerungen die Folge, Termine werden versäumt und Fahrgäste sind aufgebracht. Dieses hohe Maß an technischer Reife ist für uns zur Selbstverständlichkeit geworden. Österreichische Unternehmen haben maßgeblich Anteil an dem, was nach jahrelanger Forschung und Entwicklung zum Standard geworden ist. Viele mittelständische Unternehmen haben ihr Know-how gut vermarktet und sind am internationalen Markt oft besser vertreten als am heimischen.

Diese Entwicklung kann empfindlich gestört werden: In den letzten Jahren sind immer mehr Fälle von Wirtschaftsspionage bekannt geworden, die österreichischen Unternehmen beträchtlichen Schaden zugefügt haben.

Ein vor Jahrzehnten in Österreich gegründetes Unternehmen produziert automatische Schließsysteme und ist ein wichtiger Arbeitgeber in einem wirtschaftlich weniger entwickelten Gebiet in Österreich geworden. Seine Produkte haben eine hohe Funktionssicherheit, dadurch hat das Unternehmen internationale Bedeutung erlangt; die Aufträge kommen hauptsächlich aus dem Ausland. Die 700 Mitarbeiter konstruieren und produzieren ausschließlich in Österreich. Nach mehreren Umstrukturierungen steht das an der Börse notierte Unternehmen in mehrheitlich ausländischem Besitz. Auffassungsunterschiede und Meinungsverschiedenheiten in der Betriebsführung haben einen leitenden Mitarbeiter bewogen, das Angebot eines fernöstlichen Investors anzunehmen und sich von dem Unternehmen zu trennen. Der Manager gründete in der Nähe seines früheren Arbeitgebers ein Ingenieurbüro mit zehn Mitarbeitern und wurde im selben Marktsegment tätig. Er warb ehemalige Kollegen aus seinem früheren Unternehmen



Ausspähen von wirtschaftlichem Know-how: Die Zahl der Fälle von Wirtschaftsspionage hat in Österreich zugenommen.

ab, ließ sich Konstruktionspläne von ihnen übermitteln und bezahlte ihnen um 30 Prozent mehr Gehalt. Unter Umgehung des Patentrechts konstruierte er die gleichen Schließsysteme spiegelverkehrt. Die Herstellung erfolgte in Asien – zu einem Bruchteil der Produktionskosten in Österreich. Die Angebote konnten damit um 50 bis 60 Prozent unterboten werden. Der Manager kam so zu Aufträgen, auf die seine frühere Firma gehofft hatte. Wesentlich waren dabei auch die persönlichen Kundenkontakte, die er über seine jahrzehntelange Tätigkeit bei seinem früheren Arbeitgeber aufgebaut hatte. Dieser musste aufgrund des Auftragsrückgangs die Produktion reduzieren und Mitarbeiter abbauen. Für die betroffene Region ist jeder verlorene Arbeitsplatz ein Problem.

In einem anderen Fall erschlichen sich die Vertriebspartner eines österreichischen Maschinenherstellers nach und nach Konstruktionsunterlagen und begannen mit einem asiatischen Partner eine eigene Produktion. Kurze Zeit später etablierte sich der neue Hersteller in Österreich und bot baugleiche Maschinen am europäischen Markt zu weniger als dem halben Preis an. Der Maschinenhersteller hat deshalb mit wirtschaftlichen Problemen zu kämpfen.

Know-how-Abschöpfung. Seit einigen Jahren häufen sich Vorfälle, die darauf abzielen, in Österreich entwickelte Technik und hier erworbenes Know-how abzuschöpfen und in Billigproduk-

tionsländern gewinnbringend zu verwerten. Wesentlich ist in vielen Fällen das Verhalten der eigenen Mitarbeiter oder von Geschäftspartnern, die oft wesentliche Bestandteile der Unternehmensbasis sind. Mitarbeiter können erstes Ziel sein, um an geschützte Information eines Unternehmens zu kommen. Oft sind sie sich dessen nicht bewusst und nicht darauf vorbereitet, wie dies rechtzeitig erkannt und abgewehrt werden kann.

Die sich rasch verändernden wirtschaftlichen Gegebenheiten haben es vielen Unternehmen schwerer gemacht, sich am globalen Markt zu behaupten. Staatliche Nachrichtendienste, die ihre Ressourcen zur Zeit des Kalten Krieges auf gegnerische militärische Bündnisse konzentriert haben, widmen sich heute mehr der Unterstützung nationaler wirtschaftlichen Interessen und fördern Unternehmen ihres Landes, indem sie ihnen Informationen zur Verfügung stellen oder gegen Konkurrenzunternehmen agieren.

Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) hat sich mit diesem immer größer werdenden Problem auseinandergesetzt und festgestellt, dass viele Marktsegmente in Österreich von Spionage bedroht sind. Nachrichtendienstliche Aufklärung (Wirtschaftsspionage) ist meist anders gelagert als Konkurrenzausspähung, die sich in der Regel auf nur ein Unternehmen oder bestimmte Produkte konzentriert. Nachrichtendienste sind darauf bedacht, Mitarbeiter von Unternehmen nicht abzuwerben, sondern in bestimmte Positionen zu bringen und dann über Jahre und Jahrzehnte hindurch abzuschöpfen. Ziel ist in erster Linie, Forschungs- und Entwicklungsdefizite für zivil- oder militärisch-industrielle Bereiche auszugleichen. Der Schaden entsteht daher nicht immer unmittelbar und ist oft nicht auf einzelne Unternehmen beschränkt. Wie viele andere Geheimdienste hat der russische Auslandsaufklärungsdienst SWR die gesetzliche



Werden wichtige Informationen eines Unternehmens nicht mit der notwendigen Vertraulichkeit behandelt, kann das für die Firma fatale Folgen haben.

Verpflichtung, wirtschaftliche Aufklärung in anderen Ländern zu betreiben und auch die britische Auslandsaufklärung ist dazu verpflichtet.

„Echelon“. Das Europäische Parlament hat 2001 eine Untersuchungskommission eingesetzt, die die Existenz eines geheimen Satellitenabhörsystems namens „Echelon“ erkunden sollte. Das System wurde von den USA, Großbritannien, Kanada, Neuseeland und Australien in den 70er-Jahren als technisches Aufklärungssystem gegen die damaligen Warschauer-Pakt-Staaten eingerichtet, ist aber nach wie vor in Verwendung. Es ist in der Lage, weltumspannend Telefonate, E-Mails und Fax-

abzufangen und mit speziellen Computerprogrammen geschriebene Texte nach Schlüsselwörtern zu durchsuchen oder Stimmen von Topzielen zu erkennen.

Nach dem Untersuchungsbericht der Kommission wird das System heute zur Bekämpfung der internationalen organisierten Kriminalität, des Drogen-, Menschen- und Waffenhandels, der Proliferation und gegen den internationalen Terrorismus eingesetzt. Bis zum Terroranschlag auf das New Yorker *World Trade Center* im Jahr 2001 soll es Schätzungen zufolge zu 40 Prozent für Wirtschaftsspionage verwendet worden sein. James Woolsey, bis 2005 Direktor des US-amerikanischen Nachrichten-

dienstes *CIA (Central Intelligence Agency)*, bestätigte den Bericht der Untersuchungskommission als richtig und begründete die von den USA betriebene Wirtschaftsspionage damit, dass einige europäische Unternehmen im Verdacht stünden, Bestechungsgelder im Zusammenhang mit großen internationalen Aufträgen zu bezahlen. Ex-US-Präsident Bill Clinton hatte schon Anfang der neunziger Jahre zum Ausdruck gebracht, dass ihm Wirtschaftsspionage ein besonderes Anliegen sei.

Technische Lauschangriffe und das Abhören von Gesprächen sind meist nur detaillierte oder ergänzende Ausspähungsmethoden. Eine wesentlich größere Gefahr geht von bewusstem oder unbewusstem menschlichen Fehlverhalten aus. Werden essenzielle Informationen eines Unternehmens nicht mit der notwendigen Vertraulichkeit behandelt oder werden Mitarbeiter in vertrauensvollen Positionen angeworben, kann das im Einzelfall fatale Folgen haben. Gut geschützte Unternehmen haben daher entsprechende Vorsichtsmaßnahmen getroffen, um ungewollten Informationsabfluss rechtzeitig zu erkennen.

Von Ausspähung können aber nicht nur Großunternehmen betroffen sein. Ein Softwareentwickler, der einen Großauftrag mit einem oder zwei Programmierern erfüllt, könnte beispielsweise sehr schnell in wirtschaftliche Turbulenzen geraten, wenn ihm einer oder beide Mitarbeiter von einem Konkurrenzunternehmen an- oder abgeworben würden.

Hohe Dunkelziffer. Die Zahl von Ausspähungsdelikten ist im Verhältnis zu anderen kriminellen Delikten relativ gering. Ist aber ein Unternehmen davon betroffen, ist der Schaden meist um ein Vielfaches höher und kann bis zum Ruin führen. Ist der Schaden gering, haben betroffene Unternehmen meist kein Interesse, damit Gerichte oder Behörden zu befassen. Im Rahmen einer Schadensbegrenzung werden oft Lösungen gefunden, die dem Unternehmen nicht noch zusätzlichen Schaden zufügen. Bei Wirtschaftsspionage bzw. Konkurrenz ausspähung ist daher von einer hohen Dunkelziffer auszugehen.

Eine Studie der Universität Lüneburg geht von einem Schaden in Höhe von 50 Milliarden Euro für die Wirtschaft in Deutschland durch „unfreundlichen Informationsabfluss“ aus. Auf Österreich bezogen, liegt der Schaden bei 5 Milliarden Euro. Gefährdet sind vor allem Unternehmen, die Forschung und Entwicklung betreiben.

BVT

Partner der Wirtschaft

Mitarbeiter des Referats „Proliferation und Nachrichtendienst“ des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung haben ein Awareness-Programm entwickelt, mit dem gefährdete Unternehmen auf diese Gefahren aufmerksam gemacht werden sollen. Es bezieht sich in erster Linie darauf, welche Spionagemethoden von professionellen Nachrichtendiensten angewendet werden und erklärt, wie die Anwerbung von Mitarbeitern systematisch vorbereitet und durchgeführt wird. Darüber hinaus wird auf die Möglichkeit hingewiesen, Mitarbeiter



eines Unternehmens oder Neubewerber mit ihrer Zustimmung einer gesetzlich geregelten Sicherheitsüberprüfung zu unterziehen. Die Gefahr, dass Personen, die ein Sicherheitsrisiko darstellen, in verantwortungsvolle Positionen kommen, kann dadurch reduziert werden.

Das BVT und die Landesämter für Verfassungsschutz und Terrorismusbekämpfung (LVT) stehen österreichischen Unternehmen als Partner zur Verfügung.

Unter anderem wurden Awareness-Veranstaltungen in mehreren Großunternehmen abgehalten. Weitere Unternehmen haben ihr Interesse an den Veranstaltungen bekundet.