Schulung Wissenschaftsschutz

30.09.2024

Simon Lohmann

Referent für Informationssicherheit

BERGISCHE UNIVERSITÄT WUPPERTAL

Unerwünschten Wissens- und Datenabfluss verhindern
– Wissenschaftsschutz

- Ausnutzung der Forschungsfreiheit:
  Wissenschaftsspionage und -sabotage
- Ungleichgewicht bei Wissensweitergabe und Technologietransfer
- Verlust von Aufträgen, Patenten und finanzieller Unterstützung
- Beeinträchtigung Ihres Ansehens und Ihrer Glaubwürdigkeit in der Wissenschaftscommunity

Wissenschaftsspionage und -sabotage
– Definition

Wissenschaftsspionage

Illegale Beschaffung von Forschungsdaten durch fremde Regierungen, Organisationen oder Einzelpersonen, um eigene Vorteile gegenüber anderen zu erlangen

Wissenschaftssabotage

Absichtliche Behinderung von Forschungsprojekten, Beschädigung von Forschungsergebnissen oder Zerstörung von wissenschaftlichen Einrichtungen / Apparaten

Der Schutz der Forschung vor Spionage und Sabotage ist entscheidend für den wissenschaftlichen und gesellschaftlichen Fortschritt!

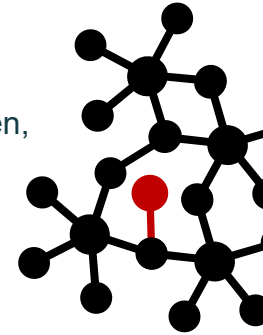
Wissenschaftsspionage und -sabotage
– Mögliche Warnsignale

Unübliche finanzielle Anreize
im Austausch für Forschungsdaten / berufliche Angebote mit besonderen Konditionen (hohes Gehalt, reichhaltige Forschungsmittel)

Plötzliche, auffällige **Verhaltensveränderungen** externer Druck oder finanzielle Anreize möglich

Ungewöhnliche fachliche Anfragen oder ungewöhnliches Interesse
an Forschungsinhalten und Technologien außerhalb des eigenen Forschungsbereichs

Verdächtige Aktivitäten
z. B. unerklärliche Datenverluste, unbekannte Netzwerkverbindungen, unautorisierte Änderungen an technischen Geräten

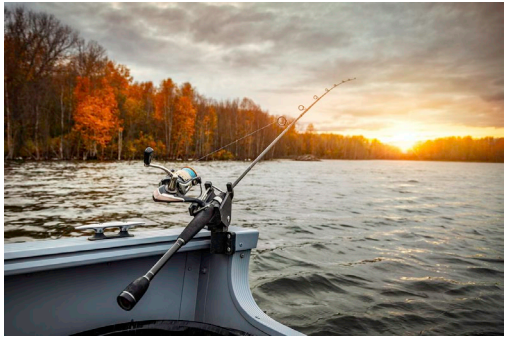


Unangekündigte Besuche
von Personen, die nicht zum Lehrstuhl / Institut gehören

Soziale Manipulation kann uns alle treffen
– Die erste Kontaktaufnahme erfolgt ...

... auf Tagungen,
bei gemeinsamen
Forschungsprojekten oder
Austauschprogrammen

... über soziale Medien
(beruflich wie privat)



... im privaten Umfeld,
z. B. über gemeinsame Hobbies

Wissenschaftsspionage
– Beispiel von der Universität Augsburg

1) **Einstellung** eines russischen Doktoranden in 2014 für einen naturwissenschaftlich-technischen Lehrstuhl im Bereich Materialwissenschaften

2) **Gezielte Ansprache** des Doktoranden im Herbst 2019 durch einen Mitarbeiter des zivilen Auslandsgeheimdiensts der Russischen Föderation (SWR)

Er habe für eine russische Bank gearbeitet und benötige Informationen für private Investitionen in die Weltraumforschung

3) **Aufbau von Vertrauen** und weitere Treffen bis Juni 2021

- Doktorand **gibt Informationen** zu Forschungsprojekten **weiter** (Bereich Luft- und Raumfahrttechnologie)
- Für diese **sensiblen Daten** bekommt er **insgesamt 2.500 Euro**

4) **Festnahme** des Doktoranden und **Verurteilung** wegen geheimdienstlicher Agententätigkeit

Soziale Manipulation kann uns alle treffen
– Entwickeln Sie eine gesunde Skepsis

Halten Sie Gespräche mit Ihnen fremden Personen **auf oberflächlicher Ebene**

Lassen Sie sich die **Identität** der Kontaktperson nach Möglichkeit **bestätigen**

Bleiben Sie **vorsichtig** bei **ungewöhnlichen** fachlichen Anfragen oder **besonderen** Anreizen, die man Ihnen bietet

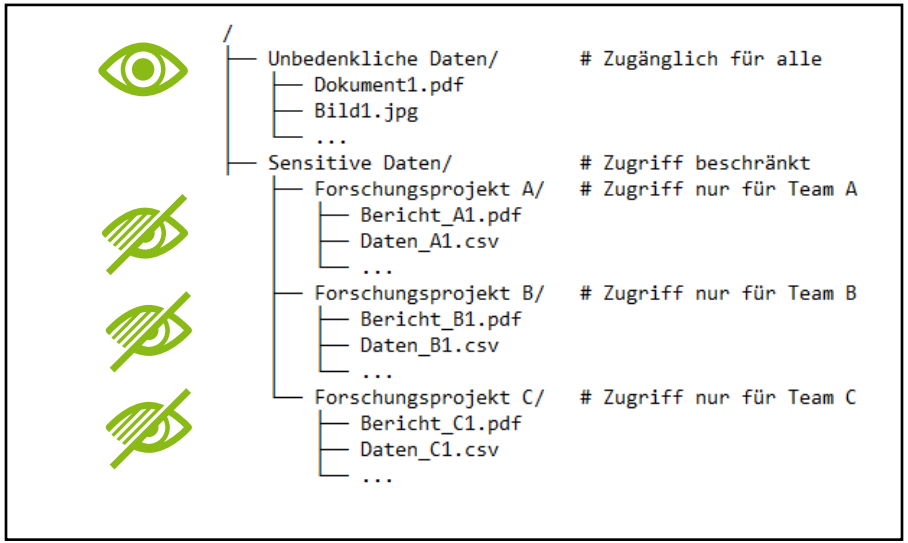
Sensible Daten kennen und vor Missbrauch schützen

- **Ordnen** Sie wissenschaftliche Daten **Sicherheitsstufen** entsprechend ihrer Sensibilität zu.
  - Arbeitshilfen zur sachgerechten Einordnung finden Sie bei Dezernat 1.4.

- **Beschränken** Sie den Zugriff auf Informationen…
  - Individuelle Zugriffsberechtigungen für Mitarbeiter*innen
  - separierte Ordnerstrukturen / getrennte Laufwerke
  - *auch:* Schließberechtigungen für Räume, Schränke, …

…nach dem **„Need to know“-Prinzip:**

Jede Person hat nur auf die Informationen Zugriff ,
die für die Ausübung ihrer spezifischen Aufgaben
unbedingt erforderlich sind.



Verschlüsselung

- **Verschlüsseln** Sie **sensible Informationen**
  auf Desktop-Computern, in Clouds und auf mobilen Endgeräten,
  um diese vor unbefugtem Zugriff zu schützen
  - https://informationssicherheit.uni-wuppertal.de/de/verschluesselung/

- Verschlüsselung eines ganzen Datenträgers/Gerätes → Bereichs-IT (sofern vorhanden) oder ZIM

Bei Reisen nach bspw. China, Russland und Israel dürfen Geräte nicht verschlüsselt werden.
→ *Speichern Sie nur die zwingend notwendige Daten auf einem „leeren" Laptop oder Smartphone.*

- **Überprüfen** Sie regelmäßig die Verschlüsselungstechnologien und **aktualisieren** Sie bei Bedarf auf einen neueren Stand der Technik. *Wenn Sie sich unsicher sind: Fragen Sie das ZIM.*

Quelle: https://zim.uni-wuppertal.de/de/unsere-dienste/it-sicherheit/it-sicherheitsvorfall-melden/

Erstellen Sie einen

Notfallplan zur schnellen Reaktion

an Ihrem Lehrstuhl bzw. Institut

- Klare Verantwortlichkeiten
- Klare Handlungsschritte
- Incident-Response-Person
  Ansprechperson bei Ihnen, die im Notfall den Kontakt mit dem ZIM aufnimmt.

Weiterführende Informationen des Bundesamtes für Verfassungsschutz (BfV)

Informationsblätter

SPOC-Magazin

Haben Sie noch Fragen? Sprechen Sie uns gerne an!

Exportkontrollbeauftragter

Karsten Draeck

Telefon +49 202 439-**1188**
draeck@uni-wuppertal.de

Informationssicherheitsbeauftragte

Stephanie Ziegler

Telefon +49 202 439-**5434**
sziegler@uni-wuppertal.de

Bei Fragen zur technischen Umsetzung:

IT-Sicherheit

Alain Michel Keller

Telefon +49 202 439-**2124**
itsec@uni-wuppertal.de

BERGISCHE
UNIVERSITÄT
WUPPERTAL