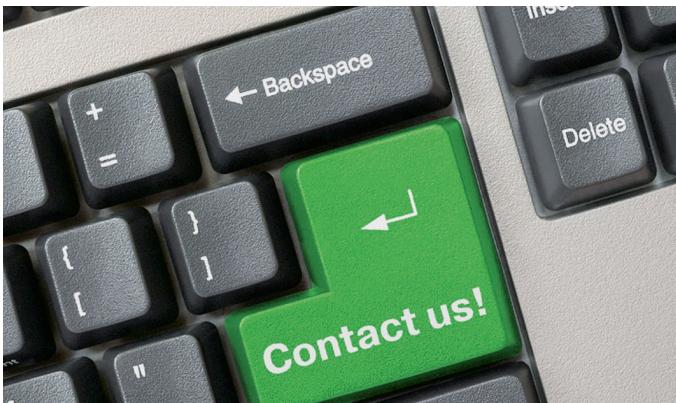


Empfehlungen

- Benennen Sie einen Ansprechpartner für Sicherheitsthemen und kommunizieren Sie dies in Ihrer Organisation
- Prüfen Sie frühzeitig die Schutzwürdigkeit Ihrer Projekte, Testaufbauten, Ergebnisse und der zugehörigen Dokumentation
- Passen Sie die organisatorischen, technischen und personellen Schutzmaßnahmen adäquat an
- Beachten Sie besonders bei der Einstellung von Gastwissenschaftlern unsere Hinweise zur Personalauswahl (*)
- Sensibilisieren Sie Mitarbeiter und Studenten – speziell im Vorfeld von Auslandsaufenthalten und -kontakte

Sprechen Sie uns an und vereinbaren Sie einen Termin für ein vertrauliches Sensibilisierungsgespräch



* siehe Flyer „Personalauswahl“

Ihre Ansprechpartner im Wirtschaftsschutz

Ministerium für Inneres und Kommunales des Landes Nordrhein-Westfalen



Wirtschaftsschutz

Ministerium für Inneres und Kommunales NRW
Abteilung Verfassungsschutz
Postfach 10 30 13
40021 Düsseldorf

Telefon: 0211 / 871-2899
Fax: 0211 / 871-2980
E-Mail: wirtschaftsschutz@mik1.nrw.de
Internet: www.mik.nrw.de/wirtschaftsschutz



Gemeinsam. Werte. Schützen.

Dort finden Sie weitere Informationen sowie die Kontaktdaten Ihrer örtlichen Ansprechpartner.



www.wirtschaftsschutz.info

Impressum

Herausgeber: Bundesamt für Verfassungsschutz für den Verfassungsschutzverbund

Bilder: © Gernot Krautberger - Fotolia.com
© ccvision
© Minerva Studio - Fotolia.com
© Nikolai Sorokin - Fotolia.com

Stand: März 2016

Verfassungsschutz



**Bund
Länder**

Wirtschaftsschutz

**Gefahren für
Forschung
und
Lehre**

Fokus Wissenschaft

Gefährdungspotential

Die Innovationen deutscher Hochschulen und Forschungseinrichtungen zeichnen die deutsche Wissenschaftslandschaft weltweit aus. Sie sind außerdem eine tragende Säule für den weltweiten Erfolg der deutschen Wirtschaft. Daher sind sie ein begehrtes Ausforschungsziel für Wettbewerber und Nachrichtendienste fremder Staaten.



**Die Wissenschaft von heute
ist die Wirtschaft von morgen**

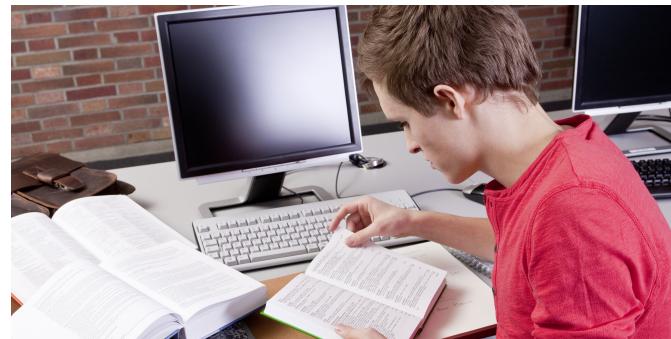
**Der Student von heute
ist der Entscheider von morgen**

Gefährdungsszenarien

Vorgeschaltetes Social Engineering (*) bildet oftmals die Basis für Angriffe wie:

- Ausforschung von Angehörigen deutscher Hochschulen und Forschungseinrichtungen
- Nachrichtendienstliche Kontaktaufnahme zu deutschen Studenten und Wissenschaftlern im Ausland
- Elektronische Angriffe auf das interne Netzwerk oder Verbundnetz wissenschaftlicher Einrichtungen
- Einschleusen von Gaststudenten und Gastwissenschaftlern in zukunftsträchtige Forschungsprojekte in Deutschland

Ein Auslandsstudium/Stipendium kann vom Entsendeländer gegenüber seinen Studenten und Wissenschaftlern an die Bereitschaft zur Spionage geknüpft werden. Diese Verpflichtung, das eigene Land zu unterstützen, wird häufig sogar als Ehre empfunden.



* siehe Flyer „Social Engineering“

Weitere Risiken

Das Erfordernis, Ergebnisse im Rahmen der Freiheit von Forschung und Lehre so breit wie möglich und auch zeitnah zu publizieren, läuft den Anforderungen des Know-how-Schutzes zuwider. Dies sollte im **wissenschaftlichen Wettbewerb** berücksichtigt werden.



Entwicklungskooperationen können dazu genutzt werden, sich widerrechtlich Wissensvorsprünge des Partners anzueignen.

Drittmittelprojekte haben einen besonderen Schutzbedarf, da hier auch das Know-how des Geldgebers und dessen Marktposition betroffen sind. Im schlimmsten Fall sind nicht nur aktuelle, sondern auch zukünftige Projekte gefährdet.

Wenn Fälle eines ungesteuerten Know-how-Abflusses bekannt werden, kann auch die **Reputation** der Forschungseinrichtung oder der Hochschule auf dem Spiel stehen.