Eine PowerPoint-Version zur Verwendung in Ihrer Organisation finden Sie unter:
https://wiskos.de/de/informationen_fuer/wissenschaftsorganisationen.html

Risiken für den deutschen Forschungsstandort

Leitfaden zum Umgang mit Wissenschaftsspionage und Konkurrenzausspähung im Wissenschaftskontext

WISKOS

Outline

- Angriffsziel Wissenschaft
- Wissenschaftsspionage – was ist das?
- Phänomenologie – wer sind die Täter, wie ist ihr Modi Operandi?
- Handlungsempfehlungen – wie können Sie präventiv oder im Schadensfall handeln?
- Ansprechpartner und weitere Informationen

Hinweis: Aus Gründen der leichteren Lesbarkeit wird in der vorliegenden Präsentation die männliche Sprachform bei personenbezogenen Substantiven und Pronomen verwendet. Sämtliche Sprachformen gelten gleichermaßen für alle Geschlechter.

Angriffsziel Wissenschaft

Begehrte Wissenschaft

Bin ich betroffen?

- Betreiben Sie/Ihre Institution Spitzenforschung?
- Forschen Sie in der Pharmabranche, Optik, Physik, Chemie aber auch anderen Bereichen?
- Entwickeln Sie Dual-Use-Güter?

→ Ja!

- Kann ich betroffen sein, obwohl ich nie etwas bemerkt habe?

→ Ja!

Begehrte Wissenschaft

- Die deutsche Forschungslandschaft gehört nicht erst seit der Hightech-Strategie 2020 zur Weltspitze.
- Die Schadenssummen im Wirtschaftssektor werden auf **Milliarden Euro** geschätzt – im Wissenschaftssektor fehlen Statistiken und Schätzungen.
- Problematisch ist, dass sich nicht alle Forschungserfolge finanziell darstellen lassen.
- Jährlich kommt es zu zahlreichen Schadensfällen durch den **Verlust von Forschungsergebnissen** oder den **Vertrauensverlust** von Kooperatoren und Drittmittelgebern.

Begehrte Wissenschaft

Besonders anfällige Forschungsfelder in der Wissenschaft sind:

- Luft- und Raumfahrt
- Physik, Chemie, Pharmazie
- (Quanten-)Optik
- Biotechnologie
- Medizin
- Klima/Energie
- Mobilität
- Kommunikations- und Informationstechnologie
- Nanotechnologie

Begehrte Wissenschaft

Wissenschaft ist oft ein leichtes Angriffziel !

- Der Schutzbedarf bzw. das schützenswerte Know-how ist häufig unbekannt.
- Das Schutzniveau ist nicht an den Schutzbedarf angepasst.
- Es gibt kein ganzheitliches Sicherheitskonzept.

Begehrte Wissenschaft

Folgen für die Wissenschaftsorganisation können sein:

- Verlust von Auftraggebern
- Aufhebung von wissenschaftlichen/ausländischen Kooperationen
- Vertrauensverlust bei Kooperatoren und Drittmittelgebern
- Imageschaden

Wissenschaftsspionage - was ist das?

Terminologie

	Wissenschaftsspionage	Konkurrenzausspähung im Wissenschaftskontext
Akteur	• Geheimdienst eines anderen Staates	• ein Unternehmen oder eine andere Forschungseinrichtung
Ziel	• Förderung der Wirtschaft oder Wissenschaft eines fremden Staates • politische Interessen	• Wettbewerbsvorteil eines konkurrierenden Unternehmens
Informations-beschaffung	• breit angelegte Informationsbeschaffung	• produktbezogene Informationsbeschaffung
Kriminalitätsbereich	• Staatsschutzdelikt • §§ 94 StGB ff	• Wirtschaftskriminalität • §§ 17 UWG ff.

Zuständigkeiten

	Wissenschaftsspionage	Konkurrenzausspähung im Wissenschaftskontext
Prävention	• Bundesamt/Landesamt für Verfassungsschutz • Polizeibehörden: → Bundeskriminalamt → Landeskriminalamt → Lokale Polizeibehörde	• Polizeibehörden: → Bundeskriminalamt → Landeskriminalamt → Lokale Polizeibehörde
Strafverfolgung	• Bundesanwaltschaft • Polizeibehörden: → Bundeskriminalamt → Landeskriminalamt → Lokale Polizeibehörde	• Staatsanwaltschaft • Polizeibehörden: → Bundeskriminalamt → Landeskriminalamt → Lokale Polizeibehörde

Phänomenologie – wer sind die Täter, wie ist ihr Modi Operandi?

Potentielle Täterschaft

Außentäter	Innentäter
„Der klassische Einsatz eines konspirativen Agenten hat keineswegs ausgedient." Boos, LfV Sachsen, „Wissenschaftsspionage: Risiken für den Forschungsstandort Deutschland in einer offenen globalen Informationsgesellschaft", 2012, S. 63.	„Der Faktor mit dem höchsten Risikopotential", da er „in der Regel über volle physische und virtuelle Zugangsmöglichkeiten zu Räumlichkeiten, Netzwerken und Datenbanken" verfügt." BfV, "Innentäter" eine unterschätzte Gefahr in Unternehmen, Sicherheitstagung von BfV und ASW, 2015, S. 6.

Potentielle Täterschaft

Außentäter	Innentäter

• Nachrichtendienste, z.B. aus:
  • China
  • Russland
  • Iran
  • Syrien
  • USA
  • aber auch aus dem europäischen Ausland
• Forscher anderer Einrichtungen
• Wirtschaftsunternehmen
	• Wissenschaftliche Mitarbeiter
	• Administrative Mitarbeiter
	  • Reinigungspersonal
	  • Zulieferer
	  • Externe Dienstleister, z.B. Mitarbeiter einer outgesourcten IT-Abteilung
	• Gastwissenschaftler
	• Tagesgäste
	• Praktikanten

Modi Operandi

Wie gehen die Täter vor?

- **Physische Kriminalität**, zum Beispiel:
  - Diebstahl von Datenträgern, Modellen und Prototypen
  - Fotografie von Skizzen
  - Unbefugtes Betreten von Institutsgeländen
  - Social Engineering, wenn Mitarbeiter durch Kontakte mit Dritten zur Weitergabe geschützter Informationen angehalten werden

- **Cybercrime**, zum Beispiel:
  - (Spear-)Phishing
  - Bot-Netze
  - DoS/DDoS-Attacken

Modi Operandi

Beispiel: Phishing-Attacke

„In der Mail war ein Link drin [...] Der Link ging auf ein Paper bei Springer-Link über die örtliche Bibliotheksmaske zum Anmelden. Darüber sollte das Passwort abgegriffen werden. Die Maske war nachgebaut und in der eigentlichen URL war ein kleiner Buchstabe geändert. Die LMU hat die Adresse „@uni-muenchen.de“. In der nachgebauten Adresse war bei „München“ das letzte „e“ durch ein „i“ ersetzt. 30-40 Wissenschaftler in Deutschland haben solche E-Mails bekommen und teilweise auf die Mails geantwortet und auf diese Antwort wieder eine Antwort bekommen. Das war richtig gut gemacht [...]“

[Interview mit dem Vertreter einer Wissenschaftsorganisation 2016]

Aufdeckung der Taten

Wie können Sie Taten aufdecken?

- **routinemäßige Kontrolle** der Datenströme und Rechneraktivitäten,
- **Hinweise** von Mitarbeitern oder Dritten,
- beobachtete auffällige **Verhaltensänderung** bei Mitarbeitern

Handlungsempfehlungen – wie können Sie präventiv oder im Schadensfall handeln?

Handlungsempfehlungen

Prävention

- **Risikoanalyse des Schutzbedarfs**
  - nach einzelnen Forschungsbereichen
- **Individuelle Festlegung/Anpassung des Schutzniveaus**
  - für die gesamte Forschungseinheit
  - für die einzelnen Forschungsabteilungen
  - für die einzelnen adminstrativen Bereiche (Rechtsabteilung, IT-Abteilung, Gründernetzwerk)
- **Entwicklung eines ganzheitlichen Schutzkonzepts** unter Verknüpfung *personeller*, *organisatorischer* und *technischer* Maßnahmen

Handlungsempfehlungen

Mögliche **personelle Einzelmaßnahmen**

- Thematische Sensibilisierung und Schulung der Mitarbeiterschaft (für Datenschutz/ Datensicherheit, bzgl. Social Engineering…).
- Einrichtung der Stelle eines Sicherheitsbeauftragten.
- Überprüfung von Bewerbern, Gastwissenschaftlern.
- Beobachtung von auffälligem Verhalten etablierter Mitarbeiter.
- Verfolgung der Karrierewege nach Verlassen der Wissenschaftsorganisation.
- Vertraulichkeitsvereinbarungen für Mitarbeiter und Kooperationspartner.

Handlungsempfehlungen

Mögliche **organisatorische Einzelmaßnahmen**

- Hinzuziehung externer Sicherheitsberater.
- Krisenpläne (rapid reaction force) und Übung kritischer Situationen durch die Simulation eines Angriffs.
- Vorschriften zur Überwachung der Hardware.
- Mitgliedschaft in und aktive Nutzung von gemeinsamen Arbeitskreisen, z.B. dem AKIF, Tagungen und Newslettern.

Handlungsempfehlungen

Mögliche **technische Einzelmaßnahmen**

- Abstufung bei den Zugangsberechtigungen sowie Zugangskontrollen technischer oder personeller Natur zu den Forschungseinrichtungen.
- Sicherheitsvorschriften zum Umgang mit sensiblen Daten.
- Limitierte Zugriffsrechte (Rechtemanagement) auf Laufwerke und Daten sowie share points ggf. mit Freigabevorgaben.
- Sicherheitsstufen beim Zugang zu Dokumenten und eine digitale Zugriffskontrolle.

Handlungsempfehlungen

Sie schöpfen Verdacht: was tun?

- Sie leiten sofort Abwehr- und Schutzmaßnahmen ein, auch bei einem scheinbar geringen Schaden.
- Sie kontaktieren sofort Ihren Ansprechpartner bei der Polizei oder die Fachdienststellen der Landeskriminalämter oder des Bundeskriminalamtes.

Handlungsempfehlungen

Was erwartet Sie?

- Ihr Anliegen wird sofort vertrauensvoll und diskret behandelt.
- Mit Ihren Informationen wird sensibel umgegangen.
- Die Ermittlungen dauern unter Umständen lange. Sie können sich bei Ihrem polizeilichen Ansprechpartner jederzeit nach dem aktuellen Status erkundigen.

Ansprechpartner und weitere Informationen

Kompetente Ansprechpartner

Bei Fragen zur **Prävention** und **Strafverfolgungen** wenden Sie sich an **Ihren Ansprechpartner bei der Polizei**

oder

an die Fachdienststellen der **Landeskriminalämter** und des **Bundeskriminalamtes**

Kompetente Ansprechpartner

Fachdienststellen der Landeskriminalämter und des Bundeskriminalamtes

LKA Baden-Württemberg (Inspektion 610)
0711 / 5401-2610
stuttgart.lka.abt6.i610@polizei.bwl.de

LKA Bayern (SG 422-EK3)
089 / 1212-3469
blka.spionage-ansprechstelle@
polizei.bayern.de

LKA Berlin (LKA 524, SG 2)
030 / 4664-952420
lka524@polizei.berlin.de

LKA Brandenburg (LKA 300)
03334 / 388-3001
zentraler.staatsschutz.fdlka@polizei.
brandenburg.de

LKA Bremen (K 63)
0421 / 362-3863
k63@polizei.bremen.de

LKA Hamburg (LKA 72)
040 / 4286-77200
lkahh72@polizei.hamburg.de

LKA Hessen (Hauptsachgebiet 53, SG 533)
0611 / 83-53000
hsg53.hlka@polizei.hessen.de

LKA Mecklenburg-Vorpommern (Dez. 32)
03866 / 64-3250
dez32.lka@lka-mv.de

LKA Niedersachsen (Dez. 42)
0511 / 26262-4244
abteilung4@lka.polizei.niedersachsen.de

LKA Nordrhein–Westfalen (Dez. 23)
Tel.: 0211 / 939-2320
33-Sachgebiet232.LKA@polizei.nrw.de

LKA Rheinland-Pfalz (Dez. 53)
06131 / 65-2364
lka.53.l@polizei.rlp.de

LKA Saarland (Dez. LPP 233)
0681 / 962-2660
lpp233@polizei.slpol.de

LKA Sachsen (Dez. 52)
0351 855-3522
ermittlungen.pst.lka@polizei.sachsen.de

LKA Sachsen – Anhalt (Dez. 53)
0391 / 250-2530
dl53.lka@polizei.sachsen-anhalt.de

LKA Schleswig-Holstein (SG 321)
0431 / 160-4302
kiel.lka3@polizei.landsh.de

LKA Thüringen (Dez. 23)
0361 / 341-1166
abteilung2.lka@polizei.thueringen.de

Bundeskriminalamt (Referat ST 23)
02225 / 89-23286
st23@bka.bund.de

Weitere Informationen und Kontaktpersonen finden Sie unter

http://wiskos.de

Max-Planck-Institut für ausländisches und internationales Strafrecht
Abteilung Kriminologie
Günterstalstr. 73
79100 Freiburg i.Br.

Tel.: +49-761-7081-0
Fax: +49-761-7081-294
www.mpicc.de

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Text: Dr. Sabine Carl, Susanne Knickmeier, M.A.
Layout: Egzona Hyseni, Susanne Knickmeier, M.A.

WISKOS