

Ecco come gli uomini dell' intelligence riescono a rubare i segreti in azienda

Tradiscono addetti alle pulizie, magazzinieri e segretarie. Tradiscono tecnici di laboratorio e ricercatori, assistenti e fornitori. Amici e concorrenti. In cima alla catena di controllo, tradiscono dirigenti, amministratori delegati e direttori generali. Tutti potenziali traditori di tutti. Il dipendente che mette le mani su un brevetto, sottrae informazioni e la fa franca può costare carissimo alle aziende. Cifre esatte sullo spionaggio industriale non esistono, ma gli incidenti sono all' ordine del giorno. In Italia i professionisti di livello sono un centinaio, tutti a libro paga delle principali società quotate. Vengono dalle forze dell' ordine, qualcuno dai servizi segreti, i più si sono fatti da soli, specializzandosi all' estero. Chi al College of criminal justice di Boston, dove si tengono corsi in "white collar crimes" e "risk management"; chi in Europa, a Parigi o Harvard, dove si studiano case history dei guru dell' intelligence. "Capita di continuo: informazioni strategiche sottratte alle aziende da rivali senza scrupoli che hanno assoldato agenzie investigative disposte ad assecondare ogni richiesta", ammette Sergio Pivato, docente di Economia e direttore dello Space Bocconi (Centro europeo per gli studi sulla protezione aziendale). "Ma i furti di brevetto avvengono anche per negligenza: basta dimenticare acceso il pc, trascurare di cambiare password di accesso ogni 15 giorni, oppure farsi soffiare la valigetta con il portatile". A questo si aggiunge il competitive intelligence, lo spionaggio attuato per controllare le mosse della concorrenza. Legale e profittevole. Un' attività che serve, per esempio, a decidere se investire su un' azienda ad alto contenuto tecnologico situata in un Paese con un regime instabile. Valutazioni di questo tipo, in Italia, sono merce rara. In fatto di investigazioni i colossi stanno Oltreoceano. Come Kroll, la multinazionale dello spionaggio assoldata da Enrico Bondi per Parmalat. Fondata nel 1972, la società newyorkese conta filiali in mezzo mondo, 2.416 dipendenti e 485 milioni di dollari di entrate operative (vedere box in basso). Ai tempi d' oro di Wall Street, con le analisi finanziarie, è diventata una leggenda. Al suo livello lavorano solo Decision strategies e Control risk. Negli anni la società, che ha sempre avuto un' impostazione aggressiva, ha attraversato diverse crisi di reputazione da cui si è puntualmente ripresa. In Sudamerica è stata assoldata da Brazil Telecom per sorvegliare i dirigenti Telecom Italia, ma l' operazione si è conclusa con la denuncia del chief executive officer Carla Cico, la chiusura della sede e l' arresto per spionaggio dell' agente Thiago Verdial. Kroll comunque arriva dove gli altri non arrivano. Riesce a scoprire chi si nasconde dietro fiduciarie e società offshore. Scova il prestanome di turno e gli strappa informazioni. Oppure punta diritto sul rappresentante legale. Quando è sbarcata in Francia, Kroll ha provocato l' allarme dei servizi segreti, che hanno sempre considerato la società uno strumento dello spionaggio americano applicato al mondo delle aziende e dei segreti industriali. E forse non a torto. Molti concorrenti non apprezzano i metodi di Kroll. "Nelle indagini hanno successo perché non si fanno scrupoli. Ma hanno commesso errori che sono costati la chiusura di varie filiali. In Italia stanno lavorando senza licenza; alcuni agenti, poi, sono molto chiacchierati", dice al Mondo un agente della Decision strategies. Effettivamente in Italia, dove ha indagato su Telecom, Tecnosistemi, Milano mare e per conto degli eredi di Calvi, Kroll si è dimostrata all' altezza della sua fama solo con l' operazione Parmalat, che ha restituito a Bondi una parte del tesoro nascosto di Calisto Tanzi. Ma come si muove Kroll ? "Raccogliono dati aggiornati in tempo reale. Scremano le informazioni rilevanti da quelle inutili e formano un dossier", spiega Danilo Bruschi, docente di sistemi informativi e sicurezza dei calcolatori al Politecnico di Milano. "Possono contare su una fitta rete di insider: consulenti, studi legali, direttori di banca, tecnici informatici e hacker. Le fonti non sono mai un problema. Accedono a bilanci, comunicazioni interne, rapporti su fornitori e clienti, note curricolari. Fanno sopralluoghi negli uffici, se serve rovistano nei cestini e nei sacchi della spazzatura. Consultano i registri degli ordini, gli albi, studiano la reputazione del management, stilano perizie sui prodotti. E vanno alle fiere per osservare da vicino i concorrenti". A questa analisi preliminare ne segue una seconda, più delicata, della due diligence e delle interrogazioni bancarie mirate. "Kroll

con le banche ha un rapporto di dare e avere: passa ai direttori informazioni e ne ottiene altre in cambio. Se il risultato non arriva, utilizza altri metodi, non sempre cristallini", dice Ernesto Savona, docente di criminologia all' università Cattolica di Milano. "Il denaro lascia sempre una traccia", aggiunge. Solo nell' ultima fase scattano i pedinamenti, le intercettazioni ambientali e telefoniche. I tempi di preparazione dei rapporti variano: le informazioni sulla stabilità di un Paese sono aggiornate continuamente, e quindi sempre disponibili. Il resto dipende dall' urgenza del cliente. Naturalmente questa è solo la parte più elementare dell' attività di intelligence. Per tutte le agenzie investigative Internet è una miniera di informazioni. Si parte con le banche dati: Dialog e Datastar, gli archivi dell' agenzia giornalistica Reuters, il Cerved per le visure societarie. Nelle indagini di competitive intelligence è fondamentale la consultazione della Banca dei brevetti, che rivela le mosse della concorrenza. Anche se i gruppi più grossi hanno imparato a depistare i competitor depositando brevetti inutili. Poi c' è l' hidden Internet, l' insieme delle informazioni che si trovano nei forum, nei news group o nelle chat. In questo caso si tratta di capire chi si nasconde dietro un nickname. Si sono modificate le regole di attacco e difesa al punto che anche le tecnologie militari sono diventate di pubblico dominio. Fino a un paio di anni fa, Carnivore era uno dei più potenti strumenti informatici della Cia. Installato sul canale entrante di un provider, ricostruiva schermata dopo schermata la navigazione di un utente. Oggi è solo uno dei tanti software pirata. "Sempre che non vi sia stata sottrazione fisica di materiale, la maggior parte dei casi di spionaggio industriale dipende da un baco del software", precisa Bruschi. "La cosa diventa grave quando questi programmi risiedono dentro calcolatori collegati a Internet: allora posso infilarci dentro qualsiasi cosa". Il danno d' immagine arrecato da un' intrusione informatica può far fibrillare la Borsa. Nel 2000 Amazon ha subito un "denial of service attack", una tecnica comunemente impiegata come strumento di concorrenza sleale. Il server, intasato dalle richieste inviate via web, si è bloccato, e nel giro di qualche ora il titolo ha accusato al Nasdaq una flessione del 30%. I manuali di business intelligence dicono che la difesa informatica va organizzata su tre livelli: prevenzione, rilevamento e risposta. Per ogni passaggio esistono software adatti. Ma chi lo fa veramente ? Di sicuro Fiat, Telecom, Enel, Pirelli e Rfi (Rete ferroviaria italiana), che sono costrette a dotarsi di dispositivi di protezione per ragioni di national security. Ma sono un' eccezione. Comunque potrebbe non bastare. In Italia vivono almeno cento persone capaci di bucare gli scudi elettronici di queste aziende. Sono specialisti in "information gathering" la raccolta di notizie sui sistemi di protezione. Se i dispositivi di difesa non sono perfettamente allineati, individuano subito un varco. Altrimenti aspettano l' errore umano: c' è sempre una password o un codice che non viene aggiornato al momento giusto. Servono solo soldi, tempo e lavoro di squadra. Maurizio Decina, docente di telecomunicazioni al Politecnico di Milano, si occupa di sicurezza infrastrutturale, e non scherza quando dice che nessuna azienda può dormire sonni tranquilli. Lui, per esempio, sostiene di poter arrivare ovunque. Con la sua società, la Ict consulting, effettua test di intrusione per conto dei principali gruppi quotati. "La tecnologia da sola è inutile", dice. "Sono gli uomini a fare la differenza". La tesi è che, senza i guardiani giusti, anche l' unità di crisi milanese di Telecom, il centro ricerche Fiat di Orbassano (Torino) o i laboratori Pirelli della Bicocca potrebbero essere violati dall' esterno. È una questione statistica. I mastini di Telecom guidati da Giuliano Tavaroli, numero uno della security italiana, solo in un mese hanno ricevuto e respinto 26 milioni di attacchi esterni. Il crescente impiego di tecnologie militari nelle azioni di spionaggio industriale complica le cose. "Lo smart dust, o polvere intelligente, è una sofisticata rete di microcomputer grandi appena qualche millimetro cubico", afferma Decina. "Installano visori ad alta definizione, sensori audio e sniffer in grado di riconoscere odori e comunicare informazioni via onde radio. Si autoalimentano con le vibrazioni o il calore. Disseminati su un' area vasta quanto la Lombardia, ne garantiscono il controllo totale". L' esercito americano ha usato la polvere intelligente in Afghanistan e Iraq. Ma un privato può ordinarla al prezzo di poche decine di dollari alla Crossbow o alla Smartdust corporation di Berkeley. Appena qualche centesimo costano le smart tag, le etichette intelligenti a radiofrequenza che entro il 2007 sostituiranno i codici a barre. Posizionate all' interno di un pc o di una penna, arriveranno presto a trasmettere grandi quantità di informazioni. Un brutto affare per le aziende globali. Laser per l' intercettazione vocale, microfoni e microtelecamere, invece, fanno

parte del corredo di qualsiasi agenzia investigativa. Tra i siti specializzati non c'è che l'imbarazzo della scelta. Forse i tempi di Echelon sono finiti. O forse tutti danno per scontato di essere spiati dai satelliti del blocco anglosassone. Nel 1995, fax e telefonate tra il consorzio europeo Airbus e le aerolinee saudite furono utilizzati per far vincere un bando di gara da 6 miliardi di dollari alla Boeing. In quell'occasione il dipartimento del Commercio Usa passò informazioni alle aziende americane, che soffiarono un appalto d'oro ai concorrenti europei. "i furti di brevetto avvengono anche per negligenza basta dimenticare di spegnere il computer" "Kroll con le banche ha un rapporto di dare e avere: Passa Informazioni e ne riceve in cambio" "la maggior parte dei casi di spionaggio industriale dipende da un baco del software .

Fonte: www.archivio900.it