Sicherheitsrisiko Kopierer: Auf neuen Geräten werden alle Kopien auf einer Festplatte gespeichert. Sie sind somit abrufbar.

Schutz vor Ausspähung

Die Gefahr für ein Unternehmen, von einem fremden Geheimdienst oder einem Konkurrenten ausgespäht zu werden, ist groß. Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung sensibilisiert Unternehmen im Hinblick auf Wirtschaftsspionage und Konkurrenzausspähung.

Österreichische Unternehmen sind am globalen Markt gut vertreten, viele von ihnen sind seit Jahren und Jahrzehnten Marktführer in ihren Bereichen. Weniger bekannt sind jene kleinen und mittleren Unternehmen (KMU), die Nischenprodukte entwickeln und Forschungsarbeit auf höchstem Niveau betreiben. Ihre Leistungen bleiben oft der breiten Öffentlichkeit unbekannt, da der wirtschaftliche Erfolg sich erst bei den Auftraggebern oder Industriemultis einstellt. Wenn ein Autohersteller beispielsweise ein neues Bremssystem präsentiert, denkt in Wirklichkeit niemand daran, dass die Entwicklung vielleicht durch ein Kleinunternehmen erfolgt ist. Ebenso werden pharmazeutische Produkte sehr oft von Kleinunternehmen entwickelt und dann von bekannten Konzernen auf den Markt gebracht.

Solche großteils wirtschaftlich von ihren Auftraggebern abhängigen KMUs sehen sich oft mit der Tatsache konfrontiert, dass die von ihnen entwickelten Produkte oder Verfahren keinen unmittelbaren Abnehmer finden, ihre Ergebnisse dann aber in veränderter Form von einem anderen Konzern oder einem Konkurrenzunternehmen vermarktet werden. Das kann darauf zurückzuführen sein, dass Informationen illegal weitergegeben oder erschlichen wurden.

Ein geschädigtes Unternehmen kann Strafverfolgung verlangen und den entstandenen Schaden am Zivilrechtsweg einklagen. In der Praxis wird das aber oft nicht gemacht, weil das Verfahren zeit- und kostenintensiv und unter Umständen deshalb für das Unternehmen wirtschaftlich nicht verkraftbar ist.

Um derartige Situationen nicht entstehen zu lassen, sind Unternehmen, die über schützenswerte Forschungs- oder Entwicklungsergebnisse oder betriebliches Know-how verfügen, gut beraten, Maßnahmen zu treffen, die Schutz vor Ausspähung bieten.

Das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) beschäftigt sich seit 2006 mit der Bekämpfung und Verhinderung von Wirtschaftsspionage und Ausspähung und sammelt auch in anderen europäischen Ländern Erfahrungen über Methoden von Ausspähung. Ein- bis zweimal jährlich finden Expertentreffen des BVT mit Vertretern aller Landesämter für Verfassungsschutz und Terrorismusbekämpfung (LVT) statt. Ziel ist es, den Wissensstand der LVT-Mitarbeiter in allen Bundesländern auf gleichem Niveau zu halten.

Spionageabwehr. Entsprechend dem Inhalt des Regierungsprogramms* hat der österreichische Verfassungsschutz sich zum Ziel gesetzt, Spionageabwehr und -prävention im Sinn der österreichischen Wirtschaft zu verstärken.

FOTO: ALEXANDER TUMA

Mit USB-Sticks können Trojaner auf das Gerät gespielt und illegal Daten abgesaugt werden.

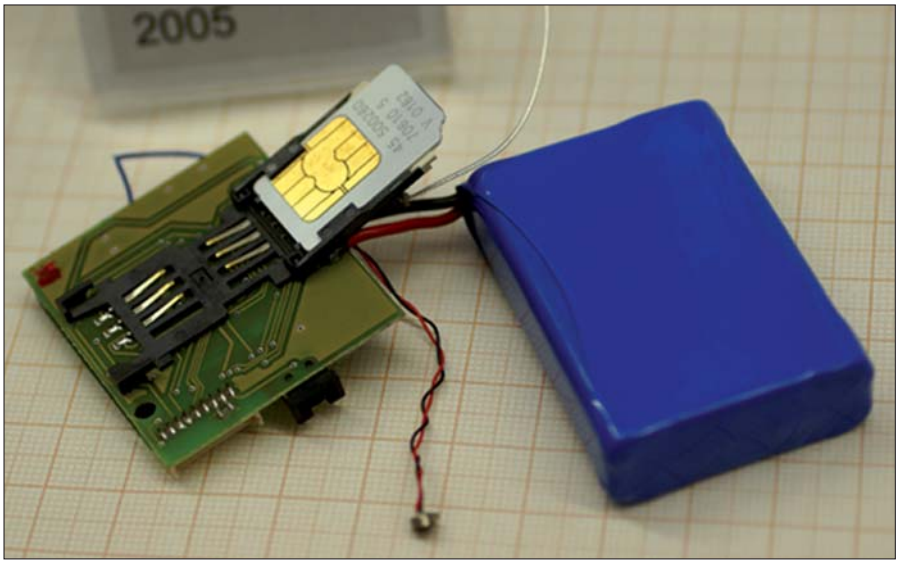
Foto: Privat

Das geschieht einerseits in der Bemühung, österreichischen Unternehmen als Ansprechpartner zur Verfügung zu stehen und Rechtsberatung in strafrechtlichen Belangen zu geben, andererseits in dem Bestreben, Unternehmen zu überzeugen, ihr Know-how zu schützen.

Bei einer Informationsveranstaltung des 2008 gegründeten Kompetenzzentrums für Umwelt- und Energietechnologie *ACT (Austrian Clean Technologies)* zum Thema „Umwelttechnik-Ausfuhren: Exporte durch Profi-Know-how absichern“, zu dem Firmen eingeladen waren, die schützenswerte Technologien und Entwicklungen im Ausland oder mit ausländischen Partner vermarkten, stellten Vertreter des BVTs und der *Internationalen Handelskammer (ICC)* die Gefahren dar, die zu ungewolltem Informationsabfluss füh-ren können.Die Ausführungen des BVT-Experten waren darauf ausgerichtet, Verantwortlichen solcher Unternehmen nahezubringen, welche Methoden Geheimdienste oder Konkurrenzunternehmen anwenden, um heimlich an schützenswerte Informationen eines Unternehmens zu kommen. Damit sollte das Management angeregt werden, Schutzmaßnahmen zu treffen.

Im Detail wurden die Unterschiede zwischen Wirtschaftsspionage und Konkurrenzausspähung erläutert: Wirtschaftsspionage ist die von ausländischen Geheimdiensten gegen österreichische Interessen betriebene wirtschaftliche Spionage und unter Konkurrenzausspähung versteht man die Ausspähung durch ein privates Unternehmen, meist im Mitbewerberbereich.

Außerdem wurden die technischen Möglichkeiten von Geheimdiensten zum systematischen Abhören von Kommunikationsstrecken dargestellt. Dazu gehören der Missbrauch von technischen Büroeinrichtungen (Kopierer, Telefone) und gezielt installierte



Ausspähung: GSM-Wanze, eingebaut in einem Mobiltelefon.

Abhöreinrichtungen. Erschreckend für die Teilnehmer war die Gefahr, die von alltäglichen technischen Geräten ausgeht und wie solche manipuliert werden können. Ein handelsübliches Handy oder ein Smartphone als Abhöreinrichtung oder für einen unbemerkten Datenabfluss zu missbrauchen, ist heute ebenso einfach wie ein GSM-Handy illegal abzuhören. Zudem birgt die Verwendung von Laptops oder Datenträgern Gefahren, die kaum bekannt sind.

Spione im eigenen Haus. Die wesentlich größere Gefahr geht von Personen aus, die im Unternehmen beschäftigt sind oder in enger Verbindung zum Unternehmen stehen (z. B. Geschäftspartner, Servicefirmen). In weit mehr als der Hälfte der Fälle waren Personen aus diesem Umfeld am illegalen Informationsabfluss maßgeblich beteiligt. Erläutert wurde, wie Geheimdienste oder Konkurrenzunternehmen an Betriebsangehörige herankommen und welche Schwachstellen sie ausnutzen, um sie zu missbrauchen und letztlich anzuwerben. Die Unternehmensführung sollte demnach angehalten sein, Verhaltensregeln für Mitarbeiter vorzugeben und sie zu sensibilisieren. Insbesondere wurde auf das Verhalten bei Geschäftsreisen ins Ausland hingewiesen. In Ländern mit anderen Rechtssystemen ist die Gefahr, einem staatlichen Geheimdienst ins Netz zu geraten, um vieles größer als in westlichen Industriestaaten.

Enormer Schaden. Ein Fall aus jüngerer Vergangenheit, durch den ein österreichisches Unternehmen großen wirtschaftlichen Schaden erlitten hat, weist zahlreiche Facetten auf, wie sie immer wieder vorkommen: Ein österreichisches Hightech-Unternehmen bezog das für die Herstellung von Spezialbeschichtungen notwendige Pulver von einer russischen Unternehmensgruppe, die auch in der Waffenproduktion tätig war. Das russische Unternehmen war an den Entwicklungen des österreichischen Unternehmens sehr interessiert und bot eine Beteiligung an, um den Zugang zu den begehrten Technologien zu finden. Die Österreicher lehnten dies stets ab, worauf die Preise für das Pulver erhöht wurden. Durch Zufall wurde der Unternehmensleitung ein Jahr später bekannt, dass der Leiter der Forschungsabteilung des österreichischen Unternehmens bei dem russischen Konkurrenten aus- und einging und man beendete das Arbeitsverhältnis einvernehmlich. Als das nunmehr sensibilisierte Unternehmen aber bald berechtigt annahm, dass weiterhin Informationen abfließen, schaltete es das LVT ein. Es stellte sich heraus, dass der bereits entlassene Leiter der Forschungsabteilung seine früheren Mitarbeiter weiter für den Zugriff auf Forschungsergebnisse missbraucht und er im Ausland ein Beratungsunternehmen gegründet hatte, über das er vom russischen Konkurrenten bezahlt wurde. Der Mann wurde festgenommen; drei Mitarbeiter des österreichischen Unternehmens wurden fristlos entlassen.

Die Anwerbung des Forschungschefs dürfte von russischen Geheimdienstmitarbeitern durchgeführt worden sein, die im Umfeld des russischen Konkurrenzunternehmens beschäftigt waren, wie das in strategisch wichtigen Unternehmen in Russland üblich ist.

Nachweisbar war auch, dass der letztlich gerichtlich verurteilte Forschungschef mehr als 90 Prozent eines äußerst kostenintensiven Forschungsprogramms und zahlreiche weitere Ergebnisse illegal aus dem Unternehmen geschleust und mit größter Wahrscheinlichkeit an die russische Konkurrenz verkauft hat.

Die Wahrscheinlichkeit, Opfer von Wirtschaftsspionage oder Konkurrenzausspähung zu werden, ist relativ gering im Verhältnis zur Gefahr, durch Wirtschaftskriminalität (Diebstahl, Betrug, Veruntreuung) geschädigt zu werden. Nach statistischen Berechnungen aus Umfragen bei Unternehmen ist die durchschnittliche Schadenshöhe bei Spionagedelikten aber 30-mal höher. Für ein KMU kann das existenzbedrohend sein.

Eine Studie der Universität Lüneburg beschreibt das von Wirtschaftsspionage und Konkurrenzausspähung ausgehende Gefährdungspotenzial für Deutschland mit etwa 50 Milliarden Euro. Im Verhältnis zur Bevölkerungsanzahl würde sie in Österreich demnach bei fünf Milliarden liegen. Schätzungen der Wirtschaftskammer belaufen sich auf drei Milliarden Euro. Repräsentative Berechnungen oder Statistiken existieren in Österreich nicht. Es ist jedoch davon auszugehen, dass es eine hohe Dunkelziffer gibt, die insbesondere darauf zurückzuführen ist, dass ein geschädigtes Unternehmen meist ausschließlich die wirtschaftliche Komponente sieht und lediglich um Schadensbegrenzung bemüht ist. Die Einschaltung von Sicherheitsbehörden wird meist nicht in Anspruch genommen, da eine Schädigung des Rufes des Unternehmens befürchtet wird. *H. B.*

**Regierungsprogramm für die XXIV. Gesetzgebungsperiode: A.3. Verstärkte Spionageabwehr und Spionageprävention: Der erfolgreiche Wirtschaftsstandort Österreich ist ein attraktives Ziel nachrichtendienstlicher Ausspähung. Anzustreben ist eine Adaptierung der entsprechenden Straftatbestände. Verstärkte Prävention durch die passende Information für Wirtschaft und Industrie ist notwendig, um Spionage zu verhindern bzw. frühzeitig und rechtzeitig zu erkennen.*

FOTO: KURT HICKISCH