Informationsschutz

in der gewerblichen Wirtschaft

-

mit Sicherheit ein Gewinn!

Vorwort

Wissen bedeutet Macht; geraten schützenswerte Informationen in falsche Hände, ist Mißbrauch vorprogrammiert. Diese Broschüre nimmt sich des Informationsschutzes als eines der zentralen Themen unserer modernen Informations- und Kommunikationsgesellschaft an und befasst sich mit den notwendigen Maßnahmen gegen die illegale Nutzung des eigenen Wissens.

Telefax, Handys, Internet, E-mail und Computernetzwerke gehören heute zum Alltag und die persönliche Abhängigkeit von diesen Systemen gewinnt immer mehr an Bedeutung. Daher muss auch dem Informationsschutz ein höherer Stellenwert zukommen.

Im Rahmen der von der Landesregierung Rheinland-Pfalz im Bereich der Inneren Sicherheit praktizierten Sicherheitspartnerschaft zwischen einer innovativen Wirtschaft, den Bürgerinnen und Bürgern sowie dem Staat will der rheinland-pfälzische Verfassungsschutz mit der vorliegenden Broschüre einen weiteren konstruktiven Beitrag zum "Informationsschutz in der gewerblichen Wirtschaft" leisten.

Den Leserinnen und Lesern wird ein Überblick über die wesentlichen Gefahren, die Wirtschaftsunternehmen durch den Verlust von Betriebsgeheimnissen drohen, und über mögliche Schutzmaßnahmen gegeben. Dies ist aber nur ein erster Einstieg in ein sehr wichtiges und komplexes Thema. Der rheinland-pfälzische Verfassungsschutz bietet darüber hinaus ein weiteres Beratungs- und Informationsangebot. Sein Motto lautet: Aufklären statt Belehren. Sein Ziel ist die Suche nach optimalen Lösungen bei vergleichsweise geringem administrativen wie finanziellen Aufwand.

Nehmen Sie dieses Angebot an. Beteiligen Sie sich damit an unserer Sicherheitspartnerschaft. Lassen Sie uns gemeinsam handeln, denn: Ihre Sicherheit ist unser aller Interesse.

Walter Zuber
Minister des Innern und für Sport

Informationsschutz
in der gewerblichen Wirtschaft
-
mit Sicherheit ein Gewinn!

Inhalt

1. Verfassungsschutz - Aufgabe Spionageabwehr, Geheim- und Sabotageschutz

Auch zehn Jahre nach Ende des Kalten Krieges ist die gegen die Bundesrepublik Deutschland gerichtete Spionage ein wichtiges und aktuelles Thema der Inneren und Äußeren Sicherheit. Die größer gewordene politische Bedeutung des wiedervereinigten Deutschlands, seine wirtschaftliche Leistungsfähigkeit sowie das hohe Niveau der Forschung und Entwicklung erklären das anhaltend intensive Aufklärungsinteresse fremder Staaten. Im Mittelpunkt der Ausspähungsbemühungen stehen die Bereiche Wirtschaft, Wissenschaft und Technik. Daneben hat aber auch die klassische Spionage mit Zielrichtung Politik und Militär eine gleichbleibend hohe Bedeutung.

Als Spionage wird landläufig das Auskundschaften schwerpunktmäßig der vorgenannten Bereiche Politik, Militär und Wirtschaft mit Mitteln der geheimen Nachrichtenbeschaffung bezeichnet. Ein besonderes Augenmerk wird dabei auf jegliche als Geheimnisse besonders geschützte Informationen gelegt.
Die Abwehr von Spionage gehört zu den originären Aufgaben des Verfassungsschutzes. Der Begriff Spionage wird allerdings ausdrücklich weder im Strafrecht noch in den Verfassungsschutzgesetzen gebraucht. Hier finden sich Bezeichnungen wie geheimdienstliche Agententätigkeit (für eine fremde Macht) oder - in den Verfassungsschutzgesetzen - **geheimdienstliche Tätigkeiten für eine fremde Macht**. Demnach ist der Verfassungsschutz gesetzlich gehalten, hierüber Nachrichten und sonstige Unterlagen zu sammeln und auszuwerten. Dabei erstreckt sich seine Zuständigkeit ausschließlich auf den Geltungsbereich der Verfassungsschutzgesetze, also auf das Staatsgebiet der Bundesrepublik Deutschland. Zu den beschriebenen geheimdienstlichen Tätigkeiten zählen mit Schwerpunkt die **Spionage**, aber auch **Sabotage** und **Subversion**

Im Hinblick auf die Aufgabenbeschreibung und die Zuständigkeiten des Verfassungsschutzes ist **jede nicht unmittelbar oder mittelbar staatlich gelenkte Ausspähungstätigkeit ohne Belang**. Somit fallen beispielsweise die Abwehr von Verratsdelikten, die Privat- oder Geschäftsgeheimnisse (vgl. §§ 203 u. 204 Strafgesetzbuch - StGB) betreffen, nicht in die Zuständigkeit der Verfassungsschutzbehörden. Hierzu

zählt insbesondere auch die Industriespionage, d.h. das Ausspähen von Betriebsgeheimnissen durch konkurrierende Firmen (sog. Konkurrenzspionage).
Spionageabwehr darf sich aber nicht nur darauf beschränken, Agenten zu enttarnen. Eine weitere originäre Aufgabe des Verfassungsschutzes ist es, nachrichtendienstlichen Angriffen durch präventive Maßnahmen wirksam zu begegnen. Dem **Geheim- und Sabotageschutz** kommt daher im Rahmen dieser Vorbeugung eine wesentliche Bedeutung zu. Seine Aufgabe ist es, die Voraussetzungen dafür zu schaffen, dass Unbefugte keine Kenntnis von im öffentlichen Interesse geheimhaltungsbedürftigen Informationen (Verschluss-Sachen) erhalten.
Der **materielle Geheimschutz** bezieht sich auf technische und organisatorische Sicherheitsmaßnahmen zum Schutz dieser Verschluss-Sachen. Der **personelle Geheimschutz** befasst sich im Wesentlichen mit der Sicherheitsüberprüfung von Personen, die eine sicherheitsempfindliche Tätigkeit insbesondere im öffentlichen Dienst ausüben sollen. Hierzu können auch Angehörige privater Unternehmen zählen.

2. Geheimschutz in der Wirtschaft

Für die Einhaltung des Geheimschutzes in der Wirtschaft ist zunächst das Bundesministerium für Wirtschaft und Technologie zuständig. Daneben wirken auch die Verfassungsschutzbehörden des Bundes und der Länder mit. Der rheinland-pfälzischen Verfassungsschutzbehörde obliegt vor allem die sicherheitsmäßige Beratung und Betreuung geheimschutzrelevanter Betriebe. Umfang und Intensität der gegenseitigen Beziehungen orientieren sich an der Bedeutung, am Auftrag sowie an der nachrichtendienstlichen Gefährdungslage des jeweiligen Schutzobjektes. Beispielsweise führt der Verfassungsschutz Sicherheitsüberprüfungen der in den Firmen tätigen Geheimnisträger durch.
In Rheinland-Pfalz befinden sich zur Zeit 50 solcher Wirtschaftsunternehmen in der behördlichen Geheimschutzbetreuung. Damit profitiert aber nur ein kleiner Teil der Betriebe in unserem Land von den staatlichen Schutzmaßnahmen. Es handelt sich dabei in erster Linie um Betriebe der Verteidigungswirtschaft, die geheimzuhaltende staatliche Aufträge ausführen. Um einen ausreichenden Schutz der auf amtliche Veranlassung geheim zu haltenden Angelegenheiten zu gewährleisten, müssen die betroffenen Unternehmen die Bestimmungen des Handbuchs für den Geheimschutz in

der Wirtschaft durch eine rechtsverbindliche Erklärung gegenüber dem Bundesminister für Wirtschaft und Technologie anerkennen.

Die formellen Mitwirkungsaufgaben beim Geheimschutz nimmt der Verfassungsschutz nur im Bereich amtlicher Schutzwürdigkeit und zur Sicherung lebens- oder verteidigungswichtiger Einrichtungen wahr. Dagegen sind die Wirtschaftsunternehmen im "offenen" Bereich grundsätzlich auf Eigeninitiative und Selbsthilfe angewiesen; sie sind somit Spionageangriffen weitgehend schutzlos ausgeliefert. Es kommt deshalb maßgeblich darauf an, welchen Stellenwert die Informationssicherheit in diesen Betrieben einnimmt. Dabei ist allerdings häufig festzustellen, dass vor allem bei den besonders ausspähungsgefährdeten mittelständischen Unternehmen und bei der Neugründung innovativer Firmen Sicherheitsüberlegungen seltener eine angemessene beachtung finden. Gerade in diesem Bereich besteht deshalb ein erhöhter Beratungsbedarf.

3. Beratung durch den Verfassungsschutz - Mit Sicherheit ein Gewinn

Der Geheim- und Sabotageschutz gewinnt in einer Zeit ständig steigender Abhängigkeit von modernen Informations- und Kommunikationssystemen und einer fortschreitenden weltweiten Vernetzung von Computersystemen zunehmend an Bedeutung. In unserer modernen Informationsgesellschaft sind Internet, ISDN, E-mail, Telefax, Handys und Computernetzwerke inzwischen selbstverständliches Arbeitsmittel.
Der Schutz von Informationen gegen unbefugte Kenntnisnahme wird somit zu einer komplexen wie wichtigen Aufgabe in allen Bereichen.
Der rheinland-pfälzische Verfassungsschutz bietet deshalb seine Unterstützung im Rahmen einer **Sicherheitspartnerschaft zwischen Staat und Wirtschaft** an. Denn: Informationsschutz durch ein erfolgreiches Sicherheitsmanagement ist eine gemeinsame Aufgabe, die in unser aller Interesse liegt.
Eine entsprechende Beratung kann Entscheidungsträgern der Führungsebene in Unternehmen zu einem erfolgreichen Sicherheitsmanagement verhelfen. Im Rahmen einer solchen Beratung durch den Verfassungsschutz werden Informationen zur Gefährdung durch Spionage, aber auch zur Gefährdung durch verfassungsfeindliche Organisationen mit Bezug zur Wirtschaft allgemein oder zu bestimmten Branchen und Be-

trieben vermittelt. Daneben werden firmenbezogene Schutzkonzepte diskutiert, bei denen das betriebliche Sicherheitswesen, Problemstellungen im personellen Bereich und Probleme bei der Absicherung von Unternehmen eine Rolle spielen. Solche Beratungsleistungen des rheinland-pfälzischen Verfassungsschutzes sind kostenfrei.
Diese Broschüre wendet sich daher in erster Linie an die Wirtschaftsunternehmen im "offenen" Bereich und gibt diesen einen Überblick über die Gefahren von Informationsverlusten und über mögliche Schutzmaßnahmen.

4. Informationsverluste - Gefahren und Folgen

In Deutschland entstehen jährlich Milliardenverluste durch Spionage und unkontrollierten Know-how Abfluss. Dies beeinträchtigt und gefährdet den Wirtschaftsstandort Deutschland im Allgemeinen und die Unternehmen, ihre Finanzkraft, ihr Ansehen und die Arbeitsplätze im Besonderen.

4.1 Gefahr durch Spionage - Schwerpunkte, Mittel und Methoden

Die Schwerpunkte der Ausspähungsaktivitäten fremder Nachrichtendienste haben sich in den vergangenen Jahren ungeachtet des politischen Umbruchs in Osteuropa nicht wesentlich verändert. Die Interessen sind breit gefächert, sie umfassen nahezu den gesamten Bereich der industriellen Forschung und Produktion, des Handels und der wirtschaftlichen Organisation. Im Vordergrund des Ausforschungsinteresses stehen dabei forschungs- und entwicklungsintensive Hochtechnologiebereiche. Die Schwerpunkte der Informationsbeschaffung sind primär im Bereich der zukunftsichernden Querschnittstechnologien mit dualer Verwendungsmöglichkeit zu finden. Dabei handelt es sich insbesondere um folgende Bereiche:

- Informationsverarbeitung/Kommunikationstechnik/Elektronik
- Luft- und Raumfahrt/Verkehrstechnik
- Werkstoffe
- Produktionstechnik
- Biotechnik und Medizin
- Energie- und Umwelttechnik

Fremde Nachrichtendienste interessieren sich auf diesen Gebieten für alle Arten von Informationen. Dabei stehen naturgemäß Betriebsgeheimnisse deutscher Unternehmen an erster Stelle. Solche Geheimnisse können auf allen Ebenen und in allen Bereichen eines Unternehmens entstehen. Im Einzelnen kann es sich dabei um folgende Informationen handeln:

- Strategische/taktische Entscheidungen der Unternehmensleitung
- Forschungsergebnisse, Produktideen und Designstudien
- Konstruktionsunterlagen, Herstellungsverfahren, Quailtätsprüfungsmaßnahmen, Spezialwerkzeuge und Steuerungssysteme
- Lieferanten, Versorgungskonzeptionen, Lagerbestände
- Verkaufsstrategien, Marketingstudien, Absatz-/Vertriebswege, Lizenzverträge, Umsätze und Kundenadressen
- Kalkulationsunterlagen, Budgetplanungen und Investitionsvorhaben
- sowie weitere Informationen aus sämtlichen Unternehmensbereichen

Gefährdet sind vor allem die Branchenführer bzw. Unternehmen mit herausragendem Know-how, wobei die Größe des Betriebs keine entscheidende Rolle spielt. Deshalb müssen auch innovative Klein- und Mittelbetriebe jederzeit damit rechnen, ein begehrtes Ausspähungsziel zu sein.

Mittel und Methoden der Spionage haben sich in den letzten Jahren teilweise verändert. Es wird heute vermehrt versucht, Informationen bereits (offen) über gesellschaftliche Kontakte und harmlos erscheinende Gespräche zu gewinnen. Hierbei kommt man in aller Regel ohne die Ausübung von Druck oder erpresserischer Methoden aus.
Auch die Auswertung anderer „offener“ Quellen genießt große Bedeutung. Hierzu zählen vor allem die systematische Erfassung von wissenschaftlichen Forschungsberichten, Diplomarbeiten, Fachliteratur, Werkszeitungen, Handbüchern, Dokumentationen und Werbe- bzw. Informationsmaterial sowie die Inanspruchnahme von Datenbanken und öffentlichen Bibliotheken, die ein breites Wissensspektrum eröffnen und Hinweise auf aktuelle Planungen und Projektverantwortliche geben.

Der offene Umgang mit Geschäftspartnern aus Osteuropa birgt zudem die Gefahr sorgloser Kontakte bei Messen, Ausstellungen, Kongressen, Symposien, Seminaren und Betriebsbesichtigungen. Der berechtigte Stolz auf die eigene Leistung kann dann z.B dazu führen, dass im Laufe einer Fachdiskussion oder eines Verkaufsgespräches notwendige Sicherheitsüberlegungen vergessen werden.

Fremde Nachrichtendienste nehmen auch durch eigens gegründete Firmen aktiv am Wirtschaftsleben in unserem Land teil. So bieten etwa "gemischte" Firmen und Joint-Ventures die Möglichkeit, nachrichtendienstlich tätige Personen abzutarnen. Fremde Nachrichtendienstoffiziere, die als angebliche Geschäftsleute Angebote einholen oder Scheinverhandlungen führen, sind gerade angesichts dieser Tarnung für Unkundige, die ihnen selten Misstrauen entgegenbringen, nicht als solche identifizierbar.

Immer mehr in den Vordergrund rückt heute die Nutzung moderner Informationstechnik. Elektronischer Datenaustausch der Wirtschaftsunternehmen mit immer leistungsfähigeren Informations- und Kommunikationsmitteln eröffnet kaum mehr kontrollierbare Zugangs- und Zugriffsmöglichkeiten berechtigter und unberechtigter Nutzer.

Eine große Gefahr für die Sicherheitsinteressen eines Unternehmens sind auch die konspirativ auftretenden Agenten eines fremden Nachrichtendienstes in dessen Zielobjekten. Die eigenen Mitarbeiter in einem Wirtschaftsunternehmen sind im Hinblick auf ihre Zugangsmöglichkeiten und ihr Wissen über innerbetriebliche Schwachstellen in der Lage, mehr Vertrauliches zu verraten als von außerhalb operierende Agenten herauszufinden vermögen. Fremde Nachrichtendienste unternehmen deshalb große Anstrengungen, hoch qualifizierte Fachleute in den für sie interessanten Unternehmen für ihre Zwecke anzuwerben.

4.2 Gefahr durch verfassungsfeindliche Organisationen

Nicht nur fremde Nachrichtendienste versuchen an Betriebsgeheimnisse von Wirtschaftsunternehmen zu gelangen, um diese Informationen für ihre Zwecke zu nutzen. Auch Organisationen, die in Verdacht stehen, verfassungsfeindliche Ziele zu verfolgen, sind daran interessiert, Firmen auszuforschen. Beispielsweise verfolgt die

„Scientology-Organisation“ (SO) das Ziel, die Wirtschaft zu unterwandern. Zu diesem Zweck bedient sie sich u.a. des im Jahre 1979 gegründeten weltweiten Verbandes „Word Institut of Scientology Enterprices“ (WISE). Durch WISE sollen die scientologische "Verwaltungstechnologie" und die damit verbundenen totalitären Kontrollmechanismen in Unternehmen zur Anwendung gelangen. Insbesondere Angebote zur Personal- und Managementschulung dienen dabei der Kontaktaufnahme im Wirtschaftsbereich.
Die SO verfolgt das Ziel, Schlüsselpositionen in Unternehmen mit ihren Mitgliedern zu besetzen und dadurch nach einer Art Schneeballsystem die Wirtschaft mit einem scientologischen Netzwerk zu überziehen.

Nähere Informationen zum Thema SO finden Sie in der Broschüre des rheinland-pfälzischen Verfassungsschutzes "Aus guten Gründen! Beobachtung der ‘Scientology’-Organisation durch den Verfassungsschutz. Darüber hinaus steht das **vertrauliche Scientology-Kontakttelefon** mit **Telefax** des rheinland-pfälzischen Verfassungsschutzes unter der Nr. **0 61 31/16-37 77** zur Verfügung.

4.3 Folgen des Informationsverlustes

Durch Spionage wollen Staaten ihre politische, wirtschaftliche und militärische Situation verbessern. Deshalb versuchen sie, hier in Deutschland illegal zu beschaffen, was legal zu teuer oder gar nicht zu haben wäre. Wettbewerbsnachteile sollen mit unlauteren Mitteln möglichst zum Nulltarif ausgeglichen werden. Wirtschaftsspionage aber auch illegaler Wissenstransfer und unkontrollierter Know-how Abfluss können die wirtschaftliche Kraft und Reputation deutscher Unternehmen gefährden und besonders kleinen und mittelständischen Firmen sogar existentielle Probleme bereiten.
Es gibt eine Fülle von Beispielen, dass Firmen immense Summen in die Entwicklung eines Produktes investiert haben , das sie später nicht mehr gewinnbringend verwerten konnten, weil die Konkurrenz vorher ein identisches Produkt erheblich preiswerter angeboten hat. Insbesondere für Klein- und Mittelbetriebe kann dies unter Umständen das wirtschaftliche Aus bedeuten. Informationsverluste werden nämlich oft erst festgestellt, wenn ein dadurch entstandener Nachteil nicht mehr ausgeglichen werden kann.

Daher: Haben Sie schon einmal Aufträge ohne nachvollziehbare Gründe verloren? Oder haben Sie vielleicht identische Entwicklungen Ihres Unternehmens auf anderen Märkten entdeckt?

Wenn Sie eine dieser Fragen mit **JA** beantworten, sollten Sie darüber nachdenken, ob Ihr Unternehmen sicher ist. Nehmen Sie sich Zeit für den kleinen Sicherheitstest, den Sie am Ende dieser Broschüre finden.

5. Informationsschutz - Was können wir gemeinsam tun?

Die gewerbliche Wirtschaft - kleine Unternehmen wie große Firmen - soll in die Lage versetzt werden, angemessen auf Gefährdungen durch Spionage, Sabotage und Extremismus reagieren zu können. Sicherheit in der Wirtschaft hilft mit, den Standort Rheinland-Pfalz zu stabilisieren und verringert die Spionageanfälligkeit bei Geschäftsverbindungen und -aufträgen in nachrichtendienstlich relevanten Bereichen. Mittelbar trägt ein angemessenes Mehr an Sicherheit dazu bei, der Wirtschaft erfolgreiche Geschäfte und Umsätze zu ermöglichen sowie Arbeitsplätze zu erhalten.
Unternehmen müssen sich des Risikos von Informationsverlusten bei ihren Außenbeziehungen bewußt werden und dagegen geeignete Maßnahmen ergreifen. Präventive Abwehrmaßnahmen müssen sodann auf der Basis einer ganzheitlichen Betrachtung des jeweiligen Unternehmens konzipiert werden.
Dabei berät und unterstützt sie auch der rheinland-pfälzische Verfassungsschutz. Ausgangspunkt sollte eine gemeinsame Analyse der Gesamtsituation des Unternehmens sein, die die Risiken und Schwachstellen erfasst. Ziel dieser Analyse ist die Entwicklung eines unternehmensbezogenen Sicherheitskonzepts. Ein solches Konzept kann aber nur erfolgreich sein, wenn alle Bereiche eines Betriebes einbezogen werden: Es müssen also personelle, organisatorische und materielle Sicherheitsmaßnahmen getroffen werden. Koordiniert und aufeinander abgestimmt ergeben diese Maßnahmen ein **unternehmensbezogenes Sicherheitskonzept**.

Ausgangsbasis für das angestrebte betriebliche Sicherheitsniveau sollte zunächst die Bestellung einer/eines mit festen Aufgaben versehenen **Sicherheitsverantwortlichen** sein, die/der möglichst hochrangig in der Firmenhierarchie angesiedelt ist. Sie/er muss in alle relevanten Abläufe und Planungen eingebunden sein und auf die Unterstützung von Spezialisten aus den einzelnen Sparten (beispielsweise Datenverarbeitung, Datensicherheit, Technik, Controlling, Revision) zurückgreifen können. Sie/er erarbeitet das Sicherheitskonzept, führt es in die Praxis ein, überwacht die Einhaltung der Richtlinien und passt das Konzept jederzeit den neuesten Erfordernissen an. Name, Erreichbarkeit und Aufgabenspektrum dieser Vertrauensperson sollten allen Belegschaftsmitgliedern bekannt sein. Nur dann steht zu erwarten, dass sicherheitserhebli-

che Vorkommnisse oder Verbesserungsvorschläge aufgenommen und umgesetzt werden.

5.1 Personelle Sicherheitsmaßnahmen

Betriebliche Sicherheitskonzeptionen müssen vor allem an den Mitarbeiterinnen und Mitarbeitern und somit zunächst an personellen Sicherheitsmaßnahmen ausgerichtet sein. Denn in allen Bereichen und auf allen Ebenen können sie mehr verraten als fremde Nachrichtendienste oder Wettbewerbskonkurrenten auf andere Weise herausfinden könnten. Personelle Sicherheitsmaßnahmen sollten mit der Personalauswahl bei Einstellungen und Versetzungen beginnen und über Personaleinsatz, -entwicklung und -betreuung bis hin zur Personalfreisetzung reichen. Die sicherheitsmäßige Sensibilisierung des Personals spielt dabei eine herausragende Rolle. Nur problembewußte Mitarbeiterinnen und Mitarbeiter sind zu präventivem Handeln in der Lage. Auch verinnerlichen sie durch die Sensibilisierung die von der Unternehmensleitung vertretene Sicherheitsphilosophie. Dadurch werden sie in ihrem Verhalten auf die Vermeidung von sicherheitsrelevantem Fehlverhalten hinwirken und auf diese Weise ihren Beitrag zur Sicherheit in dem Unternehmen leisten.

5.2 Organisatorische Sicherheitsmaßnahmen

Das zweite tragende Element innerbetrieblichen Informationsschutzes sind die organisatorischen Sicherheitsmaßnahmen. Organisatorische Einzelmaßnahmen der Unternehmenssicherheit können die Definition und Beurteilung sicherheitsempfindlicher Bereiche, die Festlegung von Zugriffsberechtigungen zu schutzbedürftigen Daten und Objekten, die Erstellung von verbindlichen Vorgaben für die gesicherte Aufbewahrung von Daten und Objekten, die Festlegung von sicherheitsrelevanten Arbeitsabläufen, Richtlinien für den Empfang und die Betreuung von Besuchern, die Festlegung routinemäßiger Sicherheits-Checks sowie die Sicherstellung einer regelmäßigen Analyse des Gefährdungspotentials im Zusammenwirken mit den Mitarbeiterinnen und Mitarbeitern sein. Ihre logische Ergänzung finden diese Maßnahmen durch die materielle Absicherung.

5.3 Materielle Sicherheitsmaßnahme

Die nachfolgende Aufzählung von materiellen Sicherheitsmaßnahmen kann bei der Komplexität des Themas und den oft sehr speziellen Sicherheitsbedürfnissen unterschiedlicher Unternehmen nur ein Denkanstoß sein. In jedem Fall ist daher eine objektbezogene Fachberatung erforderlich.
Im Außenbereich eines Unternehmens können mechanische/technische Vorkehrungen durch eine Umzäunung, eine Freigeländesicherung oder Zugangskontrollanlagen erfolgen. Organisatorische Vorkehrungen wie Bewachung/Bestreifung, Aufschaltung von Gefahrenmeldeanlagen auf Sicherheitszentralen sowie die Festlegung von Sicherheitsbereichen sind ebenfalls zu bedenken. Innerhalb konkret definierter Sicherheitsbereiche (z.B. Datenverarbeitungszentren) sind zusätzlich die räumlich sichere Unterbringung, die Installation von Gefahrenmeldeanlagen, Zugangskontrollen und Sicherheitsverglasung zu beachten.

Fazit: Insgesamt bleibt festzuhalten, dass die Kette betrieblicher Sicherheitsmaßnahmen nur so stark ist wie ihr schwächstes Glied. Ihre Wirksamkeit wird in erster Linie davon bestimmt, inwieweit die Einzelmaßnahmen sinnvoll und angemessen aufeinander abgestimmt und koordiniert sind. Alle Schutzvorkehrungen sind zudem nur in dem Maße effektiv, in dem sie die Akzeptanz der Mitarbeiterinnen und Mitarbeiter finden. Hinzu kommt, dass die Zustimmung dann am größten ist, wenn aus den Maßnahmen - sei es auch nur mittelbar - ein persönlicher Nutzen für die Beschäftigten abgeleitet werden kann (beispielsweise Stärkung der Wettbewerbsfähigkeit des Unternehmens, Erhalt von Arbeitsplätzen usw.).

6. Ein praktisches Beispiel: Der Lauschangriff - Maßnahmen und Gegenmaßnahmen

Das Schaubild in der Mitte dieser Broschüre zeigt die vielfältigen Möglichkeiten für Lauschangriffe auf geschlossene Räume, die bei der illegalen Informationsbeschaffung zur Anwendung kommen können. Diesen zahlreichen Angriffsmethoden sollten präventive Maßnahmen sowie geeignete Prüfungsmethoden gegenübergestellt wer-

den. Als Schutzmaßnahmen gegen Lauschangriffe mit dem Ziel der ungesetzlichen Ausspähung sind u.a. geeignet:

- Verlagerung des Konferenzraumes/Büros in einen anderen, von außen nicht einsehbaren Gebäudeteil
- Regelmäßige Überprüfung der Netz-, Telefon- und Datenleitungen auf Manipulationen
- Zugangskontrollen, Einrichtung eines überwachten Sicherheitsbereiches
- Verwendung von zugelassenen, abstrahlsicheren Geräten
- Verwendung von Netz-, Telefon- und Datenleitungsfiltern
- Einsatz von Einrichtungen zum Aufspüren von aktiven Minisendern
- Einsatz von akustisch gedämmten bzw. elektromagnetisch geschirmten Kabinen

7. Sicherheitstest

Nehmen Sie sich jetzt die Zeit für einen kleinen Sicherheitstest und beantworten Sie bitte noch die folgenden Fragen. Sollte Ihre Antwort in nur einem Fall **NEIN** lauten, empfiehlt sich eine Beratung durch den rheinland-pfälzischen Verfassungsschutz.

Ist bei Ihnen Sicherheit Chefsache?

Existiert in Ihrer Firma ein Sicherheitskonzept?

Gibt es in Ihrem Unternehmen einen Sicherheitsverantwortlichen?

Gibt es in Ihrem Unternehmen einen IT-Beauftragten, der für den Schutz von Daten und Programmen bei der Verarbeitung, Speicherung und Übertragung zuständig ist?

Haben Sie bei Verlust eines Auftrages geprüft, ob möglicherweise ausländische Partnerfirmen davon profitieren?

Gehen Sie der Sache nach, wenn identische Produkte Ihrer Firma von Konkurrenzunternehmen angeboten werden?

Sind Ihre Geschäftspartner bzw. Fremdfirmen in das eigene Sicherheitssystem integriert?

Sind eventuelle Geschäftsrückgänge nur auf konjunkturelle oder betriebswirtschaftliche Gründe zurückzuführen?

Sind Sie der Meinung, dass Deutlichmachen von Sicherheitsaufgaben sowie Verantwortungsbereitschaft die Unterstützung von Mitarbeitern bei der Realisierung von Sicherheitsvorhaben fördert?

Treffen Sie gezielt Sicherheitsvorkehrungen?

8. Schlussbetrachtung

Der Überblick über die Gefahren und Folgen von Informationsverlusten sowie über mögliche Schutzmaßnahmen macht deutlich, dass eine intensive Auseinandersetzung mit Fragen des Schutzes von Informationen unumgänglich ist. Die wichtigste Aufgabe liegt dabei in der Prävention, gerade auch bei kleineren Betrieben, deren Know-how unternehmensstrategische Bedeutung besitzt. Durch Präventivmaßnahmen können Schäden verhindert oder zumindest minimiert werden. Es sollten deshalb nicht erst dann Anstrengungen auf dem Gebiet des Informationsschutzes unternommen werden, wenn ein Verlust- oder Verratsfall bereits eingetreten ist. Gesellschaftliche Veränderungen und gewandelte Methoden der illegalen Informationsbeschaffung erfordern auch neue Formen der Vorbeugung. Von ausschlaggebender Bedeutung ist, dass sich jede einzelne Mitarbeiterin und jeder einzelne Mitarbeiter einer Firma - vom Konzernchef bis zur Reinigungskraft - des für das eigene Unternehmen bestehenden Risikos der Ausspähung sowie seiner ganz persönlichen Verantwortung für schützenswerte Informationen bewusst ist.

9. Ihre Ansprechpartner

Als Ansprechpartner für die dargestellten Sicherheitsfragen steht Ihnen der rheinland-pfälzische Verfassungsschutz zur Verfügung:

Ministerium des Innern und für Sport

Schillerplatz 3-5, 55116 Mainz

Postfach 3280, 55022 Mainz

Telefon: 06131/163772, Telefax: 06131/163688

Internet: http://www.verfassungsschutz.rlp.de

Darüber hinaus informiert Sie in Fragen der informationstechnischen Sicherheit das

Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 138, 53133 Bonn

Telefon: 0228/95820

10. Begriffserläuterungen

Abschöpfen (Abschöpfung, offene)
Erschließen des nachrichtendienstlich interessanten Wissens einer Person durch methodische Gesprächsführung oder durch Aufnahme des gesprochenen Wortes, ohne dass dem Betroffenen der Zweck erkennbar wird.

Agent
Person, die bewußt für einen fremden Nachrichtendienst arbeitet.

Anbahnen
Verbindungsaufnahme eines fremden Nachrichtendienstes mit einer Zielperson, um sie für eine nachrichtendienstliche Tätigkeit zu gewinnen; erfolgt meist unter Legende.

Aufklären
Zielgerichtetes Beschaffen von Informationen durch einen fremden Nachrichtendienst.

Drittland
Land, das in eine nachrichtendienstliche Operation einbezogen ist, ohne Ziel der Operation zu sein.

Dual-Use-Güter
Erzeugnisse, die neben ihrer zivilen Verwendbarkeit auch für militärische Zwecke benutzt werden können, so zum Bau von atomaren, biologischen und chemischen Waffen (ABC-Waffen) und Trägertechnologie (z.B. Raketen); bedeutsamer Gegenstand der Wirtschaftsspionage.

Einflußagent
Mitarbeiter eines fremden Nachrichtendienstes, der meinungsbildend tätig wird und so Entscheidungen beeinflussen kann.

Falsche Flagge
Anwerbung einer Person zur nachrichtendienstlichen Mitarbeit unter Täuschung über den wahren Auftraggeber und/oder die eigentlichen Absichten.

Forschen
Abklären einer Person, um festzustellen, ob sie für eine nachrichtendienstliche Tätigkeit geeignet ist.

Geheimschutz
Schutz von Informationen und Gegenständen, die als Verschluss-Sachen eingestuft sind, gegen Kenntnisnahme durch Unbefugte.

Geheimschutzbeauftragter
Unabhängiger Ansprechpartner in öffentlichen Stellen, der die Einhaltung der Geheimhaltungsvorschriften überwacht.

Hauptamtlicher Mitarbeiter (ND-Mitarbeiter)
Angehöriger eines fremden Nachrichtendienstes.

Illegaler Technologietransfer
Gesetzwidrige Verbringung von Gütern, die ausfuhrgenehmigungspflichtig oder nicht ausfuhrgenehmigungsfähig sind bzw. einem Embargo unterliegen. Betroffen sind insbesondere militärisch nutzbare Erzeugnisse der Hochtechnologie (sog. High-Tech-Produkte).

Industriespionage
Auch „Konkurrenzspionage“ genannt (siehe: Wirtschaftsspionage).

Legalresidentur
Getarnte Stützpunkte gegnerischer Nachrichtendienste in den offiziellen Vertretungen ihrer Länder im Gastland, so in Botschaften, Konsulaten, Handelsvertretungen oder Firmen.

Operative Maßnahmen
Maßnahmen, die regelmäßig der geheimen Informationsbeschaffung dienen.

Perspektivagent
Person, die sich verpflichtet hat, u.U. gegen Zahlung einer Ausbildungsunterstützung nach Abschluß des Studiums eine verantwortliche Position in einem nachrichtendienstlich interessanten Bereich (z.B. Forschung, Industrie) anzustreben und darüber nach Einstellung vertrauliche Informationen zu liefern.

Proliferation
Weitergabe von ABC-Waffen (bzw. -Komponenten) und Trägertechnologie oder Mitteln zu deren Herstellung an sog. Krisen- und Schwellenländer wie z.B. Iran, Irak, Syrien oder Nordkorea.

Residentur
Nachrichtendienstliche Führungsstelle im Operationsgebiet.

Sabotageschutz
Schutz von betrieblichen oder öffentlichen Einrichtungen gegen gezielte Beschädigungen und Manipulationen.

Sicherheitsrisiken
Umstände, die es aus Gründen des staatlichen Geheimschutzes verbieten, einer Person eine sicherheitsempfindliche Tätigkeit zu übertragen.

Sicherheitsverantwortlicher
Zentraler Ansprechpartner im einem Wirtschaftsunternehmen für alle Sicherheitsangelegenheiten.

Spionage
Systematische, zwischenstaatliche Informationsbeschaffung über politische, militärische, wirtschaftliche, wissenschaftliche oder gesellschaftlich relevante Fakten mit in der Regel verdeckten (geheimdienstlichen) Mitteln und Methoden.

Subversion
Einwirkung auf den Meinungs- und Willensbildungsprozess durch Verbreiten von Halb- und Unwahrheiten.

Verschluss-Sachen (VS)
Im öffentlichen Interesse geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse unabhängig von ihrer Darstellungsform (z.B. Schriftstücke, Zeichnungen, Karten, Fotokopien, Lichtbildmaterial, elektronische Datenträger, elektrische Signale, Geräte, technische Einrichtungen oder das gesprochene Wort). Sie werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle oder auf deren Veranlassung in die Geheimhaltungsgrade "VS-Nur für den Dienstgebrauch", "VS-Vertraulich", "GEHEIM" und "STRENG GEHEIM" eingestuft.

Werben
Gewinnen einer Person zur nachrichtendienstlichen Mitarbeit. Der Werbung gehen im Regelfall das Tippen (Hinweiserkundung auf nachrichtendienstlich interessante Personen) und das Forschen voraus. Fremde Nachrichtendienste gehen bei der Werbung oft nicht zimperlich vor. Sofern keine freiwillige Einwilligung des Betroffenen erfolgt, wird ggf. auch zu erpresserischen Methoden gegriffen. Dies können Kompromate (bloßstellende Bilder, Gesetzesverstöße im Land des anwerbenden Nachrichtendienstes etc.) oder das Ausnutzen von Abhängigkeiten (z.B. Spielsucht, hohe Verschuldung, Alkoholismus etc.) sein.

Wirtschaftsspionage
Staatlich betriebene Ausforschung der Wirtschaft eines anderen Landes mit nachrichtendienstlichen Mitteln und Methoden - im Unterschied zur Industriespionage (auch „Konkurrenzspionage“), bei der die Ausforschung zwischen einzelnen (in der Regel konkurrierenden) Firmen stattfindet. Im Gegensatz zur Industriespionage ist die Wirtschaftsspionage zumeist langfristig angelegt und durch einen erhöhten Einsatz konspirativer (geheimdienstlicher) Hilfsmittel gekennzeichnet. Betroffen sind nahezu alle Bereiche der Wirtschaft, Wissenschaft und Technik, was auch die Grundlagenforschung oder die wissenschaftliche Analysetätigkeit von Wirtschaftsforschungsinstituten mit-

einschließt. Neben der Industrie selbst zählen auch Wirtschaftsverbände und Banken zu den erklärten Spionagezielen.

11. Quellen

Neben eigenen Erkenntnissen des rheinland-pfälzischen Verfassungsschutzes beruht diese Broschüre auf einschlägigen Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik, des Bundesamtes für Verfassungsschutz sowie der Landesbehörden für Verfassungsschutz Baden-Württemberg und Berlin.