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: © Visions-AD_Fotolia_86745046_X
Stand: August 2015

Bayerisches Landesamt
für Verfassungsschutz

Geschäftsreisen ins Ausland

Sicherheitsrisiko für Unternehmen

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**

Vorbereitung:

- alle Informationsmöglichkeiten zum Reiseland nutzen (z. B. IHK, Auswärtiges Amt, Intenet, Mitarbeiter, Geschäftspartner)
- mit erforderlichen Gesetzen und Bräuchen des Reiselandes vertraut machen, um sich nicht angreifbar oder erpressbar zu machen
- Visadaten prüfen (Fehler können zum Angriffspunkt werden)
- mit leichtem IT-Gepäck reisen: Reiselaptop ohne sensible Firmendaten verwenden
- sensible Daten auf mobilem, verschlüsseltem Datenträger separat mitführen

Vor Ort:

- Gepäck (v. a. Datenträger, Firmenunterlagen) nicht unbeaufsichtigt lassen
- Hotelzimmer und Hotelsafes sind keine sicheren Aufbewahrungsorte
- besondere Vorsicht vor neugierigen Blicken und Mithören am Flughafen, im Zug, im Restaurant, an der Hotelbar, u. ä.
- Vorsicht bei Geschenken und auffälligen Kontaktversuchen
- Datenverbindung zum Firmennetzwerk nur per VPN-Tunnel aufbauen
- WLAN-Nutzung mit Bedacht: Hotspots nur für offene Inhalte verwenden
- nur eigene Kommunikationsmittel und Datenträger nutzen und nicht aushändigen
- Handys aus Besprechungen mit sensiblem Inhalt verbannen
- reagieren Sie sofort auf festgestellten Verlust sensibler Daten und Unterlagen so wie den Versuch von Ausspähung oder Übertragung von Schadsoftware

  Informieren Sie unverzüglich Ihr Unternehmen in der Heimat

Nachbereitung:

- Resumée ziehen über Auffälligkeiten, verdächtige Kontaktaufnahmen oder fehlende Unterlagen
- Mobile Geräte auf Schadsoftware/ Manipulation regelmäßig prüfen lassen
- Erfahrungen innerhalb des Unternehmens zu Verfügung stellen: davon können andere profitieren und Fehler können vermieden werden