Spionageangriffe bei Klein- und Mittelbetrieben

Die Bedeutung österreichischer Industrie- und Großunternehmen im internationalen Wettbewerb ist weitgehend bekannt. Weit weniger bekannt sind die Leistungen kleinerer und mittlerer Unternehmen in Österreich. Sie sind meist für die Entwicklung neuer Produkte oder neuer Techniken verantwortlich, die dann letztlich über internationale Multis vermarktet werden.

Entscheidend ist oft, wer mit einem neuen Produkt zuerst am Markt ist. Das bedeutet daher auch einen Wettlauf mit der Zeit. Ebenso sind die hohen Kosten für Entwicklungen entscheidend für den Verkaufspreis des Produkts. Durch einen Blick in die Karten seines Konkurrenten lassen sich solche Hürden aber manchmal umgehen.

Tausende von Angriffen auf Firmen Computer, die zu einem großen Teil auf solche Informationen gerichtet sind, machen dies deutlich. Weniger bekannt aber sind technische Lauschangriffe, über die illegal Informationen gesammelt werden. Der Markt für Abhörgeräte, die heute in guter Qualität spottbillig im Fachhandel zu haben sind, boomt.

Eine weit effizientere Art, Informationen unbemerkt aus einem Unternehmen zu schleusen, ist die Korrumpierung eines Mitarbeiters im Unternehmen, der Zugang zu entsprechendem Datenmaterial hat, oder direkt mit der Materie befasst ist. Wer sich darüber Gedanken zu machen beginnt, wird sich bald an das Sprichwort „Jeder ist käuflich, es ist nur eine Frage des Preises“, erinnern. Doch, ist es immer nur Bestechung, der Mitarbeiter verfallen können? Oft ist einfach die „berufliche Unzufriedenheit“ von Mitarbeitern als Risko zu sehen. Subjektiv empfundene Unterbezahlung, das Übergehen bei Beförderungen sowie die Nichtanerkennung von Leistungen sind nur einige von bekannten Gründen, mit denen ein derartiges Fehlverhalten gerechtfertigt wird.

Bedrohung für die Wirtschaft

Letztlich stellt sich aber die Frage, ob illegaler oder ungewollter Informations- oder Know-how-Abfluss wirklich eine Bedrohung für die österreichische Wirtschaft darstellt. Laut Kriminalstatistik der letzten Jahre, ist dies eindeutig nicht der Fall. Es sind jährlich weniger als einer Handvoll von Verdachtsfällen, die polizeilich aufgearbeitet werden. Offiziell kann daher von einer schwerwiegenden Bedrohung nicht ausgegangen werden.

880 Millionen Euro Schaden

Betrachtet man allerdings das Ergebnis anonymer Umfragen, sieht die Situation wesentlich anders aus. Der Fachbereich Risiko- und Sicherheitsmanagement der FH Campus Wien hat gemeinsam mit dem BM.I/ Bundesamt für Verfassungsschutz und Terrorismusbekämpfung im letzten Jahr eine Umfrage bei österreichischen Unternehmen durchgeführt. Beteiligt haben sich 220 Firmen. Daraus geht hervor, dass 31 % der befragten Unternehmen schon Opfer von Wirtschafts- und Industriespionage waren. Bei mehr als der Hälfte betrug der monetäre Schaden mehr als €100.000,- und bei 10 % mehr als € 1,5 Millionen. Für die Österreichische Wirtschaft entsteht durch Wirtschafts- u. Industriespionage ein hochgerechneter Schaden von jährlich ca. 880 Millionen Euro.

Dieses Ergebnis deckt sich weitgehend mit jenen großer Wirtschaftskanzleien, die solche Umfragen regelmäßig in westeuropäischen Industriestaaten durchführen. Es stellt sich daher die Frage, warum bei diesen Vorkommnissen so selten Hilfestellung seitens der Sicherheitsbehörden in Anspruch genommen wird.

Oft ist man sich gar nicht bewusst, dass dies überhaupt möglich ist und welche rechtliche oder technische Mittel den Behörden zur Verfügung stehen. Der möglicherweise zu erwartende Schaden an Reputation, der bei einer Anzeigeerstattung entstehen könnte, dürfte aber der eigentliche Grund dafür sein, warum Unternehmen den Weg zu Behörden scheuen.

An einem über Jahre hindurch dauernden Strafverfahren sind die meisten Unternehmensleitungen nicht interessiert. Zu groß ist das Risiko, dass sämtliche polizeilichen Ermittlungsergebnisse zugänglich gemacht werden müssen und damit innerbetriebliche Details öffentlich bekannt werden könnten.

Wie viele Fälle aus der Vergangenheit aber gezeigt haben, birgt eine oberflächliche Schadensbegrenzung oft eine Gefahr, die ein österr. Unternehmen mit Hilfe von Behörden rechtzeitig abwenden hat können:

Ein Mitarbeiter der Forschungsabteilung, der immer wieder Kontakt mit einem ausländischen Konkurrenzunternehmen gehabt hatte, hat sich von diesem anwerben lassen und gegen Bezahlung systematisch Forschungsergebnisse seines österreichischen Arbeitgebers verkauft. Sein „Nebenverdienst" betrug monatlich ein Mehrfaches seines offiziellen Gehaltes. Als seine „intensive Verbindung" zu dem Konkurrenten durch einen Zufall bekannt geworden ist, vereinbarte die Geschäftsleitung mit ihm eine einvernehmliche Lösung des Arbeitsverhältnisses. Einige Zeit nach dem Ausscheiden des Mannes aus dem Unternehmen war klar, dass der illegale Informationsfluss weiter ging und man suchte die Hilfe der Sicherheitsbehörde. Nach wochenlangen Ermittlungen stand letztlich fest, dass zwei weitere Mitarbeiter der Forschungsabteilung mit dem Ausgeschiedenen zusammen gearbeitet hatten und diesen weiter mit Daten und Informationen versorgt hatten.

Die hohe Dunkelziffer derartiger Vorkommnisse ist mit großer Wahrscheinlichkeit auch dafür verantwortlich, dass vielen schnell gewachsenen kleinen und mittleren Unternehmen meist nicht bekannt ist, mit welchen Mitteln versucht wird, illegal an Daten und Know-how zu kommen. Sie sind daher nicht immer vorsichtig genug und haben keine ausreichenden Schutzmechanismen installiert. So kann mit einer entsprechenden Überprüfung von Stellenbewerbern gegebenenfalls verhindert werden, dass jemand in ein Unternehmen eingeschleust wird, um an sein Know-how zu kommen. Das Verhalten der Mitarbeiter bei Kontakten mit Geschäftspartnern oder bei Reisen ins Ausland kann aber entscheidend dafür sein, ob ein Anwerbeversuch überhaupt erfolgt.

Eine zielgerichtete Sensibilisierung der Mitarbeiter kann solchen Versuchen vorbeugen. Ebenso sollte der Umgang mit elektronischen Endgeräten, Datenträgern und Hardcopies Verhaltensmaßregeln unterworfen sein, die ein hohes Maß an Sicherheit gewährleisten. Vor allem in Ländern mit anderen Rechtssystemen ist das Abhören von Telefongesprächen, das Mitlesen von Emails oder das Abfangen von Daten nicht an eine richterliche Bewilligung gebunden. Dies bedeutet, dass Polizei und Geheimdienst nicht nur alle über ein mobiles Endgerät (z.B. Smartphone) übertragenen Daten und Gespräche, sondern auch alle Standorte aufzeichnen. So kann während des gesamten Aufenthaltes in einem solchen Land ein Bewegungsbild des Nutzers hergestellt werden. Eine „zufällige Bekanntschaft" in einem Restaurant oder in der Hotelbar sollte deshalb immer auch unter diesen Gesichtspunkten gesehen werden.

• *Hubert Bartl*

Maßgebliche Bestimmungen im österreichschen Strafgesetzbuch

§ 122 - Verletzung eines Geschäfts- oder Betriebsgeheimnisses
(1) Wer ein Geschäfts- oder Betriebsgeheimnis (Abs. 3) offenbart oder verwertet, das ihm bei seiner Tätigkeit in Durchführung einer durch Gesetz oder behördlichen Auftrag vorgeschriebenen Aufsicht, Überprüfung oder Erhebung anvertraut oder zugänglich geworden ist, ist mit Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
(2) Wer die Tat begeht, um sich oder einem anderen einen Vermögensvorteil zuzuwenden oder einem anderen einen Nachteil zuzufügen, ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen.
(3) Unter Abs. 1 fällt nur ein Geschäfts- oder Betriebsgeheimnis, das der Täter kraft Gesetzes zu wahren verpflichtet ist und dessen Offenbarung oder Verwertung geeignet ist, ein berechtigtes Interesse des von der Aufsicht, Überprüfung oder Erhebung Betroffenen zu verletzen.
(4) Der Täter ist nicht zu bestrafen, wenn die Offenbarung oder Verwertung nach Inhalt und Form durch ein öffentliches oder ein berechtigtes privates Interesse gerechtfertigt ist.
(5) Der Täter ist nur auf Verlangen des in seinem Interesse an der Geheimhaltung Verletzten (Abs. 3) zu verfolgen.

§ 123 - Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses
(1) Wer ein Geschäfts- oder Betriebsgeheimnis mit dem Vorsatz auskundschaftet, es zu verwerten, einem anderen zur Verwertung zu überlassen oder der Öffentlichkeit preiszugeben, ist mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen zu bestrafen. Beide Strafen können auch nebeneinander verhängt werden.
(2) Der Täter ist nur auf Verlangen des Verletzten zu verfolgen.

§ 124 - Auskundschaftung eines Geschäfts- oder Betriebsgeheimnisses zugunsten des Auslands
(1) Wer ein Geschäfts- oder Betriebsgeheimnis mit dem Vorsatz auskundschaftet, daß es im Ausland verwertet, verwendet oder sonst ausgewertet werde, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen. Daneben kann auf Geldstrafe bis zu 360 Tagessätzen erkannt werden.
(2) Ebenso ist zu bestrafen, wer ein Geschäfts- oder Betriebsgeheimnis, zu dessen Wahrung er verpflichtet ist, der Verwertung, Verwendung oder sonstigen Auswertung im Ausland preisgibt.

§ 256 - Geheimer Nachrichtendienst zum Nachteil Österreichs
Wer zum Nachteil der Republik Österreich einen geheimen Nachrichtendienst einrichtet oder betreibt oder einen solchen Nachrichtendienst wie immer unterstützt, ist mit Freiheitsstrafe bis zu drei Jahren zu bestrafen.

§ 319 - Militärischer Nachrichtendienst für einen fremden Staat
Wer im Inland für eine fremde Macht oder eine über- oder zwischenstaatliche Einrichtung einen militärischen Nachrichtendienst einrichtet oder betreibt oder einen solchen Nachrichtendienst wie immer unterstützt, ist mit Freiheitsstrafe bis zu zwei Jahren zu bestrafen.