

G. SPIONAGEABWEHR, GEHEIM- UND SABOTAGESCHUTZ

1. Aktuelle Entwicklungen und Tendenzen

Spionage war auch im Jahr 2007 eine alltägliche Erscheinung. Gleichgültig, ob alte und neue Großmächte um wirtschaftliche Führungspositionen gerungen haben oder sich Machthaber von Staaten wie Iran, Syrien, Pakistan oder Nordkorea in den Besitz von Massenvernichtungswaffen bringen wollten und dabei auf hochwertige Güter und Spezialwissen aus Hightech-Ländern angewiesen waren - fremde Nachrichtendienste waren vielfach beteiligt.

Die Weltwirtschaft befindet sich in einem grundlegenden Wandel. Vor allem asiatische Staaten unternehmen große Anstrengungen, um den Technologierückstand zu den westlichen Industriestaaten zügig aufzuholen und bei den Innovationsaktivitäten eigene Akzente zu setzen. Dabei kommt nicht zuletzt den Nachrichtendiensten eine bedeutende Rolle zu. Besonders für Furore gesorgt haben die im September 2007 intensiv in den Medien diskutierten und China zugerechneten elektronischen Attacken auf behördliche Kommunikationssysteme, welche die Verletzlichkeit der hiesigen IT-Infrastrukturen mit aller Deutlichkeit aufgezeigt haben. Aber auch die mit wachsendem Selbstbewusstsein agierende Russische Föderation hat zu erkennen gegeben, dass sie weiterhin trotz der guten Beziehungen zur Bundesrepublik Deutschland auf Regierungsebene nicht daran denkt, auf den Einsatz von Nachrichtendiensten zur Beschaffung vor allem wirtschaftlich nutzbarer Informationen zu verzichten.

„Die Geheimdienste Chinas und Russlands gehören zu den aggressivsten beim Sammeln von Informationen über empfindliche und geschützte US-Systeme, Einrichtungen und Projekte. In diesem Bereich ist nahezu der Stand erreicht worden, den es während des Kalten Krieges gegeben hatte.“

(Michael McConnell, Director of National Intelligence (DNI) der US Navy, Quelle: „Before The Permanent Select Committee On Intelligence“, House of Representatives, September 20, 2007)

Technische Innovationen sind in einer globalisierten Welt ein wichtiges Kapital. Deutsche Firmen stellen aufgrund ihrer hohen Leistungen im Bereich Produktinnovation ein überdurchschnittlich attraktives Ziel für fremde Nachrichtendienste dar. Die Abwehr der Wirtschaftsspionage muss deshalb angesichts eines extrem harten internationalen Konkurrenzkampfes und ständig verfeinerter Angriffsmethoden - etwa im technischen Bereich - einem permanenten Anpassungs- und Optimierungsprozess unterworfen werden. Dies ist nicht nur eine berechtigte Forderung der Wirtschaft und ihrer Sicherheitsverbände, sondern auch Anspruch der Spionageabwehr des Landesamts für Verfassungsschutz Baden-Württemberg (LfV). Der Status der Informationssicherheit in deutschen Unternehmen, besonders bei kleinen und mittelständischen Betrieben, entspricht häufig nicht der tatsächlichen Gefährdungslage und lässt hier oft eine ausreichende Risiko-Strate-

gie vermissen. Das LfV reagierte mit einer verstärkten Serviceorientierung und einer Intensivierung seiner Präventionsarbeit. So nutzte das LfV beispielsweise die „SAFEKON“ in **Karlsruhe** - eine Fachmesse für Zutrittskontrolle, Gebäudesicherung und Informationsschutz - um den Bereich Wirtschaftsschutz Ausstellern und Fachpublikum aus dem Großraum **Karlsruhe** vorzustellen. Ferner wurde gemeinsam mit dem Bayerischen Landesamt für Verfassungsschutz eine Broschüre zur Wirtschaftsspionage mit Fallbeispielen aus beiden Ländern herausgegeben. Auch sie soll verdeutlichen, dass Security Awareness in den Unternehmen hohe Bedeutung zukommt.

Nachdem sich die Aufregung des letzten Jahres um die nordkoreanischen und iranischen Nuklearprogramme etwas legte, ist die weitere Entwicklung zu Beginn des Jahres 2008 wieder ungewiss. Nordkorea und die USA beschuldigten sich gegenseitig, das Abkommen über die Einstellung des nordkoreanischen Atomprogramms zum Jahresende 2007 nicht eingehalten zu haben. Die Außenminister der fünf ständigen Mitglieder des Weltsicherheitsrates und Deutschlands beschlossen eine Verschärfung der Sanktionen gegen den Iran. Der Iran wird - entgegen der Behauptung, sein Atomprogramm ausschließlich zur friedlichen Energiegewinnung zu nutzen - weiterhin beschuldigt, die Grundlagen zum Bau nuklearer Waffen schaffen zu wollen. Darin wird nach wie vor eine gefährliche Bedrohung für den Weltfrieden gesehen. Die Abwehr der Proliferation⁴⁰³ bleibt auch zukünftig eine globale sicherheitspolitische Aufgabe, weil es über den Iran hinaus noch andere Länder gibt, die sich unter Umgehung einschlägiger Bestimmungen darum bemühen, in den Besitz atomarer, biologischer oder chemischer Massenvernichtungswaffen mit den erforderlichen Trägersystemen zu gelangen sowie die zu deren Herstellung notwendigen Güter und das erforderliche Know-how zu erwerben. Außerdem haben terroristische Organisationen ein Interesse an Massenvernichtungswaffen. Der Einsatz solcher Waffen ist für die Zukunft nicht auszuschließen. Aus gutem Grunde ist deshalb die Spionageabwehr des LfV eng in die gesamtstaatlichen Anstrengungen zur Abwehr solcher Gefahren eingebunden.

2. Daten, Fakten, Hintergründe

2.1 Volksrepublik China

Der 17. Parteitag der Kommunistischen Partei Chinas (KPCh) im Oktober 2007 hat die Weichen für die Zielrichtung der Politik der nächsten fünf

⁴⁰³ Proliferation: Weiterverbreitung von Massenvernichtungswaffen beziehungsweise der zu ihrer Herstellung verwendbaren Produkte einschließlich des dafür erforderlichen Know-hows sowie von entsprechenden Waffenträgersystemen.

*Intensivierung
der Präventions-
arbeit*

*verschärfte
Sanktionen
gegen den Iran*

*Abwehr von
Proliferation,
eine globale
sicherheits-
politische
Aufgabe*

*Deutsche Firmen
im Fokus fremder
Nachrichtendienst-
dienste*

Jahre gestellt. Dabei offenbarten mehrere Ergänzungen der Parteisatzung die Absicht, die wirtschaftliche Entwicklung des Landes weiter voranzutreiben. Leitgedanken wie „*Entwicklung durch Wissenschaft*“ und das Festhalten an der „*Politik der wirtschaftlichen Öffnung*“ verdeutlichen, dass diese Ziele - unter Einbindung aller gesellschaftlichen Kräfte - oberste Priorität genießen. Die propagierte Abkehr von der „*Politik des schnellen Wachstums um jeden Preis*“ dürfte dabei die Anstrengungen staatlich gelenkter Informationsbeschaffung kaum verringern. Neben den früher vorherrschenden Nachbau von Massenprodukten tritt zunehmend das nachrichtendienstliche Interesse an der Grundlagenforschung und dem Know-how zur Weiterentwicklung bedeutsamer Technologiebereiche aus der Automobil-, Luft- und Raumfahrtbranche. Mittelfristig könnte sich die chinesische Spionage stärker den Feldern Umweltschutz und Energiepolitik zuwenden, die für die Entwicklung des Landes zusehends wichtiger werden.

Die Bedeutung, die China der Wirtschaftsspionage beimisst, wird auch durch die Ernennung des Wirtschaftsexperten Geng HUICHANG zum Leiter des zivilen In- und Auslandsdienstes MSS⁴⁰⁴ offenkundig.

„Hacker in China sind sehr gut ausgebildet. Sie verfügen über gute mathematische und kryptografische Kenntnisse.“
(Oliver Winzenried, Vorstand der WIBU-Systems AG, Karlsruhe, Quelle: Financial Times Deutschland, 8. Februar 2007)

Eine neue Dimension der verdeckten Informationsbeschaffung und -manipulation eröffnen die bereits seit einiger Zeit festzustellenden elektronischen Attacken auf deutsche Behörden und Wirtschaftsunternehmen mit mutmaßlichem Ursprung in China („China-Trojaner“).

Art und Umfang der Angriffe veranschaulichen dabei sehr nachdrücklich, welche Risiken das Internet birgt. Durch ein raffiniert vorgeschaltetes „Social Engineering“⁴⁰⁵ sollen ausgewählte E-Mail-Empfänger zum Öffnen von Dokumenten-Anhängen, die mit äußerst „signaturarmen Schadprogrammen“⁴⁰⁶ versehen sind, verleitet werden. Ziel ist es, auf den angegriffenen Rechnern Trojaner⁴⁰⁷ zu installieren, mit denen entweder unbemerkt Daten ausspioniert oder IT-Systeme sabotiert werden können.

Um Kontakte zu interessanten Institutionen und Personen in Baden-Württemberg aufzubauen und zu koordinieren, nutzen die chinesischen Nachrichtendienste auch die diplomatischen Auslandsvertretungen ihres Landes. Von dort aus ist in auffälliger Weise mit Unterstützung von Wissenschaftlern und Studenten chinesischer Herkunft, die an deutschen Instituten und

⁴⁰⁴ Ministry of State Security (Ministerium für Staatssicherheit).

⁴⁰⁵ Social Engineering (engl. angewandte Sozialwissenschaft): Social Engineering Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder die Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Aktionen zu bewegen.

⁴⁰⁶ Die Schadsoftware wird auch von aktuellen Virencannern nicht unbedingt erkannt.

⁴⁰⁷ Selbständige Programme mit einer verdeckten Schadfunktion, ohne Selbstreproduktion.

Universitäten tätig sind, versucht worden, unmittelbaren Zugang zu ausgewählten Forschungsarbeiten sowie wissenschaftlichem Know-how zu erlangen.

□ Aufschlussreiche und wissenschaftlich nützliche Forschungsdaten, die im Internet veröffentlicht werden, stoßen nicht nur in akademischen Fachkreisen auf reges Interesse. Diese Erfahrung machte ein chinesischer Diplomand eines naturwissenschaftlich-technischen Instituts in Baden-Württemberg, als er unvermittelt in den Fokus nachrichtendienstlicher Interessen geriet. Er wurde aufgefordert, seine Diplomarbeit sowie weitergehende Forschungsergebnisse seines Arbeitgebers der diplomatischen Vertretung zuzuleiten. Seine ablehnende Haltung führte zu nachteiligen persönlichen Konsequenzen.

Parallel dazu wird auch der Austausch von Wissenschaftlern zwischen Universitäten beider Staaten zur gezielten Informationsbeschaffung genutzt.

□ Bei einem im Forschungsbereich einer baden-württembergischen Hochschule tätigen chinesischen Gastwissenschaftler konnten neben seiner unzureichenden wissenschaftlichen Qualifikation, die nicht den vorgelegten Nachweisen entsprach, verschiedene auffällige Verhaltensweisen beobachtet werden. Zugriffsversuche auf gesperrte Daten, unzulässiges Fotografieren von Versuchsabläufen, Transferieren großer Datenmengen direkt vom Arbeitsplatz aus nach China sowie der enge Kontakt zum nächstgelegenen chinesischen Konsulat verstärkten zunehmend die Vermutung einer nachrichtendienstlichen Steuerung. In der Folge räumte der Wissenschaftler gegenüber einem Kollegen sogar ein, dass er die detaillierte Beschreibung eines technischen Verfahrensablaufs zur Weitergabe an eine „geheime Stelle“ in seinem Heimatland benötigen würde.

Die Bemühungen chinesischer Nachrichtendienste zur Erlangung von wissenschaftlichem Know-how in Deutschland sind nicht auf die dargestellten Vorgehensweisen und Methoden beschränkt. Ergänzend dazu entwickeln Vereine chinesischer Akademiker unter mutmaßlicher nachrichtendienstlicher Steuerung rege Anstrengungen, sich nach Fachrichtungen spezialisiert, flächendeckend zu verbreiten. Anhaltspunkte deuten darauf hin, dass die Vereinsaktivitäten eng mit Angehörigen diplomatischer Vertretungen abgestimmt werden.

„Wer in China Geschäfte machen will, muss darauf gefasst sein, ausspioniert zu werden.“
(RA Dr. Berthold Stoppeltkamp, Geschäftsführer der Arbeitsgemeinschaft für Sicherheit in der Wirtschaft (ASW), Berlin, Quelle: Spiegel Online, 26. August 2007)

Die chinesischen Nachrichtendienste waren auch bemüht, in Deutschland Informationen über Gruppierungen und Organisationen zu gewinnen, welche die Machtposition der KPCh gefährden könnten. Betroffen hiervon waren in Baden-Württemberg die Falun-Gong-Bewegung⁴⁰⁸ sowie Personen uigurischer Abstammung.

2.2 Russische Föderation

Zur Wahrung seiner politischen, wirtschaftlichen und militärischen Interessen ist es der Russischen Föderation gerade auch in Zeiten der Erweiterung der Europäischen Union (EU) und des Nordatlantischen Verteidigungsbündnisses (NATO) überaus wichtig, Informationen über diese Entwicklungen zu erlangen, die nicht öffentlich zugänglich sind. Selbst gute zwischenstaatliche Beziehungen hindern die russische Auslandsaufklärung nicht daran, Spionageaktivitäten zu entfalten.

Auch 2007 wurden die russischen Nachrichtendienste erheblich aufgewertet. Die Ernennung des bisherigen Premierministers und Außenhandelsexperten Mikhail FRADKOV zum Leiter des zivilen Auslandsnachrichtendienstes SWR⁴⁰⁹ unterstreicht die herausragende Stellung dieser Organisation. Sie ist auf die Unterstützung des wirtschaftlichen und des Verteidigungspotenzials des Landes ausgerichtet und wirkt daneben bei der Bekämpfung der Proliferation und des internationalen Terrorismus mit. Ein weiteres Aufgabengebiet umfasst die Aufklärung von Aktivitäten und Arbeitsmethoden fremder und damit auch westlicher Nachrichtendienste. Auch wurden ihr im Bereich der elektronischen Fernmeldeaufklärung weitreichende Kompetenzen zugewiesen.

Die GRU⁴¹⁰ ist der militärische Auslandsnachrichtendienst der Russischen Föderation. In der Bundesrepublik Deutschland befasst er sich schwerpunktmäßig mit der Aufklärung der Bundeswehr und der Beschaffung militärisch nutzbarer Technologien. Damit ist er eingebunden in die ehrgeizigen Aufrüstungspläne, die russischen Streitkräfte bis 2015 mit einer neuen Generation von Kampfjets, Atom-U-Booten und Interkontinentalraketen auszustatten. Hinweise auf konkrete Ausforschungsziele werden immer dann bekannt, wenn es zu spektakulären Festnahmeaktionen wie im Juni 2007 in Salzburg/Österreich kommt. Dort konnte ein unter diplomatischer Abdeckung agierender russischer Agent bei der Treffabwicklung mit einem

⁴⁰⁸ Neue religiöse Bewegung aus China stammend auf der Basis von Qi Gong.

⁴⁰⁹ „Slushba Wneschnej Raswedkij“ („Dienst für Ermittlungen im Ausland“).

⁴¹⁰ „Glawnoje Raswedywatelnoje Uprawlenije“ („Hauptverwaltung für Aufklärung“ beim Generalstab der Streitkräfte).

früheren Mitarbeiter eines internationalen Luft- und Raumfahrtunternehmens festgenommen werden.

Der größte und mächtigste Apparat in der staatlichen Sicherheitsstruktur Russlands ist der Inlandsnachrichtendienst FSB⁴¹¹. Er ist für die zivile und militärische Spionageabwehr sowie für die Bekämpfung von Terrorismus und Organisierter Kriminalität zuständig. Umfassende weitere Kompetenzen besitzt er auf dem Gebiet des Fernmeldewesens und bei der Sicherheit in der Informationstechnik. Außerdem obliegen ihm die Sicherung der Staatsgrenze und die damit verbundene Kontrolle ein- und ausreisender Personen. Die letztgenannte Zuständigkeit eröffnet ihm ideale Möglichkeiten, ausländische Staatsbürger für eine Agententätigkeit anzuwerben und ebenfalls auf dem Feld der Auslandsaufklärung mitzuwirken.

Bei den Aktivitäten der russischen Dienste in Deutschland spielen die diplomatischen und konsularischen Vertretungen der Russischen Föderation sowie die hier ansässigen Niederlassungen ihrer Medienagenturen eine ebenso wichtige Rolle wie die zentrale Agentenführung aus Moskau. Vordringliches Interesse besteht an Messtechnik, Glasfaseroptik, Umwelt- und Energietechnik, aber auch an Kommunikations- und Überwachungs-ausrüstungen. Ein Großteil der benötigten Informationen wird aus offenen Quellen wie Medienbeobachtung, Gesprächsabschöpfung, Firmen- und Messebesuchen und durch die gezielte Internet-Auswertung zusammengetragen.

Der folgende Fall zeigt beispielhaft die verdeckte Agentengewinnung durch russische Geheimdienstangehörige:

- Ein Angehöriger eines russischen Nachrichtendienstes wurde auf einen leitenden Angestellten einer in Baden-Württemberg ansässigen Hightech-Firma aufmerksam. Der leitende Angestellte hielt sich zu Geschäftsverhandlungen in Russland auf. Der zunächst offene Kontakt wurde bald auf eine vertrauliche Basis gestellt, und der deutsche Staatsbürger nach Rückkehr in die Bundesrepublik zu einem vergnüglichen Abend in ein Restaurant eingeladen. Bei Festlegung der Treffmodalitäten waren sogleich weitere Zusammenkünfte abgestimmt worden. Der Firmenvertreter meinte, die wirkliche Absicht des Russen zu erkennen und befürchtete, dass der weitere Kontakt zu seinem neuen Bekannten die Aufmerksamkeit von Sicherheitsbehörden nach sich ziehen könnte. Er wandte sich des-

⁴¹¹ „Federalnaja Slushba Besopasnosti“ („Föderaler Dienst für Sicherheit“).

halb gleich nach dem Treffen an die Spionageabwehr und schilderte seine Wahrnehmungen.

2.3 Proliferation

Die Verbreitung von Massenvernichtungswaffen oder von Bestandteilen zu deren Herstellung hat sich trotz diverser Rüstungskontrollabkommen und Handelsbeschränkungen zu einem globalen sicherheitspolitischen Problem entwickelt. Die weltweite Betroffenheit über die Atomtests Nordkoreas und Pakistans macht dies mehr als deutlich.

Staaten wie der Iran, Nordkorea, Pakistan und Syrien sehen im Besitz von Massenvernichtungswaffen ein geeignetes Mittel, politische Forderungen gegenüber Nachbarländern oder der internationalen Staatengemeinschaft durchsetzen zu können. Obwohl sie bereits in Teilbereichen darüber verfügen, halten sie weiter an ihren Beschaffungszielen fest. Bestehende Arsenale sollen komplettiert sowie die Waffen hinsichtlich Einsetzbarkeit und Wirkung perfektioniert werden. Da die Länder nicht in vollem Umfang in der Lage sind, diese Aufgaben selbst zu lösen, versuchen sie, die notwendigen technischen Komponenten vor allem in den hoch entwickelten westlichen Industrienationen zu beschaffen. Eine Reihe von Staaten nutzt dabei gezielt die weltweite Zusammenarbeit wissenschaftlicher Einrichtungen und den speziell im Bereich der Grundlagenforschung weitreichenden internationalen wissenschaftlichen Austausch.

Auch wenn das militärische Nuklearprogramm des Iran möglicherweise seit dem Jahr 2003 nicht mehr weiter verfolgt worden ist, konnten weiterhin intensive Aktivitäten zur Erlangung von Gütern und Trägertechnologien für militärische Anwendungen aller Art festgestellt werden.

Iran versucht vor allem Spezialwerkzeugmaschinen, Mixer, Kreiseltechnologie, Windkanalaurüstung, Antriebs- und Steuerungssysteme, spezielle Messgeräte und Festtreibstoffkomponenten zu beschaffen. Bei den nachgefragten Waren handelt es sich häufig um so genannte Dual-use-Güter⁴¹², welche in ihren Parametern nur geringfügig von solchen Produkten abweichen, die der Exportkontrolle unterliegen.

- Ein mittelständisches baden-württembergisches Unternehmen, das Kälteanlagen produziert, hat Geschäftsverbindungen zu mehreren

⁴¹² Als „Güter mit doppeltem Verwendungszweck“ werden Güter einschließlich Datenverarbeitungsprogrammen und Technologien bezeichnet, die sowohl für zivile als auch für militärische Zwecke verwendet werden können.

iranischen Firmen. Bei einer Lieferung mussten als Folge der Exportbeschränkungen einzelne Bauteile ausgetauscht werden, um eine missbräuchliche Verwendung definitiv auszuschließen. Die grundsätzliche Funktionsfähigkeit der Anlage war dadurch zwar nicht beeinträchtigt, jedoch bewirkte der Umbau eine 20-prozentige Leistungseinbuße.

Die konspirative Vorgehensweise iranischer Beschaffungsorganisationen hat sich auch 2007 nicht geändert. Nach wie vor werden bereits in der Vergangenheit häufig praktizierte Verschleierungstechniken - Umgehungslieferungen über Drittländer, Einschaltung von Zwischenhändlern, Vortäuschung eines unverfänglichen Endempfängers oder zivilen Verwendungszwecks - angewandt. Mitunter werden Beschaffungsprojekte auch in mehrere separate Bestellungen an verschiedene Hersteller aufgeteilt.

- Eine baden-württembergische Maschinenbaufirma erhielt von einem Unternehmen im europäischen Ausland eine Anfrage zu der aktuellen Version einer Werkzeugmaschine, die Exportbeschränkungen unterliegt, weil mit ihr grundsätzlich auch Raketenteile hergestellt werden könnten. Ermittlungen ergaben, dass eine einschlägig bekannte iranische Beschaffungsorganisation speziell zum Kauf dieser Maschine eine Tarnfirma gegründet hatte, die ihrerseits wiederum eine Vertretung in Ostasien unterhält. Diese beauftragte die europäische Gesellschaft mit dem Kauf der Maschine, um die deutschen Ausfuhrbestimmungen durch eine Lieferung nach Ostasien zu umgehen. Von dort sollte die Anlage anschließend in den Iran verbracht werden. Da die Herstellerfirma über eine effiziente und fachkundige Exportabteilung verfügt, konnte dieses Geschäft rechtzeitig durchschaut und gestoppt werden.

Durch Tests von atomwaffenfähigen Kurz- und Mittelstreckenraketen erregte Pakistan 2007 internationale Besorgnis. Mit nachrichtendienstlichen Mitteln umgesetzte Beschaffungsbemühungen konzentrieren sich auf die Bereiche Atomwaffen und Trägersysteme. Pakistanische Einkäufer interessierten sich für entsprechende Hochtechnologie aus Baden-Württemberg. Sie bedienten sich dabei häufig der Unterstützung kleinerer Vermittlerfirmen.

3. Prävention

Unter Prävention versteht man die Gesamtheit aller vorbeugenden Maßnahmen zur Verhinderung nachrichtendienstlicher Aktivitäten, zu denen

*konspirative
Vorgehensweise
iranischer
Beschaffungs-
organisationen*

*Interesse an
Hochtechnologie
aus Baden-
Württemberg*

*politisches Druck-
mittel: Massenver-
nichtungswaffen*

der Verfassungsschutz aufgrund seines gesetzlichen Auftrags verpflichtet ist beziehungsweise aus Gründen der Opportunität im jeweiligen Einzelfall ergreift. Angesichts eines weltweit verschärften Wettbewerbs und einer ständig steigenden Abhängigkeit von moderner Informations- und Kommunikationstechnik gewinnen präventive Schutzmechanismen in Verzahnung mit der repressiven Spionageabwehr immer mehr an Bedeutung.

Das wirksamste Mittel gegen die illegale Nutzung des eigenen Wissens durch fremde Staaten, Konkurrenzunternehmen oder Einzelpersonen bietet ein umfassendes Informationsschutzkonzept. Jedoch garantiert nur die Kombination sorgfältig aufeinander abgestimmter personeller, organisatorischer sowie materieller Maßnahmen eine adäquate Schutzwirkung. Der Verzicht auf einen der genannten Bestandteile führt zwangsläufig zu Sicherheitslücken.

3.1 Wirtschaftsschutz - eine Schwerpunktaufgabe der Spionageabwehr

Die Wirtschaft ist einer der wichtigsten Faktoren für Stabilität und Leistungskraft unseres Gemeinwesens. Sie zu schützen, ist deshalb selbstverständliche Pflicht des Staates. Ziel des LfV ist es, der baden-württembergischen Wirtschaft eine kompetente Beratung anzubieten, um den hierzulande erarbeiteten technologischen Vorsprung zu sichern. Häufig erkennen Unternehmen Sicherheitsmängel nicht oder sind angesichts ihrer personellen und materiellen Möglichkeiten nicht in der Lage, sich gegen professionell geführte Angriffe fremder Nachrichtendienste oder konkurrierender Konzerne zu schützen. Insbesondere kleine und mittlere Unternehmen könnten durch Spionage sehr schnell in ihrer Existenz gefährdet sein.

Nach den bisherigen Erfahrungen können immer wieder dieselben Schwachstellen in den Firmen festgestellt werden, die gleichsam die Haupteinstellstelle für erfolgreiche Spionageaktivitäten bilden. Häufig wird das Thema Sicherheit nicht als Chefsache betrachtet und deshalb auch nicht in den Unternehmenszielen verankert. Dadurch mangelt es am Sicherheitsbewusstsein innerhalb des Betriebs. Fehlende Zugriffsbeschränkungen für firmeninterne Informationssysteme können unzufriedene Mitarbeiter dazu verleiten, Informationen an Konkurrenten weiterzugeben. Sicherheitsvorschriften werden von Praktikanten oder Mitarbeitern von Fremdfirmen missachtet, ohne dass diese ernsthafte Konsequenzen zu befürchten hätten. Andererseits kann präventives Sicherheitsmanagement die Gesamtsituation eines Unternehmens durchaus positiv beeinflussen. Die Sicherung der Wettbewerbsfähigkeit, die Optimierung des betriebswirtschaftlichen Erfolgs

sowie eine Imageverbesserung sind hier zu nennen. Ebenso können Haftungsrisiken vermieden werden.

Mit einer breiten Palette praxisgerechter Maßnahmen bietet das LfV „Hilfe zur Selbsthilfe“ an. In Sensibilisierungsgesprächen werden die Unternehmen beispielsweise bei der Erstellung eines betrieblichen Informationsschutzkonzepts unterstützt, das nach Möglichkeit die Benennung eines Sicherheitsverantwortlichen mit klaren Kompetenzzuweisungen enthalten sollte. Durch eine Risiko- und Schwachstellenanalyse kann die Gefährdungslage des Unternehmens detailliert unter die Lupe genommen werden. Awareness-Kampagnen fördern das Sicherheitsbewusstsein zusätzlich und schaffen „sicherheitsfreundliche“ Rahmenbedingungen.

„Gegen Datenverlust durch Diebstahl hilft vor allem das richtige Sicherheitsbewusstsein der Mitarbeiter in Kombination mit regelmäßigem Backup.“

(Frank Bunn, Senior Solutions Marketing Manager EMEA bei der Symantec Deutschland GmbH, Ratingen. Quelle: SecurityManager.de, 16. Mai 2007)

- Ein baden-württembergischer Chemiekonzern beispielsweise bat um Beratung bei der Erstellung eines Sicherheitskonzepts. Der bereits vorliegende Entwurf ließ keine ganzheitliche Betrachtungsweise in Bezug auf Informations- und Sabotageschutz erkennen. So fehlten räumliche Abtrennungen sensibler Arbeitsbereiche und eingeschränkte Zugriffsberechtigungen der Mitarbeiter auf das IT-Netz des Unternehmens. Die bauliche, mechanische und elektronische Absicherung wichtiger Konferenzräume war ebenfalls nicht zufrieden stellend gelöst. Betriebsfremde konnten ohne große Hindernisse schutzwürdige Arbeitsbereiche betreten. Die Mitarbeiter der Spionageabwehr wiesen den Sicherheitsverantwortlichen in Beratungsgesprächen auf die vorliegenden Schwachpunkte hin und gaben Empfehlungen zu deren Behebung. Diese fanden im neuen Sicherheitskonzept des Unternehmens entsprechende Berücksichtigung.

Für die Behandlung von Fällen des Spionageverdachts gibt das LfV praktikable und Erfolg versprechende Empfehlungen. Die nachträgliche Auswertung eines abgeschlossenen Falles kann unter Umständen eine bislang noch nicht erkannte Schwachstelle im Unternehmen offenbaren und wichtige Hinweise auf notwendig werdende Präventivmaßnahmen geben. Anlassbezogen oder in allgemeiner Form können baden-württembergische Unternehmen individuelle Empfehlungen zur personellen, organisatorischen und technischen Sicherheit erhalten. Nach § 10 Abs. 4 Landesverfassungsschutzgesetz (LVSG) dürfen personenbezogene Auskünfte allerdings nur unter ganz bestimmten Voraussetzungen erteilt werden.

*technologischen
Vorsprung in
Baden-Württemberg
sichern*

*mangelndes
Sicherheitsbewusstsein, ein
Spionagerisiko*

*„Hilfe zur
Selbsthilfe“*

*Empfehlungen
zur Spionageabwehr*

Anknüpfend an die bereits im Jahr 2006 rasant gestiegene Nachfrage nach Beratungsleistungen und Vortragsveranstaltungen durch Mitarbeiter der Spionageabwehr wurden auch im Jahr 2007 Firmen, Verbände und Behörden in zahlreichen Vorträgen über die aktuelle Risikolage hinsichtlich Spionage und Sabotage unterrichtet und Empfehlungen zur Verhinderung von Schäden sowie der richtigen Verhaltensweise im Konfliktfall gegeben.

Messeauftritt bei der „SAFEKON“

Im September 2007 beteiligte sich das LfV an der in **Karlsruhe** veranstalteten Fachmesse für Zutrittskontrolle, Gebäudesicherung und Informationsschutz „SAFEKON“. Diese erstmals ausgerichtete Produkt- und Leistungsschau erwies sich als ideale Plattform, das breit gefächerte Aufgabenspektrum des Verfassungsschutzes in Baden-Württemberg und besonders des Arbeitsbereichs Wirtschaftsschutz einem interessierten Besucherkreis bekannt zu machen. In intensiven Gesprächen, die sich schwerpunktmäßig um die Komplexe Wirtschaftsspionage, Know-how-Schutz und abhörsicheres Büro drehten, zeigten die Messebesucher großes Interesse an der Aufklärungsarbeit des LfV. Ein attraktives Begleitprogramm bot Vorträge zu Methoden der Wirtschaftsspionage, zum Einsatz technischer Mittel sowie zu strategischen Gesamtkonzepten für das Gebäudemanagement an.



Ein wichtiges Element in der Verhinderung von Spionage und Sabotage stellt der förmliche Geheim- und Sabotageschutz als Teil der gesetzlich verankerten Mitwirkungsaufgaben dar. Die in § 3 Abs. 3 LVSG aufgelisteten Aufgaben umfassen unter anderem Sicherheitsüberprüfungen von Personen sowie die Festlegung organisatorischer und technischer Maßnahmen. In Baden-Württemberg sind derzeit über 200 Unternehmen in das amtliche Geheimschutzverfahren einbezogen und rund 20 als lebens- und verteidigungswichtig eingestuft. Sie werden vom LfV regelmäßig über sicherheitsgefährdende Bestrebungen sowie Aktivitäten fremder Nachrichtendienste unterrichtet und entsprechend beraten.

3.2 Sicherheitsforum Baden-Württemberg - Die Wirtschaft schützt ihr Wissen

Der Spionageabwehr des LfV ist es seit jeher ein besonderes Anliegen, flankierend zu den eigenen Sensibilisierungsmaßnahmen auch vergleichbare Aktivitäten anderer Institutionen zu unterstützen. Vor diesem Hintergrund kam der Mitarbeit in dem 1999 ins Leben gerufenen Sicherheitsforum

Baden-Württemberg - Die Wirtschaft schützt ihr Wissen - von Anfang an eine besondere Bedeutung zu.

Nach der im Jahr 2006 gestarteten Vortragsreihe zu Aspekten der Unternehmenssicherheit, mit der vor allem kleine und mittlere Unternehmen mit aktuellen Risikosituationen vertraut gemacht werden sollten, hat das aus Firmen, Forschungseinrichtungen, Verbänden, Kammern und Behörden bestehende Forum im Jahr 2007 einen neuen Ansatz gewählt, um das Bewusstsein für die Gefahren der Wirtschaftsspionage und der Ausspähung durch konkurrierende Unternehmen zu schärfen. Die erstmalige Ausschreibung eines unter der gemeinsamen Schirmherrschaft von Innenminister Heribert Rech und Wirtschaftsminister Ernst Pfister stehenden Wettbewerbs für herausragende Projekte der betrieblichen Sicherheit mit Zielrichtung Know-how-Schutz wurde als wichtiger Beitrag angesehen, um den Schutz der in Baden-Württemberg ansässigen Wirtschaft vor dem Diebstahl von Know-how, Produkt-Ideen und Innovationen zu verbessern.

Eine Fachjury hat unter den eingegangenen Bewerbungen die besten Projekte ausgewählt. Über 100 Gäste kamen am 14. September 2007 zur Verleihung des Sicherheitspreises Baden-Württemberg durch Innenminister Heribert Rech bei der Sicherheitsmesse „SAFEKON“ in **Karlsruhe**. Minister Rech hob besonders hervor, dass alle Projekte des Wettbewerbs „durch Innovationskraft, Kreativität und Engagement im Bemühen um den Schutz des Know-hows von Unternehmen und Forschungseinrichtungen überzeugen“. Zugleich werde damit dokumentiert, dass es in Baden-Württemberg bereits viele vorbildliche Projekte gibt, die Anregung und Beispiel für eigene unternehmensinterne Sicherheitsvorkehrungen sein können.



4. Bedeutung von Hinweisen - Erreichbarkeit der Spionageabwehr

Zur Wahrnehmung ihrer Aufgaben ist die Spionageabwehr auch ganz wesentlich auf Hinweise aus der Öffentlichkeit angewiesen. Häufig ermög-

*Bewusstsein
schärfen für die
Gefahren der
Wirtschafts-
spionage*

*Geheim- und
Sabotageschutz,
ein Teil der
Spionageabwehr*

lichen beispielsweise erst Informationen aus unmittelbar betroffenen Unternehmen oder wissenschaftlichen Einrichtungen die Ermittlungen zur Klärung eines Verdachts auf Wirtschaftsspionage. Viele Betroffene scheuen jedoch aufgrund einer Unterschätzung des Falles oder falsch verstandener Furcht vor Imageverlusten eine Kontaktierung der Spionageabwehr.

Das LfV unterstützt geschädigte Firmen oder Institute bei der weiteren Handhabung des Verdachtsfalls. So werden Fehler vermieden, die sonst zur Ausweitung des Schadens führen können.

Die Spionageabwehr kann - auch für Anregungen und weitere Informationen - wie folgt erreicht werden:

Landesamt für Verfassungsschutz Baden-Württemberg
Abteilung 4
Taubenheimstraße 85 A
70372 Stuttgart

Telefon 07 11 / 95 44 - 301
Telefax 07 11 / 95 44 - 444
info@verfassungsschutz-bw.de

Über die Anschlüsse

07 11 / 9 54 76 26 (Telefon) und
07 11 / 9 54 76 27 (Telefax)

werden sensible Hinweise entgegengenommen und auf Wunsch vertraulich behandelt.

Hintergrundinformationen und Aktuelles zum Thema Spionageabwehr erhalten Sie auch im Internet unter:

http://www.verfassungsschutz-bw.de/spio/start_spio.htm

