Unser Angebot

- **Sensibilisierung von Forschenden und Lehrenden Ihrer Hochschule**
- **Individuell abgestimmte Vorträge oder Besprechungen in Ihrem Hause**
- **Aufklärung über spezielle Risiken und Schutzmaßnahmen bei Auslandsreisen**
- **Beratung bei Konzeption und Optimierung Ihrer Maßnahmen zum Know-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: Schmid Druck & Medien, Kaisheim
Bildnachweis Titel: © vege_Fotolia_65526198_XL
Stand: April 2016

Bayerisches Landesamt
für Verfassungsschutz

Spitzenforschung und Auslandsreisen

Risiko für Wissenschaft und Forschung

Spionagerisiken im Ausland:

Im Bemühen der Bayerischen Hochschulen um eine wünschenswerte Globalisierung werden die Kontakte und Kooperationen mit ausländischen Hochschulen, Unternehmen, Institutionen und Behörden immer wichtiger. Für funktionierende wissenschaftliche Partnerschaften sind persönliche Kontakte besonders in der Anfangsphase unerlässlich und von größter Bedeutung, somit gehören Auslandsreisen zunehmend zum wissenschaftlichen Alltag.

Gerade bei diesen Reisen steigt das Risiko, Opfer von Know-how-Verlust zu werden. Kaum jemand wird im Ausland so genau und intensiv beobachtet wie Vertreter/innen der Wissenschaft. Dabei geht die Gefährdung nicht nur von der wissenschaftlichen Konkurrenz aus: in vielen Ländern sind die dortigen Nachrichtendienste beauftragt, wissenschaftliches Know-how auszuforschen, um dies der heimischen Wirtschaft zur Verfügung zu stellen.

Die Methoden der Angreifer sind vielfältig und professionell. Das Spektrum reicht vom Aushorchen und Ausspähen über Diebstahl und Social Engineering bis hin zum Einsatz technischer und elektronischer Mittel.

Bedenken Sie:

Alle Bereiche der Spitzenforschung (Drittmittel- und Kooperationsprojekte, Grundlagenforschung, F+E-Projekte) sind für ausländische Nachrichtendienste von Interesse, gerade im Hinblick auf deren wirtschaftliche Verwertbarkeit. Auch aus Ihrer Sicht „bekannte“ Details oder Hintergrundinformationen, die oft schon im Vorfeld einer Kooperation ausgetauscht werden, können für Angreifer lohnenswert sein. Bedenken Sie bitte, dass auch Nachrichtendienste westlicher Länder aktiv sind.

Vorbereitung:

Nutzen Sie vor Reiseantritt alle Informationsmöglichkeiten zum Reiseland (z. B. IHK, Auswärtiges Amt, Internet, Mitarbeiter, Geschäftspartner) und machen Sie sich mit erforderlichen Gesetzen und Bräuchen des Gastlandes vertraut. Überprüfen Sie Reiseunterlagen auf Richtigkeit und Gültigkeit, da Unstimmigkeiten zum Anlass für eine nachrichtendienstliche Kontaktaufnahme genutzt werden können. Reisen Sie mit „leichtem Gepäck“ - der speziell vorbereitete Reise-Laptop sollte keine sensiblen Daten beinhalten. Diese werden am besten auf einem verschlüsselten USB-Stick gespeichert, den Sie stets bei sich führen.

Vor Ort:

Lassen Sie Ihr Gepäck (v. a. Datenträger, Unterlagen) nie unbeaufsichtigt und bedenken Sie, dass Hotelzimmer und Hotelsafes keine sicheren Aufbewahrungsorte sind. Achten Sie besonders auf neugierige Blicke oder Zuhörer sowie Personen, die ohne Anlass Ihre Nähe suchen. Kontaktversuche oder Geschenke von „Fremden“ sollten kritisch hinterfragt werden. Verbannen Sie Handys aus Besprechungen mit sensiblem Inhalt. Tauschen Sie keine sensiblen Daten per Telefon, Handy oder E-Mail aus - sollte dies doch einmal unumgänglich sein, splitten Sie die Informationen auf verschiedene Kommunikationswege. Geben Sie eigene Handys und Daten (-träger) nie aus der Hand und nutzen Sie keine Fremdgeräte. Sollten trotz aller Vorsicht sensible Daten verloren gehen, zögern Sie nicht: Informieren Sie unverzüglich Ihre Hochschule!

Nachbereitung:

Bereiten Sie Ihre Reise durch eine nicht nur fachliche Nachbesprechung auf und ziehen Sie ein Resumée über Auffälligkeiten, verdächtige Kontaktaufnahmen oder fehlende Unterlagen. Lassen Sie mobile Geräte auf Schadsoftware/ Manipulation prüfen. Stellen Sie Ihre Erfahrungen in der Hochschule zur Verfügung: davon können andere profitieren und künftige Fehler werden vermieden.