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

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: @ShpilbergStudios_Fotolia_80267404_XXL
Stand: April 2016

Bayerisches Landesamt
für Verfassungsschutz

Know-how-Schutz für Spitzenforschung

Informationen zu Prävention und Sicherheit

Spitzenforschung in Gefahr

Die Wissenschaftslandschaft und damit auch die bayerischen Hochschulen und Universitäten sind im Rahmen wünschenswerter Initiativen zur Internationalisierung immer globaler geworden: Lehrende, Studierende und Mitarbeiter/innen aus der ganzen Welt kommen miteinander in Kontakt und tauschen wissenschaftliche Erkenntnisse aus - gerade im Bereich der Spitzenforschung.

Diese positive Entwicklung hat aber auch eine Schattenseite: viele Staaten beauftragen ihre Nachrichtendienste damit, wissenschaftliches Know-how durch Spionage auszuforschen, um dieses Wirtschaft und Wissenschaft des eigenen Landes zur Verfügung zu stellen. Dabei stehen in erster Linie innovative Technologien im Fokus aber auch sozial- und wirtschaftswissenschaftliche Themen sind von Interesse. Ausgeforscht werden dabei nicht nur neue technische, sondern auch strategisch wichtige Informationen.

Grundsätzlich gilt:

je besser desto begehrter.

Auch an Ihrer Hochschule gibt es sensibles Know-how, für das sich Wissenschaftsspione interessieren. Schätzen Sie daher die Bedrohung durch Spionage als ernstzunehmend ein und helfen Sie durch Ihren Beitrag mit, die Risiken zu minimieren.

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 die Angreifer lohnenswert sein. Bedenken Sie bitte, dass auch Nachrichtendienste westlicher Länder aktiv sind.

Externe Risikofaktoren:

Ausländische Mitarbeiter/innen oder Studierende werden von Nachrichtendiensten gezielt in relevante Bereiche von Hochschulen eingeschleust, um dort spezielles Know-how auszuspionieren. Daneben werden vor allem die vielfältigen elektronischen Spionagemöglichkeiten genutzt. Immer häufiger gelangen die Angreifer über sogenannte „Trojaner“ ins hauseigene Netzwerk. Eingeschleust werden diese mittels personalisierter E-Mails mit infiziertem Anhang. Die nötigen Informationen dazu stammen aus dem Internet (Homepage, Soziale Netzwerke, o. ä.) oder wurden gezielt bei der Person selbst ausgekundschaftet („Social Engineering“).

Interne Risikofaktoren:

Nachrichtendienste suchen gezielt den Kontakt zu Personen aus dem Hochschulbereich, um so an interne Informationen zu gelangen – oft ist dies den Betroffenen gar nicht bewusst. Vom unabsichtlichen Verlust von Datenträgern bis hin zum gezielten Know-how-Diebstahl reicht die Bandbreite beim „Sicherheitsfaktor Mensch“ und umfasst alle Personen, die sich innerhalb des Hochschulbereiches bewegen!

Lösungsansätze:

Definieren Sie besonders sensible Daten und legen Sie entsprechend abgestufte Zugriffsberechtigungen fest. Erarbeiten Sie für Ihre Hochschule allgemein verbindliche Sicherheitsrichtlinien, die kommuniziert, kontrolliert und fortgeschrieben werden.

Last but not least: sensibilisieren Sie Ihre Mitarbeiterinnen und Mitarbeiter.

Das Bayerische Landesamt für Verfassungsschutz unterstützt Sie dabei gerne:

neutral – vertraulich – kostenfrei