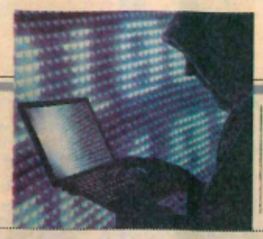
Sicurezza dei dati

REPORT GLOBALI



Il trend. L'82% delle società nel mondo ha subìto almeno una frode nell'ultimo anno: rispetto al 2015 l'aumento è del 7%

Il fronte interno dei cyber-attacchi

Per i due terzi delle imprese i maggiori rischi arrivano da dipendenti e soci

di **Fabio Grattagliano**

C'è un patrimonio nelle imprese e nei governi di tutto il mondo custodito assai distrattamente, nonostante l'enorme valore che è in grado di generare. Un asset prezioso che pure è sempre più sotto assedio, minacciato da più fronti. Le informazioni, le grandi quantità di dati, sono una preda ambita da numerosi soggetti e la loro sottrazione fraudolenta rappresenta un fenomeno in costante aumento, colpendo organizzazioni di qualsiasi dimensione e in ogni continente. Governi inclusi. Un trend che è ben delineato dall'ultimo «Global Fraud & Risk Report» messo a punto da Kroll, l'agenzia più conosciuta al mondo per la prevenzione e la protezione del rischio (fisico e informatico) e l'attività di intelligence industriale. Un primo elemento emerge nitido: se la vostra azienda è in qualche maniera sotto attacco, di qualsiasi natura esso sia, la responsabilità del danno va cercata, in primo luogo, al proprio interno.

Possibile? «Sì - conferma Marianna Vintiadis, country manager Kroll per l'Italia -. Sono proprio i nostri colleghi o soci la principale ragione di rischio». E i numeri sono lì a testimoniare che di attenzione, allora, ne serve davvero parecchia. Con tutti. Perché il 39% dei responsabili sono figure junior, il 30% senior, mentre il 27% sono dipendenti o consulenti. «In Italia in particolare - aggiunge Vintiadis - tra i colpevoli ci sono anche clienti e fornitori».

Sul banco degli indiziati, però, un posto d'onore è senz'altro conquistato dalla figura degli «ex dipendenti», categoria che risulta al primo posto in assoluto tra i responsabili di attacchi informatici, furto o distruzione proprio di dati e informazioni che per le aziende, grandi o piccole che siano, costituiscono ormai un patrimonio strategico. Non sorprende, quindi, che il report dedichi un approfondimento specifico al tema dell'*employee exit* (curato peraltro dalla stessa Vintiadis), sottolineando la criticità e i gravi rischi che le aziende spesso sottovalutano non gestendo attivamente questo processo.

Le evidenze

Tre le tipologie di rischio prese in esame dal report di Kroll: frodi, attacchi informatici e atti contro la sicurezza aziendale. Con una particolarità: l'edizione di quest'anno ha coinvolto 545 top manager delle imprese di tutto il mondo, raccogliendo anche le esperienze dei principali manager di Kroll, fornendo non solo statistiche sul fenomeno, ma anche un'ampia analisi delle tematiche evidenziate dai risultati della ricerca. Ma ecco i numeri, che sono davvero impressionanti. L'82% delle imprese nel mondo ha subìto almeno una frode nell'ultimo anno (+7% sul 2015). L'85% è stata colpita da un attacco informatico, mentre il 68% ha registrato problemi legati alla sicurezza. Per i due terzi delle imprese, appunto, le frodi sono opera del personale. Per comprendere la portata della minaccia basti considerare la vastità delle tipologie (si va dal furto vero e proprio di risorse fisiche, ai danni del sistema di fornitura o di approvigionamento e di appalti, fino alla sottrazione di informazioni e dati sensibili) e delle modalità (attacchi di tipo informatico da virus e worm, attacchi alle caselle di posta elettronica con il phishing, ai sistemi informatici con cancellazione o perdita di dati che in alcuni casi riguardano anche clienti e dipendenti dell'azienda).

Per quanto riguarda l'Italia, il report restituisce (apparentemente) una buona notizia. Infatti, nonostante una crescita del 3% rispetto al 2015, la percentuale di manager che hanno dichiarato di essere stati testimoni diretti di una frode perpetrata ai danni della propria organizzazione si attesta al 77%, cinque punti in meno rispetto alla media globale. Un gap più o meno simile anche per gli episodi legati alla cybersicurezza.

Le conseguenze

Ma qual è il danno principale che tutti questi episodi possono causare alle imprese e alle organizzazioni? Uno su tutti: il furto di *know how*. Per il 38% dei manager le frodi riguardano direttamente la proprietà industriale e intellettuale. Come dire che il lavoro dell'estro creativo e degli investimenti in ricerca e sviluppo, e quindi la propensione all'innovazione che è il fattore principale nell'economia dell'informazione in cui viviamo, finiscono nelle mani sbagliate della concorrenza. E le conseguenze economiche per le società vittime sono di tutta evidenza.

«È importante stimolare la consapevolezza dei nostri manager - sottolinea la Vintiadis -. Nell'immaginario il rischio frodi, la cybersecurity e l'attività di intelligence sono limitate agli Stati Uniti. E invece, rappresentano un problema e una sfida globale, che riguarda anche l'Italia».

E soprattutto non si limita a coinvolgere solo i grandi gruppi industriali, abbracciando loro malgrado anche i professionisti e le piccole e medie imprese.

@ilgrattacapo
fabio.grattagliano@ilsole24ore.com

Un anno sotto attacco

Percentuale di aziende che negli ultimi 12 mesi hanno registrato un episodio di frode, di attacco informatico o un problema di sicurezza

	FRODI	CYBER SECURITY	SICUREZZA
Nel mondo	82%	85%	68%
In Italia	77%	79%	68%

Fonte: Kroll-Global Fraud & Risk Report