Risiko Wirtschafts- und Wettbewerbsspionage

von Dr. Peter Roell

Vorbemerkung

Die WirtschaftsWoche führte am 25. und 26. Oktober 2007 in Hamburg eine Sicherheitskonferenz mit dem Thema „Risiko Wirtschafts- und Wettbewerbsspionage“ durch. Eingeladen waren Führungskräfte aus der Industrie und Wirtschaft, Vertreter von Behörden, den Medien, IT- und Sicherheitsberater, Rechtsanwälte, Unternehmensberater, die sich mit diesem Thema beschäftigen.

Vorliegender Konferenzbericht soll einige Themenfelder beleuchten.

Die Bedrohungslage

Wirft man einen Blick auf den Jahresbericht 2006 des Bundesamtes für Verfassungsschutz (BfV), so wird deutlich, dass die Bundesrepublik Deutschland wegen ihrer bedeutsamen Rolle in der EU und NATO und nicht zuletzt wegen zahlreicher Firmen im Bereich der Spitzentechnologie wieder ein interessantes Aufklärungsziel für ausländische Nachrichtendienste war.

Zu den Diensten zählten unverändert die der Russischen Föderation, der Republik Belarus, die der VR China, Nordkoreas sowie einiger Länder des Nahen- und Mittleren Ostens. Aber auch für westliche Dienste, so die Feststellungen des BfV, war und bleibt Deutschland wichtiges Aufklärungsziel.

Es ist deshalb nicht verwunderlich, dass Staatssekretär Dr. August Hanning (BMI) und ehemaliger Präsident des Bundesnachrichtendienstes (BND), in seiner Eröffnungsrede am 22. Oktober 2007 anlässlich der Jahreskonferenz der Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW) in Berlin darauf verwies, dass man mit großer Sorge beobachte, wie der illegale Transfer von Wissen zunehme. Der dadurch entstehende Schaden für die deutsche Wirtschaft belaufe sich pro Jahr auf etwa 20 Mrd. Euro.

Kein Wunder, dass die WirtschaftsWoche in Zeiten der Globalisierung dem an Bedeutung gewinnenden Thema Wirtschafts- und Wettbewerbsspionage besondere Aufmerksamkeit widmete.

Sehr ernüchternd die Aussagen eines Referenten, der an Beispielen darlegte, wie relativ einfach es sei, bei Konzernen und anderen großen deutschen Firmen an vertrauliche

Informationen zu gelangen. Beunruhigend auch die massive Zunahme elektronischer Angriffe auf deutsche Unternehmen, aber auch Behörden. So definierte der Vizepräsident des Bundesamtes für Verfassungsschutz, Elmar Remberg, in seinem Vortrag zunächst Wirtschaftsspionage als ausschließlich staatlich gelenkte oder unterstützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben und nannte Russland und China als besonders aktive Staaten im Bereich der Wirtschaftsspionage.

Den in seiner Ausgabe Nr. 35 vom 27. August 2007 publizierten Spiegel- Artikel mit dem Titel: „Die gelben Spione – Wie China deutsche Technologie ausspäht“, bezeichnete Remberg als weitgehend korrekt. Bereits im Februar 2007 hatte er in den Medien auf chinesische Hackerangriffe auf Rechner im Bundeskanzleramt, im Auswärtigen Amt, im Wirtschaftsministerium und im Forschungsministerium hingewiesen. Geortet wurden die Hacker in Lanzhou im Norden Chinas, in Kanton im Süden des Landes und in Peking. Sie wurden der Chinesischen Volksbefreiungsarmee (VBA) zugerechnet.

Eingesetzt haben die großen Hacker-Angriffe vor gut zwei Jahren. Zwischenzeitlich wird immer subtiler vorgegangen. Anfangs schickten die Hacker meist an alle Mitarbeiter eines Unternehmens Massenmails. Bei der Öffnung der e- mails verbreiteten sich Spionageprogramme auf den Computern der Empfänger. Nun, so Robin Kroha, Experte für Unternehmenssicherheit bei der Beratungsfirma Control Risks in Berlin, programmierten die Hacker individuelle, als persönliche Botschaften getarnte Mails.

Die meisten Betriebe, insbesondere mittelständische Unternehmen, stehen diesen Hackerangriffen weitgehend hilflos gegenüber und bemerken sie kaum, während wenige Großkonzerne geeignete Abwehrmaßnahmen eingeleitet haben.

Methoden und Ziele der Spionage

Zum methodischen Vorgehen der Nachrichtendienste merkte der Vizepräsident des BfV an, dass diese zunächst offene Zugänge nutzten; zum anderen werde mit konspirativen, geheimen Mitteln gearbeitet. So würden z.B. „klassische Agenten“ eingesetzt und als Mitarbeiter privatwirtschaftlicher Unternehmen getarnt. Diese betrieben Gesprächsaufklärung, nähmen an Forschungsprojekten teil und entfalteten nachrichtendienstliche Aktivitäten.

Dr. Andrea Berner vom Landesamt für Verfassungsschutz in Hamburg wies in ihrem Vortrag darauf hin, dass ausländische Nachrichtendienst zum Zwecke der Nachrichtengewinnung eine sogenannte Zielobjektanalyse durchführen würden. Diese beinhalte die Erkenntnisgewinnung über die Handelsbeziehungen eines Unternehmens, die Reiseaktivitäten von Firmenangehörigen, den Personalaufbau, die Unternehmensstrukturen sowie die Unternehmenspolitik. Aus dieser Zielobjektanalyse ergäben sich dann folgende Angriffsziele:

- Strategische/taktische Entscheidungen
- Forschungsergebnisse und Produktideen
- Konstruktionsunterlagen, Herstellungsverfahren und Steuerungssysteme
- Verkaufsstrategien, Marktstudien, Umsätze und Kundenstamm
- Kalkulationsunterlagen, Budgetplanungen und Umsatzvorhaben

Um an dieses Wissen zu gelangen nutzten die Dienste staatliche Offenlegungspflichten, so z.B. im Rahmen von Joint Venture Projekten, betrieben verdeckt Hotel- und Konferenzüberwachung, nutzten Dolmetscher des Gesprächspartners, Wissenschaftler,

Studenten und Praktikanten. Nachrichtendienste achteten zudem gezielt auf Verfehlungen, um eine Person unter Druck zu setzen und für eine nachrichtendienstliche Tätigkeit zu werben.

Zur Informationsgewinnung diente auch die Internet- und Telekommunikationsüberwachung sowie die Kontrolle ein- und ausreisender Personen.

Zum Thema „IT- Sicherheit zur Abwehr wirtschaftlicher Spionage“ referierte Dr. Udo Helmbrecht, Präsident des Bundesamtes für Sicherheit in der Informationstechnik. Innere Sicherheit sei heute untrennbar mit sicheren Informationsinfrastrukturen verbunden. Als Reaktion auf die qualitativ und quantitativ ansteigende IT- Bedrohungslage habe das Bundeskabinett im Sommer 2005 den „ Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI) beschlossen und das Bundesministerium des Inneren mit der weiteren Umsetzung beauftragt. Dr. Helmbrecht zeichnete Gefahrenpotentiale und Bedrohungen auf und wies in seinem Vortrag auf den „Leitfaden IT- Sicherheit“ hin. (www.bsi.bund.de)

In seinem Referat „ Spionage über und durch elektronische Netze – Informationsabflüsse im Kontext von Wirtschafts- und Konkurrenzspionage“ ging Andy Müller-Maguhn, Sprecher und Mitglied des Vorstandes, Chaos Computer Club e.V., auf Hackerethik, Angriffskategorien und Motivation, auf Datenverbrechen, Sicherheit und Unsicherheiten im Internet, Kryptographie, den Umgang mit Bestandsdaten etc. ein. Was ein zu realisierendes Sicherheitsniveau anbelangt, zitierte er: „ Das Ziel von Sicherheitsmaßnahmen kann nur sein, zwischen dem Aufwand zur Sicherung und dem Aufwand zum Durchbrechen dieser Sicherung ein Ungleichgewicht zu Ungunsten des Angreifers herzustellen“.

Sehr praktisch wurde es beim Vortrag von Peter Hölzel, Leiter Abhörschutz, Global Group Security, Deutsche Telecom, der die Möglichkeiten der illegalen Kommunikationsbeschaffung erläuterte und auf innovative Sicherheitslösungen hinwies.

Mit dem interessant klingenden Titel „Im Haifischbecken schwimmen lernen: Was man über Chinas Know-how Akquise wissen sollte“, weckte Dr. Andreas Blume, IP-Manager, Degussa GmbH, der Sinologie studierte und über interkulturelle Kompetenz verfügt, sofort die Aufmerksamkeit der Zuhörer. Er verwies zunächst auf die Staatsziele der VR China, nämlich bis ins Jahr 2020 führende Weltwirtschaftsmacht werden und ein Wirtschaftswachstum von etwa 8 Prozent aufrechterhalten zu wollen. Ferner strebe Chian an, die geostrategische Bedeutung wiederherzustellen, das F&E-Investment von 1,3% des GDP auf 2,5% GDP bis 2020 zu steigern sowie eine „Wissenschafts- und Technologiearmee“ zum Aufbau Chinas zu schaffen. Bildung und Know-how seien die Schlüssel für den Aufstieg Chinas.

Auf dem Weg, das Wirtschaftswachstum auf eine breite Basis zu stellen, käme den chinesischen Nachrichtendiensten, wie dem Ministerium für Staatssicherheit (MSS), mit mindestens 800.00 hauptamtlichen Mitarbeitern sowie dem Militärische Nachrichtendienst (MID) eine besondere Bedeutung zu. Ein Zitat des Meisters Sunzi, „Wenn Du Dich und Deinen Feind kennst, brauchst Du den Ausgang von Hundert Schlachten nicht zu fürchten“, habe auch heute noch seine Gültigkeit. Im Visier Chinas stünden strategische Entwicklungsbranchen wie:

- Nanotechnologie
- Werkstoffe/Produktionstechnik
- Rüstungstechnologie, Optoelektronik
- Eisenbahn, Kraftfahrzeuge, Luft- und Raumfahrt
- Energie- und Umwelttechnik, erneuerbare Energien

- Biotechnologie, Gentechnik
- Maschinenbau

Zur Vorgehensweise chinesischer Nachrichtendienst nannte Dr. Blume einige Beispiele. Ein Mitarbeiter einer Forschungseinheit eines bekannten deutschen Unternehmens aus der Chemiebranche wurde zu einem Symposium eingeladen. Selbstverständlich würde die chinesische Seite alle Kosten tragen. Er sollte einen hochspezifischen Vortrag halten, dann bekäme er einen Professortitel einer chinesischen Universität. Ferner ist bekannt, dass chinesische Professoren, die im Rahmen von Forschungskooperationen Know-how erlangen, dieses nach Peking weiterleiten.

Im Fokus der chinesischen Dienste stünden auch deutsche Unternehmen, die Nischentechnologieführer seien und noch wenig oder keinen Kontakt zu China hätten. Ihnen unterbreite man verlockende Scheingeschäfte und lade sie nach China ein. Dort angekommen, erfolge eine offene oder verdeckte Informationsabschöpfung.

Abschließend gab Dr. Blume Hinweise für deutsche Unternehmen, wie man sich vor Produktpiraterie und dem Vorgehen chinesischer Dienste schützen könne.

Mit einem Vortrag über strafrechtliche Konsequenzen bei Geheimnisverrat fand der erste Tag der Sicherheitskonferenz seinen Abschluss. Rechtliche Themen wie „Der zivilrechtliche Schutz vor Spionage, Haftung der Unternehmensführung bei fehlendem Risikomanagement, Innovationsschutz und Produktpiraterie, Joint Ventures – Schutz von Betriebsgeheimnissen und Know-how“, wurden am zweiten Tag umfassend behandelt.

In seinem Vortrag „Auf den digitalen Spuren der Spione – Elektronische Verfolgung“ befasste sich Reinhold Kern, Leiter Computer Forensik und E- Discovery, Kroll Ontrack GmbH, mit illegalen Praktiken des Zugriffs auf elektronische Daten, aber auch mit Möglichkeiten der Entdeckung und der Abwehr solcher Angriffe. Thomas Königshofen, Sicherheitsbevollmächtigter, Deutsche Telecom AG, widmete sich dem Thema „Präventionsmaßnahmen zum Schutz vor Wirtschafts- und Wettbewerbsspionage“, schilderte klassische operative Informationsschutzmaßnahmen und ihre Grenzen und berichtete u.a. aus der Praxis über Awareness- Kampagnen und Abschreckungskonzepte.

Wertung

Mit sehr guten Referenten und einem breiten Themenspektrum vermittelte die Sicherheitskonferenz der WirtschaftsWoche umfassendes Wissen über Wirtschafts- und Wettbewerbsspionage. In Zeiten der Globalisierung gewinnt der Satz „Wissen ist Macht“ an Bedeutung. Zwar gehören Politik und Militär auch weiterhin noch zu den Aufklärungszielen von Nachrichtendiensten, der Fokus hat sich jedoch bereits verschoben. Wirtschaftliche Entwicklungen und wissenschaftliche Forschung genießen Priorität.

Aus diesen Bereichen in Deutschland beschaffte nachrichtendienstliche Erkenntnisse werden von einigen Diensten Wettbewerbern oder Staatsunternehmen im eigenen Land zur Verfügung gestellt. Dies schädigt die deutsche Wirtschaft und gefährdet die strategischen Interessen der Bundesrepublik Deutschland.

Welche Gegenmaßnahmen sollten ergriffen werden? Die Abwehrkapazitäten staatlicher Institutionen und die der Wirtschaft müssen erhöht, Lagebeurteilungen ausgetauscht werden. Ferner sollten sich Staat und Wirtschaft gegenseitig intensiver über Organisation, Zielsetzungen und Methodik bestimmter Nachrichtendienste informieren.

Der Auffassung von Staatssekretär Dr. August Hanning (BMI), Verfassungsschutz und Wirtschaft müssten enger kooperieren, da ansonsten der Wettbewerbsvorteil Deutschlands gefährdet sei, kann man uneingeschränkt zustimmen. Eine graduelle Sensibilisierung für das Thema Wirtschafts- und Wettbewerbsspionage ist in der deutschen Wirtschaft und bei staatlichen Institutionen erkennbar. Es gilt, diese nachhaltig zum Wohle unseres Landes und seiner Menschen auszubauen.

Anmerkung: Der Beitrag gibt die persönliche Auffassung des Autors wieder.

Der Autor ist Präsident des Instituts für Strategie- Politik- Sicherheits- und Wirtschaftsberatung (ISPSW), Berlin. Auf Einladung der WirtschaftsWoche nahm er in seiner Funktion als freier Journalist und Mitglied in der Vereinigung Europäischer Journalisten (VEJ) sowie als Sino-Politologe an der Sicherheitskonferenz der WiWo am 25. und 26. Oktober 2007 in Hamburg teil.