Info Blatt

Informationsblätter zum Wirtschaftsschutz

Methoden der Spionage: HUMINT

Ausländische Nachrichtendienste gehen in Deutschland Spionageaktivitäten nach und nutzen dabei auch menschliche Quellen (HUMINT). Mit verschiedenen Methoden versuchen sie, sowohl deutsche als auch eigene Staatsangehörige zu einer Zusammenarbeit zu bewegen.

Mögliche Gefährdungen lassen sich jedoch minimieren. Dabei können auch die Sicherheitsbehörden hinzugezogen werden. Der Verfassungsschutz ist für die Abwehr von Spionage und Sabotage durch ausländische Nachrichtendienste zuständig und steht als vertraulicher Ansprechpartner zur Verfügung.

1 Was ist HUMINT?

- Ausländische Nachrichtendienste versuchen mittels Spionage **wirtschaftliche, wissenschaftliche, militärische und politische Informationen** zu erlangen. Dabei kommen verschiedene ***Methoden der Informationsgewinnung*** zum Einsatz.
- HUMINT steht für Human Intelligence und beschreibt die **Gewinnung von Informationen mittels menschlicher Quellen.**
- Die Zielpersonen werden **gezielt ausgewählt** und ausgeforscht. Oftmals sind sich diese gar nicht über den Wert Ihres Wissens bewusst.

- ***Methoden der Informationsgewinnung***
  Nachrichtendienste bedienen sich neben des HUMINT-Ansatzes weiterer Methoden.

  OSINT *(Open Source Intelligence):*
  Informationsgewinnung aus offenen Quellen
  - *Lesen und Auswerten von Internetseiten, gezielte Recherche nach öffentlich zugänglichen Informationen, Anlegen von Social-Media-Profilen, Einsatz von Skripten, kommerzieller Software und speziellen Recherchetools, zielgerichtete legendierte Kommunikation mit der Zielperson*

  SIGINT *(Signals Intelligence):*
  Auswertung elektronischer Signale aller Art
  - *Einsatz von Erfassungs- und Filtertechniken zur Auswertung großer Datenströme*

SPIONAGEABWEHR

- *Die Abwehr staatlich betriebener Ausforschung gehört zu den Kernaufgaben des Verfassungsschutzes. Soweit Spionage gegen die Bundesrepublik Deutschland gerichtet ist, kommt eine Strafbarkeit gemäß § 93 ff. StGB in Betracht.*

2 Methoden und Ansätze einer Anbahnung.

Grundsätzlich kommen für ausländische Nachrichtendienste alle Personen für eine Anwerbung („Anbahnung“) infrage. Entscheidend dabei ist der mögliche Zugang zu bestimmten Informationen.

- Eine **HUMINT-Spionageaktion** kann in verschiedene Schritte untergliedert werden.

Vorbereitung

Auswahl der Zielperson, Umfeldforschung z. B. mittels OSINT (Interessen, Hobbys etc.)

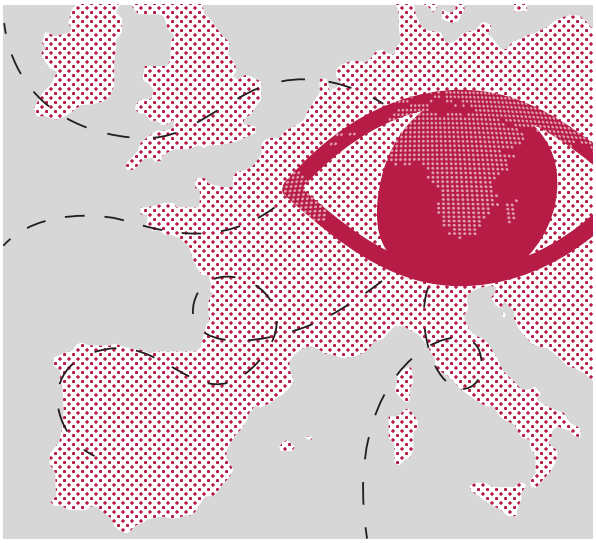
Erstkontakt/Aufbau

z. B. über Geschäftskontakt, private Begegnung, Aufbau von Vertrauen und Stabilität, ggf. Ausübung von Druck, Hinführung zu beruflichen Themen

Abschöpfung

Bitte um Informationsbeschaffung bzw. „fachlichen Rat“, ggf. längere Zusammenarbeit, möglichst unbemerkter Informationsabfluss

Ausländische Nachrichtendienste verfügen über umfangreiche Ressourcen und Know-how, um sich auf die Zielperson einzustellen. Die eingesetzten Methoden können in Umfang, Qualität und Dauer variieren und auch miteinander verknüpft werden. Zudem gehen ausländische Nachrichtendienste zumeist verdeckt vor, so dass die Zielperson keinen oder zu spät Verdacht schöpft.



Beim Erstkontakt bzw. in der Aufbauphase nutzen ausländische Nachrichtendienste verschiedene Werkzeuge, um Sie zu einer Mitarbeit zu bewegen.

Kompromittierung
- Sie werden mit vorher erbeuteten sensiblen persönlichen Daten (sexuelle Orientierung, Fehlverhalten etc.) zur Zusammenarbeit gezwungen.

Ego
- Für manche Personen steht die außergewöhnliche Erfahrung und die eigene Bedeutsamkeit im Mittelpunkt. Auch eine berufliche Unzufriedenheit bzw. eine geringe Loyalität zum Unternehmen können Auslöser für eine Spionagetätigkeit sein.

Ideologie
- Sie gehen aufgrund Ihrer weltanschaulichen Überzeugungen auf das Angebot ein (oder weil sie Ihrem Heimatland dienen wollen).

Belohnung
- Ihnen werden für Informationen Vergünstigungen angeboten: Geld, eine attraktive berufliche Position, Reisen, Teilnahme an Veranstaltungen, Auszeichnungen etc. Die Annahme kann zur weiteren Kompromittierung genutzt werden.

WORKING IN GERMANY

Insbesondere ausländische Arbeitskräfte aus autoritären Staaten oder Personen mit familiären Verbindungen in diese Länder können zusätzlich unter Druck gesetzt werden.

Repression
- Ihnen oder Ihren Verwandten werden im Heimatland medizinische Behandlungen, Reisegenehmigungen, eine Universitätszulassung etc. erschwert oder sogar verwehrt.

Zwangsverpflichtung
- Sie werden durch Ihr Heimatland aufgrund gesetzlicher Bestimmungen zur Zusammenarbeit verpflichtet. Bei Verweigerung drohen Sanktionen.

3 So schützen Sie sich.

Maßnahmen mit Blick auf Spionage (HUMINT)

ALS GESCHÄFTSFÜHRUNG / SICHERHEITSVERANTWORTLICHE

- Führen Sie ein ***Schutzkonzept*** ein.
- Klassifizieren Sie Unternehmensdaten nach **Vertraulichkeitsklassen**.
- Setzen Sie das „**Need-to-know-Prinzip**“ um.
- Führen Sie bei der Personalauswahl **Hintergrund-Checks** durch.
- Schaffen Sie ein **angenehmes Arbeitsumfeld** – zufriedene Beschäftigte sind loyal.
- Etablieren Sie eine **konstruktive Fehlerkultur und Meldewege**.
- **Schulen Sie die Beschäftigten auch im Hinblick auf mögliche Anbahnungsversuche.**

ALS BESCHÄFTIGTE

- Seien Sie vorsichtig bei **Gefälligkeiten oder beruflichen Angeboten** mit unüblichen Konditionen.
- Lassen Sie sich die **Identität** des Ansprechpartners ggf. **bestätigen**.
- Schützen Sie Ihre Daten durch **sichere Passwörter**.
- Lassen Sie Skepsis walten bei **ungewöhnlichen fachlichen Anfragen**.
- Nehmen Sie im Zweifelsfall Kontakt mit der **sicherheitsverantwortlichen Stelle** bzw. den Sicherheitsbehörden auf.
- Insbesondere als Staatsangehörige eines **autoritär geführten Landes** müssen Sie mit Ansprachen durch Nachrichtendienste rechnen, z. B. bei **Heimreisen oder bei Besuchen in diplomatischen Vertretungen** in Deutschland.

Die Einführung eines Schutzkonzepts

1. **RISIKOANALYSE**
   - *Welches sind die schützenswerten Güter?*
   - *Wer könnte Interesse an diesen haben?*
   - *Wie könnten Angreifer an diese gelangen?*
2. **SCHUTZKONZEPT**
   - *Leiten Sie aus der Risikoanalyse Schutzmaßnahmen ab.*
   - *Bereiche: physische Sicherheit, IT-Sicherheit, personelle Sicherheit*
   - ***BSI IT-Grundschutz, Wirtschaftsgrundschutz***
3. **KONTROLLE**
   - *Prüfen Sie Schutzkonzept und Maßnahmen auf deren Wirksamkeit.*
4. **ANPASSUNG**
   - *Passen Sie ggf. Schutzkonzept und Maßnahmen an.*

IT-Grundschutz und Wirtschaftsgrundschutz
*Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist ein Ansatz für den Schutz der Informationstechnik. Analog dazu zielt der Wirtschaftsgrundschutz der **Initiative Wirtschaftsschutz** auf physische, personelle, prozessuale und organisatorische Aspekte der Sicherheit.*

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