TECHNOPOL
Un modulo del programma di sensibilizzazione Prophylax

IL MONDO ACADEMICO NEL MIRINO

Spionaggio e proliferazione in ambito accademico

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Servizio delle attività informative della Confederazione SIC

TECHNOPOL
Un modulo del programma di sensibilizzazione Prophylax

IL MONDO ACADEMICO NEL MIRINO

Spionaggio e proliferazione in ambito accademico

INDICE

INTRODUZIONE

Sin dal 2004 il Servizio delle attività informative della Confederazione (SIC) conduce il programma di sensibilizzazione Prophylax, inteso ad attirare l'attenzione di imprese, organizzazioni dell'economia e istituti di ricerca sulle minacce provenienti dalla proliferazione e dallo spionaggio . Prophylax adempie il mandato assegnato al SIC dal legislatore di gestire programmi di informazione e sensibilizzazione in merito alle minacce per la sicurezza interna ed esterna (Art. 6 cpv. 6 della legge federale). In quanto elemento integrante di Prophylax, Technopol ha lo scopo di sensibilizzare università, scuole universitarie e istituti di ricerca in Svizzera e nel Liechtenstein.

Technopol si rivolge ai membri di università, scuole universitarie e istituti di ricerca e illustra le ragioni che li rendono un obiettivo interessante agli occhi dei servizi di intelligence stranieri. Parallelamente attira l'attenzione sulle minacce derivanti dallo spionaggio e sul potenziale di abusi insito nelle conoscenze e nel know how di cui dispongono la dottrina, la ricerca e le amministrazioni delle suddette istituzioni. Oltre alle attività di sensibilizzazione, Technopol propone ai suoi destinatari misure concrete di sicurezza per meglio proteggersi contro il trasferimento di conoscenze e tecnologie e contro la fuga indesiderata di informazioni e dati.

Per atenei e istituti di ricerca lo scambio a livello internazionale di informazioni scientifiche e risultati della ricerca è un fattore di vitale importanza. L'Unione europea (UE) incoraggia fortemente questo scambio e nello Spazio europeo della ricerca (SER), nella governance in cui la Svizzera può essere coinvolta come principale Paese terzo secondo un approccio caso per caso, promuove la libertà di movimento e il libero accesso ai risultati della ricerca e della tecnologia. I programmi quadro dell'UE pluriennali di ricerca e innovazione rappresentano il più importante strumento per l'attuazione del SER. Gli atenei europei oppure i partner di ricerca che vogliono usufruire del SER e partecipare ai programmi quadro sono tenuti a contribuire attivamente al trasferimento di conoscenze condividendo i risultati delle loro attività di ricerca.

Tuttavia, sebbene i risultati della ricerca siano pubblicamente accessibili, università e istituti di ricerca sono esposti alla minaccia dello spionaggio e delle attività di proliferazione, come illustrano le seguenti considerazioni.

ATENEI E ISTITUTI DI RICERCA NEL MIRINO

RAFFORZARE LA CONSAPEVOLEZZA

La collaborazione internazionale e la mobilità di studenti e ricercatori nonché lo scambio di conoscenze rivestono un'importanza cruciale per il settore della ricerca e non devono essere impediti. È però importante che atenei e istituti di ricerca siano consapevoli della minaccia che deriva dallo spionaggio e dalla proliferazione e che gestiscano con prudenza il know how critico. Questa gestione prudente comprende la sensibilizzazione di tutti i membri dell'ateneo o istituto di ricerca (ricercatori, professori, collaboratori, ecc.) nonché conoscenze sulle tecnologie sottoposte a controllo all'esportazione e sull'obbligo di richiedere un'autorizzazione alla Segreteria di Stato dell'economia (SECO) per esportare all'estero tali tecnologie.

La Svizzera e gli atenei e istituti di ricerca presenti sul suo territorio hanno il dovere di impedire che il sapere prodotto o acquisito da studenti e ricercatori ivi operanti venga sfruttato abusivamente per scopi illeciti. Il fatto di ignorare le minacce che ne derivano potrebbe avere gravi conseguenze per un'istituzione che dovesse trovarsi effettivamente toccata da attività di spionaggio o proliferazione. In particolare, essa rischia di perdere mandati e fondi per la ricerca, di essere esclusa dagli enti di ricerca internazionali, di subire un danno reputazionale e di essere declassata nel ranking internazionale. Inoltre, la fuga all'estero di risultati scientifici confidenziali può compromettere a lungo andare la competitività internazionale della Svizzera nel campo della ricerca. Le persone che svolgono attività di spionaggio per incarico di un servizio di intelligence straniero a discapito di interessi svizzeri mettono in gioco il proprio avvenire, rischiando l'incarcerazione e mettendo a repentaglio la propria carriera.

CULTURA APERTA

L'elevato livello tecnologico e delle conoscenze e l'apertura e la cultura dell'accoglienza che caratterizzano le università, le scuole universitarie e gli istituti di ricerca svizzeri sono apprezzati nel mondo intero. In Svizzera i ricercatori stranieri trovano ad esempio laboratori all'avanguardia, dove hanno la possibilità di realizzare i loro esperimenti scientifici.

Ma la facilità d'accesso agli edifici, la politica di libero scambio delle informazioni scientifiche, la collaborazione con imprese del settore tecnologico e la composizione internazionale del corpo insegnante e degli studenti fanno delle università svizzere anche un obiettivo allettante per le attività di spionaggio di servizi di intelligence stranieri. Questi tentano di ottenere pareri di esperti o dati scientifici riguardanti tecnologie sensibili (p. es. robotica, nuovi materiali, nanotecnologie) per colmare le lacune nelle conoscenze a disposizione dei loro Paesi. Grazie a queste attività di spionaggio i loro Stati e le loro industrie risparmiano i costi di ricerche scientifiche condotte in proprio, poiché è generalmente più vantaggioso ottenere dati su determinate tecnologie o prodotti che investire risorse finanziarie e umane in proprie ricerche e attività di sviluppo.

ESEMPIO

Nel 2014 venne arrestato un fisico straniero che svolgeva attività di ricerca presso di un'università neerlandese in quanto sospettato di avere rivelato contenuti scientifici confidenziali al servizio di intelligence esterno russo SVR. Il fisico aveva attirato i sospetti dell'Ufficio federale tedesco della protezione della Costituzione (Bundesamt für Verfassungsschutz, BfV), che teneva sotto osservazione un diplomatico russo del Consolato generale della Federazione russa a Bonn identificato come agente dell'SVR. Il diplomatico fittizio incontrava il fisico una volta al mese ad Aquisgrana (Germania), dove era solito consegnargli denaro. Per partecipare a questi incontri il fisico percorreva ogni volta in automobile il tragitto tra i Paesi Bassi e la città tedesca. In seguito al suo arresto l'università condusse un'inchiesta interna e gli revocò l'accesso all'ateneo. Il Ministero della giustizia neerlandese lo definì «un pericolo per la sicurezza interna del Paese», gli revocò il visto Schengen ed emise un divieto d'entrata.

COLLABORAZIONE CON TERZI

Numerosi istituti di ricerca cooperano con imprese private e autorità statali, che finanziano anche alcuni progetti di ricerca. Questi progetti di cooperazione consentono ai ricercatori che vi partecipano di accedere a conoscenze specialistiche e informazioni sensibili. Per rendere proficui i loro investimenti nella ricerca, imprese e autorità devono poter essere le prime a sfruttare concretamente i risultati a livello commerciale. Il furto di dati e risultati delle attività di ricerca commesso mediante attività di spionaggio è paragonabile al furto di risorse finanziarie e compromette la futura cooperazione con l'istituto di ricerca interessato. Inoltre, il fatto che qualcuno pubblichi anticipatamente o applichi concretamente prima di loro i risultati di un progetto di ricerca priva i ricercatori del debito riconoscimento per le loro scoperte rivoluzionarie.

RICERCA

Nell'ottica di un possibile trasferimento illegale di conoscenze, il SIC considera particolarmente critiche le attività di ricerca applicata in settori specialistici tecnico-scientifici quali ad esempio l'ingegneria meccanica, le tecnologie aeronautiche e aerospaziali, l'elettrotecnica, le scienze dei materiali, la chimica, la biologia o l'informatica. Ma anche la ricerca di base può costituire un ambito delicato se studenti o ricercatori apprendono metodi e tecniche che possono divulgare o utilizzare in seguito per altri scopi (c.d. ricerca a duplice uso, dual-use research of concern, DURC). Inoltre, un'autorità statale straniera potrebbe interessarsi anche di un settore non tecnico che riguarda ad esempio temi politici inerenti allo Stato a cui essa appartiene.

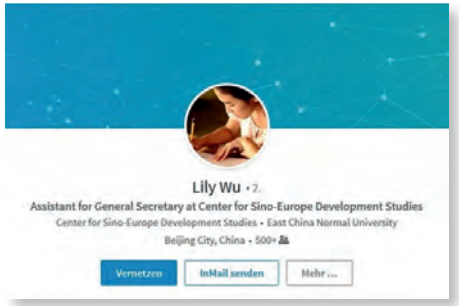
ATTIVITÀ DI SERVIZI DI INTELLIGENCE STRANIERI

SPIONAGGIO

Con il termine «spionaggio» si intende l'acquisizione di informazioni e dati riguardanti la politica, l'economia, il settore militare, la scienza e la tecnologia a discapito della Svizzera, della sua popolazione o delle sue autorità, imprese o istituzioni, per trasmetterli ad attori stranieri (Stati, gruppi, imprese, persone, ecc.).

ESEMPIO

Un giovane ricercatore presso un'università europea ricevette, tramite la rete professionale Linkedin, una richiesta di contatto da parte di un collaboratore di un think tank asiatico, che si diceva interessato al suo lavoro e a uno scambio scientifico. Il think tank invitò il ricercatore all'estero assumendosi interamente i costi di viaggio e di soggiorno. Durante il suo soggiorno il ricercatore incontrò collaboratori del think tank, che in realtà erano agenti del servizio di intelligence nazionale. In tale contesto gli agenti del servizio di intelligence tentarono di reclutare il ricercatore come fonte di informazioni al fine di potere accedere a informazioni sensibili del suo campo di attività.



Un profilo fittizio su Linkedin, utilizzato da un servizio di intelligence cinese per entrare in contatto con persone potenzialmente interessanti

TALENT SPOTTING

Per un agente dei servizi di intelligence la partecipazione a eventi pubblici accademici (conferenze, seminari, ecc.) è un'occasione perfetta per entrare in contatto con i convenuti senza creare sospetti. Può interessarsi agli esperti e, con tecniche di conversazione efficaci e raffinate, tentare di carpire loro informazioni riservate (p. es. su progetti di ricerca in corso). Ma può anche tenere d'occhio le persone con determinate opinioni politiche o ideologiche e cercare di individuare giovani accademici che potrebbero avere le potenzialità per occupare in futuro un posto sensibile in seno a un'autorità governativa o esercitare una funzione sensibile in un'impresa nel settore dell'alta tecnologia. I rapporti amichevoli con queste persone vengono coltivati a lungo termine, allo scopo di ottenere informazioni degne di protezione in caso di assunzione.

ESEMPIO

Una studentessa di un Paese europeo si recò per un soggiorno di studio di un anno in un Paese asiatico, dove un professore le fece conoscere una collaboratrice del servizio di intelligence nazionale, presentatasi sotto le false spoglie di studentessa del posto. In tale contesto fu chiesto alla studentessa europea di redigere rapporti a pagamento per un istituto di ricerca. In realtà si trattava di un istituto di copertura, di cui il servizio di intelligence nazionale si serviva per avvicinare studenti europei da reclutare in vista di una collaborazione a lungo termine.

OSSERVAZIONE DI PROPRI CONNAZIONALI

I servizi di intelligence di alcuni Paesi stranieri spiano i propri connazionali che vivono all'estero, per esempio dissidenti e membri della diaspora. Svolgono queste attività anche negli atenei e negli istituti di ricerca, dove filmano e registrano i presenti, ad esempio in occasione di eventi pubblici organizzati da gruppi di dissidenti. Inoltre, gli Stati sfruttano abusivamente anche le associazioni studentesche organizzate a livello nazionale e insediate presso le università. Per controllare gli studenti le ambasciate li invitano spesso a eventi da esse organizzati. In Svizzera queste attività di sorveglianza sono vietate e contravvengono all'articolo 272 del Codice penale svizzero (spionaggio politico).

In particolar modo gli Stati governati da regimi autoritari chiedono lealtà ai loro cittadini e li incitano a rendersi utili alla patria mettendo le conoscenze acquisite all'estero a disposizione del loro Paese di origine, ad esempio partecipando a progetti di ricerca per lo sviluppo di sistemi d'arma. Taluni Stati premiano i loro migliori studenti offrendo loro l'opportunità di trascorrere qualche semestre all'estero per proseguire gli studi o conseguire un dottorato. Spesso il soggiorno all'estero di queste persone è finanziato dallo Stato, che in cambio si aspetta una controprestazione. In genere, al loro rientro questi studenti sono obbligati a lavorare per un certo numero di anni in patria, in un'impresa statale o privata o per un'autorità.

ESEMPIO

Un dottorando straniero immatricolato in un'università svizzera si presentò in polizia dicendo di sentirsi sorvegliato da alcuni suoi connazionali, membri dell'associazione degli studenti del suo Paese di origine. Dalle indagini condotte dalla polizia emerse che queste persone erano state incaricate dalla loro ambasciata di tenere sotto osservazione gli altri studenti loro connazionali. L'incarico consisteva nel fare rapporto all'ambasciata qualora uno studente non si fosse comportato conformemente alle aspettative e agli orientamenti politici del Paese di origine.

SOGGIORNI DI STUDIO ALL'ESTERO

All'estero il rischio di cadere vittima di atti di spionaggio aumenta. Studenti e ricercatori che trascorrono uno o più semestri in un'università o in un istituto di ricerca all'estero sono esposti al rischio di essere contattati dai servizi di intelligence locali, intenzionati ad appropriarsi di conoscenze, tecnologie, dati sensibili e informazioni non accessibili al pubblico. Questi servizi potrebbero ad esempio tentare di imbastire una relazione duratura con uno studente e di convincerlo a cercare un posto in patria presso un'autorità governativa di importanza strategica per potere così accedere a informazioni classificate. La consegna di simili informazioni a un servizio di intelligence straniero, che avviene perlopiù dietro pagamento o mediante altri compensi, costituisce un reato di spionaggio a profitto di uno Stato straniero.

CIBERATTACCHI

Dato l'elevato numero di utenti, la spesso scarsa attenzione per la protezione delle informazioni, le poche restrizioni all'accesso e i numerosi punti di accesso a Internet, l'infrastruttura di rete di un ateneo o di un istituto di ricerca è particolarmente esposta al rischio di ciberattacchi. Specialmente le banche dati elettroniche di università e istituti di ricerca sono obiettivi interessanti per lo spionaggio, poiché contengono spesso informazioni importanti e sensibili sulle attività di ricerca scientifica. Sempre più spesso i ciberattacchi alle reti informatiche delle università vengono sferrati per ottenere, per esempio con mail di phishing, i dati di accesso degli studenti o dei collaboratori (c.d. credential phishing). Ma un aggressore può anche abusare dell'infrastruttura di rete di un'università come punto di partenza per attaccare altre organizzazioni o imprese.

ESEMPI DI SPIONAGGIO

Approccio di studenti di scambio

- Nell'allacciare una relazione con uno studente partecipante a un programma di scambio, un agente di un servizio di intelligence straniero dissimula la propria identità presentandosi ad esempio come studente o come membro di un think tank, di un istituto di ricerca, di una scuola di lingue o di una società di consulenza. Contatta lo studente con una scusa insospettabile, ad esempio offrendo un posto di lavoro o di stage interessante, un lavoro scritto retribuito o uno scambio linguistico. Lo studente viene contattato di persona o per via elettronica. In modo particolare le reti sociali online come Linkedin o Facebook consentono ai servizi di intelligence stranieri di raccogliere informazioni su una persona che hanno preso di mira e di instaurare con lei un primo contatto in vista di un suo possibile reclutamento.

- Un servizio di intelligence straniero chiede a uno studente di svolgere determinati lavori o procurare determinate informazioni dietro pagamento. Non deve necessariamente trattarsi di informazioni sensibili. Scopo di tale agire è verificare se l'interessato è idoneo a fungere da potenziale informatore.

- Il servizio di intelligence di un Paese straniero incarica un professore di reclutare studenti stranieri.

- Il Paese ospitante accusa uno studente di presunti reati o contravvenzioni per esercitare in tal modo una pressione su di lui e costringerlo a collaborare con i servizi di intelligence.

- Con il pretesto di un sondaggio generale (p. es. con un questionario) sugli studenti stranieri che soggiornano sul territorio del Paese ospitante e sulle loro impressioni, il servizio di intelligence nazionale tenta di tracciare il profilo di uno studente e di ottenere informazioni sui suoi interessi, sulla sua cerchia di conoscenze o sulle sue eventuali debolezze.

ABUSO DELLE CONOSCENZE E TECHNOLOGIE

PROLIFERAZIONE

Con il termine «proliferazione» si intende la diffusione, da un lato, di armi di distruzione di massa (armi nucleari, biologiche e chimiche) e dei loro vettori (missili balistici, missili da crociera, velivoli ipersonici e droni) e, dall'altro, di beni di equipaggiamento, materiali e tecnologie utilizzabili, oltre che per altri scopi, anche per la fabbricazione di queste armi (c.d. beni a duplice impiego).

ESEMPIO

Uno scienziato proveniente da uno Stato interessato a conoscenze utili per la tecnologia militare si stava specializzando in un'università svizzera, poiché nel suo Paese di origine non esisteva la possibilità di sviluppare l'alta tecnologia in questione. L'acquisizione della tecnologia era pilotata dallo Stato: lo scienziato agiva su incarico dei servizi di intelligence del suo Paese. Dato che si trattava di una tecnologia a duplice uso (ossia di conoscenze utilizzabili tanto a fini civili quanto a fini militari), per l'università svizzera in questione fu difficile capire fino a che punto le conoscenze acquisite in Svizzera dallo scienziato straniero fossero destinate a essere applicate nell'ambito di un progetto militare all'estero.

TRASFERIMENTO IMMATERIALE DI COMPETENZE E TECNOLOGIA

Le attività di spionaggio, e quindi il trasferimento illegale di diritti di proprietà intellettuale, competenze e tecnologie (trasferimento intangibile di tecnologia, Intangible Transfer of Technology ITT), sono spesso legate a tentativi di acquisizione rilevanti per la proliferazione. Per impedire il proliferare di armi di distruzione di massa esistono accordi internazionali, regimi di controllo delle esportazioni e sanzioni che limitano l'esportazione non solo di beni critici (c.d. beni a duplice impiego) ma anche di conoscenze, tecnologie e assistenza tecnica qualora sussista un certo rischio di un loro impiego in un programma di sviluppo o produzione di armi di distruzione di massa o dei loro vettori. Infatti, è possibile che le competenze trasmesse nell'ambito di un progetto di ricerca civile siano poi utilizzate per un'applicazione militare. Le restrizioni riguardano tanto le esportazioni in forma fisica (p. es. la spedizione di un documento per posta) quanto quelle in forma immateriale, e segnatamente in forma elettronica (p. es. mediante servizi cloud, e-mail, fax, protocollo FTP). Per aggirare le misure di controllo i servizi di intelligence stranieri cercano di reclutare scienziati che hanno avuto o hanno accesso a tecnologie sensibili e sono in grado di trasmettere utili informazioni al riguardo. I servizi di intelligence stranieri inviano anche i loro agenti in università o istituti di ricerca all'estero affinché, sotto copertura di dottorando o scienziato ospite, riescano a impadronirsi di risultati di ricerche e conoscenze critiche. In talune circostanze riescono anche a ottenere l'autorizzazione di accesso a infrastrutture critiche o laboratori di ricerca di imprese private che collaborano con l'università ospitante. Ai servizi di intelligence stranieri possono interessare anche tecnologie ancora in fase di sviluppo e non classificate se il campo di applicazione della tecnologia, una volta giunta allo stadio di maturazione, può essere qualificato come campo critico.

VIOLAZIONE DEL REGIME DI CONTROLLO DELLE ESPORTAZIONI

Un'istituzione scientifica procede soltanto ad accertamenti contestuali minimi sui nuovi studenti e ricercatori. L'aspetto più importante è sapere se l'interessato possiede le competenze necessarie per gli studi o il programma di ricerca in questione. Se emerge che membri di un ateneo o di un istituto di ricerca hanno messo a disposizione di un'autorità o impresa straniera conoscenze critiche acquisite in Svizzera (p. es. conoscenze utilizzabili nell'ambito di un programma di produzione di armi di distruzione di massa), l'ateneo o istituto di ricerca in questione può essere chiamato a risponderne, poiché può avere violato la normativa vigente in materia di controllo delle esportazioni.

ESEMPIO

Un professore di fisica di un Paese europeo lavorava ad una serie di progetti nel campo della tecnologia aerospaziale per conto dell'Agenzia spaziale europea (ESA). Le sue ricerche si inserivano nel settore civile, ma potevano avere un'utilità anche nel settore militare. Il fisico assumeva spesso ricercatori ospiti stranieri, tra cui una ricercatrice cinese, che aveva dichiarato di appartenere all'Accademia cinese delle scienze (un istituto civile). In una rete sociale, tuttavia, aveva indicato come indirizzo di contatto un istituto di ricerca militare della Repubblica popolare cinese e citato un articolo di suo pugno sul grado di precisione delle armi antisatellite. Il professore si insospettì ulteriormente allorquando constatò che la ricercatrice cinese gli poneva molte domande sulle possibili applicazioni militari del suo campo di ricerca. Alla fine il professore interruppe il loro rapporto di collaborazione.

ESEMPI D'ACQUISTO

Indicatori possibili di abuso di conoscenze o fuga di dati

- Richieste di collaborazione a programmi di ricerca o visite a laboratori
- Soggiorni di ricerca per dottorandi o ricercatori ospiti stranieri
- Presa di contatto attraverso le reti sociali (p. es. Linkedin) o nell'ambito di eventi pubblici, con richiesta di discussione o di perizia tecnica in merito a un tema preciso
- Inviti non richiesti a scienziati e professori per conferenze o una discussione accademica all'estero, per la presentazione di contributi destinati a riviste scientifiche o per la verifica di documentazione di ricerca (peer review)
- Partecipazione a congressi scientifici sulle tecnologie a duplice uso
- Dottorando proveniente dall'estero che si disinteressa del lavoro di ricerca ma chiede ampi diritti di accesso a progetti in corso e risultati delle ricerche. Curiosità evidente, oltre il limite del normale
- Cambiamento di materia dopo l'inizio degli studi (per gli studenti provenienti da states of concern, il corso di studi previsto viene accuratamente controllato prima del rilascio del visto; in determinate circostanze il visto può essere negato se l'interessato vuole assolvere i suoi studi in un settore specialistico considerato critico)
- Perdita o furto di materiale di laboratorio o informatico
- Accessi non autorizzati a sistemi informatici o banche dati dell'università o istituto di ricerca
- Ricercatori ospiti provenienti da un ateneo o un istituto di ricerca sanzionato
- Professori e ricercatori originari di states of concern (Stati fonte d'inquietudine) o che intrattengono relazioni con questi Stati [1]
- Dottorandi o ricercatori ospiti beneficiari di una borsa finanziata da un ente pubblico, in particolare se si tratta di persone che non possiedono conoscenze specialistiche o linguistiche (le cui conoscenze non corrispondono a quanto indicato nel curriculum vitae)
- Visite di delegazioni scientifiche straniere
- Cooperazioni, programmi di scambio, dichiarazioni di intenti, ecc., con università, laboratori di ricerca, think tank o imprese che possiedono legami con l'industria degli armamenti o che, secondo fonti accessibili al pubblico, potrebbero essere coinvolti in attività di proliferazione o collegati a servizi di intelligence
- Progetti e cooperazioni per la ricerca in ambiti sensibili, finanziati da un'impresa straniera (p. es. del settore degli armamenti) o da uno Stato straniero
- Corsi di studio o istituti creati o finanziati da organizzazioni straniere presso università svizzere

[1] Per states of concern (Stati fonte d'inquietudine) si intendono attualmente l'Iran, la Corea del Nord, il Pakistan e la Siria. È comprovato che detti Stati conducono programmi per lo sviluppo di armi di distruzione di massa o producono già siffatte armi. Tali Paesi rappresentano una minaccia per la sicurezza internazionale, poiché si teme che possano ricorrere all'uso di armi di distruzione di massa per imporre le loro rivendicazioni politiche oppure nell'ambito di un conflitto armato.

Abuso delle conoscenze e technologie

MISURE DI PROTEZIONE E BUONE PRATICHE

ISTITUZIONI

- Sapere quali tecnologie sono sottoposte al controllo all'esportazione (conoscenza delle vigenti leggi in materia di esportazione e controllo dei beni), introdurre un controllo interno del rispetto delle norme in materia di controllo delle esportazioni (Internal Compliance Programme, ICP) e designare un interlocutore centrale a livello di direzione per le questioni che riguardano tale controllo
- Definire i settori specialistici e i campi di ricerca critici dell'ateneo o istituto
- Esaminare il rischio di proliferazione nell'ambito di tecnologie sensibili al momento dell'ammissione di studenti o ricercatori stranieri in un settore specialistico considerato critico
- Verificare regolarmente l'inventario del materiale critico di laboratorio
- Designare i responsabili della sicurezza delle informazioni ed effettuare controlli regolari della sicurezza delle informazioni
- Sensibilizzare regolarmente scienziati, ricercatori, professori e altri collaboratori dell'ateneo o istituto di ricerca sull'impiego abusivo della ricerca (dual-use research of concern), su beni e tecnologie a duplice impiego e sui temi riguardanti la sicurezza delle informazioni e la sicurezza informatica
- Limitare i diritti di accesso di collaboratori, ricercatori e studenti ai dati e alla rete informatica dell'ateneo o istituto di ricerca
- Separare le reti informatiche (la rete della ricerca deve essere separata dal resto della rete informatica dell'istituzione e da Internet)
- Creare una rete di responsabili della sicurezza degli atenei e degli istituti di ricerca tramite la quale potere scambiare esperienze e informazioni sugli incidenti

PERSONALE [1]

- Non aprire gli allegati e i link contenuti nelle mail di persone sconosciute
- Usare prudenza di fronte a tentativi di contatto non richiesto (tramite posta elettronica, reti sociali, ecc.), ad esempio per collaborazioni nel campo della ricerca o programmi di scambio
- Cifrare il disco duro di computer e notebook ovvero i dati che essi contengono
- Utilizzare una connessione sicura (Virtual Private Network, VPN) per accedere dall'esterno alla rete dell'ateneo o istituto di ricerca
- Utilizzare unicamente una connessione VPN per collegarsi a Internet tramite le reti pubbliche WLAN di terzi anche se protette da password (p. es. in alberghi, bar o aeroporti) oppure, se nel Paese ospitante il VPN è bloccato, accedere a Internet mediante trasferimento di dati 3G/4G/5G in roaming
- Non lasciare mai incustoditi notebook e altri dispositivi elettronici (p. es. durante la pausa caffè in occasione di una conferenza o anche soltanto per andare in bagno)
- Non utilizzare né collegare al proprio notebook o alla propria rete apparecchi periferici (penne USB, dischi duri esterni, telefoni cellulari, macchine fotografiche digitali, ecc.) ricevuti in prestito o in regalo o appartenenti ad altri
- Segnalare gli avvenimenti sospetti ai responsabili della sicurezza dell'ateneo o istituto di ricerca

[1] Scienziati, professori et altri collaboratori

STUDENTI

- Prestare attenzione nel scegliere le informazioni professionali e personali che si divulgano sulle reti sociali (quanto necessario, il meno possibile)
- Diffidare di offerte finanziarie allettanti
- Usare prudenza nell'accettare prestazioni gratuite di sostegno all'estero, in particolare se si tratta di pratiche amministrative come il rilascio di un visto o la proroga di un permesso di soggiorno
- Essere vigilanti, in particolare quando una persona è troppo curiosa o invadente. Non trasmettere informazioni precise o dare assensi e interrompere tempestivamente le relazioni con persone dall'apparenza sospetta
- Controllare se l'istituzione o il campo di attività indicato da una persona esiste davvero e se il nome della persona in questione compare nel sito web dell'istituzione indicata
- Segnalare le attività sospette a una rappresentanza di Svizzera all'estero (ambasciata, consolato), all'università di origine o al SIC

Per ulteriori misure di protezione e consigli in merito alla sicurezza durante i viaggi di lavoro all'estero si rimanda all'opuscolo Prophylax.

www.sic.admin.ch – IT – Documenti e pubblicazioni – Ricerca – Prophylax – Pubblicazioni

ULTERIORI INFORMAZIONI

SPIONAGGIO E PROLIFERAZIONE

Programma di sensibilizzazione Prophylax

www.sic.admin.ch – IT – Sicurezza – Acquisizione di informazioni – Spionaggio economico

Il programma di sensibilizzazione Prophylax è orientato alla protezione della piazza industriale e di ricerca svizzera dalla fuga involontaria di dati e dai tentativi di acquisizione illegale. Nell'ambito di Prophylax il SIC sensibilizza le imprese, le scuole universitarie e gli istituti di ricerca nei confronti delle minacce legate alle attività di spionaggio e alla proliferazione (diffusione di armi di distruzione di massa e dei loro vettori nonché tentativi di acquisizione illegale di beni a duplice impiego).

Cortometraggio «Nel mirino»

www.sic.admin.ch – IT – Sicurezza – Acquisizione di informazioni – Spionaggio economico

Il cortometraggio «Nel mirino» fa parte del programma di sensibilizzazione Prophylax condotto dal SIC. Il film ha lo scopo di sensibilizzare la piazza industriale e di ricerca svizzera in merito alle minacce derivanti dallo spionaggio economico.

Spiegazioni sui metodi di spionaggio presentati nel film e misure di protezione opportuni: *www.sic.admin.ch – Spionaggio economico - Documenti*

Promemoria e schede informative complementari

www.sic.admin.ch – IT – Sicurezza – Acquisizione di informazioni – Spionaggio economico – Documenti

- Prophylax
- Cosa intraprende il SIC contro lo spionaggio?
- Promemoria sullo spionaggio economico
- Management Summary Studio «Wirtschaftsspionage in der Schweiz»
- Promemoria sulla sicurezza delle informazioni per le PMI

CIBERSICUREZZA

Centro nazionale per la cibersicurezza (National Cyber Security Centre — NCSC)

www.ncsc.admin.ch

Il Centro nazionale per la cibersicurezza (National Cyber Security Centre — NCSC) è il centro di competenza della Confederazione per la cibersicurezza e di conseguenza il primo servizio di contatto per l'economia, l'amministrazione, gli istituti di formazione e la popolazione per tutte le questioni relative alla cibersicurezza.

Segnalazione di mail di phishing

www.antiphishing.ch

antiphising.ch è un sito web amministrato del Centro nazionale per la cibersicurezza NCSC della Confederazione, con lo scopo di fornire alla popolazione uno strumento di facile utilizzo per segnalare tentativi di phishing.

Standard minimo per il miglioramento della resilienza TIC

www.ufae.admin.ch – Temi – TIC – Standard minimo per le TIC

La crescente digitalizzazione che caratterizza tutti i settori della vita costituisce un grande potenziale economico e sociale per la Svizzera, ma implica anche nuovi rischi che vanno affrontati rapidamente e in maniera sistematica. Il documento «Standard minimo per migliorare la resilienza delle TIC» dall'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) fornisce uno strumento di aiuto e offre delle indicazioni concrete per migliorare la resilienza delle TIC.

ECONOMIA

Prescrizioni in materia di controllo all'esportazione

www.seco.admin.ch – IT – Economia esterna e cooperazione economica – Relazioni economiche – Controlli all'esportazione e sanzioni – Elic – Internal Compliance Programme-ICP

Il Documento spiega perché le aziende esportatrici devono effettuare un controllo interno, illustra le basi giuridiche svizzere pertinenti e precisa i criteri che il programma interno di conformità (Internal Compliance Programme, ICP) deve soddisfare. È dunque da considerarsi come un ausilio per creare un simile programma o ottimizzare un programma esistente.

Domande nell'ambito dei beni a duplice impiego

www.elic.admin.ch

Dal 1° ottobre 2014 tutte le richieste (domande, domande di parere preliminare ecc.) nell'ambito dei beni a duplice impiego, del materiale bellico e dei beni militari speciali dovranno essere registrate, elaborate e gestite elettronicamente in Elic. I dossier cartacei non potranno più essere presi in considerazione.

Ricerca di dati di sanzione

www.seco.admin.ch – IT – Economia esterna e cooperazione economica – Relazioni economiche – Controlli all'esportazione e sanzioni – Sanzioni / Embarghi – Sanzioni della Svizzera – Ricerca dei destinatari delle sanzioni

La Confederazione può disporre misure coercitive per applicare sanzioni volte a far rispettare il diritto internazionale pubblico – in particolare i diritti dell'uomo – adottate dall'Organizzazione delle Nazioni Unite, dall'Organizzazione per la sicurezza e la cooperazione in Europa o dai principali partner commerciali della Svizzera (art. 1 cpv. 1 della legge sugli embarghi).

La banca dati SESAM permette la ricerca di persone, imprese e organizzazioni sanzionate.

ALTRI

Segreteria di Stato per la formazione, la ricerca e l'innovazione (SEFRI)

www.sbfi.admin.ch

La Segreteria di Stato per la formazione, la ricerca e l'innovazione SEFRI nel Dipartimento federale dell'economia, della formazione e della ricerca DEFR è il centro di competenza della Confederazione per le questioni nazionali e internazionali connesse alla politica in materia di formazione, ricerca e innovazione.

Soggiorno all'estero

www.dfae.admin.ch – IT – Consigli di viaggio e rappresentanze – Informazioni generali di viaggio – Consigli di viaggio in breve

I Consigli di viaggio del Dipartimento federale degli affari esteri (DFAE) forniscono informazioni sulle condizioni di sicurezza all'estero e vanno a integrare altre fonti d'informazione. Chi viaggia si assume la responsabilità di decidere in merito ai preparativi e alla realizzazione di un viaggio.

Il potenziale dell'uso improprio e la bioprotezione nella ricerca biologica

Accademia svizzera di scienze naturali (SCNAT)
www.scnat.ch

Il potenziale dell'uso improprio e la bioprotezione nella ricerca biologica (swiss academies reports Vol 12 No 3, 2017) è una base di discussione per gli scienziati su come affrontare il dilemma del duplice uso nella ricerca biologica.

COME PROCEDERE IN CASO DI SOSPETTO / CONTATTO

In caso di sospetto spionaggio o di sospette attività di proliferazione (p. es. richieste dubbie di collaborazione o comportamento sospetto di dottorandi, studenti, professori o ricercatori), non esitate a contattare i vostri responsabili della sicurezza, la vostra Polizia cantonale o il SIC. Mettete al sicuro le possibili prove e non cancellate le mail sospette.
Il SIC raccoglie e analizza gli indizi e garantisce discrezione nel trattamento del caso.

Servizio delle attività informative della Confederazione SIC
Papiermühlestrasse 20
CH-3003 Berna
www.sic.admin.ch
prophylax@ndb.admin.ch

Il SIC, in collaborazione con i servizi informazioni cantonali, contribuisce a informare, sensibilizzare e consigliare le imprese, gli atenei e gli istituti di ricerca svizzeri e del Liechtenstein in merito alla proliferazione e allo spionaggio.

Diritti relativi alle immagini

Prima pagina, FHNW Campus Muttenz, © Gataric Fotografie

Pagina 2, UNIGE, © Righetti Nicolas

Pagina 4, Lichthof UZH, © Meissner Ursula

Pagina 6, HSLU

Pagina 10, EPFL, © Christinat Olivier

Pagina 16, UZH, © Walter Stefan

Pagina 22, EPFL, © Christinat Olivier

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

TECHNOPOL
Programma di sensibilizzazione Prophylax
Servizio delle attività informative della Confederazione SIC
Papiermühlestrasse 20
CH-3003 Berna

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

Chiusura della redazione
Dicembre 2022