Info Blatt

Informationsblätter zum Wirtschaftsschutz

Spionage in Wissenschaft und Forschung

Universitäten und Forschungseinrichtungen in Deutschland stehen im Fokus von Spionage durch ausländische Nachrichtendienste. Diese nutzen verschiedene Wege, um an Know-how und Informationen zu gelangen. Die Gefahr eines unkontrollierten Know-how-Abflusses lässt sich durch die Einführung und Einhaltung von Sicherheitsstandards minimieren.

Der Verfassungsschutz ist für die Abwehr von Spionage und Sabotage durch ausländische Nachrichtendienste sowie von Extremismus zuständig und steht als vertraulicher Ansprechpartner zur Verfügung.

Ziele und Folgen von Wissenschaftsspionage

- Vorrangiges **Ziel der Wissenschaftsspionage** durch ausländische Staaten ist es, **Informationen zu erlangen**, um sich so einen **Wissensvorsprung zu verschaffen** oder bestehende Know-how-Lücken zu schließen.
- Staatliche Angreifer greifen auf **umfangreiche personelle und finanzielle Ressourcen** zurück und gehen planvoll, geschickt und langfristig ausgerichtet vor.
- Dem gegenüber steht eine Wissenschaftslandschaft, in der teilweise ***Sicherheitsaspekte*** und die Gefahr durch Spionage noch **zu wenig berücksichtigt** sind.

- ***Sicherheitsaspekte***
  Die Einhaltung grundlegender Sicherheitsaspekte erschwert einen ungewollten Know-how-Abfluss.
  - *Das schützenswerte Know-how und der jeweilige Schutzbedarf sind bekannt.*
  - *Das Schutzniveau ist dem Schutzbedarf angepasst.*
  - *Es gibt ein ganzheitliches Sicherheitskonzept.*

GEFAHR

Wissenschaftsspionage kann für die Einrichtung erhebliche negative Folgen haben:

- *der Verlust von Aufträgen, Patenten und Geld*
- *die Aufhebung wissenschaftlicher Kooperationen*
- *Vertrauensverlust und Imageschaden*

Wissenschaftsspionage bedroht langfristig auch den Wirtschafts- und Wissenschaftsstandort Deutschland.

BESONDERS GEFÄHRDETE FORSCHUNGSFELDER

Bestimmte Länder definieren Branchen, in denen sie eine **führende Rolle auf dem Weltmarkt bzw. mehr Unabhängigkeit** erreichen wollen. Das dafür notwendige Know-how wird sowohl **mit legalen als auch mit illegalen Methoden** gewonnen. Verschiedene **Forschungsfelder** stehen dabei besonders **im Fokus**.

- Schiffbau und Meerestechnik
- Energieeinsparung und Elektromobilität
- Informations- und Kommunikationstechnologien
- Automatisierung und Robotik
- Elektrizitätsanlagen
- Anlagen für Luft- und Raumfahrttechnik
- neue Werkstoffe und Materialien
- Landwirtschaft
- moderne Anlagen für den Schienenverkehr
- Biomedizin und High-Performance Medizingeräte

Wissenschaftsspionage: Angriffswege und Schutzmaßnahmen

Zur Informationsbeschaffung nutzen ausländische Nachrichtendienste verschiedene Wege und kombinieren diese auch miteinander. Um sich zu schützen, benötigen Wissenschaftseinrichtungen ein ganzheitliches Schutzkonzept, welches auch die folgenden Aspekte berücksichtigt.

Ausländische Studierende / Gastwissenschaftlerinnen und -wissenschaftler

AUSGANGSLAGE

- Ausländische Nachrichtendienste nutzen auch **Gaststudierende und Gastforschende**, um an Forschungsergebnisse zu gelangen.
- Staatsangehörige werden **zur Mitarbeit verpflichtet, unter Druck gesetzt oder mit Anreizen geködert**. Auch kann die Zusammenarbeit aus patriotischen Gründen **gänzlich freiwillig** erfolgen.
- Teilweise werden evtl. **staatliche Verbindungen** absichtlich gegenüber der Gasteinrichtung **verschleiert**.

Beispiel: *Ein Gastwissenschaftler, Spezialgebiet: Steuerungstechnik, hält sich zu Forschungszwecken an einer deutschen Universität auf. Was er der Universität verheimlicht: Er leitet in der Heimat ein Militärlabor für Raketentests.*

SCHUTZMASSNAHMEN

- Führen Sie bei der Auswahl wissenschaftlichen Personals **Hintergrundchecks** durch. Schauen Sie insbesondere auf **Verbindungen zu Militäreinrichtungen**.
- Schließen Sie **Vertraulichkeitsvereinbarungen** mit Beschäftigten ab.
- Verfolgen Sie die **Karrierewege der Gastforschenden** auch nach Verlassen der Einrichtung.

Beachten Sie auch die Informationsblätter „Methoden der Spionage: HUMINT“, „Pre-Employment Screening“ und „Bedrohung durch Innentäter“ auf ***www.verfassungsschutz.de*** *(Service > Publikationen).*

EXKURS: CHINA

China will bis 2049 wirtschaftlich, wissenschaftlich und militärisch global führend sein. Gleichzeitig wird eine zunehmende wirtschaftliche Unabhängigkeit vom Ausland angestrebt.

- China benötigt dafür auch umfangreiches westliches Know-how. Zur Informationsbeschaffung werden sowohl legale Mittel als auch illegale Mittel eingesetzt.
- Langfristig angelegte Strategien und Programme unterstützen die Zielerreichung, u. a. werden Wirtschaft, akademische Institutionen und Militär zunehmend stark verflochten *(SEVEN SONS OF NATIONAL DEFENCE).*
- Internationale Forschungskooperationen und wissenschaftliche Auslandsaufenthalte werden gezielt gefördert, um spezielles Wissen ins Land zu holen. Insbesondere spielen Forschungsergebnisse eine wichtige Rolle, die sich auch für ***Dual-Use Güter*** nutzen lassen (z. B. Materialforschung).

SEVEN SONS OF NATIONAL DEFENCE

Bei den „Sieben Söhnen“ handelt es sich um Universitäten, die dem Militär in Forschung und Lehre besonders nahestehen. Aber auch für andere Forschungs- und Wissenschaftseinrichtungen lassen sich Verbindungen zum Militärsektor nachweisen. Die Datenbank ***China Defence Universities Tracker*** *unterstützt eine Risiko-Einschätzung möglicher wissenschaftlicher Kooperationen.*

https://unitracker.aspi.org.au

Dual-Use Güter

Dual-Use Güter sind Waren und Produkte, die sowohl für zivile Anwendungen als auch für militärische Zwecke geeignet sind. Aufgrund dieses Gefährdungspotenzials unterliegt der Export diese Güter in außereuropäische Länder bestimmten Kontrollen und Restriktionen.

Wissenschaftsspionage: Angriffswege und Schutzmaßnahmen

Finanzierung / Kooperationen

AUSGANGSLAGE

- Auch **Forschungskooperationen und fremd-finanzierte Projekte** können von ausländischen Akteuren dazu missbraucht werden, an relevantes Wissen zu gelangen.
- Forschungsergebnisse können im Heimatland für **wirtschaftliche und militärische Zwecke** genutzt werden. Hier spielen Dual-Use-Güter bzw. auch ➔ ***proliferationsrelevantes Wissen*** eine wichtige Rolle.

Beispiel: *Eine deutsche Universität forscht zusammen mit einer ausländischen Forschungseinrichtung im materialwissenschaftlichen Bereich. Es ist bekannt, dass die ausländische Universität dem Militär nahesteht und sich die Forschungsergebnisse auch für hochmoderne Waffensysteme verwenden lassen.*

➔ ***Proliferationsrelevantes Wissen***

Dabei handelt es sich um Know-how, das benötigt wird, um Technologien für Massenvernichtungswaffen und Trägersysteme zu entwickeln. Wissenschaftliche Erkenntnisse können vielfach sowohl für zivile als auch für militärische Zwecke verwendet werden. Problembewusstsein ist die Voraussetzung, um proliferationsrelevante Informationen zu schützen.

SCHUTZMASSNAHMEN

- **Bewerten Sie das Potenzial** von Technologien und schätzen Sie die **Forschungsfolgen** gründlich ab.
- Beleuchten Sie potentielle Kooperationspartner auf **Verbindungen zu staatlichen Stellen** und prüfen Sie die Forschungskooperation hinsichtlich möglicher **Missbrauchspotentiale**.
- **Dokumentieren Sie Vereinbarungen** über die Verwendung der Forschungsdaten und -ergebnisse.

Cyberangriffe

AUSGANGSLAGE

- Universitäten und andere Forschungseinrichtungen können in das Visier staatlich gesteuerter Cyberangriffe geraten, die darauf abzielen, sensible Forschungsdaten zu erbeuten.

Beispiel: *Mittels einer Phishing-E-Mail werden Studierende auf die nachgestellte Anmeldeseite der Universitätsbibliothek geleitet. Die Angreifer können die erbeuteten Zugangsdaten nutzen, um in das Computernetzwerk einzudringen.*

SCHUTZMASSNAHMEN

- Implementieren Sie als **Teil eines ganzheitlichen Sicherheitsansatzes** eine Cybersicherheitsstrategie.

Daten/Prozesse

- *sensible Informationen identifizieren und klassifizieren*
- *Zugriffsrechte auf Laufwerke und Daten limitieren und regelmäßig prüfen*
- *Krisenpläne, Richtlinien und Checklisten aufstellen*
- *Datenströme auf verdächtiges Verhalten überwachen*
- *Zugänge durch starke Passwörter schützen*

Hard- und Software

- *aktuelle Betriebssysteme und Programme verwenden*
- *Sicherheitslücken schließen und neueste Updates installieren*
- *Backups anfertigen und separat aufbewahren*
- *Netzwerksicherheitstools (IDS/IPS) einsetzen*
- *E-Mails mit Transport- oder Ende-zu-Ende-Verschlüsselung schützen*

Beschäftigte

- *Beschäftigte zu allgemeinen Sicherheitsvorkehrungen sensibilisieren*
- *Thematische Schulungen durchführen (Datensicherheit, Social Engineering, Phishing etc.)*
- *Verhalten im Krisenfall üben*
- *vertrauliche Meldewege für Beschäftigte etablieren*

Anbahnungsversuche

AUSGANGSLAGE

- Ausländische Nachrichtendienste versuchen mit verschiedenen Methoden **wissenschaftliche Fachkräfte**, z. B. bei Auslandsreisen, zu **einer Zusammenarbeit** zu bewegen, um so direkt an sensible Forschungsdaten zu gelangen.

Beispiel: *Eine Forscherin wird während eines Auslandsaufenthalts durch einen vermeintlichen Kollegen angesprochen und gegen eine Entlohnung um eine fachliche Stellungnahme gebeten. Später wird zunehmend Interesse an den eigentlichen Forschungsergebnissen gezeigt.*

SCHUTZMASSNAHMEN

- **Schulen Sie wissenschaftliches Personal** im Hinblick auf mögliche Anbahnungsversuche durch ausländische Nachrichtendienste.
- Stellen Sie sicher, dass **Verhaltensregeln** für Auslandsaufenthalte **existieren und bekannt** sind.

→ *Informationsblätter: „Sicherheit auf Geschäftsreisen“, „Methoden der Spionage: HUMINT“*

Gastbesuche

AUSGANGSLAGE

- Teilnehmende einer Besuchsdelegation können versuchen, Ihnen **Informationen zu entlocken**, **Sicherheitsvorkehrungen zu umgehen** oder **unerlaubte elektronische Geräte mit einzubringen**.

Beispiel: *Zu einer Führung durch eine Forschungsabteilung erscheinen unangekündigt fünf zusätzliche ausländische Delegationsmitglieder. Während der Führung entfernen diese sich immer wieder unerlaubt von der Gruppe, teilweise werden Fotoaufnahmen der Einrichtung gemacht.*

SCHUTZMASSNAHMEN

- Stellen Sie verbindliche Regeln auf, wie mit **technischen Geräten** und **nicht angekündigten Besuchenden** umgegangen wird.
- Stellen Sie sicher, dass alle Mitglieder der Besuchsgruppe **eine Freigabe** haben und ggf. **ein Hintergrund-Check durchgeführt** wurde.
- Überlegen Sie bei **sicherheitssensiblen Bereichen**, ob dort ein Besuch wirklich notwendig ist.
- Überprüfen Sie vorab die Besichtigungsstrecke auf **einsehbare sensible Informationen** (Aushänge, Bildschirme etc).
- Halten Sie die Gruppe zusammen und achten Sie auf die **Einhaltung der Verhaltensregeln**.

Wirtschaft & Wissenschaft.
Zukunftssicher.
Verfassungsschutzverbund des Bundes und der Länder

Das Bundesamt für Verfassungsschutz und die 16 Landesbehörden für Verfassungsschutz bilden gemeinsam den Verfassungsschutzverbund. Auch im Bereich des präventiven Wirtschaftsschutzes arbeitet dieser eng zusammen. Auf diese Weise entsteht ein starkes Netzwerk bis zu Ihnen vor Ort. Eine Übersicht über die Ansprechbarkeiten in den Landesbehörden finden Sie unter ***www.verfassungsschutz.de****.*

initiative wirtschaftsschutz
Gemeinsam. Werte. Schützen.

Die Initiative Wirtschaftsschutz ist ein Zusammenschluss von BfV, BKA, BND und BSI. Auf der Informationsplattform ***www.wirtschaftsschutz.info*** *stellen sie zusammen mit verschiedenen Partnerverbänden ihre Expertise im Bereich Wirtschaftsschutz zur Verfügung. Dazu gehört das Thema Cyberkriminalität genauso wie Wirtschafts- und Wissenschaftsspionage oder das Thema IT-Sicherheit.*

Ihr direkter Kontakt zum Wirtschaftsschutz

Ministerium des Innern und für Sport Rheinland-Pfalz
Wirtschaftsschutz
Schillerplatz 3-5
55116 Mainz
Tel.: 06131/16-3773
Email: wirtschaftsschutz@mdi.rlp.de

Scannen Sie den QR-Code und gelangen Sie direkt zu allen bisher erschienenen Infoblättern.