Der frustrierte Wirtschaftsspion

Waren zu Zeiten des Kalten Krieges die klassischen Ziele der Geheimdienste die Ausspionierung von Militärgeheimnissen, bespitzeln heute Geheimdienste und Konkurrenten die nichts ahnende Konkurrenz. Die Verluste der durchleuchteten Firmen gehen in die Milliarden.

von Irena Ristic

Waren während des Kalten Krieges die Geheimdienste ausschliesslich auf das Ausspionieren von militärischen und politischen Zielen spezialisiert, weiteten sie nach dem Zusammenbruch des Ostblocks ihr Betätigungsfeld auf die Beschaffung von geheimen Wirtschaftsdaten aus. Es ist ein offenes Geheimnis, dass die «Secret Services» der USA und Grossbritanniens routinemässig auf diesem Gebiet mit ihrer heimischen Industrie zusammenarbeiten.

Doch auch die Dienste von Frankreich oder der Staaten des ehemaligen Ostblocks, wie zum Beispiel das russische FSB oder die rumänische Securitate, lauschen und klauen, wo es nur geht. In Zeiten wirtschaftlicher Stagnation wächst auch die Bereitschaft der Manager, sich geheime Daten bei der Konkurrenz zu besorgen, anstatt in kostenaufwändige Forschungsarbeiten zu investieren.

«Kein Unternehmen ist vor Wirtschaftskriminalität geschützt», warnt Dr. Maximilian Burger, Experte und Lehrbeauftragter für Wirtschaftskriminalität an der Uni Luzern (siehe Interview). «Jeder kann Opfer sein, unabhängig von der Grösse des Unternehmens», präzisiert er. Nur die wenigsten merken, wenn jemand auf der Leitung sitzt, sensible Daten mithört und aufzeichnet.

Laut einer Studie von Price Waterhouse Coopers waren 34 Prozent der europäischen Unternehmen in den vergangenen zwei Jahren von Wirtschaftskriminalität betroffen. Am meisten gefährdet sind Firmen der Pharma-, Computer-, Biotech- und Automobilindustrie. Gerade in diesen Bereichen entscheidet oftmals ein Forschungsvorsprung gegenüber der Konkurrenz über den Erfolg einer Unternehmung.

Hauptgefahr: Der frustrierte Mitarbeiter

Die Methoden sind vielfältig, doch wer meint, dass die meisten Informationen über hoch komplizierte technologische Systeme beschafft werden, der irrt sich. Es muss nicht gleich die Wanze unter dem Tisch des General Managers sein. Viele Informationen können problemlos über die firmeneigene Homepage abgerufen werden. So erstellen spezialisierte Beratungsfirmen aufgrund dieser «Open Source» völlig legal Konkurrenzanalysen für ihre Kunden.

Eine grosse Gefahr geht auch von enttäuschten und unzufriedenen Mitarbeitern aus. Sie haben als Beschäftigte des Betriebes direkten Zugang zu Informationen. Wirtschaftsspione nutzen ganz bewusst menschliche Schwächen aus und umgarnen ihre Opfer auf perfide Weise. Vorzugsweise in Gaststätten, Bars oder Fitnesscenter verwickeln sie ihre Opfer in vermeintlich harmlose Gespräche über den Job. Ganz nebenbei kommen sie so an firmeninterne Informationen des Arbeitgebers.

«Oftmals ist der zweite Mann hinter dem Big Boss der Frustrierte», erklärt Burger, «aber dieser weiss meist fast genauso viel wie sein vorgesetzter Manager.»

Oft werden auch gezielt Headhunter auf ausgesuchte Mitarbeiter angesetzt. «Es ist von vornherein klar, dass der angebliche Kandidat keine Aussicht auf einen Job hat. Der einzige Sinn und Zweck des Tuns einiger Headhunter ist die Konkurrenzspionage», weiss Burger aus seiner Berufspraxis zu berichten. Kommen die Angreifer auf diesem Weg nicht weiter, so verschaffen sie sich, als Putzfrauen oder Elektriker getarnt, ohne grosse Probleme Zugang zu den Büros. Zettel

im nicht geleerten Papierkorb, liegen gelassene Unterlagen auf dem Schreibtisch oder nicht gesicherte Laptops mit Finanzdaten sind eine regelrechte Einladung für Spione.

Konkurrenz hört mit

Technisch gesehen sind die Kommunikationsmittel Fax, Telefon oder elektronisch übermittelte Daten am meisten von einem Lauschangriff betroffen. So werden Millionen von Daten von der National Security Agency (NSA) über das globale Spionagesystem Echelon (siehe Kasten) analysiert und aufbereitet. In dem Moment, wo ein Wort aus einer speziellen Schlagwortliste in einem Gespräch auftaucht, wird das System aktiv und zeichnet die Verbindung auf. «Jedes Unternehmen wird seine Kommunikation mit moderner Kryptografie schützen müssen», sagt IT-Experte Edmund Lindau. Mit Hilfe der so genannten Public-Key-Kryptografie verwenden Versender und Empfänger einen privaten und einen öffentlich zugänglichen Schlüssel.

Bei Mobiltelefonen vertrauen Politiker und Wirtschaftsbosse auf das Krypto-Handy des deutschen Herstellers Rhode & Schwarz. Die speziell gesicherten Geräte tauschen bei jedem Verbindungsaufbau einen neuen 128-Bit-Schlüssel, der per Zufallsverfahren ausgewählt wird. So dürfen führende Mitarbeiter des deutschen Energiekonzerns Aral seit geraumer Zeit nur noch mit diesen speziellen Geräten mobil telefonieren.

Wie effektiv ein Verschlüsselungssystem sein kann, zeigt sich am Beispiel von Airbus Industries. 1995 verlor Airbus einen Grossauftrag an Boeing und McDonnell Douglas, weil Details des geplanten Deals ausspioniert wurden. Der Schaden für Airbus belief sich damals nach Firmenangaben auf mindestens sechs Milliarden Euro.

Trotz dieser negativen Erfahrung führte Airbus erst vor vier Jahren ein Verschlüsselungs- und Sicherheitskonzept ein. Letztes Jahr verkaufte Airbus erstmals wieder weltweit mehr Flugzeuge als Boeing, doch Lindau glaubt in diesem Fall nicht an Zufall: «Es würde mich nicht überraschen, wenn die Verkaufsbilanz in direkter Verbindung mit der neuen Sicherheitspolitik von Airbus stehen würde.»

Vorfälle werden verharmlost

Der österreichische Journalist Gerald Reischl beschreibt in seinem Buch «Unter Kontrolle» die unsauberen Machenschaften von US-Herstellern. So baut Cisco, Marktführer bei Internet-Routern, standardmässig in jedes Gerät eine Abhörvorrichtung ein. Das bedeutet nichts anderes, als dass jedes Cisco-Gerät in Europa über eine Schnüffelfunktion verfügt – und das bei einem Marktanteil von 95 Prozent! Das kommt nicht von ungefähr: Das Amerikanische Federal Communications Assistance for Law Enforcement Act (Calea) verpflichtet einheimische Hersteller von Kommunikationsgeräten, ihre Anlagen mit Abhörapplikationen auszurüsten. So können sich die Behörden mühelos über jeden Cisco-Router bei jedem beliebigen User einloggen.

Während grosse Konzerne zunehmend in aufwändige Sicherheitssysteme investieren, ist die Sensibilität in kleineren und mittelständischen Firmen oft nur schwach ausgeprägt. Gerade sie sind sich nicht im Klaren, über welche technischen Spionagemöglichkeiten die Mitbewerber verfügen. Nur drei von hundert Spionageangriffen werden erkannt, die Dunkelziffer ist dementsprechend hoch.

Wie schwer Wirtschaftsspionage ein Unternehmen schädigen kann, zeigte sich unlängst am Fall des ostfriesischen Windanlagenherstellers Enercon. 1994 spionierte ein US-amerikanischer Mitbewerber dessen neuste Entwicklung aus und meldete kurze Zeit später ein entsprechendes Patent in den USA an. Obwohl Enercon die Spionage nachweisen konnte, wurde über das Unternehmen per Gerichtsbeschluss ein Importverbot in die USA verhängt. Bis heute entgingen der deutschen Firma dadurch Umsätze im Wert von 50 Millionen Euro. ◆

DAS GLOBALE ABHÖRSYSTEM ECHELON

Echelon ist ein Satelliten-Abhörsystem der so genannten Ukusa-Staaten, denen neben den USA und Grossbritannien auch Kanada, Australien und Neuseeland angehören. Herzstück von Echelon sind sieben von Boeing gebaute Satelliten. Am 18. Mai 2001 präsentierte ein Untersuchungssausschuss dem europäischen Parlament in Strassburg den Echelon-Bericht, der die Existenz dieses Lauschsystems nachweisen konnte. Echelon-Satelliten überwachen den Datenverkehr über Internet, «saugen» Telefon-, Handy- und Faxdaten ab und übermitteln sie an den amerikanischen Geheimdienst NSA. Die bislang bekannten europäischen Abhörstationen befinden sich im bayerischen Bad Aibling und in mehreren Orten in Grossbritannien. Weitere Lauscherbasen befinden sich in den USA, in Australien, Puerto Rico, Japan und Neuseeland.

«Jede Restrukturierung öffnet der Wirtschaftsspionage Tür und Tor.»

Interview mit Sicherheitsexperte Maximilian Burger

ICT Kommunikation:
Herr Burger, wer attackiert wen und warum?
Maximilian Burger: Jeder attackiert jeden. Es sind immer wirtschaftliche Gründe und es geht darum, sich einen Wettbewerbsvorteil zu verschaffen. Dies geht von kleinen privaten Firmen mit fünf Mitarbeitern bis hin zu internationalen Firmen. Je nach Bedeutung der Firma am Weltmarkt, ist eventuell auch ein US-Amerikaner oder Japaner interessiert. Geheimdienste, die früher politisch und militärisch spioniert haben, nutzen heute ihr Know-how und betreiben Betriebsspionage zugunsten eigener, als staatstragend empfundener Firmen.

Wie wird spioniert?
Schon über den Webauftritt einer Firma ist erstaunlich viel an Informationen herausholen, wie etwa Bilanzzahlen, Auftraggeber oder Produkt-Informationen. Bei Messeauftritten werden verschiedene Leute auf einen Verkäufer angesetzt, die getrennt voneinander einzelne Fragen stellen. Sie müssen nicht unbedingt den Topmann attackieren – der zweite, dritte Mann weiss meist fast genauso viel, ist aber leichter anzugreifen und häufiger der Frustrierte. Oft geht Wirtschaftsspionage mit Korruption und der daraus resultierenden Erpressbarkeit einher. Denn wer schon mal genommen hat, wird erpressbar.

Wo sind, im Hinblick auf den technologischen Hintergrund, die grössten Schwachstellen?
Die grösste «technische» Schwachstelle ist der Mensch. Nur 20 Prozent der Angriffe sind durch technische Hilfsmittel zu verhindern. Machen Sie vor einer Firma bei Betriebsbeginn Interviews und fragen nach dem letzten Urlaub, nach dem Namen der Kinder, des Hundes etc. Ich garantiere Ihnen, dass Sie innerhalb von fünf Minuten mindestens zwei Passwörter erfahren, mit denen Sie in ein System einsteigen können. Viele Firmen haben eine Firewall, doch die ist oft veraltet. Dann gibt es noch die Risikofaktoren, die mit der Verschlüsselung sensibler Daten zu tun haben.

Sind sich die Firmen der Gefahrenquellen bewusst?
Nein, sie verdrängen sie. Security ist heute kein aufregendes neues Geschäft mehr, was paradox ist. Fälschlicherweise wird oft dem IT-Manager die Verantwortung für die ganze Sicherheit übertragen. Dieser steht aber in der «Hackordnung» einer Firma weit unten und kann wichtige Investitionen nicht durchbringen. Zudem hat der IT-Manager meist wenig Ahnung und wenig Einfluss auf die Managementmethoden der Firma. So werden Managemententscheidungen leider vielfach nach dem Motto «Sicherheit kostet, und wer will bei uns schon was ausspionieren?» gefällt.

Wie ist die Situation in der Schweiz?
Die Schweiz ist voraus, obwohl der allgemeine Sicherheitsstandard global gesehen nicht sehr hoch ist. Ich glaube aber, dass die Schweizer insofern weiter sind, als dass sie sich dieser Problematik bewusst sind. Mir ist jedenfalls kein anderes Land bekannt, das einen Lehrgang wie jenen in Luzern anbietet, wo ein Nachdiplomstudium zum Thema Wirtschaftskriminalität durchgeführt wird. ◆

ZUR PERSON

Dr. Maximilian Burger-Scheidlin, Geschäftsführer der ICC, befasst sich seit vielen Jahren mit dem Thema Wirtschaftskriminalität. Er ist als Lehrbeauftragter an der Wirtschaftsuniversität Wien und der Universität Luzern tätig, wo er den Lehrgang «Prävention von Wirtschaftskriminalität» leitet.