



Sicherheitsfaktor Mensch –

Risiko oder Chance
für den Know-how-Schutz

Informations- und Beratungs-
angebot des Bayerischen Landes-
amts für Verfassungsschutz

Stand: August 2011

Prävention durch Information

Das Bayerische Landesamt für
Verfassungsschutz bietet Ihnen an:

- Sensibilisierung von Management und Mitarbeitern zu Wirtschaftsspionage und Know-how-Schutz
- Vorträge im Unternehmen zu allen Aspekten des Wirtschaftsschutzes
- Aufklärung über spezielle Risiken und Schutzmaßnahmen bei Auslandsreisen
- Individuelle Gefährdungs- und Schwachstellenanalyse
- Beratung bei Konzeption und Optimierung Ihrer Maßnahmen zum Know-how-Schutz
- Aufbau einer langfristig angelegten Sicherheitspartnerschaft
- Hilfestellung bei Verdachtsmomenten oder Sicherheitsvorfällen
- absolut vertrauliche Behandlung aller Informationen

**Alle Informations- und Beratungsangebote
sind kostenfrei**

Kontakt

Ihr Kontakt für Fragen und Mitteilungen zu Wirtschaftsspionage und Wirtschaftsschutz:

Tel.: 089 / 31201 - 500
E-Mail: wirtschaftsschutz@lfv.bayern.de

Ihr Kontakt für Fragen und Mitteilungen zur IT-Sicherheit:

Tel.: 089 / 31201 - 193
E-Mail: iswi@lfv.bayern.de

Zusätzliche Informationen und Publikationen zum Download finden Sie auf unserem Informationsportal:
www.wirtschaftsschutz.bayern.de

Herausgeber:

**Bayerisches Landesamt für
Verfassungsschutz
Knorrstr. 139
80937 München**



Wirtschaftsspionage

Die Bedrohung ist konkret:

- Viele Staaten beauftragen ihre Nachrichtendienste mit Wirtschaftsspionage (Hauptakteure sind China und Russland)
 - Innovative Technologien stehen im Fokus (Medizin, Biotechnik, Maschinen- und Anlagenbau, IT, Telekommunikation, Energie- und Umwelttechnik,...)
 - Ausgeforscht werden technische und strategische Informationen
- Gezielte Angriffe mit Spionagehintergrund nehmen zu

- Besitzen Sie schutzwürdiges innovatives Know-how?
- Schätzen Sie die Bedrohung durch Spionage als ernstzunehmende Gefahr für Ihr Unternehmen ein?
- Gibt es in Ihrer Firma ganzheitliche Schutzkonzepte unter Einbeziehung der IT ?

→ Frühzeitige Information und gezielte Prävention schützen

Risikofaktor Mensch

Externe:

- verschaffen sich auf illegale Weise Zutritt zum Unternehmen oder Zugriff auf schützenswertes Know-how
- werben Mitarbeiter aus dem Unternehmen gezielt als „Informanten“ an
- gelangen durch „Social Engineering“ auf persönlichem oder elektronischem Wege an sensible Informationen

Interne:

- alle Personen innerhalb eines Unternehmens mit entsprechenden Zutritts- oder Zugriffsberechtigungen (auch: Praktikanten, Fremdpersonal, Reinigungskräfte)
- mangelndes Sicherheitsbewusstsein und unzureichende Schulung der Mitarbeiter
- Motive für absichtlichen Know-how-Diebstahl: Unzufriedenheit, Rache, Geldgier
- menschliche Schwächen: Geltungssucht, Geschwätzigkeit, Unkenntnis, Verlust oder Diebstahl von Unterlagen oder Datenträgern

Lösungsansätze im Rahmen eines ganzheitlichen Schutzkonzeptes:

- sicherheitsorientierte Personalauswahl
- Definition, Strukturierung und Klassifizierung sensibler Unternehmensbereiche und Informationen
- Festlegung abgestufter Zugriffsberechtigungen anhand ihrer Schutzbedürftigkeit
- Sensibilisierung, Information und Einbindung der Mitarbeiter
- Kommunikation, Kontrolle und Fortschreibung verbindlicher Sicherheitsrichtlinien