



Promemoria sullo spionaggio economico

Introduzione

Lo spionaggio perseguibile penalmente consiste nella raccolta di informazioni o dati di natura politica, economica e militare volutamente confidenziali o tenuti segreti ai danni della Svizzera o delle sue imprese, istituzioni o persone in Svizzera, nonché nella trasmissione di tali informazioni ad attori esteri (Stato, organizzazione, impresa, persona, ecc.).

In che maniera lo spionaggio minaccia la vostra impresa? Come individuate lo spionaggio e come potete proteggere la vostra impresa? Una protezione completa non esiste; è possibile però ridurre il rischio di spionaggio mediante misure adeguate. Le enumerazioni che seguono non sono esaustive.

Per quale motivo un'impresa rientra nel mirino dello spionaggio?

- L'impresa fabbrica beni nel settore delle tecnologie d'avanguardia e possiede un know-how specifico
- È leader a livello mondiale di un mercato di nicchia (*hidden champion*)
- I suoi beni sottostanno ai controlli delle esportazioni
- Pratica la ricerca applicata e lo sviluppo
- Intrattiene relazioni d'affari con Stati a rischio

Quali conseguenze ha lo spionaggio per un'impresa che ne è vittima?

- Perdita di segreti d'affari
- Perdita di mandati
- Perdita di clienti
- Danni alla reputazione – a seconda del caso anche per la Svizzera
- Danni finanziari fino al fallimento

Da dove proviene la minaccia di spionaggio?

- Visite di delegazioni straniere
- Joint venture, progetti di ricerca congiunti, intenzioni di investimento dall'estero, partecipazioni a o acquisizione di imprese ai fini di trasferimento di tecnologia
- Collaboratrici e collaboratori che trasmettono senza autorizzazione informazioni o dati aziendali confidenziali a esterni, per dolo o costrizione (cosiddetti autori interni, *insider threat*) o per sbadataggine
- Social engineering: tra l'altro attacchi di spear phishing¹, presa di contatto tramite i social network o il telefono, e-mail falsificate a nome di un superiore (truffa ai danni del CEO)
- Prestatori di servizi e consulenti esterni, fornitori
- Fiere, conferenze
- Cyberattacchi

¹ A differenza delle mail di phishing, che vengono distribuite largamente, le mail o i messaggi SMS di spear phishing vengono indirizzati in modo mirato a singole persone o gruppi all'interno di un'impresa o di un'organizzazione e sono formulati di conseguenza. La persona destinataria viene invitata a rivelare informazioni personali (p. es., nel caso del cosiddetto credential phishing, dati di accesso a un account [login] o password) oppure ad aprire un allegato o a cliccare un link contenente malware, che infetta così il computer della persona bersaglio e quindi la rete aziendale.

Misure di protezione

- Creazione e attuazione di un piano per la sicurezza delle informazioni e designazione di un relativo responsabile, che con l'appoggio della direzione imponga le misure di sicurezza
- Controlli sistematici e centralizzati delle informazioni pubblicate dall'impresa e dalle sue collaboratrici e dai suoi collaboratori (livello di direzione compreso). Definire cosa non andrebbe pubblicato dal punto di vista della protezione delle informazioni
- Controllo degli accessi e accompagnamento costante di delegazioni e visitatori esterni
- Segmentazione delle reti informatiche (ad es. la rete del settore di ricerca è separata dal resto della rete aziendale e non è collegata a Internet)
- Disciplinamento e restrizione dei diritti d'accesso delle collaboratrici e dei collaboratori a dati, atti e prodotti, in particolare ai risultati delle ricerche e ai prototipi (principio del «need to know»)
- Nessun collegamento di chiavette USB private, cellulari, portatili, ecc., alla rete aziendale
- Impiego dell'autenticazione a due fattori per gli accessi a computer, notebook ed e-mail
- Sensibilizzazione regolare delle collaboratrici e dei collaboratori per le questioni di sicurezza informatica e delle informazioni
- Nessun colloquio confidenziale in luoghi pubblici quali ristoranti, treni, camere d'albergo o taxi, e nemmeno per telefono; divieto di prendere con sé il cellulare a riunioni di lavoro in cui vengono discussi temi sensibili

Viaggi d'affari all'estero

- Prendere con sé soltanto gli apparecchi elettronici assolutamente necessari, provvedere al loro crittaggio e non lasciarli mai incustoditi (vale anche per i documenti cartacei)
- Utilizzare un portatile che viene impiegato solo per i viaggi all'estero e che non contiene dati sensibili (i cosiddetti portatili da viaggio), protetto con firewall e antivirus
- Accedere alla rete aziendale dall'esterno soltanto tramite un canale crittato (Virtual Private Network, VPN) e autenticazione a due fattori
- Utilizzare reti WLAN pubbliche – e in certi casi anche reti WLAN protette da password – soltanto tramite un collegamento VPN o tramite roaming; disattivare WLAN, bluetooth e servizi di localizzazione in caso di mancato uso
- Non conservare documenti confidenziali nella camera dell'albergo o nella cassaforte dell'albergo
- Al momento dell'entrata in un Paese straniero accendere il cellulare soltanto dopo il controllo alla frontiera; al momento dell'uscita dal Paese straniero spegnerlo prima del controllo d'uscita
- Usare prudenza in caso di tentativi di approccio, inviti e regali costosi (contropartita)

In caso di sospetto di azioni di spionaggio

- Assicurare gli indizi
- Notificare il caso il più rapidamente possibile:
 - alla polizia cantonale
 - al Servizio delle attività informative della Confederazione (www.sic.admin.ch)

Il SIC analizza gli indizi e garantisce un trattamento discreto del caso di spionaggio.

Link utili

- **Dossier sullo spionaggio economico:** www.ndb.admin.ch/spionaggio-economico
 - **Prophylax:** Programma di prevenzione e di sensibilizzazione del SIC sulle minacce provenienti dallo spionaggio e dalla proliferazione (opuscolo disponibile)
 - **Filmato di sensibilizzazione** sullo spionaggio “*Nel mirino*” nonché **spiegazioni** sui metodi di spionaggio mostrati nel filmato e sulle corrispondenti misure di protezione
 - Vari **promemoria e schede** sui temi dello spionaggio e della proliferazione
- Per domande o informazioni sul programma di prevenzione Prophylax: prophylax@ndb.admin.ch
- Centrale d'annuncio e d'analisi per la sicurezza dell'informazione: www.melani.admin.ch
- Annuncio di e-mail e pagine di phishing: www.antiphishing.ch