



Ministerium des Innern und für Sport



Informationsschutz
in der gewerblichen Wirtschaft
—
mit Sicherheit ein Gewinn!

Mainz, August 2008

1. Auflage

Nachdruck nur mit schriftlicher Genehmigung
des Herausgebers

Ministerium des Innern
und für Sport Rheinland-Pfalz

Vorwort

Sehr geehrte Leserinnen
und Leser,

Wissen bedeutet Macht und ist die Grundlage gesellschaftlichen und wirtschaftlichen Fortschritts. Im Zeitalter zusammenrückender Märkte und zunehmender wissenschaftlicher Kooperationen steigt der Bedarf an zeitnahe digitalen Datenaustausch.



Der beruflichen und persönlichen Abhängigkeit vom Einsatz moderner Informations- und Kommunikationstechnologie kann sich heute kaum jemand auf Dauer entziehen. Der Daten- und Informationsschutz gewinnt in der digitalen Welt deshalb immer mehr an Bedeutung; 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 bietet einen Überblick über Risiken, die Unternehmen und wissenschaftlichen Einrichtungen durch den Verlust von sensiblen Daten drohen. Zugleich werden Hinweise auf mögliche Schutzmaßnahmen gegen die illegale Nutzung betrieblichen Know-hows gegeben.

Im Rahmen der Sicherheitspartnerschaft zwischen der Landesregierung und der rheinland-pfälzischen Wirtschaft will das Ministerium des Innern und für Sport mit dieser Broschüre einen informativen Beitrag leisten. Darüber hinaus bietet der rheinland-pfälzische Verfassungsschutz weitergehende Beratungen durch Experten an.

A handwritten signature in blue ink, consisting of the initials 'KP' followed by a stylized, cursive name.

Karl Peter Bruch
Minister des Innern und für Sport

**Informationsschutz
in der gewerblichen Wirtschaft
–
mit Sicherheit ein Gewinn!**

Inhalt	Seite
1. Verfassungsschutz – Aufgabe Spionageabwehr, Geheim- und Sabotageschutz	5
2. Informationsverluste – Gefahren und Folgen	6
2.1 Gefahr durch Spionage – Schwerpunkte, Mittel und Methoden	6
2.2 Elektronische Angriffe	9
2.3 Folgen des Informationsverlustes	14
3. Geheimschutz in der Wirtschaft	14
4. Beratung durch den Verfassungsschutz – Mit Sicherheit ein Gewinn	15
5. Informationsschutz – Was können wir gemeinsam tun?	15
5.1 Personelle Sicherheitsmaßnahmen	16
5.2 Organisatorische Sicherheitsmaßnahmen	17
6. Ein praktisches Beispiel: Der Lauschangriff – Maßnahmen und Gegenmaßnahmen	17
7. Sicherheitstest	18
8. Zusammenfassung	19
9. Ihre Ansprechpartner	19
10. Quellen	19

1. Verfassungsschutz – Aufgabe Spionageabwehr, Geheim- und Sabotageschutz

Die gegen die Bundesrepublik Deutschland gerichtete Spionage ist nach wie vor ein wichtiges und aktuelles Thema der Inneren und Äußerer Sicherheit. Die größer gewordene politische Bedeutung Deutschlands, seine wirtschaftliche Leistungsfähigkeit sowie das hohe Niveau der Forschung und Entwicklung erklären das anhaltende 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 ihren gleichbleibend hohen Stellenwert behalten.

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 neben **Spionage** auch **Sabotage** und **Subversion**.

Neben der Enttarnung von Agenten und der Kenntnis über ihr methodisches Vorgehen und ihre operativen Ziele hat die Spionageabwehr nachrichtendienstlichen Angriffen durch präventive Maßnahmen wirksam zu begegnen.

Geheim- und Sabotageschutz kommen im Rahmen dieser Vorbeugung eine wesentliche Bedeutung zu. Sie haben die Voraussetzungen dafür zu schaffen, dass Unbefugte keine Kenntnis von im öffentlichen Interesse geheimhaltungsbedürftigen Informationen (sog. Verschlussachen) erhalten.

Der **materielle Geheimschutz** bezieht sich auf technische und organisatorische Sicherheitsmaßnahmen zum Schutz dieser Verschlusssachen. Der **personelle Geheimschutz** befasst sich im Wesentlichen mit der Sicherheitsüberprüfung von Personen, die eine sicherheitsempfindliche Tätigkeit im öffentlichen Dienst oder im Einzelfall auch als Angehörige privater Unternehmen ausüben sollen.

2. 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.

2.1 Gefahr durch Spionage – Schwerpunkte, Mittel und Methoden

Die **Schwerpunkte** der Ausspähungsaktivitäten fremder Nachrichtendienste haben sich in den vergangenen Jahren nicht wesentlich verändert. Im Rahmen der Globalisierung sind die Interessen breit gefächert. Sie umfassen nahezu den gesamten Bereich der industriellen und wissenschaftlichen Forschung sowie der Produktion, des Handels und der wirtschaftlichen Organisation. Primär gefährdet ist dabei die forschungs- und entwicklungsintensive Hochtechnologie.

- Informationsverarbeitung/
Kommunikationstechnik/Elektronik
- Luft- und Raumfahrt/Verkehrstechnik
- 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
- Qualitätsprüfungsmaßnahmen, Spezialwerkzeuge und Steuerungssysteme
- Lieferanten, Versorgungskonzeptionen, Lagerbestände
- Verkaufsstrategien, Marketingstudien, Absatz-/Vertriebswege
- Lizenzverträge, Umsätze und Kundenadressen
- Kalkulationsunterlagen, Budgetplanungen und Investitionsvorhaben

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, begehrtes Ausspähungsziel zu sein.

Mittel und Methoden der Spionage haben sich in den letzten Jahren teilweise verändert. Vermehrt wird heute versucht, Informationen bereits (offen) über Internet, gesellschaftliche Kontakte und harmlos erscheinende Gespräche zu gewinnen.

Auch die Auswertung anderer „offener“ Quellen sind für die Erkenntnisgewinnung relevant. Insbesondere die systematische Erfassung von wissenschaftlichen Forschungsberichten, Diplomarbeiten, Fachliteratur, firmen- und verbandsinternen Publikationen, Handbüchern, Dokumentationen, Werbe- bzw. Informationsmaterialien, Datenbanken und Bibliotheken eröffnen ein breites Wissensspektrum und geben in aller Regel Hinweise auf aktuelle Planungen und Projektverantwortliche.

Der sorglose Umgang mit Gesprächs- und zukünftigen Geschäftspartnern birgt zudem die Gefahr unbeabsichtigter Preisgabe von Betriebsinternas – bei Messen, Ausstellungen, Kongressen, Symposien, Seminaren und Betriebsbesichtigungen. Der berechtigte Stolz auf die eigene Leistung kann dazu führen, dass im Laufe einer Fachdiskussion oder eines Verkaufsgesprächs notwendige Sicherheitsüberlegungen vergessen werden.

Fremde Nachrichtendienste nehmen durch eigens gegründete Firmen und darin nachrichtendienstlich abgetarnte Personen auch aktiv am Wirtschaftsleben teil. Nachrichtendienstoffiziere, die als angebliche Geschäftsleute Angebote einholen oder Scheinverhandlungen führen, sind gerade angesichts dieser Tarnung für Unkundige schwer identifizierbar.

Konspirativ tätige Agenten im Zielobjekt gefährden die Sicherheitsinteressen eines Unternehmens in besonderem Maße. Die eigenen Mitarbeiter sind im Hinblick auf ihre Zugangsmöglichkeiten und ihr Wissen über innerbetriebliche Sicherheitslücken in der Lage, mehr Vertrauliches zu verraten als dies von außerhalb operierende Agenten herauszufinden vermögen. Fremde Nachrichtendienste unternehmen deshalb große Anstrengungen, qualifiziertes Fachpersonal für ihre Zwecke anzuwerben und als sog. Quelle im Objekt zu platzieren.

Gefährdungen ganz anderer Art sind mit der Nutzung moderner Informationstechnik verbunden. Mit dem rasant zunehmenden elektronischen Datenaustausch und damit steigender wirtschaftlicher Effizienz wachsen gleichzeitig die Risiken illegaler Zugriffe.

2.2 Elektronische Angriffe

Seit langem publizieren Sicherheitsexperten die Gefahren und Techniken der elektronischen Ausspähung über das Medium Internet.

Das Spektrum potentieller Angreifer reicht von Privatpersonen bis hin zu staatlichen Stellen.

Aktuell wird vor allem vor den weltweit festgestellten umfangreichen elektronischen Angriffen gewarnt, deren Ursprung in der VR China zu liegen scheint.

Diese Angriffe richten sich primär gegen Industrienationen. Betroffen sind auch deutsche Regierungsstellen, Universitäten, Forschungseinrichtungen und die Wirtschaft. Im Fokus stehen fast alle Branchen und Hochtechnologiebereiche. Gemeldet werden Angriffe auf Rüstungsunternehmen, Luft-, Raumfahrt- und Automobilindustrie, Chemie- und Pharmaunternehmen.

Insgesamt gilt für die elektronischen Attacken, dass ihnen offensichtlich ein umfangreiches „Social Engineering“ vorausgegangen sein muss. Dazu werden Informationen über die potentiellen Zielpersonen gesammelt bspw. Visitenkarten, Tätigkeitsfelder, bestehende dienstliche und persönliche Kontakte/Interessen sowie Informationsquellen wie Zeitungen oder Online-Tickermeldungen, Veröffentlichungen, etc. entsprechend aufbereitet und eingesetzt.

Eine häufig genutzte Angriffsmethode besteht in der Versendung von E-Mails mit manipulierten Anhängen. An gezielt ausgesuchte Personen oder bestimmte Organisationseinheiten eines Unternehmens werden Nachrichten versendet, die im Betreff interessante Themen ansprechen und wegen weiterer Details auf das mitübersandte Dokument verweisen.

Eventuell vorhandene Bedenken eines Adressaten, eine unerwartete E-Mail und ihren Anhang zu öffnen, sollen durch gefälschte Angaben eines vermeintlich vertrauenswürdigen Absenders beseitigt werden.

Die mit der Angriffs-E-Mail „eingeschleuste“ signaturarme¹ Schadsoftware wird beim Öffnen des Dokumentes unbemerkt installiert und gestartet. Von einigen kommerziellen Virencannern wurde die Schadstoffware erst Monate nach der Sicherstellung erkannt.

Nach der Installation versucht das aktivierte Schadprogramm selbständig Kontakt mit einem ihm vorgegebenen Computer im Internet aufzunehmen, der **NICHT** der Ausgangspunkt des Angriffs ist. Bei erfolgreicher Kontaktaufnahme werden weitere Befehle übertragen, die den eigentlichen „Auftrag“ enthalten. So kann der Ausspähungsbefehl zur Sammlung und Übertragung bestimmter Informationen an einen vorgegebenen Empfänger (des Angreifers) erteilt werden.

Denkbar sind auch Angriffe, um Dateien, Rechner und Netzwerke gezielt zu beschädigen oder außer Funktion zu setzen.

Zur Verschleierung des wahren Angreifers und der Herkunft der Angriffs-E-Mail werden neben „State of the Art“-Techniken, wie bspw. sogenannte Bot-Netze², auch speziell aufgebaute Strukturen eingesetzt.

Neben den beschriebenen Attacken mit manipulierten E-Mail-Anhängen gibt es auch die Variante, dass die Angriffs-E-Mail lediglich auf ein Dokument im Internet verweist. So kann die Schadsoftware unter Umgehung von Sicherheitsmechanismen auf den Mailservern in das System eingebracht werden. Aber auch Linkverweise auf (infizierte) Webseiten werden an die Zielpersonen verschickt. Bei dieser Methode wird dem Opfer beim ansurfen der Webseite bereits der Schadcode untergeschoben und über Sicherheitlücken im Browser zur Ausführung gebracht. Eines ist bei allen Variationen gleich: Die angesprochenen Themen sind auf die Interessenlage der Opfer abgestimmt.

Branchentypische Webseiten, wie z. B. der Rüstungsindustrie oder des Automobilsektors, unterliegen einer besonderen Missbrauchsgefahr. Gelingt es einem Angreifer eine solche Webseite unbemerkt vom Betreiber zu manipulieren und in ihr Schadsoftware zu platzieren,

¹ Signaturarm heißt, dass die Schadsoftware auch von aktuellen Virenskannern nicht unbedingt erkannt wird.

² Der Begriff bot ist abgeleitet von robot (engl. Roboter) und bezeichnet ein Computerprogramm, das weitgehend selbständig bestimmte oft zu wiederholende Aufgaben ausführt. Bot-Netze sind ein fernsteuerbarer Zusammenschluss einer großen Anzahl mit Bots infizierten Rechnern, die bspw. häufig zur Verbreitung von SPAM-Mails missbraucht werden.

ist jeder gefährdet, der diese Webseite öffnet. Der Angreifer kann sich somit ein aufwendiges „Social Engineering“ im Vorfeld ersparen.

Jeder IT-Nutzer sollte sich der Gefahren der „asymmetrischen IT-Auseinandersetzung“ bewusst sein, da der Aufwand zur Durchführung von elektronischen Angriffen sehr viel geringer ist, als der Aufwand zu ihrer Abwehr.

Zum Schutz gegen die Vielzahl und Vielfalt elektronischer Attacken gibt es keine Patentrezepte. Gleichwohl bieten sich einige grundlegende Möglichkeiten zur Verbesserung des IT-Schutzes:

Ein Schutz an zentraler Stelle, bspw. einem E-Mail-Gateway, lässt sich nur gegen bislang bekannte Muster erreichen. Aufgrund der Variationen der Schadsoftware müssen präventive Maßnahmen eingeführt werden, die auch gegen bisher unbekannte Muster Wirkung zeigen können. Diese sind dezentral auf den Clients durchzuführen.

- Keine Etablierung von Administrationsrechten als Standard auf den Rechnern (verhindert Installation von Schadprogrammen)
- Einrichtung einer Whitelist für startbare Programme auf den Rechnern
- Installation einer Desktop-Zweiwege-Firewall auf den Rechnern

Eine Trennung von IT-Netzen in einen internen und öffentlich zugänglichen Bereich durch Segmentierung oder bevorzugt durch physikalische Trennung vermindert Risiken.

Auch wenn diese Sicherheitsmaßnahmen mit Komforteinbußen und erhöhtem Verwaltungsaufwand verbunden sein dürften, sollten sie nicht von vornherein ausgeschlossen werden. Hier gilt es in Abhängigkeit von den Anforderungen an Produktivität und Sicherheit einen ausgewogenen Kompromiss zu finden. Diese Entscheidung sollte von den Verantwortlichen bewusst und in voller Kenntnis der potentiellen Risiken getroffen werden.

Möglichkeiten fü

ir Lauschangriffe

2.3 Folgen des Informationsverlustes

Wirtschaftsspionage, illegaler Wissenstransfer und unkontrollierter Know-how Abfluss sowie proliferationsrelevante Aktivitäten können die Wirtschaftskraft und Reputation deutscher Unternehmen gefährden und besonders kleinen sowie mittelständischen Firmen unter Umständen sogar der wirtschaftliche Ruin bedeuten.

Viele Beispiele belegen, dass Unternehmen immense Summen in die Entwicklung ihrer Produkte investieren, die sie später nicht mehr gewinnbringend verwerten konnten. Die Konkurrenz hatte bereits vorher ein Plagiat erheblich preiswerter angeboten.

Haben Sie schon einmal Aufträge ohne nachvollziehbare Gründe verloren? Oder haben Sie vielleicht Fälschungen von Erzeugnissen Ihres Unternehmens auf anderen Märkten entdeckt?

Wenn Sie eine dieser Fragen mit **JA** beantworten, machen Sie zu Ihrer Sicherheit den Test, den Sie am Ende dieser Broschüre (Kapitel 7) finden.

3. Geheimschutz in der Wirtschaft

Für die Einhaltung des Geheimschutzes in der Wirtschaft ist das Bundesministerium für Wirtschaft und Technologie zuständig. Daneben wirken auch die Verfassungsschutzbehörden des Bundes und der Länder mit. Den Verfassungsschutzbehörden obliegt vor allem die sicherheitsmäßige Beratung und Betreuung hier ansässiger geheimschutzrelevanter Firmen. 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 ca. 50 Wirtschaftsunternehmen in der behördlichen Geheimschutzbetreuung. 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 anerkennen.

Die formellen Mitwirkungsaufgaben beim Geheimschutz nimmt der Verfassungsschutz nur im Bereich amtlicher Schutzwürdigkeit und zur Sicherung lebens- oder verteidigungswichtiger Einrichtungen wahr. Andere Wirtschaftsunternehmen sind grundsätzlich auf Eigeninitiative und Selbsthilfe angewiesen. Maßgeblich kommt es darauf an, welchen Stellenwert die Informationssicherheit in diesen Betrieben einnimmt. Dabei ist häufig festzustellen, dass vor allem bei den besonders ausspähungsgefährdeten mittelständischen Unternehmen und bei der Neugründung innovativer Firmen Sicherheitsüberlegungen seltener eine angemessene Beachtung finden. In diesem Bereich besteht ein erhöhter Handlungsbedarf.

4. Beratung durch den Verfassungsschutz – mit Sicherheit ein Gewinn

Der rheinland-pfälzische Verfassungsschutz bietet seine Unterstützung im Rahmen einer **Sicherheitspartnerschaft zwischen Staat und Wirtschaft** an.

Eine entsprechende Beratung verhilft Entscheidungsträgern der Führungsebene in Unternehmen zu einem erfolgreichen Sicherheitsmanagement. Im Rahmen eines solchen Beratungsgesprächs mit dem Verfassungsschutz werden Informationen zur Gefährdung durch Spionage oder durch verfassungsfeindliche Organisationen mit Bezug zur Wirtschaft vermittelt.

5. Informationsschutz - Was können wir gemeinsam tun?

Die gewerbliche Wirtschaft 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 stärken und verringert die Spionageanfälligkeit. Mittelbar trägt ein angemessenes Mehr an Sicherheit dazu bei, den Unternehmen erfolgreiche Geschäfte und Umsätze zu ermöglichen sowie Arbeitsplätze zu erhalten.

Unternehmen müssen sich des Risikos von Informationsverlusten bewusst werden und dagegen geeignete Maßnahmen ergreifen. Präventive Abwehrmaßnahmen müssen sodann auf der Basis einer ganzheitlichen Betrachtung des jeweiligen Unternehmens konzipiert werden.

Ausgangspunkt aller Überlegungen ist eine Analyse der Gesamtsituation des Unternehmens, die die Risiken und Schwachstellen erfasst. Daraus sind in erster Linie solche Unternehmensstrukturen und -bereiche heraus zu arbeiten und zu bestimmen, die das wirtschaftliche Überleben der Firma garantieren und somit als „Kronjuwelen“ anzusehen sind. Für diese Kernbereiche müssen also personelle, organisatorische und materielle Sicherheitsmaßnahmen getroffen werden. Koordiniert und aufeinander abgestimmt ergeben diese Maßnahmen ein **unternehmensbezogenes Sicherheitskonzept**.

Hierfür ist die Bestellung einer/eines mit festen Aufgaben versehenen **Sicherheitsverantwortlichen** unumgänglich, 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 (bspw. 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 sicherheitserhebliche Vorkommnisse oder Verbesserungsvorschläge aufgenommen und umgesetzt werden.

5.1 Personelle Sicherheitsmaßnahmen

Personelle Sicherheitsmaßnahmen beginnen bei der Personalauswahl und enden mit einem Belehrungsgespräch beim Ausscheiden von Mitarbeitern.

Die betriebliche Sicherheitskonzeption muss die umfassende Sensibilisierung des Personals hinsichtlich der Risiken des ungewollten Informationsabflusses umfassen.

Nur gut informierte und problembewusste Mitarbeiter und Mitarbeiterinnen sind zu präventivem Handeln in der Lage und verinnerlichen die von der Unternehmensleitung vorgegebene Sicherheitsphilosophie.

5.2 Organisatorische Sicherheitsmaßnahmen

Das zweite tragende Element innerbetrieblichen Informationsschutzes bilden organisatorische Sicherheitsmaßnahmen, die in ihrer konzeptionellen Ausgestaltung aufeinander abgestimmt sein sollten. Hierzu zählen insbesondere

- sicherheitsempfindliche Bereiche bestimmen,
- restriktive Zugriffsberechtigungen zu schutzbedürftigen Daten und Objekten vergeben,
- die gesicherte Aufbewahrung von Daten und Objekten durch verbindliche Vorgaben regeln,
- sicherheitsrelevante Arbeitsabläufe organisieren und Richtlinien für den Empfang und die Betreuung von Besuchern erlassen,
- Sicherheitschecks regelmäßig durchführen und
- Mitarbeiterinnen und Mitarbeiter in die Bewertung neuer Gefahrenpotentiale einbeziehen.

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

Das Schaubild im Mittelteil der Broschüre zeigt die vielfältigen Möglichkeiten für Lauschangriffe auf geschlossene Räume, die bei illegaler Informationsbeschaffung zur Anwendung kommen können. Als Schutzmaßnahmen gegen Lauschangriffe eignen sich u.a.

- 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 Sicherheitsbereichs

- Verwendung von zugelassenen, abstrahlsicheren Geräten
- Verwendung von Netz-, Telefon- und Datenleitungsfiltern
- Aufspüren von aktiven Minisendern
- Einsatz von akustisch gedämmten bzw. elektromagnetisch abgeschirmten Kabinen

7. Sicherheitstest

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

- Ist bei Ihnen Sicherheit Chefsache?
- Gibt es in Ihrer Firma ein Sicherheitskonzept?
- Hat Ihr 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 nach dem Verlust eines Auftrages geprüft, ob möglicherweise ausländische Partnerfirmen davon profitieren?
- Sie stellen fest, dass Konkurrenzunternehmen Plagiate zu Ihren Produkten anbieten. Verfolgen Sie solche Fälle von offensichtlicher Produktpiraterie?
- Sind Fremdfirmen auch Bestandteil Ihres Sicherheitskonzepts?
- Haben Sie unerklärliche Geschäftseinbrüche zu verzeichnen?

8. Zusammenfassung

Der Überblick über die Gefahren und Folgen von Informationsverlusten sowie über mögliche Schutzmaßnahmen macht deutlich, dass eine intensive Auseinandersetzung mit Fragen umfassender betrieblicher Sicherheit unabdingbar ist. Durch Präventivmaßnahmen können Schäden verhindert oder minimiert werden. Anstrengungen auf dem Gebiet des Informationsschutzes dürfen deshalb nicht erst dann unternommen werden, wenn bereits ein Verratsfall eingetreten ist.

Die betriebliche Verantwortung ist umfassend, d. h. vom Vorstandsvorsitzenden, Geschäftsführer bis hin zu allen Beschäftigten des Unternehmens zu verstehen.

9. Ansprechpartner

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>

E-Mail: verfassungsschutz@ism.rlp.de

Bundesamt für Sicherheit in der Informationstechnik

Postfach 200 363

53133 Bonn

Telefon: 0228/999 582-0

E-Mail: bsi@bsi.bund.de

10. Quellen

Neben eigenen Erkenntnissen des rheinland-pfälzischen Verfassungsschutzes beruht diese Broschüre auf einschlägigen Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik und des Bundesamtes für Verfassungsschutz.

Für weitere Informationen
wenden Sie sich bitte an:



Ministerium des Innern und für Sport

Schillerplatz 3-5 · 55116 Mainz

55022 Mainz, Postfach 3280

Telefon (06131) 16 37 72

Internet: www.verfassungsschutz.rlp.de

Herausgeber: Ministerium des Innern und für Sport
Gesamtherstellung: Satz und Druck Werum GmbH

Hinweis:

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit des Ministeriums des Innern und für Sport herausgegeben. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern im Zeitraum von sechs Monaten vor einer Wahl zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Landtags-, Bundestags-, Kommunal- oder Europawahlen. Mißbräuchlich ist während dieser Zeit insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken und Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zwecke der Wahlwerbung.

Auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl darf die Druckschrift nicht in einer Weise verwendet werden, die als Parteinahme der Landesregierung zugunsten einzelner politischer Gruppen verstanden werden könnte. Den Parteien ist es gestattet, die Druckschrift zur Unterrichtung ihrer eigenen Mitglieder zu verwenden.