# Unser Angebot

- **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 Beratung bei Konzeption und Optimierung Ihrer Maßnahmen zum Kow-how-Schutz**
- **Aufbau einer langfristig angelegten Sicherheitspartnerschaft**
- **Hilfestellung bei Verdachtsmomenten oder Sicherheitsvorfällen**

**neutral**

**vertraulich**

**kostenfrei**

# Ihr Kontakt


**Team Wirtschaftsschutz**

Für Fragen und Mitteilungen zu
Wirtschaftsschutz und -spionage:
Telefon: 089 31201-500
E-Mail: wirtschaftsschutz@lfv.bayern.de

**Geheimschutz in der Wirtschaft**

Telefon: 089 31201-234
E-Mail: gswi@lfv.bayern.de

**Cyber-Allianz-Zentrum Bayern**

Für Fragen und Mitteilungen zu
elektronischen Attacken:
Telefon: 089 31201-222
E-Mail: caz@lfv.bayern.de


WIRTSCHAFTSSCHUTZ BAYERN

Weitere Informationen und Publikationen:
www.wirtschaftsschutz.bayern.de


Herausgeber: Bayerisches Landesamt für Verfassungsschutz
Knorrstr. 139, 80937 München
Gestaltung: Bayerisches Landesamt für Verfassungsschutz
Druck: Datadruck GmbH, 89278 Nersingen
Bildnachweis Titel: © Rawpixel_Fotolia_88834172_X
Stand: August 2015



Bayerisches Landesamt
für Verfassungsschutz


# Sicherheitsfaktor Mensch


**Risiko oder Chance**
**für den Know-how-Schutz**

**Die Bedrohung ist konkret:**

- Viele Staaten beauftragen ihre Nachrichtendienste mit Wirtschaftsspionage
- Innovative Technologien stehen im Fokus (Medizin, Biotechnik, Automotive, Maschinen- und Anlagebau, IT, Telekommunikation, Energie- und Umwelttechnik,...)
- Ausgeforscht werden technische **und** strategische Informationen

→ **Gezielte Angriffe mit Spionagehintergrund nehmen stetig 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**

**Externe Faktoren:**

- illegaler Zutritt zum Unternehmen oder Zugriff auf das Unternehmensnetzwerk, um so an schützenswertes Know-how zu gelangen
- gezielte Anwerbung von Mitarbeitern aus dem Unternehmen als „Informanten“
- „Social Engineering“ - Angriff (Vorbereitung insbesondere mittels Informationen aus sozialen Netzwerken)
- Diebstahl und Einbruchdiebstahl

**Interne Faktoren:**

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

**Lösungsansätze im Rahmen eines ganzheitlichen Schutzkonzeptes:**

- sicherheitsorientierte Personalauswahl (einschl. vertraglicher Vereinbarungen)
- Klassifizierung sensibler Unternehmensbereiche und entsprechender Daten
- Festlegung abgestufter Zugriffsberechtigungen anhand ihrer Schutzbedürftigkeit
- Sensibilisierung, Information und Einbindung der Mitarbeiter (Awareness)
- Kommunikation, Kontrolle und Fortschreibung verbindlicher Sicherheitsrichtlinien