Oberstleutnant d.R.
Dipl.-Ing. Günter Holzhauser

Wirtschaftsspionage – Die unterschätzte Bedrohung

Fremde Nachrichtendienste und global agierende Unternehmen beschaffen sich das Know-how zur Entwicklung ihrer eigenen Märkte in Deutschland. Militär und Verteidigungsindustrie sind betroffen. Seit jeher gehört Deutschland zu den bevorzugten Aufklärungszielen fremder Geheimdienste. Als aktuell stärkste Nation in der EU und als eines der innovationsstärksten Länder der Erde steht Deutschlands Politik, Militär, Wirtschaft und Wissenschaft an der Spitze der Aufklärungsziele im Kontext von Spionage. Günter Holzhauser ist Sektionsleiter Rhein-Main der Deutschen Gesellschaft für Wehrtechnik und Geschäftsführer der BUSINESS INTELLIGENCE & SECURITY in Eschborn.

Collage: businesscomputingworld.co.uk

WIRTSCHAFTSSPIONAGE MACHT AUCH VOR KLEINEN UND MITTELSTÄNDISCHEN UNTERNEHMEN NICHT HALT

Die stark zunehmende Globalisierung und Vernetzung unserer Welt wird durch die rasante Entwicklung von neuen Technologien getrieben. Machtblöcke auf der Erde verschieben sich, Machtblöcke gehen und neue entstehen. Die Regionen Asien, Mittlerer Osten und Süd- und Lateinamerika erfahren einen wirtschaftlichen Aufschwung. Die weltweite Sicherheitsarchitektur und Bedrohungskulisse ist aktuell stark in Bewegung. China und Russland betreiben eine aggressive Außenpolitik, die eine Spirale der militärischen Aufrüstung der Anrainerstaaten und in der Region in Gang setzt. Gleich dem Gesetz militärische Stärke = politische Stärke = wirtschaftliche Stärke haben z.B. China und Russland ihre Verteidigungsbudgets deutlich erhöht. Der Ausbau der militärischen Fähigkeiten vollzieht sich in einem rasanten Tempo.

In diesem Kontext entstehen große Risiken durch Spionage gegen Deutschland. Neben der politischen Spionage ist die Spionage gegen Militär und Wirtschaft ein Schwerpunkt. Zur Entwicklung der eigenen und oft unterentwickelten Fähigkeiten greifen andere Staaten und auch deren Industrien auf Mittel der Spionage zurück. Die Vorgaben von Nationalstaaten an ihre Geheimdienste ist die strategisch organisierte und getarnte Beschaffung von nicht öffentlich zugänglichen Informationen. Denn, was im eigenen Land nicht entwickelt oder gekauft werden kann, wird mit anderen Mitteln beschafft, dem Mittel der Spionage.

Spionageziele in Deutschland

Zielobjekt der Spionage in Deutschland sind die deutsche Sicherheits- und Vereidigungspolitik, die deutschen Verteidigungsstrukturen mit dem Link zu NATO und EU, die Bundeswehr mit ihrer führenden Ausstattung und natürlich die deutsche Verteidigungsindustrie, die mit ihren Produkten und ihrer Innovationsfähigkeit Weltgeltung besitzt. Eines der Hauptmotive staatlich gelenkter Spionage gegen Deutschland ist das Aufholen des Wissens- und Zeitvorsprungs, das den Wettbewerbsvorteil Deutschlands gegenüber anderen Nationen ausmacht.

Dipl.-Ing. Günter Holzhauser, Jahrgang 1965, arbeitet selbstständig und branchenunabhängig im Bereich Wirtschaftsschutz und Spionageabwehr. Er verfügt über Hochschulausbildungen im Bereich Maschinenbau, Security Management und Wirtschaftsschutz (Spionageabwehr). Er hat 24 Jahre Branchenerfahrung in Defence & Security, national und international für Wirtschaft, Regierungsorganisationen, Spezialkräfte und Dienste. Die Dienstleistungen für Wirtschaft und Organisationen liegen unter anderem im Kontext der Spionageabwehr in den Bereichen Bedrohungs- und Risikoanalysen, Umfeldanalysen und Lagebilder für die relevanten Einzelbedrohungen. Schwerpunkt ist der Informationsschutz. Für Spionageabwehr Sicherheitsstrategien, -konzepte und -maßnahmen und Security im Unternehmensprozess.

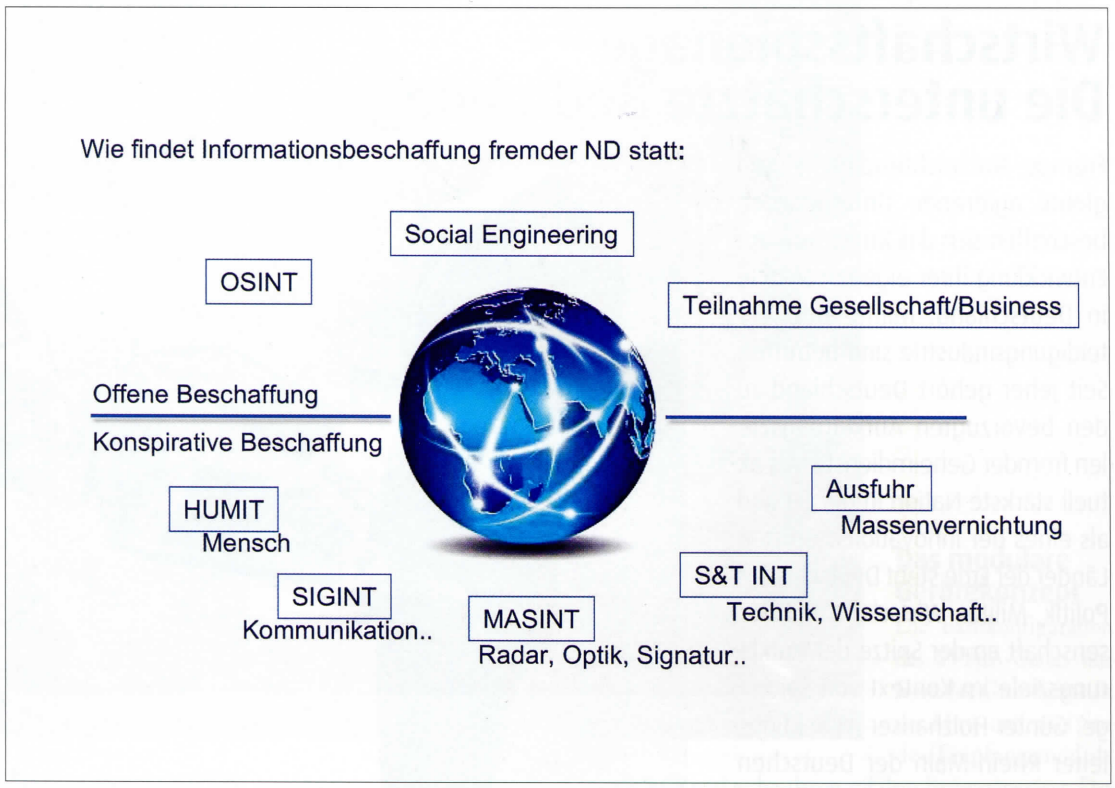

Abb.: Autor

In erster Linie sind es China und Russland, die Spionage gegen Deutschland betreiben. Arabische Länder, Iran, Nordkorea, Pakistan und andere betreiben ebenfalls weiterhin Spionage gegen Deutschland. Angriffe finden in Deutschland, auf dem Territorium anderer Staaten und in der virtuellen und vernetzten Welt statt. In der Sprache der Militärs ist gerade heute die Aussage zulässig, dass die Zielobjekte von Spionage durchaus einer 360 Grad Bedrohung ausgesetzt sind. Die globalisierte und vernetzte Welt macht es möglich.

Die in Deutschland zuständigen Sicherheitsorgane gehen davon aus, dass in der Verteidigungsindustrie fast alle Unternehmen und die Fachverbände und -vereine betroffen sind. In den Fachverbänden und -vereinen halten fremde und getarnte Agenten mit „Legende" Ausschau nach potenziellen Zielobjekten. Zielobjekte können z.B. Unternehmen, Mitarbeiter von Ministerien, Behörden und Soldaten der Streitkräfte sein. Aber auch die elektronische Aufklärung und Überwachung der Kommunikation dieser Zielobjekte stellt für professionelle Angreifer keine Hürde dar. Die technischen Möglichkeiten führender Geheimdienste sprengen unsere Vorstellungskraft.

Wege der Spionage

Ein Großteil der ausländischen Agenten ist in Deutschland in sogenannten Legalresidenturen platziert. Hierbei handelt es sich um Standorte von Nachrichtendiensten in offiziellen und halboffiziellen Vertretungen in Deutschland. Zu den offiziellen Vertretungen gehören Botschaften und Konsulate. Zu den halboffiziellen Organisationen können Presse- und Medienagenturen, Reisebüros und Fluggesellschaften gehören. Die Agenten betreiben legale und illegale Informationsbeschaffung über verschiedenste Kanäle und Quellen in Deutschland. Diplomaten und Journalisten z.B. haben erleichterten Zugang zu ihren Quellen, Diplomaten haben den Status der Immunität und bei Journalisten ist es nicht auffällig, wenn sie wissbegierig sind und viele Fragen stellen. Im Falle einer Enttarnung profitieren Agenten vom Status der Immunität oder besonderen Regelungen, die sie vor der Strafverfolgung in Deutschland schützen.

Nennenswert als Bedrohung ist weiterhin die Ausspähung durch „Non Professionals" in Deutschland. Hierbei handelt es sich um Wissenschaftler, Studenten, Doktoranden, Ingenieure, Praktikanten und Trainees, die in Organisationen und der Wirtschaft positioniert werden. Sie werden mit entsprechenden Lebensläufen, Bewerbungsunterlagen und Legenden „kultiviert" und in Schlüsselpositionen gebracht. Die Schäden, die durch solche Innentäter verursacht werden können, sind enorm.

Akteure und ihre Methoden

Hauptakteure im Kontext von Wirtschaftsspionage sind fremde Geheimdienste und Wirtschaftsunternehmen, die Industrie- oder Wettbewerbsspionage betreiben. Wobei Wirtschaftsunternehmen oft mit ihren Geheimdiensten zusammenarbeiten. Die Angriffsarten und Methoden sind nahezu gleich.

Ein Großteil der deutschen Wirtschaft denkt in erster Linie in ihrem Verständnis von Sicherheit an IT und physikalischen Schutz. Das gesamtheitliche Verständnis für Schutz und das breite Spektrum der Bedrohungen und Angriffe sowie die Quellen für ungewollten Informationsabfluss fehlen meist. Studien belegen, dass der Großteil der Schadensfälle für ungewollten Know-how-Verlust nicht über die IT kommt. Das Problem ist die Verortung der Information, die Migration der Information und die Zugänge zur Information. In bis zu 80% der Fälle ist der Mensch die Schwachstelle.

Die Angriffsmethoden und damit die Bedrohungen sind äußerst vielfältig. Schwachstellen und fehlende Schutzmaßnahmen sind in der Regel im Bereich Innen-/Außentäter, Social Engineering, Social Media, IT/Hacking, Kommunikation,

Abb.: Autor

NICHT NUR IM WEHRTECHNISCHEN BEREICH SIND VERSTÄRKTE SICHERHEITSMASSNAHMEN ESSENTIELL GEGEN SPIONAGEAKTIVITÄTEN

Geschäftsreisen, Besucher/Delegationen, Wirtschaftspartner und externe Dienstleister zu finden. Übergeordnet ist die größte Schwachstelle meist der Schutz der kritischen Information eines Unternehmens. Hier fehlen neben der gesamtheitlichen Betrachtung die unternehmensspezifischen Schutz- und Präventionskonzepte für das Know-how.

Zukünftige Entwicklungen – Die Ausbaustufe zu „Spionage 10.0"

Was sind die aktuellen neuen Entwicklungen und die Themen der Zukunft? Social Media, mobile Endgeräte, Internet der Dinge, Fabrik 4.0 und die Metaebene Social Business respektive Social Enterprise. Die Vernetzung von Mensch und Unternehmen schreitet unaufhörlich und mit rasantem Tempo voran. Territoriale Grenzen verschwinden. Die klassischen hierarchischen Organisationen von Unternehmen werden sukzessive durch autonome und virtuelle Organisationen ersetzt. Die Manager von morgen moderieren eher virtuelle Mitarbeiterteams. Diese hybriden Unternehmensorganisationen werden die Entscheidungsprozesse in Unternehmen verändern. Im Vordergrund dieser Bestrebungen steht die Erhöhung der Produktivität durch Vernetzung und die Sichtbarmachung von Menschen und Wissen.

Im Sinne des Philosophen Walter Benjamin lässt sich trefflich vorhersagen, dass die Veränderung der Medien die Menschen und die Gesellschaft verändern wird. Wir leben in dieser Zeit des Umbruchs.

Im Kontext der Sicherheit und der Spionage können diese Entwicklungen für Gesellschaft, Personen und die Wirtschaft verheerende Folgen haben, wenn für diese Entwicklungen die Sicherheitsarchitektur vernachlässigt wird. Fremde Geheimdienste und Angreifer freuen sich sicherlich über diese Entwicklung. Mit den bereits heute vorhandenen Technologien der Nachrichtendienste eröffnet sich ein breites Spektrum für Angriffe von Innentätern, Social Engineering, Hacking bis hin zu Sabotage mit ungeahnten Ausmaßen. Die Bedrohung durch OSINT (Open Source Intelligence) wird zunehmen. Bereits heute liegt der Anteil des OSINT-Wissens, das mit Methodik und Tools durch die Nachrichtendienste beschafft wird, bei bis zu 80%. Überschreitet man z.B. die Grenze in Richtung illegale Informationsbeschaffung, dann öffnet sich ein unermesslicher Fundus an Daten, Fakten und letztendlich Information, die als Grundlage für Angriffe genutzt werden können.

Was kann getan werden?

Wir sollten uns bewusst werden, dass wir in Deutschland an der Spitze der auszuspähenden Länder liegen. Als natürliche Person, Wissenschaftler, Soldat, Behörde oder Unternehmer kann man sehr leicht Zielobjekt von Spionage werden. Entscheidend ist, was an Information „angeboten" werden kann.

Wirtschaftsspionage z.B. ist unabhängig von Unternehmensgröße, Branche und Wertschöpfungstiefe. Kleine mittelständische Unternehmen sind genau so betroffen wie große Konzerne. Entscheidend ist die Kernkompetenz des Unternehmens und der handelnden Akteure.

Das ganze Thema Wirtschaftsspionage wird in Deutschland massiv unterschätzt – gerade im Mittelstand. Viele Unternehmen haben keine Transparenz über die eigenen Bedrohungen und Risiken, die im Kontext ihrer unternehmerischen Tätigkeit existieren. Bedrohungs- und Risiko analysen, Umfeldanalysen und Lagebilder sind in vielen Unternehmen Fremdwörter. Die Problematik gilt sicherlich auch für Regierungsorganisationen, Behörden und die Hochschulen.

Absolute Sicherheit kann selbst mit enormen finanziellen Mitteln nicht hergestellt werden. Ziel kann es nur sein, durch Methodik, Tools, geeignete Prozesse und entsprechende Schulungsmaßnahmen die Hürde für Angreifer entsprechend höher zu legen. Schutzmaßnahmen und Prozesse müssen Akzeptanz finden und gelebt werden.

Die besten Schutzmaßnahmen können nicht helfen, wenn den Akteuren die Einsicht fehlt. ■

Abb.: Autor

JEDES UNTERNEHMEN IST SELBST FÜR DIE EIGENE SICHERHEIT VERANTWORTLICH