TECHNOPOL
Ein Modul des Sensibilisierungs-
programms Prophylax

AKADEMISCHE WELT IM VISIER

Spionage und Proliferation im akademischen Bereich

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Nachrichtendienst des Bundes NDB

TECHNOPOL
Ein Modul des Sensibilisierungsprogramms Prophylax

AKADEMISCHE WELT IM VISIER

Spionage und Proliferation im akademischen Bereich

INHALTS-VERZEICHNIS

EINLEITUNG

Seit 2004 führt der Nachrichtendienst des Bundes (NDB) das Sensibilisierungsprogramm Prophylax, das Unternehmen, Wirtschaftsorganisationen und Forschungseinrichtungen auf die Bedrohungen durch Proliferation und Spionage aufmerksam macht. Prophylax erfüllt den gesetzlichen Auftrag des NDB, Programme zur Information und Sensibilisierung betreffend Bedrohungen der inneren und äusseren Sicherheit zu führen (Art. 6 Abs. 6 des Bundesgesetzes über den Nachrichtendienst). Als Bestandteil von Prophylax dient Technopol der Sensibilisierung von Universitäten, Hochschulen und Forschungsinstituten in der Schweiz und in Liechtenstein.

Technopol richtet sich an Angehörige von Universitäten, Hochschulen und Forschungsinstituten und zeigt auf, weshalb sie für ausländische Nachrichtendienste ein interessantes Ausforschungsziel darstellen können. Gleichzeitig soll das Bewusstsein für die Spionagebedrohung und für das Missbrauchspotenzial des vermittelten Wissens und Know-hows in Lehre, Forschung und Administration der genannten Institutionen geschärft werden. Nebst der Sensibilisierung bietet Technopol dem Zielpublikum konkrete Sicherheitsmassnahmen zum besseren Schutz vor illegalem Wissens- und Technologietransfer sowie ungewolltem Informations- und Datenabfluss.

Hochschulen und Forschungsinstitute leben vom internationalen Austausch wissenschaftlicher Informationen und Forschungsergebnisse. Dieser Austausch wird von der Europäischen Union stark gefördert. Im Europäischen Forschungsraum (EFR), in dessen Gouvernanz die Schweiz als relevantes Drittland fallweise eingebunden werden kann, wird die freie Mobilität für Forscherinnen und Forscher sowie der offene Zugang zu Forschungsergebnissen und Technologien angeregt. Die mehrjährigen EU-Rahmenprogramme für Forschung und Innovation sind ein wichtiges Instrument für die Umsetzung des EFR. Um vom EFR profitieren und an den Rahmenprogrammen teilnehmen zu können, sind europäische Hochschulen bzw. Projektpartner verpflichtet, aktiv am Wissenstransfer teilzunehmen, indem sie eigene Forschungsdaten teilen.

Doch trotz öffentlich zugänglichen Forschungsergebnissen sind Hochschulen und Forschungsinstitute von Spionage und Proliferationsaktivitäten bedroht, wie die folgenden Erläuterungen aufzeigen.

HOCHSCHULEN UND FORSCHUNGS-INSTITUTE IM VISIER

BEWUSSTSEIN STÄRKEN

Die internationale Zusammenarbeit und Mobilität von Studentinnen und Studenten sowie Wissenschaftlerinnen und Wissenschaftlern und der Wissensaustausch sind für den Forschungsbereich von zentraler Bedeutung und sollen nicht behindert werden. Es ist aber wichtig, dass sich Hochschulen und Forschungsinstitute der Spionage- und Proliferationsbedrohung bewusst sind und einen vorsichtigen Umgang mit kritischem Know-how pflegen. Dazu gehören die Sensibilisierung und Schulung aller Angehörigen der Hochschule bzw. des Forschungsinstituts (Wissenschaftlerinnen und Wissenschaftler, Professorinnen und Professoren, Mitarbeiterinnen und Mitarbeiter usw.) sowie Kenntnisse über exportkontrollierte Technologien und die Einholung von Exportbewilligungen beim Staatssekretariat für Wirtschaft (SECO), sollte eine solche Technologie ins Ausland transferiert werden.

Die Schweiz und die hier ansässigen Hochschulen und Forschungsinstitute tragen eine Verantwortung, dass das hierzulande von Studentinnen und Studenten sowie Wissenschaftlerinnen und Wissenschaftlern geschaffene oder angeeignete Wissen nicht zu illegalen Zwecken missbraucht wird. Die damit verbundenen Bedrohungen zu ignorieren, kann für eine Institution schwerwiegende Konsequenzen haben, sollte sie tatsächlich von Spionage- oder Proliferationstätigkeiten betroffen sein. Unter anderem drohen ihr der Verlust von Aufträgen und Forschungsmitteln, der Ausschluss aus internationalen Forschungsgremien, Reputationsverlust sowie eine schlechtere Position im internationalen Ranking. Zudem kann der Abfluss von vertraulichen Forschungsergebnissen ins Ausland langfristig zur Verschlechterung der internationalen Wettbewerbsfähigkeit der Schweiz in der Forschung führen. Personen, die im Auftrag eines ausländischen Nachrichtendiensts gegen Schweizer Interessen spionieren, setzen ihre Zukunft aufs Spiel. Sie riskieren Gefängnis und Karriere.

OFFENE KULTUR

Der hohe technologische Standard und Wissensstand sowie die Offenheit und Willkommenskultur der Schweizer Universitäten, Hochschulen und Forschungsinstitute werden weltweit geschätzt. Ausländische Forscherinnen und Forscher finden hier z. B. modernste Forschungslabors vor, in denen sie ihre wissenschaftlichen Versuche durchführen können.

Doch der einfache Zugang zu den Gebäuden, die Politik des offenen Austausches von wissenschaftlichen Informationen, die Zusammenarbeit mit Technologieunternehmen sowie die internationale Durchmischung des Lehrkörpers und der Studentenschaft machen Hochschulen auch zu einem attraktiven Ausforschungsziel ausländischer Nachrichtendienste. Diese versuchen, an Expertenmeinungen oder Forschungsdaten mit Bezug zu sensiblen Technologien (z. B. Robotik, neue Werkstoffe, Nanotechnologie) zu gelangen, um Wissenslücken in ihrem Herkunftsland zu schliessen. Dadurch sparen der Staat und seine Industrie eigene Forschungskosten, denn es ist meist günstiger, eine gesuchte Technologie oder ein Produkt auszuspionieren als finanzielle und personelle Ressourcen in die eigene Forschung und Entwicklung zu investieren.

FALLBEISPIEL

2014 wurde ein ausländischer Physiker verhaftet, der an einer niederländischen Universität forschte. Er wurde verdächtigt, dem russischen Auslandgeheimdienst SWR vertrauliche Forschungsinhalte verraten zu haben. Auf den Physiker aufmerksam geworden war das deutsche Bundesamt für Verfassungsschutz, als es einen russischen Diplomaten des Generalkonsulats in Bonn observierte, den es als Offizier des SWR enttarnt hatte. Einmal im Monat trafen sich der falsche Diplomat und der Physiker in Aachen, wo der Diplomat dem Physiker Geld übergab. Der Physiker fuhr für diese Treffen jedes Mal mit dem Auto aus den Niederlanden nach Aachen. Anlässlich der Verhaftung des Physikers leitete die Universität eine interne Untersuchung ein und entzog ihm daraufhin seine Zulassung. Das niederländische Justizministerium betrachtete ihn als „Gefahr für die nationale Sicherheit des Landes", entzog ihm sein Schengenvisum und verhängte gegen ihn ein Einreiseverbot.

ZUSAMMENARBEIT MIT DRITTEN

Viele Forschungsinstitute unterhalten Kooperationen mit Privatunternehmen und staatlichen Behörden, die entsprechende Forschungsprojekte auch finanzieren. Durch solche Kooperationen erhalten die am Projekt beteiligten Wissenschaftlerinnen und Wissenschaftler Zugang zu Expertisen und sensiblen Informationen. Damit sich die Forschungsinvestitionen für Unternehmen und Behörden lohnen, sind sie auf eine erste praktische Anwendung der Forschungsresultate auf dem Markt angewiesen. Fliessen Forschungsdaten und -ergebnisse aufgrund eines Spionageangriffs an Dritte ab, kommt dies einem Diebstahl von Finanzmitteln gleich. Dies setzt die künftige Zusammenarbeit mit dem Forschungsinstitut aufs Spiel. Auch die erhoffte Anerkennung von Wissenschaftlerinnen und Wissenschaftlern für bahnbrechende Forschungsarbeiten kann ausbleiben, wenn jemand die Forschungsergebnisse zuerst veröffentlicht oder praktisch erfolgreich anwendet.

FORSCHUNG

Im Hinblick auf einen illegalen Wissenstransfer betrachtet der NDB die angewandte Forschung in technischen und naturwissenschaftlichen Fachbereichen wie z. B. Maschinenbau, Luft- und Raumfahrttechnik, Elektrotechnik, Materialwissenschaften, Chemie, Biologie oder Informatik als besonders kritisch. Doch auch die Grundlagenforschung kann heikel sein, wenn Studentinnen und Studenten oder Wissenschaftlerinnen und Wissenschaftler Methoden und Techniken lernen, die sie entweder weitergeben oder später für andere Zwecke missbrauchen können (sog. dual-use research of concern). Ferner kann auch ein nichttechnischer Bereich das Interesse einer ausländischen staatlichen Behörde wecken, wenn dieser sich z. B. mit politischen Themen auseinandersetzt, die diesen Staat betreffen.

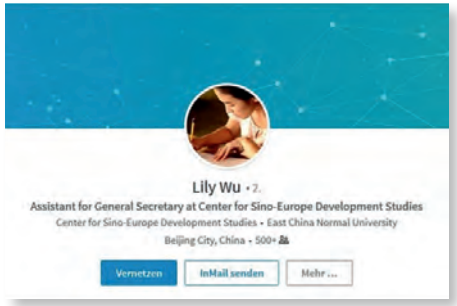
AKTIVITÄTEN AUSLÄNDISCHER NACHRICHTENDIENSTE

SPIONAGE

Beim verbotenen Nachrichtendienst (Spionage) geht es um die Beschaffung von Informationen und Daten aus den Bereichen Politik, Wirtschaft, Militär, Wissenschaft und Technologie, sofern dies zum Nachteil der Schweiz, ihrer Bevölkerung oder ihrer Behörden, Unternehmen oder Institutionen geschieht und die Informationen an einen ausländischen Akteur (Staat, Gruppierung, Unternehmen, Person usw.) weitergegeben werden oder dazu bestimmt sind.

FALLBEISPIEL

Ein junger Wissenschaftler an einer europäischen Universität erhielt eine Kontaktanfrage über das berufliche Netzwerk Linkedin von einem Mitarbeiter eines asiatischen Think Tanks. Dieser zeigte Interesse an der Arbeit des Wissenschaftlers und an einem fachlichen Austausch. Der Think Tank lud den Wissenschaftler ins Ausland ein, wobei er die Gesamtkosten der Reise und des Aufenthalts übernahm. Während seines Aufenthalts traf sich der Wissenschaftler mit Mitarbeitern des Think Tanks, die in Wahrheit Vertreter des staatlichen Nachrichtendienstes waren. Hier erfolgte der Versuch des Nachrichtendiensts, den Wissenschaftler als Informationsquelle anzuwerben, um an sensible Informationen aus seinem Arbeitsbereich zu gelangen.



Ein falsches Profil auf Linkedin, das von einem chinesischen Nachrichtendienst zur Kontaktaufnahme mit potenziell interessanten Personen verwendet wurde.

TALENT SPOTTING

Die Teilnahme an öffentlichen Universitätsanlässen (Konferenzen, Seminare usw.) bietet einem Nachrichtendienstoffizier die perfekte Gelegenheit, unverfänglich mit anwesenden Personen ins Gespräch zu kommen. Er interessiert sich für Expertinnen und Experten und versucht, ihnen durch geschickte und subtile Gesprächsführung nicht öffentliche Informationen (z. B. zu aktuellen Forschungsprojekten) zu entlocken. Er hält aber auch Ausschau nach Personen mit bestimmten politischen oder ideologischen Ansichten sowie nach jungen Akademikerinnen und Akademikern, die das Potenzial haben könnten, in Zukunft einen sensiblen Posten in einer Regierungsbehörde oder eine sensible Funktion in einer Firma im Hochtechnologiebereich zu besetzen. Die freundschaftliche Beziehung zu diesen Personen wird langfristig gepflegt, mit dem Ziel, im Falle einer Anstellung an schützenswerte Informationen zu gelangen.

FALLBEISPIEL

Eine europäische Studentin reiste für einen einjährigen Studienaufenthalt in ein asiatisches Land. Vor Ort stellte ihr ein Professor der Universität eine als lokale Studentin getarnte Mitarbeiterin des staatlichen Nachrichtendienstes vor. Dabei wurde die europäische Studentin angefragt, gegen Bezahlung Berichte für ein Forschungsinstitut zu schreiben. In Wirklichkeit handelte es sich um ein Tarninstitut, das der staatliche Nachrichtendienst zur Anbahnung europäischer Studenten verwendete, um diese für eine langfristige Zusammenarbeit zu rekrutieren.

BEOBACHTUNG EIGENER STAATSANGEHÖRIGER

Gewisse ausländische Nachrichtendienste forschen ihre im Ausland lebenden Mitbürgerinnen und Mitbürger aus, darunter Regimegegnerinnen und -gegner sowie Mitglieder der Diasporagemeinschaft. Dies tun sie u. a. an Hochschulen und Forschungsinstituten, wo sie z. B. anlässlich öffentlicher Veranstaltungen oppositioneller Gruppierungen Bild- und Tonmaterial über die anwesenden Personen sammeln. Ferner missbrauchen Staaten national organisierte Studentenvereinigungen an Universitäten zur Kontrolle der Studentinnen und Studenten. Zu Kontrollzwecken laden Botschaften diese oft zu Veranstaltungen ein. Solche Überwachungsaktivitäten sind in der Schweiz illegal und verstossen gegen Art. 272 (Politischer Nachrichtendienst) des Strafgesetzbuchs.

Insbesondere autoritär regierte Staaten appellieren an die Loyalität ihrer Staatsangehörigen, der Heimat zu dienen. Sie sollen ihr im Ausland angeeignetes Wissen dem Staat zur Verfügung stellen, indem sie z. B. an Forschungsprojekten zur Entwicklung von Waffensystemen mitwirken. Bestimmte Staaten belohnen ihre besten Studentinnen und Studenten mit der Möglichkeit, ihr Studium oder Doktorat für ein oder mehrere Semester im Ausland fortzusetzen. Ein solcher Aufenthalt wird oft vom Staat finanziert. Allerdings erwartet jener dafür eine Gegenleistung dieser Personen. Meistens sind sie verpflichtet, nach ihrer Rückkehr eine bestimmte Anzahl Jahre in ihrem Heimatland zu arbeiten, sei es für ein staatliches oder privates Unternehmen oder für eine Behörde.

FALLBEISPIEL

Ein an einer Schweizer Universität eingeschriebener ausländischer Doktorand meldete sich bei der Polizei, weil er sich von einigen seiner Landsleute, die Teil der Studentenvereinigung ihres Herkunftslandes sind, überwacht fühlte. Nachforschungen der Polizei ergaben, dass diese Landsleute von ihrer Botschaft beauftragt waren, ihre Mitstudentinnen und Mitstudenten zu beobachten. Ihr Auftrag war es, der Botschaft Bericht zu erstatten, wenn sich eine Studentin oder ein Student nicht gemäss den Erwartungen und den politischen Leitlinien des Herkunftslandes verhielt.

AUSLANDAUFENTHALTE

Im Ausland erhöht sich das Risiko, Opfer von Spionage zu werden. Studentinnen und Studenten sowie Wissenschaftlerinnen und Wissenschaftler, die ein oder mehrere Semester an einer Hochschule oder einem Forschungsinstitut im Ausland absolvieren, können vom dortigen Nachrichtendienst angegangen werden. Dessen Ziel ist es, an Wissen und Technologien sowie an vertrauliche Daten und nicht öffentlich zugängliche Informationen zu gelangen. Er kann z. B. versuchen, eine langfristige Beziehung zu einer Studentin oder einem Studenten aufzubauen und diese Person zu motivieren, sich im Heimatland um eine Anstellung in einer strategisch wichtigen Regierungsbehörde zu bemühen, die den Zugriff auf klassifizierte Informationen erlauben würde. Die Übergabe solcher Informationen an den ausländischen Nachrichtendienst erfolgt meist gegen Bezahlung oder durch andere Anreize. Dabei handelt es sich um verbotenen Nachrichtendienst zugunsten eines fremden Staats.

CYBERANGRIFFE

Die Netzwerkinfrastruktur einer Hochschule oder eines Forschungsinstituts ist aufgrund der hohen Anzahl Benutzerinnen und Benutzer, des oft geringen Bewusstseins für den Schutz von Informationen, der wenigen Zugriffseinschränkungen und der vielen Internetzugangspunkte besonders exponiert. Insbesondere elektronische Datenbanken von Hochschulen und Forschungsinstituten sind lohnenswerte Spionageziele, denn sie enthalten oft wichtige und sensible Forschungsinformationen. Zunehmend erfolgen Cyberangriffe auf IT-Netzwerke von Hochschulen, um z. B. mittels Phishing-Mails (sog. Credential-Phishing) an Zugangsdaten von Studentinnen und Studenten oder Mitarbeiterinnen und Mitarbeitern zu gelangen. Eine Angreiferin oder ein Angreifer kann aber auch die Netzwerkinfrastruktur einer Universität dazu missbrauchen, um von dort aus Unternehmen oder Organisationen anzugreifen.

SPIONAGEBEISPIELE

Anbahnung von Austauschstudentinnen und -studenten

- Ein ausländischer Nachrichtendienstoffizier gibt sich während des Aufbaus einer Beziehung zu einer Austauschstudentin bzw. zu einem Austauschstudenten nicht als Mitarbeiter eines Nachrichtendiensts aus, sondern tarnt sich z. B. als Student oder Mitglied eines Think Tanks, eines Forschungs- oder Sprachinstituts oder einer Beratungsfirma. Er kontaktiert die Studentin bzw. den Studenten unter einem unverdächtigen Vorwand wie der Vermittlung einer interessanten Arbeits- oder Praktikumsstelle, einer bezahlten Schreibarbeit oder eines Sprachaustauschs. Die Kontaktaufnahme erfolgt entweder in Person oder elektronisch. Insbesondere soziale Online-Netzwerke wie Linkedin oder Facebook ermöglichen es ausländischen Nachrichtendiensten, Informationen über eine Zielperson zu sammeln und im Hinblick auf eine mögliche Rekrutierung einen ersten Kontakt mit ihr herzustellen.

- Ein ausländischer Nachrichtendienst fragt eine Studentin oder einen Studenten an, gegen Bezahlung bestimmte Arbeiten zu erledigen oder bestimmte Informationen zu beschaffen. Dabei muss es sich nicht unbedingt um sensible Informationen handeln. Ziel ist es, die Tauglichkeit der Person als potenzielle Informantin oder potenzieller Informant zu prüfen.

- Ein ausländischer Nachrichtendienst beauftragt eine Professorin oder einen Professor, ausländische Studentinnen und Studenten zu rekrutieren.

- Das Gastland wirft einer Studentin oder einem Studenten angebliche Gesetzesverstösse oder Ordnungswidrigkeiten vor, um diese Person unter Druck zu setzen und zu einer Zusammenarbeit mit dem Nachrichtendienst zu zwingen.

- Unter dem Vorwand einer allgemeinen Umfrage zum Aufenthalt einer Studentin oder eines Studenten im Gastland und zu den Eindrücken dieser Person (z. B. mittels Fragebogen) versucht der ausländische Nachrichtendienst, ein Profil einer Studentin oder eines Studenten zu zeichnen und Informationen über Interessen, Bekanntenkreis oder Schwachpunkte zu erhalten.

MISSBRAUCH VON WISSEN UND TECHNOLOGIE

PROLIFERATION

Unter Proliferation versteht man die Weiterverbreitung zum einen von Massenvernichtungswaffen (atomare, biologische und chemische Waffen) sowie von deren Trägersystemen (ballistische Lenkwaffen, Marschflugkörper, hypersonische Fluggeräte und Drohnen) und zum anderen von Ausrüstungsgütern, Materialien und Technologien, die neben anderen Einsatzzwecken auch zur Herstellung dieser Waffen verwendet werden können (sog. Dual-use-Güter).

FALLBEISPIEL

Ein Wissenschaftler aus einem Staat, der an für Militärtechnologie nutzbarem Know-how interessiert war, bildete sich an einer Schweizer Hochschule weiter, da es in seinem Herkunftsland keine Möglichkeit der Entwicklung dieser Hochtechnologie gab. Die Beschaffung der Technologie war staatlich gesteuert: Der Wissenschaftler erhielt den Auftrag vom Nachrichtendienst seines Heimatlands. Da es sich bei der entsprechenden Technologie um eine sogenannte Dual-use-Technologie handelte (d. h. Wissen, das sowohl für zivile als auch militärische Zwecke genutzt werden kann), war es für die Schweizer Hochschule schwierig zu erkennen, inwiefern das durch den Wissenschaftler in der Schweiz angeeignete Wissen zur Anwendung in einem militärischen Projekt im Ausland bestimmt war.

IMMATERIELLER TRANSFER VON WISSEN UND TECHNOLOGIE

Spionage und der damit verbundene illegale Transfer von geistigem Eigentum, Know-how und Technologien (immaterieller Technologietransfer, ITT) sind oft mit proliferationsrelevanten Beschaffungsbemühungen verbunden. Um die Weiterverbreitung von Massenvernichtungswaffen zu verhindern, existieren internationale Übereinkommen, Exportkontrollregime und Sanktionen. Diese schränken nicht nur den Export von kritischen Gütern (sog. Dual-use-Güter) ein, sondern auch von Wissen, Technologien und technischen Unterstützungen, wenn ein gewisses Risiko besteht, dass diese in einem Programm für die Entwicklung oder Herstellung von Massenvernichtungswaffen oder deren Trägersystemen eingesetzt werden. Denn ein Know-how-Transfer kann auch von einem zivilen Forschungsvorhaben zu einer militärischen Anwendung stattfinden. Die Einschränkungen umfassen Exporte in physischer Form (z. B. Versand eines Dokuments über den Postweg) wie auch in immaterieller, namentlich elektronischer Form (z. B. über Cloud-Dienste, E-Mail, Fax, FTP). Um Kontrollmassnahmen zu umgehen, versuchen ausländische Nachrichtendienste Wissenschaftlerinnen und Wissenschaftler zu rekrutieren, die Zugang zu sensiblen Technologien haben oder hatten und entsprechende Informationen dazu übermitteln können. Ausländische Nachrichtendienste entsenden auch ihre eigenen Nachrichtendienstoffiziere an Universitäten oder Forschungsinstitute im Ausland, um dort als Doktorandin oder Doktorand bzw. Gastwissenschaftlerin oder Gastwissenschaftler getarnt an Forschungsergebnisse und kritisches Know-how zu gelangen. Unter gewissen Umständen erhalten sie auch Zugang zu kritischen Infrastrukturen oder zu Forschungslabors von privaten Unternehmen, mit denen die Gastuniversität zusammenarbeitet. Auch Technologien, die noch in der Entwicklung stehen und nicht klassifiziert sind, können für ausländische Nachrichtendienste von Interesse sein, wenn der Anwendungsbereich der ausgereiften Technologie später als kritisch eingestuft wird.

VERSTOSS GEGEN DIE EXPORTKONTROLLE

Eine wissenschaftliche Einrichtung unternimmt nur minimale Hintergrundabklärungen zu neuen Studentinnen und Studenten sowie Wissenschaftlerinnen und Wissenschaftlern. Sie interessiert primär, ob die Person die für das Studium oder Forschungsprogramm vorausgesetzten Kompetenzen mitbringt. Stellt sich heraus, dass Angehörige einer Hochschule oder eines Forschungsinstituts in der Schweiz angeeignetes kritisches Wissen (z. B. Wissen, das in einem Massenvernichtungswaffenprogramm angewendet werden kann) einer ausländischen Behörde oder Firma zur Verfügung gestellt haben, kann die Hochschule bzw. das Forschungsinstitut dafür verantwortlich gemacht werden, da sie bzw. es eventuell gegen geltende Exportkontrollvorschriften verstossen hat.

FALLBEISPIEL

Ein europäischer Physikprofessor arbeitete im Bereich der Raumfahrttechnologie an Projekten für die Europäische Weltraumorganisation (ESA). Seine Forschung war zivil, konnte aber auch militärisch verwendet werden. Der Physiker stellte öfters ausländische Gastforscher ein, darunter eine chinesische Forscherin, die angab, von der chinesischen Akademie der Wissenschaften (ein ziviles Institut) zu sein. Doch in einem sozialen Netzwerk gab sie als Kontaktadresse eine chinesische militärische Forschungseinrichtung an und erwähnte einen von ihr geschriebenen Artikel über die Präzision von Antisatellitenwaffen. Der Professor wurde weiter misstrauisch, als sie ihm viele Fragen zur militärischen Anwendung seines Forschungsbereichs stellte. Schliesslich löste er die Zusammenarbeit mit der chinesischen Forscherin auf.

BESCHAFFUNGSBEISPIELE

Mögliche Indikatoren für einen Wissensmissbrauch oder Datenabfluss

- Anfragen für Forschungszusammenarbeiten oder Laborbesichtigungen
- Forschungsaufenthalte ausländischer Doktorandinnen und Doktoranden oder Gastwissenschaftlerinnen und Gastwissenschaftler
- Kontaktaufnahme über soziale Netzwerke (z. B. Linkedin) oder an öffentlichen Veranstaltungen, mit der Bitte um einen Austausch oder ein fachliches Gutachten zu einem bestimmten Thema
- Unaufgeforderte Einladungen von Wissenschaftlerinnen und Wissenschaftlern sowie Professorinnen und Professoren zu Konferenzen oder zu einem akademischen Austausch im Ausland, zur Einreichung von Beiträgen für wissenschaftliche Journals oder zur Überprüfung von Forschungspapieren (peer review)
- Teilnahme an wissenschaftlichen Konferenzen zu Dual-use-Technologien
- Desinteresse einer Doktorandin oder eines Doktoranden aus dem Ausland an der Forschungsarbeit, aber Frage nach breiten Zugriffsrechten auf laufende Projekte und Forschungsdaten. Auffällige Neugier, die über das normale Mass hinausgeht
- Fachwechsel nach Studienbeginn (der vorgesehene Studiengang einer Studentin oder eines Studenten aus einem Risikoland wird vor der Visumserteilung genau geprüft. Unter Umständen kann ein Visum verweigert werden, wenn die Studentin oder der Student in einem als kritisch erachteten Fachbereich studieren will.)
- Verlust/Diebstahl von Labor- oder IT-Material
- Unberechtigte Zugriffe auf IT-Systeme oder Datenbanken der Hochschule oder des Forschungsinstituts
- Gastwissenschaftlerinnen und Gastwissenschaftler, die von einer sanktionierten Universität oder Forschungsinstitution kommen
- Professorinnen und Professoren sowie Wissenschaftlerinnen und Wissenschaftler aus oder mit Beziehungen zu Risikostaaten[1]
- Ausländische Doktorandinnen und Doktoranden oder Gastwissenschaftlerinnen und Gastwissenschaftler mit einem staatlich finanzierten Stipendium, insbesondere, wenn der Person das Fachwissen oder Sprachkenntnisse fehlen (entspricht nicht den Kenntnissen, die die Person in ihrem Lebenslauf angibt)
- Besuche ausländischer wissenschaftlicher Delegationen
- Kooperationen, Austauschprogramme, Absichtserklärungen usw. mit ausländischen Hochschulen, Forschungslabors, Think Tanks oder Unternehmen, die Verbindungen zur Rüstungsindustrie haben oder über die sich in offenen Quellen Hinweise auf Proliferationstätigkeiten oder Verbindungen zu Nachrichtendiensten finden lassen
- Forschungsprojekte und -kooperationen in sensiblen Bereichen, die von einem ausländischen Unternehmen (z. B. aus dem Rüstungsbereich) oder Staat finanziert werden
- Von ausländischen Organisationen gegründete oder finanzierte Studienprogramme oder Institute an Schweizer Hochschulen

[1] Als Risikostaaten gelten heute Iran, Nordkorea, Pakistan und Syrien. Diese Staaten unterhalten nachweislich Programme zur Entwicklung von Massenvernichtungswaffen bzw. stellen solche bereits her. Da befürchtet wird, dass diese Länder Massenvernichtungswaffen zur Durchsetzung politischer Forderungen oder in einem bewaffneten Konflikt einsetzen, stellen sie eine Bedrohung für die internationale Sicherheit dar.

SCHUTZMASSNAHMEN UND BEST PRACTICES

INSTITUTIONEN

- Wissen, welche Technologien der Exportkontrolle unterliegen (Kenntnisse der geltenden Export- und Güterkontrollgesetze) und Implementierung einer internen Kontrolle der Einhaltung der Exportkontrollvorschriften (Internal Compliance Programme, ICP) sowie Bestimmung einer zentralen Ansprechperson auf Führungsebene für Fragen der Exportkontrolle

- Definieren der kritischen Fach- und Forschungsbereiche der Hochschule bzw. des Forschungsinstituts

- Prüfung des Proliferationsrisikos sensibler Technologien bei der Aufnahme ausländischer Studentinnen und Studenten oder Wissenschaftlerinnen und Wissenschaftler in einem als kritisch definierten Fachbereich

- Regelmässige Überprüfung des kritischen Labormaterialinventars

- Ernennung von Informationssicherheitsverantwortlichen und Durchführung regelmässiger Kontrollen zur Informationssicherheit

- Regelmässige Sensibilisierung von Wissenschaftlerinnen und Wissenschaftlern, Forscherinnen und Forschern, Professorinnen und Professoren und weiteren Mitarbeiterinnen und Mitarbeitern der Hochschule bzw. des Forschungsinstituts für die missbräuchliche Verwendung von Forschung (dual-use research of concern), Dual-use-Gütern und -Technologien sowie für Themen der Informations- und IT-Sicherheit

- Einschränkung der Zugriffsrechte von Mitarbeiterinnen und Mitarbeitern, Wissenschaftlerinnen und Wissenschaftlern sowie Studentinnen und Studenten auf Daten und das IT-Netzwerk der Hochschule bzw. des Forschungsinstituts

- Trennung der IT-Netzwerke (Forschungsnetzwerk ist vom restlichen IT-Netzwerk der Institution und vom Internet getrennt)

- Schaffung eines Netzwerks von Sicherheitsverantwortlichen der Hochschulen und Forschungsinstitute, in dem Erfahrungen und Informationen zu Vorfällen ausgetauscht werden können

PERSONAL [1]

- E-Mailanhänge und Links von unbekannten Personen nicht öffnen
- Vorsicht bei unaufgeforderten Kontaktaufnahmen (über E-Mail, soziale Netzwerke usw.), z. B. für Forschungszusammenarbeiten oder Austauschprogramme
- Verschlüsselung der Festplatte von Computern und Notebooks bzw. der darauf gespeicherten Daten
- Verwendung einer gesicherten Verbindung (Virtual Private Network, VPN), um von aussen auf das Hochschul- oder Institutsnetzwerk zuzugreifen
- Internetverbindungen über frei zugängliche – auch passwortgeschützte – fremde WLAN (z. B. in Hotels, Cafés oder Flughäfen) nur über eine VPN-Verbindung nutzen oder – falls VPN im Gastland blockiert wird – via 3G/4G/5G-Datenübertragung im Roaming
- Notebooks und anderes elektronisches Material nie unbeaufsichtigt liegen lassen (z. B. während der Kaffeepause auf einer Konferenz oder auch nur für den Toilettenbesuch)
- Keine geliehenen, geschenkten oder fremden externen Peripheriegeräte (USB-Stick, externe Festplatte, Mobiltelefon, digitaler Fotoapparat usw.) verwenden oder solche an das eigene Notebook oder Netzwerk anschliessen
- Verdächtige Vorkommnisse den Sicherheitsverantwortlichen der Hochschule bzw. des Forschungsinstituts melden

[1] Wissenschaftlerinnen und Wissenschaftler, Professorinnen und Professoren sowie weitere Mitarbeiterinnen und Mitarbeiter

STUDIERENDE

- Darauf achten, welche persönlichen und beruflichen Informationen man in den sozialen Netzwerken preisgibt (so viel wie nötig, so wenig wie möglich)
- Misstrauen gegenüber verlockenden finanziellen Angeboten
- Vorsicht bei kostenlosen Unterstützungsleistungen im Ausland, insbesondere, wenn es sich um amtliche Angelegenheiten wie die Erteilung eines Visums oder die Verlängerung einer Aufenthaltsbewilligung handelt
- Aufmerksamkeit walten lassen, insbesondere, wenn Personen zu neugierig oder aufdringlich sind. Keine genauen Informationen weitergeben oder Zusagen machen und Beziehungen zu Personen, die einem verdächtig vorkommen, frühzeitig abbrechen
- Überprüfen, ob die angegebene Institution oder der Arbeitsbereich einer Person wirklich existiert und ob ihr Name auf der Webseite der angegebenen Institution aufgeführt ist
- Verdächtige Aktivitäten der Schweizer Vertretung im Ausland (Botschaft, Konsulat), der Heimuniversität oder dem NDB melden

Weitere Schutzmassnahmen sowie Sicherheitshinweise für Geschäftsreisen im Ausland sind der Broschüre Prophylax zu entnehmen.

www.vbs.admin.ch – DE – Startseite – Dokumente und Publikationen – Suche – Prophylax – Publikationen

WEITERFÜHRENDE INFORMATIONEN

SPIONAGE UND PROLIFERATION

Sensibilisierungsprogramm Prophylax

www.ndb.admin.ch – DE – Sicherheit – Nachrichtenbeschaffung – Wirtschaftsspionage

Das Sensibilisierungsprogramm Prophylax ist auf den Schutz des Schweizer Werk- und Forschungsplatzes vor ungewollten Datenabflüssen und illegalen Beschaffungsbemühungen ausgerichtet. Mit Prophylax sensibilisiert der NDB Unternehmen, Hochschulen und Forschungsinstitute für Bedrohungen, die von Spionage und Proliferation (Verbreitung von Massenvernichtungswaffen und deren Trägermittel sowie von Dual-use-Gütern) ausgehen.

Kurzfilm *„Im Visier“*

www.ndb.admin.ch – DE – Sicherheit – Nachrichtenbeschaffung – Wirtschaftsspionage

Der Kurzfilm „Im Visier“ ist Teil des Sensibilisierungsprogramms Prophylax des NDB. Der Film hat zum Ziel, den Schweizer Werk- und Forschungsplatz für die Bedrohungen durch Spionage zu sensibilisieren.

Erläuterungen zu den im Film gezeigten Spionagemethoden und entsprechende Schutzmassnahmen: *www.vbs.admin.ch – Sicherheit – Nachrichtenbeschaffung – Wirtschaftsspionage – Dokumente*

Weitere Merk- und Faktenblätter

www.ndb.admin.ch – DE – Sicherheit – Nachrichtenbeschaffung – Wirtschaftsspionage – Dokumente

- Prophylax
- Was macht der NDB gegen Spionage?
- Merkblatt Wirtschaftsspionage
- Studie „Wirtschaftsspionage in der Schweiz“
- Management Summary „Wirtschaftsspionage in der Schweiz“
- Merkblatt Informationssicherheit für KMU
- Erläuterungen zum Kurzfilm „Im Visier“

CYBERSICHERHEIT

Nationales Zentrum für Cybersicherheit (National Cyber Security Centre — NCSC)

www.ncsc.admin.ch

Das Nationale Zentrum für Cybersicherheit (National Cyber Security Centre — NCSC) ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen.

Meldung von Phishing-Mails

www.antiphishing.ch

antiphishing.ch wird vom NCSC betrieben, um der Bevölkerung eine einfache Möglichkeit zu geben, Phishing-Versuche zu melden.

Minimalstandard zur Verbesserung der IKT-Resilienz

www.bwl.admin.ch – DE– Themen – IKT – IKT-Minimalstandard

Die zunehmende Digitalisierung aller Lebensbereiche eröffnet für die Schweiz grosses ökonomisches und gesellschaftliches Potenzial. Gleichzeitig aber entstehen durch die Digitalisierung neue Risiken, denen schnell und konsequent begegnet werden muss. Das Dokument Minimalstandard zur Verbesserung der IKT-Resilienz vom Bundesamt für wirtschaftliche Landesversorgung (BWL) dient als Hilfestellung und bietet konkrete Handlungsanweisungen zur Verbesserung der eigenen IKT-Resilienz.

WIRTSCHAFT

Exportkontrollvorschriften

www.seco.admin.ch – DE – Aussenwirtschaft & Wirtschaftliche Zusammenarbeit – Wirtschaftsbeziehungen – Exportkontrollen und Sanktionen – Elic – Internal Compliance Programme-ICP

Das Merkblatt zur firmeninternen Kontrolle der Einhaltung der Exportkontrollvorschriften (Internal Compliance Programme, ICP) zeigt auf, weshalb exportorientierte Unternehmen eine firmeninterne Kontrolle implementieren müssen, welche schweizerischen Rechtsgrundlagen bestehen und welche Kriterien ein effektives ICP erfüllen sollte. Das Merkblatt soll Sie dabei unterstützen, ein ICP aufzubauen bzw. ein bestehendes zu optimieren.

Anträge im Bereich Dual-use-Güter

www.elic.admin.ch

Ab dem 1. Oktober 2014 müssen alle Anträge (Gesuche, Voranfragen, etc.) im Bereich Dual-Use Güter, Kriegsmaterial sowie besondere militärische Güter mit Elic elektronisch erfasst, bearbeitet und verwaltet werden. Papierdossiers können nicht mehr berücksichtigt werden.

Sanktionsdaten Suche

www.seco.admin.ch –DE –Aussenwirtschaft & Wirtschaftliche Zusammenarbeit – Wirtschaftsbeziehungen – Exportkontrollen und Sanktionen – Sanktionen/Embargos – Sanktionsmassnahmen – Suche nach Sanktionsadressaten

Der Bund kann Zwangsmassnahmen erlassen, um Sanktionen durchzusetzen, die von der Organisation der Vereinten Nationen, der Organisation für Sicherheit und Zusammenarbeit in Europa oder von den wichtigsten Handelspartnern der Schweiz beschlossen worden sind und die der Einhaltung des Völkerrechts, namentlich der Respektierung der Menschenrechte, dienen (Art. 1, Abs. 1 Embargogesetz).

In der Sanktionsdatenbank SESAM kann nach sanktionierten Personen, Unternehmen und Organisationen gesucht werden.

WEITERE

Staatssekretariat für Bildung, Forschung und Innovation (SBFI)
www.sbfi.admin.ch

Das Staatssekretariat für Bildung, Forschung und Innovation SBFI im Eidgenössischen Departement für Wirtschaft, Bildung und Forschung WBF ist das Kompetenzzentrum des Bundes für national und international ausgerichtete Fragen der Bildungs-, Forschungs- und Innovationspolitik.

Auslandaufenthalt
www.eda.admin.ch – DE – Reisehinweise & Vertretungen – Länderunabhängige Reiseinformationen – Reisehinweise kurz erklärt

Die Reisehinweise des Eidgenössischen Departements für auswärtige Angelegenheiten (EDA) bieten Informationen zur Sicherheitslage im Ausland. Sie sind eine Ergänzung zu anderen Informationsquellen. Über Vorbereitung und Durchführung einer Reise entscheidet der/die Reisende in Eigenverantwortung.

Missbrauchspotenzial und Biosecurity in der biologischen Forschung
Akademie der Naturwissenschaften Schweiz (SCNAT)
www.scnat.ch

Missbrauchspotenzial und Biosecurity in der biologischen Forschung (swiss academies reports Vol. 12 Nr. 3, 2017) ist eine Diskussionsgrundlage zur Frage des Umgangs mit dem Dual-use-Dilemma in der wissenschaftlichen Praxis.

VORGEHEN BEI VERDACHT / KONTAKT

Bei Verdacht auf Spionage oder Proliferationsaktivitäten (z. B. im Falle von dubiosen Anfragen für Zusammenarbeit oder suspektem Verhalten von Doktorandinnen und Doktoranden, Studentinnen und Studenten, Professorinnen und Professoren oder Wissenschaftlerinnen und Wissenschaftler) zögern Sie nicht, Ihre Sicherheitsverantwortlichen, Ihre Kantonspolizei oder den NDB zu kontaktieren. Sichern Sie mögliche Beweise und löschen Sie verdächtige E-Mails nicht. Der NDB sammelt und wertet die Hinweise aus. Er garantiert eine diskrete Behandlung des Falls.

Nachrichtendienst des Bundes NDB
Papiermühlestrasse 20
CH-3003 Bern
www.ndb.admin.ch
prophylax@ndb.admin.ch

Der NDB hilft in Zusammenarbeit mit den Kantonalen Nachrichtendiensten, die schweizerischen und liechtensteinischen Universitäten, Hochschulen, Forschungsinstitute und Unternehmen über Proliferation und Spionage aufzuklären, zu sensibilisieren und zu unterstützen.

Bildrechte

Titelseite, FHNW Campus Muttenz, © Gataric Fotografie

Seite 2, UNIGE, © Righetti Nicolas

Seite 4, Lichthof UZH, © Meissner Ursula

Seite 6, HSLU

Seite 10, EPFL, © Christinat Olivier

Seite 16, UZH, © Walter Stefan

Seite 22, EPFL, © Christinat Olivier

Seite 26, UZH, © Bibliothek Rechtswissenschaftliches Institut, © Walter Stefan

TECHNOPOL
Sensibilisierungsprogramm Prophylax
Nachrichtendienst des Bundes NDB
Papiermühlestrasse 20
CH-3003 Bern

www.ndb.admin.ch
prophylax@ndb.admin.ch

Redaktionsschluss
Dezember 2022