Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Servizio delle attività informative della Confederazione SIC

PROPHYLAX

Programma di prevenzione e di sensibilizzazione del
Servizio delle attività informative della Confederazione

Indice

Introduzione

I prodotti svizzeri godono nel mondo intero di un'eccellente reputazione. Il know-how e la capacità innovativa di imprese e istituti di ricerca svizzeri sono fattori chiave per la competitività dell'economia del Paese e rappresentano il fondamento del ruolo di punta assunto dalla Svizzera in molti settori dell'economia e della ricerca. Questo know-how e i prodotti altamente tecnologici dell'industria svizzera attirano l'interesse non solo delle aziende concorrenti, ma anche di Stati esteri. Per molti servizi di intelligence stranieri l'acquisizione di prodotti e tecnologie che, a causa di sanzioni e del controllo delle esportazioni, non possono ottenere sul libero mercato fa parte dei compiti fondamentali, e così pure lo spionaggio di aziende estere.

Per attirare l'attenzione delle imprese e degli istituti di ricerca svizzeri su queste minacce, nel 2004 l'allora Servizio di analisi e prevenzione[1] crea il programma di prevenzione e di sensibilizzazione Prophylax. Il programma adempie tuttora il mandato assegnato dal legislatore di gestire programmi di informazione e sensibilizzazione in merito alle minacce per la sicurezza interna e esterna.[2]

Il Servizio delle attività informative della Confederazione (SIC), in stretta collaborazione con i servizi informazioni cantonali, si incarica di sensibilizzare le imprese, le scuole universitarie e gli istituti di ricerca svizzeri e del Liechtenstein in merito alle minacce legate allo spionaggio e alla proliferazione. Il programma Prophylax

1 Dalla fusione nel 2010 dei servizi di intelligence interno ed estero è nato il Servizio delle attività informative della Confederazione.

2 Cfr. art. 6 cpv. 6 della legge federale del 25 settembre 2015 sul Servizio delle attività informative della Confederazione (LAIn; RS 121).

è inteso a rafforzare il controllo delle esportazioni di tecnologie e beni critici rilevanti per la proliferazione (segnatamente i cosiddetti beni a duplice impiego o dual use[1]), facendo in modo che le attività illecite di acquisizione vengano identificate tempestivamente e impedite. Ciò è fondamentale poiché la Svizzera è uno dei principali esportatori mondiali di beni a duplice impiego. Diversi Stati conducono programmi analoghi per sensibilizzare le loro aziende attive nell'ambito commerciale e delle tecnologie. Con il programma Prophylax il SIC contribuisce all'impegno internazionale nella lotta alla proliferazione delle armi di distruzione di massa.

La proliferazione e lo spionaggio economico possono essere intimamente connessi. Il SIC e i servizi informazioni cantonali sensibilizzano imprese e istituzioni anche in merito ai rischi di spionaggio, e in particolare anche sulle minacce provenienti dallo spionaggio cibernetico. Imprese e istituzioni devono farsi più guardinghe nel trattare informazioni degne di protezione, prevenendo in tal modo involontarie fughe di informazioni e dati.

1 Beni a duplice impiego, ossia utilizzabili sia in ambito civile sia in ambito militare.

Proliferazione

Definizione

Con il termine «proliferazione» s'intende la diffusione, da un lato, di armi di distruzione di massa e dei loro vettori (missili balistici, missili da crociera e droni) e, dall'altro, di beni d'equipaggiamento, materiali e tecnologie utilizzabili anche per la fabbricazione di queste armi (i cosiddetti beni a duplice impiego).

Limitata inizialmente al settore delle armi nucleari, la nozione di proliferazione si estende oggi alle armi biologiche e chimiche di distruzione di massa e ai rispettivi prodotti di base.

A destra:
missile balistico nordcoreano a raggio intermedio (IRBM)
HWASONG-12 al momento del lancio (Korean Central News Agency)

States of concern *(Stati fonte d'inquietudine)*

La proliferazione rappresenta una minaccia per la pace e la sicurezza a livello mondiale. Essa è praticata da Paesi che, per ragioni politico-militari, sono determinati a contrastare l'ordine internazionale o regionale. Sviluppando armi nucleari, biologiche e chimiche (cosiddette armi NBC) e i relativi vettori, questi Paesi tentano di rafforzare le loro capacità belliche, di accrescere il loro potenziale di minaccia e deterrenza e di imporre le loro rivendicazioni politiche. Tali Stati costituiscono un rischio sia per la stabilità regionale sia per quella internazionale e sono pertanto considerati states of concern. Questa classificazione è giustificata tanto da ragioni tecniche quanto da ragioni politiche e obbliga la comunità internazionale ad adottare misure attive contro determinate attività dei Paesi in questione. Oggi sono ritenuti states of concern gli Stati seguenti: l'Iran, la Corea del Nord, il Pakistan e la Siria. È comprovato che questi Stati conducono programmi per lo sviluppo di armi di distruzione di massa, o addirittura fabbricano già armi di questo tipo. Tuttavia, per sviluppare, fabbricare e potenziare gli arsenali esistenti hanno bisogno di beni e know-how provenienti dall'estero. Quindi tentano di eludere i meccanismi di controllo internazionali con attività di acquisizione clandestine, ad esempio occultando l'uso previsto per un prodotto o costituendo società paravento. Inoltre alcuni Paesi, quali ad esempio la Malesia, gli Emirati Arabi Uniti (tra cui Dubai) o Singapore, fungono da zone di transito per gli affari importanti in materia di proliferazione. Particolare prudenza è indicata anche nei rapporti commerciali con altri Stati che presumibilmente coltivano ambizioni nel campo della proliferazione.

I programmi di ricerca e di sviluppo delle armi di distruzione di massa e dei loro vettori si trovano a differenti stadi di avanzamento nei diversi states of concern. Dal punto di vista tecnico-militare, tali Paesi intendono sviluppare ulteriormente i programmi d'armamento al fine di completare i loro arsenali, migliorare la sicurezza d'immagazzinamento e affinare le possibilità d'impiego, la precisione, la portata e l'efficacia dei loro sistemi d'arma. Inoltre, essi mirano a un'ampia indipendenza nella tecnica d'armamento.

Controllo delle esportazioni e basi legali in vigore

La lotta contro la proliferazione è compito della comunità internazionale. La Risoluzione 1540 del Consiglio di sicurezza delle Nazioni Unite, adottata all'unanimità il 28 aprile 2004, invita gli Stati membri a «adottare e applicare misure efficaci per istituire controlli interni volti a prevenire la proliferazione di armi nucleari, chimiche o biologiche e dei loro vettori, anche introducendo controlli adeguati sui materiali connessi». A tal fine esistono sul piano internazionale quattro regimi di controllo delle esportazioni. Per quanto riguarda le armi chimiche e biologiche, sussistono inoltre convenzioni internazionali giuridicamente vincolanti, il cui scopo è la messa al bando mondiale di tali armi. La Svizzera è membro di tutti i regi-

A sinistra:
presunta installazione di armi chimiche del Scientific Studies Research Center in Siria bombardata da Israele il 7 settembre 2017 (ripresa PLE del 24 settembre 2017)

mi e convenzioni sopracitati. La politica svizzera in materia di controllo degli armamenti e di disarmo si prefigge di garantire la sicurezza nazionale e internazionale mantenendo il più basso possibile il livello di armamento sul piano mondiale. La Svizzera si impegna affinché le armi di distruzione di massa non vengano diffuse (non proliferazione) e vengano completamente eliminate (disarmo). Quale membro dei regimi internazionali di controllo delle esportazioni, la Svizzera funge da solido anello della catena di Paesi che applicano misure contro la proliferazione. Nel diritto nazionale svizzero il controllo delle esportazioni è disciplinato dalle seguenti basi legali[1]:

- Legge sul controllo dei beni a duplice impiego (LBDI); RS 946.202
- Ordinanza sul controllo dei beni a duplice impiego (OBDI); RS 946.202.1
- Ordinanza sul controllo dei composti chimici (OCCC); RS 946.202.21
- Legge federale sul materiale bellico (LMB); RS 514.51
- Legge federale sull'energia nucleare (LENu); RS 732.1
- Legge federale sulle armi, gli accessori di armi e le munizioni (LArm); RS 514.54
- Legge federale sugli esplosivi (LEspl); RS 941.41
- Legge federale sull'applicazione di sanzioni internazionali (LEmb); RS 946.231
- 24 Ordinanze ai sensi della Legge sugli embarghi.

1 Vedi anche www.seco.admin.ch/it (Politica esterna e cooperazione economica → Controlli all'esportazione e sanzioni → Controllo degli armamenti → Basi legali).

Occorre precisare che anche i beni che non figurano esplicitamente negli elenchi dei regimi di controllo delle esportazioni soggiacciono a un obbligo di notifica e autorizzazione se l'esportatore sa o ha motivo di credere che un bene sia destinato alla fabbricazione o all'impiego di armi di distruzione di massa (clausola *catch-all*). Inoltre, il controllo delle esportazioni si estende anche a determinate tecnologie.
Le attività di proliferazione in Svizzera possono non solo violare il diritto nazionale o contravvenire agli obblighi internazionali, ma anche pregiudicare le relazioni politico-commerciali con l'estero e nuocere alla credibilità della politica svizzera. Imprese, istituti di ricerca e scuole universitarie implicati, anche involontariamente, in attività di proliferazione perdono la loro buona reputazione, possono subire danni finanziari considerevoli od essere oggetto di misure di ritorsione.

In quale misura la proliferazione riguarda le imprese, le scuole universitarie e gli istituti di ricerca?

Sforzi di acquisizione

Le armi di distruzione di massa e i relativi vettori non sono ottenibili sul libero mercato, e le contromisure della comunità internazionale servono a ostacolare gli sforzi di acquisizione degli states of concern. I tentativi di acquisizione, però, non si limitano solo ai beni, ma si estendono anche alle corrispondenti conoscenze. Il rischio di cadere nel cosiddetto trasferimento intangibile di tecnologia (Intangible Transfer of Technology, ITT) incombe soprattutto su atenei, scuole universitarie professionali e istituti di ricerca.

Per eludere i controlli sulle esportazioni e ottenere beni critici gli attori rilevanti nell'ambito della proliferazione utilizzano diversi metodi e reti di acquisizione tenute segrete:

- i consumatori finali statali si celano dietro una ragione sociale insospettabile, un'organizzazione d'armamento convenzionale o un'università, che si presenta come ordinante o acquirente, oppure costituiscono una società paravento. A tal fine ricorrono anche al sostegno dei rispettivi servizi di intelligence;
- aziende commerciali neutrali vengono utilizzate per nascondere alle aziende fornitrici che l'acquisto è in realtà destinato a imprese controllate dallo Stato;
- gli attori rilevanti nell'ambito della proliferazione costituiscono una piccola azienda per un'unica transazione e la chiudono dopo la conclusione dell'affare. Al fine di occultare il reale destinatario finale si avvalgono di diversi intermediari per la fornitura e il pagamento della merce e la fanno transitare in Paesi terzi (percorsi obliqui). L'esistenza di simili aziende è stata accertata in particolare nei Paesi di transito;
- gli attori rilevanti nell'ambito della proliferazione utilizzano progetti con denominazioni banali, che sembrano appartenere al settore civile, e sfruttano l'inesperienza di talune aziende fornitrici nel settore delle esportazioni. Essi cercano in modo mirato aziende, e in particolare PMI, che non dispongono di un controllo delle esportazioni e di un sistema di compliance efficaci;

- questi attori sfruttano aziende in Paesi produttori o fornitori per occultare acquisizioni illecite dietro lo schermo di affari leciti, e presentano documenti di esportazione contraffatti o certificati di uso finale contenenti indicazioni non vere;
- suddividono l'acquisizione in varie piccole ordinazioni per rendere difficoltoso il riconoscimento della loro rilevanza in materia di proliferazione;
- cercano materiali ed equipaggiamenti di rimpiazzo per sostituire i prodotti figuranti negli elenchi dei beni assoggettati al controllo delle esportazioni.

Tale modo di procedere rende difficile alle aziende fornitrici il riconoscimento dell'utilizzazione effettiva del loro prodotto. Particolarmente problematici sono i beni a duplice impiego *(dual-use)*, che ben si adattano ad applicazioni sia civili sia militari.

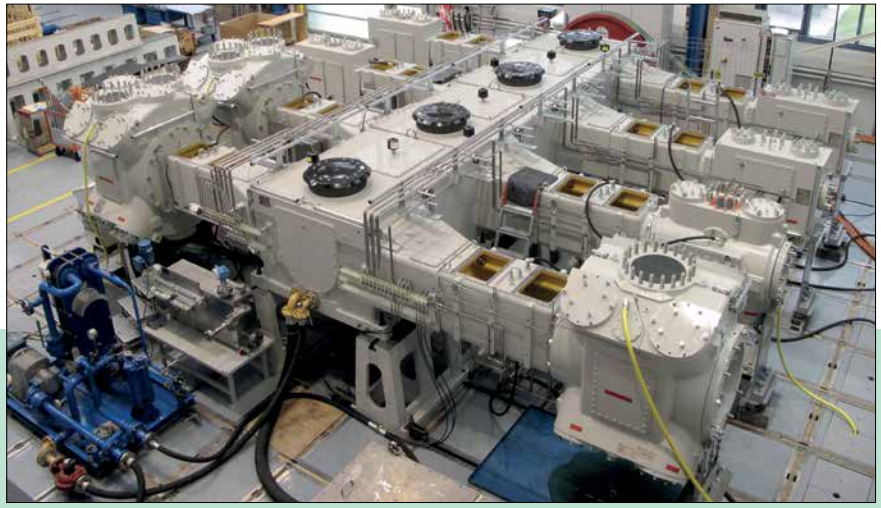

Immagine a destra:
secondo alcune informazioni, compressori simili di produzione svizzera avrebbero dovuto essere utilizzati nell'ambito del programma di armi nucleari pakistano (fotografia privata)

Come riconoscere gli affari illegali?

Spesso non è possibile riconoscere unicamente dall'ordinazione se la merce è destinata allo sviluppo di armi di distruzione di massa o sistemi missilistici. Occorre pertanto verificare accuratamente le modalità di ordinazione, di trasporto e di pagamento. A tal fine è necessaria l'acquisizione di informazioni dettagliate sul Paese di destinazione, sul consumatore e su eventuali intermediari.

L'esperienza ha mostrato che i seguenti comportamenti e modi di procedere da parte dell'acquirente possono essere indizi di un affare rilevante in materia di proliferazione.

Consumatore finale

- L'identità di un nuovo cliente è incerta: vengono date risposte elusive sul profilo aziendale e sugli interlocutori oppure non vengono presentate referenze convincenti;
- il cliente non pone alcuna delle domande commerciali o tecniche che usualmente vengono poste nell'ambito di trattative d'affari o nella pertinente documentazione;
- il cliente chiede di portare a termine un progetto che era già stato iniziato da un'altra azienda;
- il cliente esige una riservatezza inconsueta ed esagerata sul luogo di destinazione o sui prodotti ordinati. Senza una ragione comprensibile, nega al venditore l'accesso ad alcuni settori dell'impianto. L'azienda acquirente invia collaboratori in Svizzera per la formazione quando invece sarebbe più pratico e ragionevole organizzare una corrispondente formazione in loco, oppure il cliente rinuncia completamente alla formazione, al servizio o a prestazioni di garanzia.

Uso previsto

- La descrizione dei beni richiesti è confusa o i beni sembrano essere esageratamente specificati;
- il cliente non dispone delle necessarie conoscenze specialistiche e ignora manifestamente le misure di sicurezza usuali nell'impiego dei beni ordinati. Non è in grado di indicare l'uso previsto (o si rifiuta di indicarlo);
- l'uso dei beni previsto dal fornitore differisce notevolmente da quello previsto dall'acquirente;
- la destinazione finale della merce non è chiara o non è plausibile.

Svolgimento dell'affare

- Vengono interposti intermediari senza una ragione apparente;
- il cliente offre condizioni di pagamento insolitamente vantaggiose (pagamenti in contanti o cospicui acconti e provvigioni superiori alla media);
- il cliente esige misure di sicurezza che sembrano esagerate, considerato l'uso previsto. L'imballaggio richiesto non è giustificato (ad es. imballaggio per trasporto marittimo per una fornitura in territorio europeo) oppure richiede un'etichettatura, marcatura o un contrassegno speciale;
- geograficamente o economicamente, le vie di trasporto previste dal cliente sono insensate;
- i beni sono destinati all'immagazzinamento in un deposito doganale.

Scambio di conoscenze e proliferazione

La diffusione a livello mondiale di conoscenze acquisite dalla scienza e dalla ricerca è auspicabile e non deve essere impedita o controllata. La cooperazione in ambito scientifico può però essere sfruttata anche per fini rilevanti per la proliferazione.

Particolarmente problematico è il trasferimento intangibile di tecnologie (ITT). Esso può verificarsi sia mediante il trasferimento di know-how nell'ambito di consulenze specialistiche, conferenze, corsi di formazione o programmi di scambio accademici, programmi congiunti di ricerca e sviluppo, sia mediante la trasmissione di informazioni tecniche non in forma fisica, per esempio tramite posta elettronica, fax, siti Internet o cloud. Questo genere di trasferimento di tecnologie è aumentato sensibilmente con la digitalizzazione e la diffusione e lo sviluppo delle tecnologie dell'informazione e della comunicazione (TIC), e costituisce una particolare sfida per il controllo delle esportazioni, poiché – contrariamente all'esportazione di beni – non è fisicamente controllabile alle frontiere nazionali.

Uno dei casi più significativi di trasferimento illecito di know-how e tecnologie è quello della rete internazionale collegata all'ingegnere e scienziato nucleare pakistano Abdul Qadeer Khan, noto come «padre della prima bomba atomica del Pakistan». Negli anni 1960 Khan aveva studiato metallurgia in Europa occidentale. Nel 1972, dopo aver conseguito il dottorato, aveva lavorato nei Paesi Bassi presso il Physics Dynamics Research Laboratory svolgendo ricerche sui metalli ad alta resistenza per lo sviluppo di apparecchiature per la centrifugazione dei gas. Il laboratorio era un subappaltatore del gruppo Urenco, il quale tra varie cose gestisce un impianto per l'arricchimento dell'uranio nei Paesi Bassi e produce uranio arricchito destinato alle centrali nucleari nei Paesi Bassi e in altri Stati. Urenco aveva autorizzato Khan ad accedere ai piani di costruzione di ultracentrifughe a gas affinché provvedesse alla traduzione della documentazione olandese per i partner tedeschi e inglesi del consorzio Urenco. Dopo che l'India aveva sganciato la sua prima bomba atomica nel 1974, Khan offrì spontaneamente le sue conoscenze al governo del Pakistan, consentendogli di realizzare un impianto per l'arricchimento dell'uranio per il programma di armamento nucleare nazionale. In seguito fornì le sue conoscenze all'Iran, alla Corea del Nord e alla Libia e procurò a questi Paesi anche i beni necessari per lo sviluppo e il potenziamento di un programma nucleare.

Gli attori rilevanti nell'ambito della proliferazione approfittano del libero scambio di informazioni e possono in tal modo impadronirsi, mediante un trasferimento intangibile di tecnologie, di conoscenze tecniche e scientifiche necessarie allo sviluppo di armi di distruzione di massa e dei loro vettori. In tale contesto si interessano in particolar modo di ambiti specialistici i cui contenuti trovano applicazione nello sviluppo di armi di distruzione di massa e dei relativi vettori, quali ad esempio la meccanica, l'ingegneria, la metrologia, le scienze naturali, e così via.

Per di più gli states of concern non esitano a impiegare i loro servizi di intelligence per impossessarsi – con l'ausilio di agenti del servizio di intelligence stesso, agenti reclutati o altri metodi occulti – delle competenze necessarie nei Paesi fornitori. È difficile individuare e combattere, presso istituti di ricerca e scuole universitarie, questi agenti e il loro modo di agire.

Per proteggere le informazioni confidenziali o rilevanti in materia di proliferazione e per minimizzare il rischio di perdita di reputazione e credibilità, le imprese, le scuole universitarie e gli istituti di ricerca dovrebbero essere consapevoli del rischio ITT, e verificare e adattare di conseguenza le loro direttive e linee d'azione interne.

Che cosa fanno le autorità?

Le aziende e gli istituti scientifici sono in primo luogo responsabili del rispetto delle disposizioni di controllo delle esportazioni. La Segreteria di Stato dell'economia (SECO), in quanto istanza di autorizzazione delle esportazioni, può informare in merito al modo di procedere e ai prodotti che soggiacciono all'obbligo dell'autorizzazione o all'obbligo della dichiarazione.[1] Altre istanze federali e cantonali, quali l'Amministrazione federale delle dogane (AFD), il Dipartimento federale degli affari esteri (DFAE), il SIC e i servizi informazioni cantonali, sono coinvolte nell'esecuzione delle suddette disposizioni.

Sovente gli ambienti scientifici ed economici non sono in grado di individuare la dissimulazione delle reali intenzioni dei loro partner provenienti dai Paesi critici. Può dunque succedere che un'impresa o un istituto di ricerca commetta inconsapevolmente un reato fornendo beni critici o tecnologie che vengono impiegati in un programma di produzione di armi di distruzione di massa. Per contro, soltanto essi dispongono delle conoscenze necessarie per giudicare se i beni ordinati possono corrispondere, in base al quantitativo e alle specifiche, all'impiego indicato dall'acquirente e in quale misura questi beni o tecnologie possono essere impiegati abusivamente.

A tale scopo il SIC e i servizi informazioni cantonali contattano, consigliano e sensibilizzano gli ambienti scientifici, economici e industriali con la dovuta discrezione e in un clima di collaborazione.

1 Vedi anche www.seco.admin.ch/it → Politica esterna e cooperazione economica → Controlli all'esportazione e sanzioni.

PROLIFERAZIONE

A destra:
strumento di analisi che, secondo alcune informazioni, avrebbe dovuto essere utilizzato nell'ambito del programma di armi nucleari pakistano (fotografia privata)

Spionaggio

Definizione

Con il termine spionaggio si intende l'acquisizione di informazioni e dati confidenziali o segreti riguardanti la politica, l'economia, il settore militare, la scienza e la tecnologia a discapito della Svizzera o delle sue imprese, istituzioni o di persone in Svizzera, nonché la trasmissione di tali informazioni ad attori esteri (Stati, gruppi, imprese, persone, ecc.).

Nel caso particolare dello spionaggio economico, un segreto di fabbrica o d'affari viene rivelato e quindi reso accessibile a un'autorità o a un'organizzazione estera, oppure a un'azienda privata o ai suoi agenti.

La violazione del segreto di fabbrica o commerciale e le attività illecite di spionaggio sono contemplate nel Codice penale svizzero (artt. 162, 271, 272, 273, 274 e 301).

Imprese e scuole universitarie svizzere nel mirino dello spionaggio

La Svizzera, polo del settore dell'alta tecnologia, sede di gruppi e organizzazioni internazionali, Paese di accoglienza di negoziati internazionali e sede di importanti centri di dati, è un obiettivo interessante per le attività di spionaggio di attori statali e non.

I motivi che determinano la scelta di un'azienda come bersaglio di attività di spionaggio economico possono essere diversi. Da un lato, può trattarsi di un'impresa che produce beni altamente tecnologici, che possiede un know-how critico, e i cui prodotti soggiacciono al controllo delle esportazioni. D'altro lato, sono un bersaglio interessante anche le aziende leader sul piano internazionale che occupano un mercato di nicchia (cosiddetti *hidden champions*). Ma anche le imprese e le scuole universitarie che si occupano di ricerca applicata e di sviluppo o coltivano contatti con Stati critici (per es. partecipando a joint venture o ad attività congiunte nel campo della ricerca) sono esposte a un rischio accresciuto di spionaggio.

Le nuove tecnologie dell'informazione e della comunicazione hanno permesso di realizzare molti progressi, in particolare nel campo della memorizzazione e dell'analisi di dati. Ma queste tecnologie sono anche vulnerabili, e per imprese e scuole universitarie il loro impiego imprudente può costituire un fattore di rischio. Nel mondo intero gli attacchi di spionaggio cibernetico si fanno sempre più numerosi e ogni impresa, ogni scuola universitaria, ogni istituto di ricerca può diventare bersaglio di simili attacchi.

Alcuni servizi di intelligence stranieri sono esplicitamente incaricati di acquisire know-how all'estero per sostenere attivamente l'economia e le aziende del loro Paese e recuperare in tal modo il loro ritardo nel campo dell'evoluzione tecnologica. Gli attacchi di spionaggio perpetrati ai danni di imprese e istituti di ricerca svizzeri hanno conseguenze negative durature per la competitività economica e tecnologica della Svizzera.

Ricerca legale di informazioni

Open Source Intelligence

L'acquisizione di informazioni da fonti accessibili al pubblico (ad es. siti Internet, opuscoli di prodotti, reti sociali) definita Open Source Intelligence (OSINT) non è vietata. Tra i compiti ordinari dei delegati dei Paesi esteri in Svizzera vi è anche quello di raccogliere informazioni nell'ambito di conferenze, fiere o incontri diplomatici. Occorre però richiamare l'attenzione sul fatto che proprio i servizi di intelligence stranieri e le aziende concorrenziali possono individuare, grazie a simili informazioni, possibili bersagli di spionaggio (imprese, organizzazioni, persone, ecc.). Il problema consiste, da un lato, nel fatto che il prodotto di un'azienda o di un istituto deve essere presentato con grande effetto pubblicitario e, dall'altro, che non dovrebbero essere pubblicati dettagli. Questi potrebbero infatti essere utilizzati dalla concorrenza. Anche in occasione di esposizioni, conferenze e progetti di ricerca internazionali è possibile acquisire, mediante attività di OSINT, informazioni sulle tecnologie, sulla situazione economica di un'azienda, sugli investimenti relativi a progetti, sulla ricerca e sullo sviluppo, sui collaboratori nonché sui clienti e contratti futuri. La condivisione di informazioni personali e professionali nelle reti sociali online offre ai servizi di intelligence stranieri l'occasione di cercare in modo mirato persone e profili di attività interessanti e di scegliere le persone con cui tentare un approccio.

La valutazione delle pubblicazioni accessibili al pubblico e lo scambio di risultati scientifici conseguiti dalla ricerca generano un'ampia gamma di conoscenze, forniscono preziose indicazioni riguardo ai progetti attuali e consentono azioni mirate contro le fonti. Chi pubblica informazioni ha la possibilità di decidere fino a che punto informare in merito a un progetto, un prodotto, un istituto o a un'azienda e ai suoi collaboratori.

Metodi di spionaggio

I servizi di intelligence stranieri, ma anche attori privati, si servono di diversi metodi di spionaggio. Nell'ombra, continuano a lavorare con mezzi tradizionali quali le attività di Human Intelligence (HUMINT) e Communications Intelligence (COMINT). Mediante attività di HUMINT si scelgono e si ingaggiano informatori. Nell'ambito delle attività di COMINT si utilizzano mezzi elettronici altamente sviluppati, che consentono di intercettare e analizzare comunicazioni elettroniche vocali o testuali di qualsiasi tipo. La crescente digitalizzazione di informazioni, dati e processi operativi produce collezioni di dati sempre più voluminose e sempre più critiche. Anche la crescente diffusione di sistemi di dispositivi e oggetti interconnessi – e perlopiù mal protetti – (cosiddetto Internet of Things, o «Internet delle cose») rende questi ultimi vulnerabili. Di conseguenza, l'acquisizione illecita di informazioni e dati degni di protezione viene condotta sempre più spesso con i mezzi dello spionaggio cibernetico. Inoltre, i servizi di intelligence e le imprese impiegano agenzie private (agenzie investigative, fiduciarie o uffici informazioni, aziende di consulenza o di ristrutturazione, ecc.), ma anche hacker per procurarsi dati e informazioni confidenziali.

Communications Intelligence

La COMINT consiste nell'intercettazione e nell'analisi di comunicazioni di aziende o privati cittadini trasmesse via cavo, per satellite o per onde radio (per es. conversazioni telefoniche, messaggi di posta elettronica, SMS) per ricavarne informazioni utili riguardanti obiettivi economici o strategici. Le email e i messaggi via fax possono essere oggetto di sistematiche ricerche attraverso parole chiave, e le conversazioni telefoniche possono essere analizzate grazie al riconoscimento vocale automatico.

Human Intelligence

Operato sotto copertura

Agendo sotto copertura in veste di diplomatici, giornalisti, scienziati o persone d'affari, per esempio, gli agenti dei servizi di intelligence stranieri entrano in contatto in Svizzera con decisori del mondo politico, militare, economico e scientifico. Possono in tal modo raccogliere prime informazioni e contattare persone senza rendersi sospetti. Gli agenti dei servizi di intelligence stranieri assistono spesso a manifestazioni pubbliche e prendono di mira quelle persone che possono detenere informazioni di loro interesse. A tal fine utilizzano in particolare tattiche di social engineering, vale a dire tentativi mirati di manipolazione volti a ottenere determinate informazioni. Interpreti e traduttori hanno spesso accesso a informazioni confidenziali, così come praticanti e dottorandi. Anche loro sono dunque un bersaglio privilegiato dei servizi di intelligence stranieri.

In occasione di una conferenza pubblica sulla sicurezza cibernetica un agente di un servizio di intelligence straniero sotto copertura diplomatica ha rivolto la parola ad uno specialista informatico svizzero. Ne è seguito un incontro nel corso del quale l'agente del servizio di intelligence si è intrattenuto con lo specialista su questioni inerenti alla sicurezza cibernetica in Svizzera. Scopo dell'agente era ottenere informazioni dettagliate e possibilmente riservate in merito.

A sinistra:
falso profilo su Linkedin utilizzato da un servizio di intelligence cinese per contattare persone potenzialmente interessanti (Ufficio federale tedesco per la protezione della Costituzione)

Più di una semplice rappresentanza commerciale diplomatica

In particolare membri di rappresentanze commerciali estere che agiscono in veste di diplomatici e sono attivi nei servizi di intelligence cercano di rivolgersi a aziende operanti nel settore delle tecnologie d'avanguardia. Queste persone invitano a partecipare a esposizioni, seminari e congressi internazionali, ma si presentano anche spontaneamente presso imprese o istituti di ricerca. Si mostrano interessati ai progetti di ricerca e ai processi aziendali, richiedono offerte dal contenuto molto dettagliato o chiedono di avere i manuali aziendali interni.

Dal contatto leale a quello subdolo

Gli agenti dei servizi di intelligence stranieri instaurano gradatamente un rapporto di fiducia ed eventualmente un rapporto di dipendenza con le persone prese di mira. Inizialmente cercano di ottenere informazioni non classificate e accessibili al pubblico. Con piccoli regali e inviti coltivano l'amicizia – e la persona presa di mira rivela sempre più informazioni confidenziali. Il rapporto di fiducia si approfondisce e alla fine vengono rivelate anche informazioni segrete. La persona presa di mira è sempre più coinvolta e non è più in grado di togliersi da questa situazione; nel ricordare quali informazioni ha già illecitamente fornito, viene esercitata su di essa una pressione a scopo ricattatorio.

Ricatto

L'accettazione di denaro, in particolare, compromette la persona presa di mira e la vincola all'agente del servizio di intelligence straniero. Le possibilità di ricatto possono essere create anche dai servizi di intelligence stessi. In certi Stati, ad esempio, alle persone prese di mira vengono rimproverate violazioni della legge. I rimproveri possono essere motivati o pretestuosi, in occasione ad esempio di un incidente della circolazione. In simili casi, un servizio di intelligence può offrire il proprio aiuto in cambio di informazioni e collaborazione. Le possibilità di ricatto possono essere create anche mediante sorveglianza, ad esempio documentando intrecci amorosi, consumo di stupefacenti, illeciti valutari o accettazione di denaro.

Imprese e istituti di ricerca nel mirino

Oltre ai metodi di spionaggio summenzionati, nel settore dello spionaggio economico l'acquisizione di informazioni confidenziali avviene usualmente con i seguenti metodi:

- visite di delegazioni estere presso aziende, con o senza accompagnamento di un rappresentante dell'ambasciata;
- progetti di investimento esteri (in particolare in aziende start up), partecipazione a società comuni (joint venture) o acquisizione di aziende ai fini del trasferimento di tecnologia e insediamento di nuovi collaboratori in ambiti sensibili;
- collaborazione nel campo della ricerca con aziende ai fini di accaparrarsi il know-how tecnico per la realizzazione e la gestione di un impianto di produzione;
- cooperazione scientifica con scuole universitarie e istituti di ricerca per avere accesso a costosi strumenti e impianti di ricerca;
- attacchi a clienti, fornitori di servizi esterni, consulenti o fornitori dell'azienda presa di mira;
- sfruttamento di fragilità nell'organizzazione dell'azienda presa di mira consistenti, per esempio, nel fatto di permettere ai collaboratori di collegare alla rete aziendale dispositivi mobili privati quali computer portatili, tablet o smartphone;

- restrizioni previste da leggi e regolamenti in altri Stati per le succursali di società estere, che per esempio costringono queste ultime a salvare i loro dati su server del Paese in cui ha sede la succursale;
- reclutamento di un impiegato come informatore al fine di accedere a informazioni confidenziali, ma anche sfruttamento dei contatti con ex impiegati che avevano accesso ad ambiti e informazioni sensibili e conoscono i processi interni.

Il cortometraggio «Nel mirino» realizzato dal SIC illustra i metodi utilizzati dagli agenti dei servizi di intelligence stranieri e i mezzi che essi impiegano per appropriarsi del know-how di un'azienda svizzera.[1]

1 Disponibile all'indirizzo www.ndb.admin.ch/spionaggio-economico

Autori interni

In molti casi di spionaggio un collaboratore interno trasmette a persone non autorizzate (concorrenti, servizi di intelligence stranieri) dati aziendali confidenziali, intenzionalmente o sotto costrizione. I fattori che motivano simili atti sono di varia natura. Spesso vi sono segnali di allarme che sfuggono o vengono ignorati. I seguenti modelli di comportamento possono essere indizio dell'esistenza di un autore interno:

- orari di lavoro o di accesso all'edificio insoliti (per es. la mattina molto presto o la sera tardi, per essere possibilmente solo in ufficio);
- stampa o fotocopiatura di documenti aziendali in quantità esagerata;
- salvataggio di un volume di dati particolarmente cospicuo su supporti elettronici;
- presa con sé non autorizzata di documenti confidenziali al di fuori del perimetro aziendale;
- introduzione non autorizzata di dispositivi elettronici in reparti sensibili;
- accesso a dati aziendali di cui il collaboratore non ha bisogno per il proprio lavoro;
- frustrazione sul posto di lavoro, per esempio delusione dovuta a una promozione non ottenuta o ad altre situazioni di disagio percepite, rancore nei confronti dei superiori e dei colleghi;
- agiatezza inspiegabile e improvvisa;
- ricattabilità (per es. a causa di una relazione extraconiugale, del consumo di stupefacenti, di infrazioni alla legge);
- mancanza di discrezione;

- spericolatezza, noncuranza e deliberato disprezzo delle prescrizioni di sicurezza;
- contatti personali con rappresentanti di ambasciate o diplomatici stranieri sconosciuti alla direzione aziendale e da questa non autorizzati.

Se si constata un comportamento del genere da parte di un collaboratore, occorre segnalarlo immediatamente alla persona responsabile della sicurezza aziendale.

Quali minacce comporta l'impiego delle TIC per imprese e scuole universitarie?

Spionaggio cibernetico e furto di dati

Il Codice penale svizzero distingue i delitti seguenti:

- Art. 143 acquisizione illecita di dati;
- Art. 143bis accesso indebito a un sistema per l'elaborazione di dati;
- Art. 144bis danneggiamento di dati;
- Art. 147 abuso di un impianto per l'elaborazione di dati.

L'utilizzo delle tecnologie dell'informazione e della comunicazione (TIC) per acquisire informazioni cui non si avrebbe accesso con mezzi comuni ha avuto una rapida crescita negli ultimi anni. Criminali, concorrenti, Stati, terroristi o gruppi indipendenti utilizzano le TIC per accedere a sistemi informatici e ottenere informazioni sensibili. Lo spionaggio cibernetico e il furto di dati tramite Internet permettono di mantenere l'anonimato dell'aggressore e di diminuire i costi di acquisizione illegale. Sempre più questi attori ricorrono ad attacchi mirati utilizzando codici nocivi altamente sofisticati; impiegano risorse finanziarie e umane notevoli per un periodo di tempo considerevole allo scopo di attaccare in modo mirato le vittime prescelte (Advanced Persistent Threat, APT). Dietro questi attacchi complessi si celano in genere attori statali che, per fini di spionaggio o di sabotaggio, mirano a rimanere clandestinamente e a lungo nella rete di un'azienda o di un'organizzazione. Tali attori possono anche abusare della rete per condurre operazioni cibernetiche contro ulteriori obiettivi. Inoltre, un presunto attacco cibernetico criminale sferrato tramite ransomware può nascondere un attacco ancora più importante: in questi casi all'aggressore non interessa ottenere un riscatto ma piuttosto sottrarre o distruggere dati.

Le imprese e le scuole universitarie non sono confrontate solo a piccoli criminali dotati di capacità limitate, ma sono anche esposte alla minaccia e all'attacco da parte di gruppi organizzati e con elevate competenze tecniche. Spesso, tuttavia, non si rendono sufficientemente conto di questa minaccia. Al contrario, molti la considerano semplicemente un fenomeno virtuale e quindi innocuo.

Raccolta di dati voluminosa

Spesso le aziende si affidano a compagnie esterne per prestazioni in ambito TIC, dando in gestione l'infrastruttura TIC e le informazioni ivi contenute a soggetti terzi, le cui attività non possono essere sempre controllate in maniera adeguata. Le comunicazioni necessarie per lo svolgimento di attività economiche e di ricerca (ad es. tramite reti informatiche o di telefonia mobile) possono diventare oggetto di attenzione di Stati terzi dotati delle tecnologie per acquisire un massiccio flusso di dati, che poi analizzano e sfruttano a loro proprio vantaggio o a vantaggio di aziende o organizzazioni concorrenti. Le aziende e le scuole universitarie devono essere coscienti che ogni informazione che esce dalla propria rete potrebbe essere

raccolta, analizzata e sfruttata da un'entità terza: di conseguenza assicurare la confidenzialità di un'informazione rientra oggigiorno tra i compiti fondamentali di sicurezza.

Danneggiamento di dati

L'accesso non autorizzato a un sistema per l'elaborazione di dati può avere come obiettivo anche la distruzione di questi ultimi. Il motivo di simili azioni risiede spesso nell'intenzione di anticipare la concorrenza o di bloccare una trattativa in corso. Le informazioni rappresentano un bene degno di particolare protezione. Il loro valore determina quali misure di sicurezza devono essere adottate.

Interferenze nella rete

Se un servizio di rete è indisponibile per un periodo prolungato per gli utenti autorizzati, l'interruzione può causare un grave danno all'impresa o alla scuola universitaria in questione. Un tipico esempio di questo tipo di situazione è quello degli attacchi distribuiti tramite interruzione del servizio (distributed denial-of-service attack, DDoS attack). Questi attacchi mirano a sovraccaricare uno o più elementi di un'infrastruttura informatica inondandola di false richieste di accesso, per provocare in tal modo un deficit di prestazione e rendere inefficiente un servizio Internet. Le aziende che dipendono per la loro funzionalità da un tempo di attività pressoché continuo di un sistema informatico potrebbero pregiudicare i propri guadagni se i loro sistemi informatici non fossero adeguatamente protetti contro gli incidenti di abuso di risorse.

Che cosa possono fare imprese e scuole universitarie per prevenire una fuga di informazioni e dati?

L'inasprimento della competitività internazionale e la crescente dipendenza dai moderni sistemi di informazione e comunicazione creano nuove vulnerabilità e sfide per le imprese, le scuole universitarie e altre istituzioni. Proteggersi contro l'uso illecito delle proprie conoscenze da parte di persone non autorizzate è un compito sempre più importante. Grazie ai loro progetti innovativi di ricerca e sviluppo e al know-how che possiedono, le piccole e medie imprese rappresentano spesso un obiettivo interessante per lo spionaggio. Con l'aumentare dell'interconnessione, la sicurezza dell'infrastruttura informatica diventa un compito prioritario. L'interruzione delle reti di comunicazione nonché il furto, la manipolazione o la perdita di dati possono diventare un rischio esistenziale per l'economia, la società e lo Stato.

La sicurezza delle informazioni non può fermarsi allo stretto ambito di un'azienda o ai confini nazionali. Le imprese attive internazionalmente devono essere consapevoli che sono possibili perdite di informazioni presso succursali, società del gruppo o partner commerciali all'estero. Negli ultimi anni alcuni Stati hanno varato leggi severe in materia di sicurezza cibernetica, che obbligano le aziende estere a salvare i propri dati su server del Paese ospitante. Se vuole trasferire i propri dati all'estero, l'impresa necessita dell'autorizzazione ufficiale del Paese ospitante. Taluni Stati sottopongono il codice sorgente delle tecnologie estere vendute nel loro territorio a una verifica da parte delle loro autorità. Per le aziende estere è dunque sempre più grande il rischio che i loro dati e le loro informazioni finiscano a loro insaputa nelle mani di terzi o vengano sfruttati abusivamente.

Misure di protezione

Non è possibile una protezione integrale dalla fuga di informazioni; tuttavia, l'adozione di misure appropriate per limitare i rischi può offrire una protezione efficace e finanziariamente sostenibile. Possono, tra l'altro, essere adottate le misure preventive seguenti.

Sicurezza delle informazioni

- Elaborazione e applicazione di un documento programmatico sulla sicurezza dell'informazione e nomina di una persona responsabile che esegue controlli con il supporto della direzione e fa rispettare le misure di sicurezza previste.
- Disciplinamento e limitazione dei diritti di accesso dei collaboratori a dati e documenti.
- Divieto di portare con sé il telefono cellulare alle riunioni di lavoro in cui si discute di temi sensibili nonché divieto di tenere conversazioni confidenziali con il telefono cellulare.
- Clean desk policy («politica della scrivania pulita»): quando non sono al loro posto di lavoro, per esempio durante la pausa pranzo o al di fuori degli orari di lavoro, i collaboratori mettono sotto chiave tutti i documenti (e in particolare le informazioni confidenziali o segrete). Il computer dovrebbe essere sempre bloccato, anche in caso di breve assenza (bloccaschermo).
- Distruzione sicura di documenti e supporti di dati confidenziali quali chiavette USB (per es. mediante un tritadocumenti).
- Esame approfondito dei collaboratori prima dell'assunzione (per es. estratto del casellario giudiziale, controllo di sicurezza relativo alle persone).

- Formazione, perfezionamento e sensibilizzazione periodici dei collaboratori riguardo alla sicurezza delle informazioni, alla sicurezza informatica e alle minacce legate allo spionaggio.
- Controllo sistematico e centralizzato delle informazioni pubblicate dall'azienda e dai suoi collaboratori (sul sito web aziendale, nelle reti sociali, negli opuscoli dei prodotti, ecc.).
- Direttive sul comportamento dei collaboratori in occasione di fiere, conferenze, eventi e viaggi d'affari.

Esterni

- Controllo degli accessi e accompagnamento costante di visitatori e delegazioni esterni, tra cui verifica dei dati personali dei membri delle delegazioni, badge per visitatori, garanzia di un accompagnamento adeguato e sensibilizzazione sia delle persone incaricate di tale compito che di altri collaboratori che ricevono visite, definizione di un'agenda, divieto di introdurre apparecchiature elettroniche per i membri delle delegazioni, ecc.
- Verifica di fornitori, consulenti e altri fornitori di servizi.

Sicurezza informatica e sicurezza dei dati

Informazioni e dati possono finire nelle mani sbagliate a causa di operazioni involontarie nell'approntamento e nell'uso delle TIC, per esempio un errore umano o un guasto tecnico, oppure a causa di azioni deliberate e illecite (attacchi cibernetici). In un'impresa o una scuola universitaria, e anche nella sfera privata, ci si dovrebbe sempre dotare di soluzioni tecniche come, ad esempio, un firewall che filtra il traffico di dati in entrata e in uscita e un programma antivirus; inoltre occorre aggiornare regolarmente e rapidamente il sistema operativo e i software utilizzati. Sono però necessarie ulteriori misure come la cifratura del disco fisso (in particolare dei computer portatili che vengono utilizzati anche al di fuori del perimetro aziendale), il blocco di tutte le porte dei computer aziendali per il collegamento di supporti di memoria esterni (chiavette USB, carte SD, ecc.) e la separazione (virtuale o fisica) della rete interna ed esterna. Per gli accessi personali a computer fissi, computer portatili e posta elettronica si dovrebbe di principio ricorrere all'autenticazione a due fattori (ad es. per mezzo di token crittografici o di chiavi di sicurezza USB) o mediante smart card (per es. tessera PKI). Inoltre, conviene adottare soluzioni di sicurezza anche per la trasmissione dei dati. Le informazioni sensibili dovrebbero essere cifrate prima di essere convogliate in una rete esterna (per es. trasmettendole per posta elettronica) e i dati dovrebbero essere trasmessi attraverso un canale sicuro, per esempio un VPN (Virtual Private Network), in particolare se i collaboratori accedono alla rete aziendale dall'esterno. Prudenza è d'obbligo anche nell'uso di servizi cloud, in particolare se i server sono ubicati all'estero. L'uso della posta elettronica è spesso il principale punto debole nel sistema di protezione di un'impresa o di un'organizzazione contro gli attacchi cibernetici e, in caso di uso imprudente, può spalancare le porte a un malintenzionato che vuole penetrare nella rete di un'azienda o di un'organizzazione (per es. con un attacco di spear phishing[1]).

Le aziende e le scuole universitarie necessitano inoltre di strumenti atti a individuare gli accessi illegali sulla propria infrastruttura di rete. Speciali soluzioni come gli Intrusion Detection Systems (IDS) o gli Intrusion Prevention Systems (IPS) dovrebbero essere implementati per aumentare il grado di sicurezza della rete. La protezione dei terminali della rete, la sorveglianza delle attività sui terminali e la registrazione degli accessi alla rete (indirizzi IP, porte) e ai dati consentono di identificare e gestire gli incidenti. D'altro canto, per prevenire un abuso delle risorse bisogna ricorrere a soluzioni che proteggano la rete da attacchi esterni, soluzioni che vengono spesso fornite dal proprio provider di rete (anti-DDoS).

Regole di comportamento e formazione

Nel settore dell'informatica sono necessarie direttive che siano applicabili non soltanto durante l'orario di lavoro, ma anche nella vita privata. Nelle direttive interne concernenti l'impiego dei mezzi informatici a scopi professionali occorre definire la posizione dell'azienda o dell'istituto di ricerca in merito all'utilizzo di Internet e disciplinare l'uso della posta elettronica privata sul posto di lavoro. Inoltre, l'impresa o l'istituto di ricerca dovrebbe organizzare regolarmente corsi di formazione e perfezionamento per tutti i collaboratori sui rischi attuali connessi all'uso delle TIC.

1 Metodo di phishing che punta in modo mirato a singole persone o gruppi all'interno di un'azienda o di un'organizzazione. A differenza delle mail di phishing, che vengono distribuite diffusamente, una mail (o un SMS) di spear phishing è personalizzato in base al destinatario e ai suoi interessi. Il destinatario viene invitato a rendere note informazioni personali (per es. i dati per il login e le password), ad aprire un allegato o a cliccare un link che contiene software nocivo e una volta cliccato infetta il computer del destinatario e quindi la rete aziendale.

Scelta del partner e delle soluzioni IT

Le PMI in particolare mancano spesso delle risorse finanziarie e di personale necessarie per garantire in modo capillare la sicurezza delle loro reti informatiche. Perciò è consigliabile investire in un supporto esterno. Tuttavia, nella scelta di un partner IT le aziende dovrebbero considerare diversi fattori. La competenza tecnica e la qualità del servizio sono indubbiamente elementi fondamentali nella scelta di un partner. Se si vuole però evitare una trasmissione involontaria di dati o un danneggiamento delle reti IT, le differenti condizioni giuridiche e politiche alle quali il partner IT è sottoposto o l'appartenenza a programmi statali di raccolta di informazioni sono aspetti decisivi da esaminare al momento della scelta.

Aiuti / supporto

L'Ufficio federale per l'approvvigionamento economico del Paese ha pubblicato uno standard minimo per le TIC, che propone istruzioni concrete per il miglioramento della resilienza di queste tecnologie.[1] Le istruzioni sono rivolte in particolare ai gestori di infrastrutture critiche, ma possono essere adottate da qualsiasi azienda o organizzazione. L'autovalutazione e uno strumento di analisi permettono di stimare lo stato dell'attuazione.

ICTswitzerland ha sviluppato appositamente per le PMI un breve test online sulla sicurezza cibernetica. Questo strumento[2] consente alle imprese di verificare se soddisfano gli standard minimi.

1 Disponibile sotto www.bwl.admin.ch/bwl/it/home/themen/ikt/ikt_minimalstandard.html
2 Disponibile in tedesco e in inglese sotto www.cybersecurity-check.ch

Sicurezza durante i viaggi di lavoro all'estero

Durante i viaggi di lavoro all'estero il rischio di cadere vittima di atti di spionaggio aumenta. Un servizio di intelligence straniero o un concorrente possono prendere di mira una persona direttamente, a causa della sua attività, del suo know-how o di informazioni e dati elettronici che reca con sé. Dispositivi elettronici quali computer portatili, smartphone, tablet e supporti di dati (ad es. chiavette USB) sono apparecchiature delicate da cui eventuali malintenzionati possono ricavare informazioni all'insaputa del proprietario. Alcuni Stati sorvegliano il traffico di dati in Internet, le telecomunicazioni e la corrispondenza postale; in questi Stati i bagagli vengono ispezionati e i dispositivi elettronici e i supporti di dati dei viaggiatori vengono manipolati. Certi Stati sono persino disposti a creare situazioni compromettenti, fingere incidenti della circolazione o impedire il rientro in patria della persona presa di mira per costringerla a consegnare informazioni confidenziali o addirittura per reclutarla come informatore. In determinati Stati le autorità raccolgono informazioni già prima dell'arrivo di una persona, ad esempio effettuando ricerche nelle reti sociali. A seguito di una richiesta di visto un servizio di intelligence straniero può stabilire se una persona è un bersaglio interessante; in particolare risposte sulla sua attività professionale possono rivelare dettagli importanti.

Scenari verosimili

- A un valico di frontiera un doganiere chiede a un viaggiatore di consegnargli temporaneamente i suoi dispositivi elettronici. Il viaggiatore ignora però cosa ne abbia fatto il doganiere dopo la consegna. Anche organi statali stranieri possono essere interessati a gettare uno sguardo nei dati professionali e privati dei viaggiatori.

- Una persona che si trova all'estero in viaggio d'affari deve trasmettere informazioni sensibili con il suo telefono cellulare. Il segnale emesso dal telefono è criptato, ma solo nella parte radio e con tecnologie a basso costo; è possibile quindi decriptare il segnale e ascoltare la conversazione. Quando passa dalla parte radio alla rete fissa il segnale non è comunque più criptato.
- La rappresentante di un'azienda ha bisogno di un'informazione e accede a Internet dall'estero: le sue comunicazioni possono essere intercettate nei luoghi più diversi (hotel, aeroporto, stazione, bar, ecc.).
- Durante un viaggio di lavoro il responsabile della ricerca si concede qualche ora per visitare la città e lascia il suo materiale elettronico nella stanza d'albergo: la sua camera può essere perlustrata (cassaforte compresa) per cercare materiale interessante.
- In occasione di una conferenza tutti i partecipati escono dalla sala durante la pausa caffè e lasciano il proprio computer portatile aperto sul tavolo. Qualcuno potrebbe tener pronta una chiavetta USB per copiare i dati memorizzati sui computer o caricare un software nocivo.
- Dopo un incontro di lavoro il rappresentante di un'azienda rimane privatamente in contatto con una collaboratrice dell'azienda estera. La collaboratrice invia al rappresentante un regalo costoso o lo invita nel suo Paese per una visita privata a sue spese. In cambio può aspettarsi una controprestazione, per esempio sotto forma di informazioni commerciali sensibili.

SPIONAGGIO

Misure di sicurezza personali

- Quando vi recate all'estero portate con voi soltanto i dispositivi elettronici di cui avete assolutamente bisogno per la vostra attività e che non contengono informazioni sensibili. Conviene utilizzare computer portatili e cellulari speciali, destinati solo ai viaggi di lavoro e configurati in modo tale da poter essere riconfigurati facilmente al vostro rientro. I dispositivi sono vulnerabili anche se li tenete sempre con voi.
- Assicuratevi che i sistemi operativi e le applicazioni installate sui vostri dispositivi elettronici siano sempre aggiornati. Utilizzate password sicure e uniche (caratteri alfanumerici, maiuscole e minuscole, caratteri speciali) che non contengono informazioni personali come la data di nascita. Le password dovrebbero essere composte da almeno 12 caratteri, ad esempio iniziali di diverse parole (per es. la password Mvoma7apcic! significa **M**ario **v**a **o**gni **m**attina **a**lle **7** **a** **p**asseggio **c**on **il** **c**ane**!**).
- Il disco fisso del vostro computer, e più precisamente i dati che vi sono memorizzati, dovrebbero essere criptati. Siccome in alcuni Paesi è vietato entrare con dati criptati, dovreste viaggiare con un computer che non contiene dati sensibili. Nel momento in cui vi trovate all'estero collegatevi attraverso una connessione sicura (Virtual Private Network, VPN), scaricate i dati sul vostro computer e, una volta non più necessari, cancellate completamente i dati con un software apposito.

- Consegnate i vostri dispositivi elettronici (per es. al valico di frontiera) soltanto se potete seguire fisicamente il funzionario che ve li chiede. Così saprete che cosa succede con il vostro materiale. Se ciò non è possibile, presumete che sia stato manipolato.
- Non lasciate mai il vostro materiale elettronico incustodito (per es. durante la pausa caffè in occasione di una conferenza o semplicemente per recarvi al bagno).
- Non utilizzate periferiche esterne prestate o regalate (chiavi USB, dischi fissi esterni, telefoni cellulari, fotocamere digitali o altro) e non permettete a nessuno di allacciare una periferica al vostro computer (per es. se si vuole usare il vostro computer per una presentazione o per caricare un cellulare altrui). Se siete voi ad avere inserito una periferica su un computer sconosciuto, formattatela prima di riutilizzarla.
- In genere, i collegamenti a Internet tramite WLAN liberamente accessibili – e in parte anche tramite reti protette da password – (per es. in hotel, bar o aeroporti) non sono criptati e quindi non sono sicuri: dovreste utilizzarli soltanto tramite un collegamento VPN oppure – se il VPN è bloccato nel Paese in cui vi trovate – accedere a Internet tramite connessione a 3G/4G/5G in roaming. Assicuratevi che la comunicazione tra il vostro web browser e l'indirizzo web al quale volete accedere sia criptata (http**s**://...).
- Se non necessari, disattivate le interfacce wireless come WLAN e Bluetooth e i servizi di localizzazione.
- Se non potete accedere a una riunione o a uno stabile con il vostro telefono cellulare, spegnetelo e conservatelo in una custodia sicura (busta antimanomissione o contenitore di sicurezza).

- Siate prudenti nel rivelare informazioni personali nelle reti sociali o professionali online.
- Siate guardinghi in caso di tentativi di approccio da parte di persone a voi sconosciute che non hanno niente a che fare con il vostro viaggio di lavoro.
- Prima della partenza informatevi in merito alle leggi vigenti e agli usi e costumi del Paese di destinazione.
- Siate sempre vigili e prestate attenzione se qualcuno cerca di cogliere di nascosto ciò che avviene sul vostro schermo (per es. in treno, in aereo o a una conferenza).

Dopo il rientro

- Cambiate tutte le password che avete utilizzato durante il viaggio all'estero.
- Se avete dei sospetti, chiedete al reparto IT della vostra azienda o a un fornitore di servizi IT privato di verificare ed eventualmente riconfigurare i vostri dispositivi elettronici.
- Segnalate gli avvenimenti sospetti al vostro servizio di sicurezza e al SIC.

Contatto

Quale aiuto vi può dare il SIC?

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

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

Sensibilizzazione per lo spionaggio economico

www.ndb.admin.ch/spionaggio-economico

- Cortometraggio di sensibilizzazione sullo spionaggio economico «Nel mirino»
- Commento ai metodi di spionaggio presentati nel cortometraggio e alle relative misure di protezione
- Promemoria e schede informative sui temi della proliferazione e dello spionaggio
- Opuscolo Prophylax

Come procedere in caso di sospetto

In caso di sospetto spionaggio o di sospette attività di proliferazione (per es. richieste su prodotti oppure ordinazioni sospette) non esitate a contattare il SIC o la vostra Polizia cantonale. Assicurate le possibili prove e non cancellate le mail sospette. Il SIC raccoglie e analizza gli indizi e garantisce discrezione nel trattamento del caso.

Ulteriori informazioni

Segreteria di Stato dell'economia

www.seco.admin.ch/it

→ Politica esterna e cooperazione economica → Controlli all'esportazione e sanzioni

- Elic (e-licensing): sistema elettronico di autorizzazione per la redazione e il trattamento di richieste assoggettate al controllo delle esportazioni (beni a duplice impiego, materiale bellico e beni militari speciali) (disponibile anche all'indirizzo www.elic.admin.ch)
- Sanzioni/embarghi: ricerca di persone, imprese e organizzazioni colpite da sanzioni (banca dati SESAM)
- Prodotti industriali (dual use) e beni militari speciali (licensing):
  - documento Controllo interno del rispetto delle prescrizioni in materia di controlli all'esportazione (Programma interno di conformità, PIC) (sotto Moduli e fogli di istruzioni)

Dipartimento federale degli affari esteri

www.dfae.admin.ch

→ Rappresentanze e consigli di viaggio

Valutazione delle proprie misure di sicurezza in ambito informatico

Centrale d'annuncio e d'analisi per la sicurezza dell'informazione

www.melani.admin.ch
www.antiphishing.ch/it (segnalazione di mail di phishing)

Ufficio federale per l'approvvigionamento economico del Paese

www.ufae.admin.ch
→ Temi → Standard minimo per le TIC
Standard minimo TIC per il miglioramento della resilienza dei gestori di infrastrutture critiche, imprese e organizzazioni (incluso lo strumento di valutazione)

ICT Switzerland

www.cybersecurity-check.ch
Breve test online sulla sicurezza cibernetica per le PMI (disponibile in tedesco e in inglese)

Redazione
Servizio delle attività informative della Confederazione SIC

Chiusura della redazione
Febbraio 2019

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